INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM DIREITO
DOUTORADO ACADÊMICO EM DIREITO CONSTITUCIONAL

FEDRA TEIXEIRA GONÇALVES SIMÕES DE LYRA

O USO SECUNDÁRIO DE BASES DE DADOS PESSOAIS CUSTODIADAS PELO PODER PÚBLICO:

UMA ANÁLISE À LUZ DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Brasília
2025

FEDRA TEIXEIRA GONÇALVES SIMÕES DE LYRA

O USO SECUNDÁRIO DE BASES DE DADOS PESSOAIS CUSTODIADAS PELO PODER PÚBLICO:

UMA ANÁLISE À LUZ DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Tese de Doutorado apresentada como requisito parcial para obtenção do título de Doutora em Direito Constitucional, pelo Programa de Pós-Graduação em Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP.

Orientadora: Prof.ª Dr. ª Laura Schertel Ferreira Mendes.
Coorientadora: Prof.ª Dr. ª Lúcia Maria Teixeira Ferreira.

Brasília
2025

Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP

SGAS Quadra 607, Conjunto D, Módulo 49 S/N – L2 Sul – Brasília/DF – 02.474.172/0001-22

Lyra, Fedra Teixeira Gonçalves Simões

L992u O uso secundário de bases de dados pessoais custodiadas pelo poder público: uma análise à luz do direito fundamental à proteção de dados pessoais/ Fedra Teixeira Gonçalves Simões Lyra – 2025.

186 f.: il.

Tese (Doutorado Acadêmico em Direito Constitucional). Instituto Brasileiro

Orientadora: Profa. Dra. Laura Schertel Ferreira Mendes

1. Direitos fundamentais. 2. Proteção de Dados Pessoais. 3. Poder Público. I. Mendes, Laura Schertel Ferreira (Orient.). II. Ferreira, Lúcia Maria Teixeira (Coorient.). III. Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa– IDP. III. Título.

IDP

CDD: 342.81

Elaborado por Miriam Portela Wanderley de Medeiros – CRB-4/1183

FEDRA TEIXEIRA GONÇALVES SIMÕES DE LYRA

O USO SECUNDÁRIO DE BASES DE DADOS PESSOAIS CUSTODIADAS PELO PODER PÚBLICO:

UMA ANÁLISE À LUZ DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Tese de Doutorado apresentada como requisito parcial para obtenção do título de Doutora em Direito Constitucional, pelo Programa de Pós-Graduação em Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP).

Orientadora: Prof.ª Dr. ª Laura Schertel Ferreira Mendes.
Coorientadora: Prof.ª Dr. ª Lúcia Maria Teixeira Ferreira.

Brasília, 30 de outubro de 2025.

BANCA EXAMINADORA

Prof.ª Dr. ª Laura Schertel Ferreira Mendes
Orientadora
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

Prof. Dr. Victor Oliveira Fernandes
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa
Membro Interno

Prof.ª Dr. ª Miriam Wimmer
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa
Membro Externo

Prof. Dr. Marco Bruno Miranda Clementino
Universidade Federal do Rio Grande do Norte – UFRN
Membro Externo

Dedico ao Divino Espírito Santo.

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus, por sua Bondade Infinita.

Agradeço aos Professores integrantes da banca, Prof.ª Dr. ª Laura Schertel Ferreira Mendes, Prof. Dr. Victor Oliveira Fernandes, Prof.ª Dr. ª. Miriam Wimmer e Prof. Dr. Marco Bruno Miranda Clementino, por terem sido Faróis que iluminaram a minha navegação acadêmica.

Agradeço à Coorientadora, Prof.ª Dr. ª Lúcia Maria Teixeira Ferreira, por sua Generosidade e pelo amparo essencial.

Agradeço ao Prof. Me. Alisson A. Possa, por sua valorosa colaboração.

Agradeço à minha Coordenadora, Cristiane Fernandes Viana, e aos colegas Gleicy D´Lyzandra Silva do Nascimento, Júlio César da Silva, Guilherme Borba Dantas e Alaim Matos Henriques Nascimento, por terem sido fundamentais para a minha descoberta da cultura de proteção de dados pessoais.

Agradeço ao Tribunal Regional Federal da 5ª. Região, na pessoa da sua Diretora-Geral, Dr. ª Telma Roberta Vasconcelos Motta, por todo o apoio que me foi proporcionado.

Quando o amor vos chamar, segui-o.
Apesar do seu caminho ser duro e íngreme.
Khalil Gibran.

RESUMO

O presente trabalho tem como objetivo analisar os limites e as possibilidades do compartilhamento e do uso secundário de dados pessoais pelo Poder Público, à luz da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) e da Emenda Constitucional nº 115/2022, que consagrou a proteção de dados como direito fundamental autônomo. A pesquisa parte da premissa de que o tratamento de dados pelo Estado deve observar os princípios constitucionais da legalidade, finalidade, necessidade, proporcionalidade e transparência, de modo a garantir a autodeterminação informativa dos titulares e a integridade do Estado Democrático de Direito. A fundamentação teórica baseia-se na Teoria dos Direitos Fundamentais e perpassa a Limites dos Limites, que impõe restrições às próprias limitações estatais sobre direitos fundamentais. Fundamenta-se também no Regime Jurídico Administrativo, que enquadra o compartilhamento de dados como manifestação da função administrativa, sujeita aos princípios do artigo 37 da Constituição Federal. Autores como Robert Alexy, Lorenzo Dalla Corte, Laura Schertel Mendes e Miriam Wimmer são centrais como referenciais teóricos. A jurisprudência do Supremo Tribunal Federal, especialmente nas ADIs nº 6387 e nº 6649, reforça a exigência de finalidade pública legítima, proporcionalidade e segurança jurídica no tratamento de dados pelo Estado. Conclui-se que o compartilhamento e o uso secundário de dados pessoais pelo Poder Público são juridicamente admissíveis, mas não ilimitados, estando condicionados à observância de um regime jurídico estrito que exige formalização, motivação, controle e transparência. A pesquisa propõe ainda a adoção de salvaguardas institucionais e técnicas, como o princípio da única vez (*Once-Only Principle*), o *privacy by design* e a elaboração de relatórios de impacto à proteção de dados (RIPD), como formas de garantir a eficiência administrativa sem comprometer os direitos fundamentais. Em um cenário de crescente digitalização estatal, a proteção de dados pessoais revela-se não apenas uma exigência legal, mas um imperativo democrático essencial à confiança da sociedade na gestão ética e responsável das informações pelo setor público.

Palavras-chave: Proteção de dados pessoais; Poder Público; compartilhamento; usos secundários; limites.

ABSTRACT

This study aims to analyze the limits and possibilities of the sharing and secondary use of personal data by public authorities, in light of the Brazilian General Data Protection Law (Law No. 13,709/2018 – LGPD) and Constitutional Amendment No. 115/2022, which enshrined data protection as an autonomous fundamental right. The research is based on the premise that data processing by the State must comply with the constitutional principles of legality, purpose, necessity, proportionality, and transparency, in order to ensure the data subjects' informational self-determination and uphold the integrity of the Democratic Rule of Law. The theoretical framework is grounded in the Theory of Fundamental Rights and incorporates the Theory of the Limits of Limits, which imposes constraints on the State's own limitations of fundamental rights. It also draws upon the Administrative Legal Regime, which frames data sharing as an expression of administrative function, subject to the principles set forth in Article 37 of the Federal Constitution. Authors such as Robert Alexy, Lorenzo Dalla Corte, Laura Schertel Mendes, and Miriam Wimmer serve as central theoretical references. The jurisprudence of the Federal Supreme Court, particularly in ADIs No. 6387 and No. 6649, reinforces the requirement of legitimate public purpose, proportionality, and legal certainty in State data processing activities. The study concludes that the sharing and secondary use of personal data by public authorities are legally permissible, but not unlimited, being subject to a strict legal regime that demands formalization, justification, oversight, and transparency. The research further proposes the adoption of institutional and technical safeguards, such as the Once-Only Principle, privacy by design, and the development of Data Protection Impact Assessments (DPIAs), as means to ensure administrative efficiency without compromising fundamental rights. In a context of increasing state digitalization, personal data protection emerges not only as a legal requirement but as a democratic imperative essential to fostering public trust in the ethical and responsible management of information by the public sector.

Keywords: Personal data protection; public authorities; data sharing; secondary uses; limits.

LISTA DE ABREVIATURAS E SIGLAS

ABIN - Agência Brasileira de Inteligência

ADI – Ação Direta de Inconstitucionalidade

ADPF - Arguição de Descumprimento de Preceito Fundamental

ANPD – Agência Nacional de Proteção de Dados

ARPA - Advanced Research Projects Agency

CadÚnico - do Cadastro Único para Programas Sociais do Governo Federal

CBC - Cadastro Base do Cidadão

CCGD - Comitê Central de Governança de Dados

CDC - Código de Defesa do Consumidor

CF – Constituição da República Federativa do Brasil

CFOAB - Conselho Federal da Ordem dos Advogados do Brasil

CNJ - Conselho Nacional de Justiça

CPF - Cadastro de Pessoa Física

DUDH - Declaração Universal dos Direitos Humanos

EUDECO - European Data Science Academy for Data Reuse and Privacy

IBGE - Instituto Brasileiro de Geografia e Estatística

INSS - Instituto Nacional do Seguro Social

Incra - Instituto Nacional de Colonização e Reforma Agrária

LGPD - Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)

OECD - Organização para a Cooperação e Desenvolvimento Econômico

RFB - Receita Federal do Brasil

RGPD - Regulamento Geral sobre a Proteção de Dados (União Europeia)

RIPD - Relatórios de Impacto à Proteção de Dados Pessoais

RNDS - Rede Nacional de Dados em Saúde

SECAD - Secretaria Nacional do Cadastro Único

SERPRO - Serviço Federal de Processamento de Dados

STF - Supremo Tribunal Federal

SUS - Sistema Único de Saúde

SUMÁRIO

1 INTRODUÇÃO

1.1 VISÃO GERAL DO PROBLEMA DE PESQUISA E A METODOLOGIA DA TESE

> O que está em jogo hoje é assegurarmos que a modernização da administração pública, através de uma gestão e planejamento que façam uso de informações, seja acompanhada de garantias contra os riscos ao cidadão derivados do tratamento de seus dados pessoais.[1]

Era o ano de 2016 quando Klaus Schwab, fundador do Fórum Econômico Mundial, escreveu sobre o que denominou de Quarta Revolução Industrial[2] e afirmou que somos testemunhas das mudanças profundas que ocorrem em todos os setores da sociedade, geradas pelas inovações tecnológicas (Schwab, 2019).

Mais do que testemunhas – posto que não apenas assistimos aos acontecimentos – vivenciamos, na atualidade, a Quarta Revolução Industrial, também referida por Indústria 4.0[3]. Trata-se de um fenômeno que altera significativamente múltiplos aspectos da coletividade, desde a economia até as relações sociais, por envolver um amplo sistema de tecnologias disruptivas e avançadas, tais como inteligência artificial, neurotecnologia, robótica, *internet* das coisas, *blockchain* e computação em nuvem. Essas tecnologias, de forma muito acelerada, estão transformando as formas como as pessoas vivem e trabalham, não somente no Brasil, mas no cenário mundial.

A rápida transformação digital afeta as mais diversas dimensões da vida cotidiana e se caracteriza por sua velocidade em um ritmo exponencial e não linear; por sua amplitude e profundidade capaz de redefinir paradigmas nos modelos de negócios e nas formas de produção; e por seu impacto sistêmico com repercussões de interconectividade (conexão física e lógica entre sistemas e dispositivos) e de interoperabilidade (capacidade dos sistemas e dispositivos conectados trocar e interpretar dados de modo eficaz) a permitir fluxos instantâneos de grandes volumes de informações aptos a gerar uma rede global de conhecimento.

Esse fenômeno da integração entre grandes volumes de informação como ferramenta de negócios, referido na academia e na indústria como *Big Data* (De Mauro; Greco; Grimaldi,

---

[1] Danilo Doneda. Sustentação oral na ADI nº. 6649.

[2] A versão original em inglês, com o título "The Fourth Industrial Revolution" foi publicada em 2016 pelo World Economic Forum, Geneva, Switzerland. A versão brasileira, com a qual trabalhamos, é do ano de 2019.

[3] O termo "Indústria 4.0" surgiu na Alemanha, em 2011, na feira de Hannover, mencionado para descrever a revolução das cadeias globais de valor ocasionadas pela tecnologia digital. (Schwab, 2019).

2015), impulsionou o avanço da coleta e do compartilhamento de dados pessoais, tanto no âmbito dos agentes de tratamento privados, quanto na esfera do Poder Público.

Nessa conjuntura, é pressuposto que as interações entre as pessoas jurídicas de direito público[4] e os cidadãos também são impactadas pela revolução na interconectividade digital. O uso das tecnologias que processam dados pessoais passa a ser condição necessária para o exercício da cidadania e para a realização de direitos básicos[5]. Grandes volumes de dados são diariamente coletados e tratados por órgãos e entidades, como insumos necessários para criar condições para aumentar a eficiência na prestação dos serviços públicos.

Mundialmente, entidades como a Organização para a Cooperação e Desenvolvimento Econômico[6] promovem a concepção de um setor público orientado pelo compartilhamento de dados (Organisation for Economic Co-operation and Development, 2019). No mesmo sentido, a União Europeia tem envidado esforços coletivos para a transformação digital da administração pública baseada em estruturas de interoperabilidade[7].

No contexto brasileiro, o Poder Público[8] é detentor de vastas bases de dados pessoais, intercomunicáveis e essenciais para a prestação eficiente de serviços e a efetivação das políticas públicas. Dentre essas, destaca-se a base da Receita Federal do Brasil (RFB), especialmente o Cadastro de Pessoa Física (CPF), cuja utilização é imprescindível para a resolução de diversas situações cotidianas, tais como, o recebimento de benefícios previdenciários concedidos pelo Instituto Nacional do Seguro Social (INSS) ou a realização de transações básicas no sistema financeiro.

O Programa de Governo Eletrônico surgiu no ano 2000[9]. Em sua fase inicial, priorizou-se a modernização do setor público por meio da conversão de dados e processos analógicos em formatos legíveis por máquinas, processo conhecido como **digitização**. Com o rápido avanço

---

[4] Seguindo o disposto no Art. 23 da Lei nº 13.709, de 14 de agosto de 2018 (LGPD), cuida-se aqui daquelas pessoas jurídicas referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

[5] Em voto proferido no julgamento da ADI 6649/DF, o Ministro Gilmar Mendes aduz a essa reflexão as pertinentes e relevantes palavras de Wolfgang Hoffmann-Riem: *"Na maioria dos aspectos da vida, os cidadãos são hoje obrigados a utilizar as novas tecnologias para não serem social e economicamente marginalizados"*.

[6] OCDE é uma organização econômica intergovernamental com 38 países membros, fundada em 1961 para estimular o progresso econômico e o comércio mundial:<< https://www.oecd.org/en/countries/brazil.html>>

[7] Declaração de Tallinn sobre Governo Eletrônico na reunião ministerial durante a Presidência da Estônia do Conselho da EU, em 6 de outubro de 2017.

[8] Adota-se neste trabalho a definição segundo a ANPD: O termo "Poder Público" é definido pela LGPD de forma ampla e inclui órgãos ou entidades dos entes federativos (União, Estados, Distrito Federal e Municípios) e dos três Poderes (Executivo, Legislativo e Judiciário), inclusive das Cortes de Contas e do Ministério Público. Também se incluem no conceito de Poder Público: (i) os serviços notariais e de registro (art. 23, § 4º); e *(ii)* as empresas públicas e as sociedades de economia mista (art. 24), neste último caso, desde que (*ii.i.)* não estejam atuando em regime de concorrência; ou (*ii.ii*) operacionalizem políticas públicas, no âmbito da execução destas. (Brasil, 2023).

[9] Linha do tempo disponível em Brasil, 2024b.

tecnológico, alcançou-se a fase da transformação digital, caracterizada pela **digitalização** — ou seja, o uso de tecnologias digitais e dados interconectados, com compartilhamento de informações (ENAP, 2023). A estrutura digital do setor público, orientada pela interoperabilidade entre sistemas informatizados, tornou-se uma realidade promissora, capaz de ampliar a eficácia dos gastos públicos, fortalecer a responsabilização e promover a inclusividade institucional.

Nesse cenário de interconectividade e a interoperabilidade, diversos órgãos públicos passaram a atuar de forma sistêmica e colaborativa, extrapolando seus campos tradicionais de competência por meio do compartilhamento e reuso de dados. Tal dinâmica, por um lado, proporciona benefícios notáveis — como a redução de custos para o Estado e para o cidadão, além da maior celeridade na prestação de serviços (ENAP, 2023). Por outro lado, intensifica os riscos de violação a direitos e liberdades fundamentais, impondo a adoção de salvaguardas eficazes quanto à governança e à proteção de dados pessoais.

É dizer, a interoperabilidade de dados pelo Poder Público tanto pode configurar uma ferramenta de eficiência e governança, quanto pode vir a se transformar numa ferramenta de abusiva vigilância, caso não sejam observados os limites constitucionais e legais.

Nesse contexto de serviço público digital se insere o **tema central** desta tese: o uso secundário de dados pessoais sob a custódia do Poder Público, ou seja, a reutilização daquelas informações coletadas, armazenadas e utilizadas por órgãos e entidades estatais no exercício de suas funções administrativas, regulatórias, judiciais ou de prestação de serviços públicos[10] em finalidades distintas daquelas originalmente previstas no momento da coleta, o que pode ocorrer por meio de reciclagem, reaproveitamento ou por recontextualização de dados, conforme a taxonomia proposta por Bart Custers e Helena Ursic (2017).

Ancorada nos resultados preliminares do projeto europeu EUDECO[11], a taxonomia de reutilização de dados proposta por Custers e Ursic (2017), sob a ótica do controlador[12],

[10] Em um Seminário realizado pela Procuradoria-Geral do Distrito Federal, Rodrigo Borges Valadão, Procurador do Estado do Rio de Janeiro e Doutor em Direito Público pela Albert-Ludwig-Universität Friburg (Alemanha) referiu-se a este uso secundário como "tredestinação" no tratamento de dados pessoais (Tredestinação [...], 2021). Posteriormente, juntamente com Fabrício da Mota Alves, aprofundou a análise da referência ao instituto da tredestinação para verificação de legitimidade do tratamento de dados pelo Poder Público (Alves, Valadão, 2023).

[11] O projeto EUDECO (*European Data Science Academy for Data Reuse and Privacy*) foi financiado pela Comissão Europeia no âmbito do programa-quadro Horizon 2020 (Grant Agreement nº 645244). Seu objetivo principal foi investigar os aspectos legais, técnicos e sociais da reutilização de dados no contexto do Big Data, com foco na proteção de dados pessoais e na promoção de práticas responsáveis de ciência de dados. Os resultados preliminares desse projeto serviram de base empírica e conceitual para a formulação da taxonomia apresentada por Custers e Ursic (2017).

[12] Os autores também propuseram uma taxonomia de reutilização sob a perspectiva do titular de dados: compartilhamento de dados *(data sharing)* e portabilidade de dados *(data portability)*.

estrutura-se em três categorias analíticas que refletem diferentes graus de afastamento da finalidade original da coleta de dados.

A primeira categoria, denominada reciclagem de dados (*data recycling*), refere-se à reutilização de dados para o mesmo propósito inicial, ainda que em um novo contexto operacional ou temporal. O reaproveitamento de dados (*data repurposing*) caracteriza-se pelo uso dos dados para finalidades distintas, porém ainda relacionadas ao escopo original, exigindo uma reinterpretação da compatibilidade entre os fins. Por fim, a recontextualização de dados (*data recontextualisation*) representa a forma mais desvinculada do propósito original, na qual os dados são aplicados em contextos completamente diferentes.

Essa taxonomia revela-se particularmente útil para a análise crítica do uso secundário de dados pessoais pelo Poder Público - prática cada vez mais recorrente em iniciativas de formulação de políticas públicas baseadas em dados, fiscalização, segurança pública e gestão de benefícios sociais - circunstâncias onde a distinção entre reciclagem, reaproveitamento e formas mais distantes da finalidade original de reutilização permite identificar, com maior precisão, os riscos e os benefícios associados à reutilização de dados, especialmente no que se refere à potencial violação dos princípios da finalidade, da necessidade e da transparência.

Por exemplo, o cruzamento de bases de dados pessoais administrativas para fins de controle antifraude pode configurar um reaproveitamento ou mesmo uma recontextualização – o que, por si só, não deve ser considerado um impedimento à utilização secundária, mas pode ensejar a adoção de salvaguardas adicionais, como a realização de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), conforme previsto na Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

A consolidação de um regime jurídico de proteção de dados pessoais no Brasil reflete uma transformação normativa e cultural em curso, impulsionada pela crescente centralidade da informação nas dinâmicas sociais, econômicas e institucionais contemporâneas. Nessa senda, a promulgação da Lei nº 13.709/2018 — a Lei Geral de Proteção de Dados Pessoais (LGPD) — representou um marco regulatório fundamental, ao estabelecer diretrizes para o tratamento de dados pessoais por agentes públicos e privados. Em vigor desde setembro de 2020[13], a LGPD

[13] A LGPD entrou em vigor de maneira escalonada, conforme previsto em seu Art. 65.:

- Em 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B, que tratam da constituição da então Autoridade Nacional de Proteção de Dados – ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade – CNPD;
- Em 18 de setembro de 2020, quanto aos demais artigos da Lei, com exceção dos dispositivos que tratam da aplicação de sanções administrativas; e
- Em 1º de agosto de 2021, quanto aos arts. 52, 53 e 54, que tratam das sanções administrativas.

Em análise meticulosa, Lucas Borges de Carvalho (2023) pondera que o verdadeiro fatiamento da vigência da LGPD pode ser interpretado como uma tentativa de excluir o poder público da incidência da lei.

impõe que toda atividade de tratamento observe a boa-fé e uma série de princípios, entre os quais se destaca o da finalidade.

Desdobramento direto do direito à autodeterminação informativa[14], o princípio da finalidade — previsto no art. 6º, inciso I, da LGPD — impõe que o tratamento de dados pessoais seja orientado por propósitos legítimos, específicos, explícitos e previamente informados ao titular, vedando-se, de forma expressa, qualquer reutilização incompatível com tais finalidades.

Nesse sentido, a norma conduz à compreensão de que o uso secundário de dados pelo Poder Público, ou por agentes privados, somente será legítimo se houver compatibilidade material entre a nova finalidade pretendida e aquela originalmente informada, sob pena de violação aos fundamentos constitucionais da proteção de dados pessoais.

O reconhecimento constitucional da proteção de dados pessoais como direito fundamental, por meio da Emenda Constitucional n.º 115/2022, que introduziu o inciso LXXIX ao artigo 5º da Constituição da República, reforçou ainda mais a centralidade desse tema na ordem jurídica brasileira. Ao conferir *status* constitucional, o legislador constituinte derivado não somente fortaleceu o arcabouço normativo existente, mas também reafirmou o interesse público na observância rigorosa dos princípios que regem o tratamento de dados, especialmente o da finalidade. Tal avanço normativo consolida a autodeterminação informativa como um vetor estruturante da proteção da dignidade da pessoa humana na era digital.

Nesse contexto, observa-se um processo de amadurecimento institucional e cultural, no qual a sociedade brasileira passa a compreender a proteção de dados pessoais não mais como um mero desdobramento do direito à privacidade, mas como um direito fundamental autônomo, dotado de densidade normativa própria. Esse direito emerge como instrumento essencial à salvaguarda da dignidade e da personalidade dos indivíduos em uma sociedade cada vez mais orientada pelo uso intensivo de dados. A análise crítica do uso secundário de dados pessoais pelo Poder Público, especialmente à luz do princípio da finalidade, revela-se, portanto, imprescindível para assegurar a compatibilidade entre inovação tecnológica, eficiência administrativa e respeito aos direitos fundamentais.

Ante os avanços culturais e normativos em matéria de proteção de dados pessoais, constata-se, paralelamente, a intensificação das práticas de coleta e compartilhamento de informações pessoais, tanto por agentes privados quanto por entes do Poder Público. Esse

[14] A autodeterminação informativa é o direito de controle pessoal sobre o trânsito de dados relativo ao próprio titular – e, portanto, uma extensão das liberdades do indivíduo (Rony Vainzof *in* Maldonado; Blum, 2021). Há autores que mais se alinham à doutrina portuguesa e utilizam a expressão "autodeterminação informacional". Nesse sentido: Nobre Junior, 2020.

movimento, embora muitas vezes orientado por finalidades legítimas, acarreta riscos concretos à autodeterminação informativa dos titulares, especialmente quando não acompanhado de salvaguardas adequadas.

A crescente assimetria informacional entre o Estado e o cidadão comum tende a acentuar desequilíbrios estruturais de poder, impondo uma análise crítica sobre as possibilidades de reutilização de dados pessoais para finalidades distintas daquelas que motivaram sua coleta original, conjuntura que exige vigilância normativa e institucional, a fim de evitar que o tratamento secundário de dados comprometa direitos fundamentais e fragilize a confiança social nas instituições públicas.

Posto esse cenário, exsurge a **pergunta** a ser respondida pela pesquisa: ***quais são os limites e as possibilidades para o compartilhamento e uso secundário de dados pessoais no âmbito do Poder Público?***

A pesquisa tem como **objetivo geral** investigar a problemática proposta, com o intuito de identificar os riscos e benefícios associados ao uso secundário de dados pelo Poder Público. Ademais, busca-se examinar a aderência à lógica procedimental de salvaguardas na Lei Geral de Proteção de Dados Pessoais, com o propósito de oferecer uma contribuição relevante no campo doutrinário, de modo a cooperar para a consolidação e o aprofundamento da compreensão do direito fundamental à proteção de dados pessoais, bem como para reafirmar sua centralidade no ordenamento jurídico contemporâneo.

Para alcançar seu objetivo geral, a presente pesquisa se propõe a cumprir os seguintes **objetivos específicos**:

a) analisar a Teoria dos Direitos Fundamentais como referencial teórico aplicável à proteção de dados pessoais, especialmente no que tange às restrições ao princípio da finalidade no contexto do uso secundário de dados pelo Estado;

b) refletir sobre o compartilhamento de dados pessoais pelo Poder Público como exercício de função administrativa, sujeito a controle, a partir do referencial teórico do Regime Jurídico Administrativo;

c) examinar o regime jurídico brasileiro relativo ao tratamento de dados pessoais pelo Poder Público, com ênfase nos dispositivos constitucionais, legais e regulamentares que disciplinam a reutilização de dados;

d) reflexionar acerca do poder informacional do Estado e sobre o *trade-off* entre o princípio da eficiência e a proteção de dados pessoais pelo Poder Público;

e) estudar os julgamentos paradigmáticos do Supremo Tribunal Federal, notadamente as decisões proferidas nas ADIs nº 6387 e nº 6649, com o intuito de identificar os parâmetros constitucionais estabelecidos para o uso secundário de dados;

e) investigar práticas concretas de compartilhamento de dados pessoais pelo Poder Público posteriores aos referidos julgamentos, com base em análise documental e normativa, a fim de verificar a aderência às salvaguardas previstas na LGPD; e

f) propor mecanismos jurídicos e institucionais que promovam aprimoramentos normativos e técnicos para o compartilhamento de dados pelo poder público, com destaque para o princípio da única vez (*Once-Only principle*) e outras boas práticas de governança de dados.

Espera-se, como **resultado da investigação**, oferecer subsídios teóricos e práticos que contribuam para a formulação de soluções que assegurem aos cidadãos um tratamento informacional compatível com os parâmetros do devido processo informacional (*informational due process privacy right*), entendido como expressão da dimensão subjetiva do direito fundamental à proteção de dados pessoais.

Em uma abordagem voltada para uma ancoragem do trabalho no empírico com atravessamento pelo teórico (Carvalho, 2013), foi realizada uma pesquisa jurisprudencial, por meio de estudo de casos de referência (*leading cases*), com análise documental de processos judiciais que definiram os critérios que orientam a interpretação do Supremo Tribunal Federal sobre o uso secundário de dados pessoais pelo Poder Público.

Nessa abordagem, o primeiro caso-paradigma selecionado para análise revela-se de especial relevância, uma vez que o Supremo Tribunal Federal nele reconheceu, de forma inequívoca, a proteção constitucional autônoma dos dados pessoais — para além da tutela tradicional conferida ao sigilo das comunicações. Trata-se de uma decisão paradigmática porque eleva a autodeterminação informativa à condição de princípio constitucional implícito, ao mesmo tempo, fortalece sua positivação no ordenamento jurídico infraconstitucional.

Tratava-se das discussões sobre a Medida Provisória n º 954, de 2020, que determinava o compartilhamento de dados entre empresas de telecomunicações e o Instituto Brasileiro de Geografia e Estatística – IBGE, com vistas à realização censo por telefone no contexto da pandemia do COVID-19.

Contra aquele texto legal foram ajuizadas as Ações Diretas de Inconstitucionalidade n º 6387, 6388, 6389, 6393 e 6390, que alegavam violação das regras constitucionais da dignidade da pessoa humana, da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, do sigilo dos dados e da autodeterminação informativa.

As ações tramitaram conjuntamente e a decisão proferida na ADI n º 6387 – ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil - foi reproduzida nos demais processos.

O segundo caso paradigmático que serve de base para a reflexão aqui empreendida é o julgamento da Ação Direta de Inconstitucionalidade nº 6.649, ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) contra o Decreto n. º 10.046, de 9 de outubro de 2019 da Presidência da República, 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.

Com a declarada finalidade de aumentar a qualidade e a eficiência das operações internas da administração pública federal, o referido Decreto possibilitou o amplo compartilhamento e os usos secundários com cruzamento de informações, contudo, sem estabelecer medidas que garantissem o tratamento adequado, seguro e transparente dos dados pessoais.

No julgamento daquela Ação Direta de Inconstitucionalidade nº 6.649, o Supremo Tribunal Federal conferiu interpretação conforme a Constituição ao Decreto n. º 10.046/2019, estabeleceu fronteiras ao exercício de direitos fundamentais e designou um âmbito de proteção para o tratamento de dados pessoais pelo poder público.

Após aquele julgado – e, supostamente, para que houvesse alinhamento aos pressupostos fixados pelo Supremo Tribunal Federal – foi editado o Decreto n. º 11.266, de 25 de novembro de 2022, que altera aqueloutro Decreto nº 10.046, de 9 de outubro de 2019.

Na sequência, a pesquisa, avança em seu objetivo de averiguar se, após aqueles parâmetros fixados pelo Supremo Tribunal Federal nos casos paradigmáticos, o tratamento secundário de dados pessoais realizado pelo Poder Público se ajusta a lógica procedimental de salvaguardas conforme a Lei Geral de Proteção de Dados Pessoais e conforme a Constituição.

E, nesse **intuito de verificar os consectários** práticos dos julgamentos ADI n º 6387 e ADI nº 6.649, considerando que no ambiente digital integrado e interoperável, múltiplas são as possíveis conexões entre bases e usos secundários de dados pessoais, foi necessário ser estabelecido um filtro na pesquisa. Assim, um caso não judicializado foi selecionado, referente ao Decreto nº 12.428, de 3 de abril de 2025, que, ao regulamentar os requisitos para concessão, manutenção e revisão do benefício de prestação continuada previsto na Lei nº 8.742, de 7 de dezembro de 1993, disciplina o compartilhamento de dados pelos órgãos públicos federais e pelas prestadoras de serviços públicos.

A pesquisa ainda examina se, nesse caso de uso secundário de dados pelo Poder Público, foram observadas as orientações da Agência Nacional de Proteção de Dados (ANPD)[15], consoante expostas em seu Guia Orientativo Tratamento de dados pessoais pelo Poder Público (Brasil, 2023).

A investigação parte de duas **hipóteses centrais: a primeira** sustenta que, no contexto da proteção de dados pessoais — especialmente após a promulgação da Emenda Constitucional nº 115/2022, que elevou esse direito à categoria de direito fundamental — a Teoria dos Direitos Fundamentais oferece um instrumento teórico robusto para a análise das restrições que devem ser impostas aos usos secundários de dados pelo Poder Público. Essa análise encontra respaldo na doutrina de Laura Schertel Mendes (2018), Danilo Doneda (2019), Sarlet e Saavedra (2020) e Mendes e Fernandes (2020).

E, inserida no âmbito da Teoria dos Direitos Fundamentais, destaca-se a abordagem da Teoria dos Limites dos Limites (*Schranken-Schranken*), originalmente formulada na tradição constitucional alemã a partir de uma conferência proferida por Karl August Bettermann. Esse referencial tem sido amplamente acolhido na doutrina nacional (Barroso, 2014; Mendes, Branco, 2024), bem como por autores do direito comparado (Alexy, 2008; Pieroth, Schilink, 2012; Luque, 1993), consolidando-se como instrumento teórico essencial para a proteção contra restrições desproporcionais aos direitos fundamentais.

Utilizada como critério para a avaliação das restrições a direitos fundamentais, a Teoria dos Limites dos Limites permeia o presente estudo ao estabelecer que há balizas às próprias limitações desses direitos, exigindo que qualquer restrição seja necessária, adequada e proporcional à finalidade legítima que se pretende alcançar.

A segunda hipótese adotada considera que os argumentos de eficiência não podem imunizar o Poder Público ao controle de suas atividades administrativas. Nesse sentido, adota-se como **referencial teórico** o Regime Jurídico Administrativo, que, no Estado Democrático de Direito, compreende o princípio do controle da atividade administrativa como um dos instrumentos essenciais de limitação ao poder estatal[16].

Considerando que o direito administrativo consiste na formalização de sistemas de controles sociais sobre os exercentes de funções administrativas, com base na observância das

[15] Em virtude da edição da Medida Provisória nº 1.317, de 17 de setembro de 2025, a Autoridade Nacional de Proteção de Dados foi transformada em Agência Nacional de Proteção de Dados (também chamada de ANPD), autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública.

[16] O Direito Administrativo deve ser considerado "um conjunto de limitações aos poderes do Estado ou, muito mais acertadamente, como um conjunto de deveres da Administração em face dos administrados." (Bandeira De Mello, 2009).

formas estatuídas no ordenamento jurídico pátrio, privilegia-se aqui a doutrina nacional como fonte teórica (Meirelles, 1988; Araújo, 2005; Bandeira De Mello, 2009; Carvalho Filho, 2013; Di Pietro, 2012; Justen Filho, 2005).

Para a condução deste estudo, foi adotada uma **abordagem metodológica** predominantemente descritiva e qualitativa, adequada à análise de fenômenos jurídicos em sua complexidade e inserção social. A pesquisa descritiva, conforme Gil (2010), visa caracterizar sistematicamente determinado fenômeno ou população, sem a interferência do pesquisador, sendo especialmente útil no campo jurídico para mapear práticas normativas, decisões judiciais e estruturas institucionais. Já a abordagem qualitativa permite uma compreensão aprofundada dos significados atribuídos aos fenômenos jurídicos pelos sujeitos envolvidos, valorizando a interpretação e a contextualização. Segundo Nascimento (2016), a abordagem qualitativa é a mais apropriada para pesquisas da área das ciências sociais, porquanto é baseada na interpretação dos fenômenos observados e no significado que carregam, ou no significado atribuído pelo pesquisador, dada a realidade na qual os fenômenos estão inseridos.

Como o objeto da pesquisa diz respeito à discussão de parâmetros para o compartilhamento e uso secundário de dados pessoais no âmbito do Poder Público, a abordagem qualitativa foi empregada, porquanto foram estudados aspectos da realidade que não são quantificáveis e que englobam um conjunto heterogêneo de perspectivas e de análises.

Foi adotado o método indutivo na análise bibliográfica, com recurso à doutrina brasileira e estrangeira, de modo a examinar as publicações relevantes a respeito do objeto sob investigação, identificando-se as diversas posições teóricas sobre o assunto. Também foi utilizado o recurso documental, com exame de normas, julgados e decisões administrativas, precipuamente pela técnica de análise de conteúdo, que tem os documentos como fonte de pesquisa.

Encontra-se na literatura jurídica nacional vários textos que tratam a respeito dos vícios que eivaram o Decreto n. º 10.046/2019 de inconstitucionalidade, que inclusive serão abordados ao longo desta dissertação; porém, não encontramos análises que se ocuparam em verificar os consectários dos julgamentos paradigmas aqui reportados. Portanto, a **relevância** do presente estudo reside no seu contributo para se pensar em formas de utilização de dados pessoais pelo Poder Público para alcançar a prestação de serviços públicos e a execução de políticas e funções públicas de modo seguro, eficiente e consoante a observância aos direitos dos cidadãos.

Para além deste introdutório, a pesquisa assim se estruturou:

No Capítulo 1, são apresentados marcos teóricos que sustentam o direito fundamental à proteção de dados pessoais: a perspectiva jusfilosófica e jurídica, conforme delineada por

Doneda, Sarlet e Saavedra; o constitucionalismo digital, segundo os argumentos de Mendes e Fernandes (2020); e a teoria da autodeterminação informativa, desenvolvida pelo Tribunal Constitucional Federal Alemão e difundida no Brasil por Laura Schertel Mendes (2018). Também é abordada a Teoria dos Limites dos Limites com o **objetivo específico** de evidenciar a sua aplicabilidade ao objeto de investigação, notadamente às possíveis limitações ao princípio da finalidade, que orienta o uso secundário de dados pessoais pelo Poder Público; e o Regime Jurídico Administrativo como justificador do necessário controle sobre os compartilhamentos e usos secundários de dados pessoais pelo Poder Público na condição de atividades administrativas.

O Capítulo 2 dedica-se à análise dos regramentos constitucionais, legais e infralegais que regulam o tratamento de dados pessoais pelo Poder Público, com o **objetivo específico** de construir uma compreensão sistêmica da proteção de dados como um ecossistema normativo multifacetado. Esse ecossistema é composto por um conjunto heterogêneo de normas que abrange desde princípios constitucionais — como a dignidade da pessoa humana, a privacidade e a autodeterminação informativa — até normas legais específicas, diretrizes técnicas, regulamentos administrativos e procedimentos operacionais. A abordagem proposta reconhece a interdependência entre esses níveis normativos e destaca a necessidade de uma interpretação integrada e teleológica, capaz de assegurar a efetividade do direito fundamental à proteção de dados no exercício da função administrativa.

O Capítulo 3 propõe uma reflexão crítica acerca dos contornos normativos e das implicações práticas do tratamento de dados pessoais pelo Poder Público no contexto contemporâneo. A análise considera, de forma central, os desafios impostos pela tecnovigilância e pelo crescente poder informacional do Estado, fenômenos que tensionam os limites da atuação administrativa frente à salvaguarda dos direitos fundamentais. Nesse cenário, impõe-se a necessidade de ponderação entre a busca por eficiência administrativa — frequentemente associada à coleta e ao compartilhamento massivo de dados — e a proteção efetiva dos direitos à privacidade e à autodeterminação informativa. A abordagem adotada tem por **objetivo específico** enfatizar a importância de critérios de proporcionalidade e de controle jurídico rigoroso, como forma de assegurar que o exercício do poder informacional pelo Estado se mantenha compatível com os parâmetros constitucionais de proteção de dados pessoais.

O Capítulo 4 examina, à luz dos limites estabelecidos pelo ordenamento jurídico vigente, dois julgamentos paradigmáticos do Supremo Tribunal Federal — a ADI nº 6387 e a ADI nº 6649 — com o **objetivo específico** de identificar os marcos interpretativos fundamentais que orientam a definição dos limites constitucionais para o compartilhamento de dados pessoais

pelo Poder Público. A análise dessas decisões permite compreender como o STF tem consolidado parâmetros normativos e hermenêuticos que equilibram a atuação estatal com a proteção dos direitos fundamentais à privacidade e à autodeterminação informativa, especialmente diante da crescente complexidade das práticas de tratamento de dados no contexto digital. Trata-se, portanto, de uma abordagem que articula jurisprudência constitucional com os princípios estruturantes da proteção de dados, contribuindo para o delineamento de uma atuação administrativa compatível com os valores democráticos e com o Estado de Direito.

O Capítulo 5 tem por **objetivo específico** verificar a conformidade das práticas administrativas com os parâmetros interpretativos firmados pelo Supremo Tribunal Federal, especialmente nas ADIs nº 6387 e nº 6649. Para tanto, sistematizam-se os principais pontos de convergência entre esses julgados e as diretrizes normativas emanadas pela Agência Nacional de Proteção de Dados (ANPD). Em seguida, procede-se à análise das alterações introduzidas no Decreto nº 10.046/2019, que institui a governança no compartilhamento de dados no âmbito da Administração Pública federal, com destaque para a criação do Cadastro Base do Cidadão e do Comitê Central de Governança de Dados. Examina-se também a Política de Governança e Compartilhamento de Dados e o Decreto nº 12.428, de 3 de abril de 2025, que regulamenta o compartilhamento de dados pessoais por órgãos públicos federais e prestadoras de serviços públicos, estabelecendo critérios técnicos, jurídicos e operacionais para o tratamento de dados, inclusive em formato pseudonimizado, com vistas à concessão e revisão de benefícios sociais, conforme os princípios da Lei Geral de Proteção de Dados Pessoais.

O Capítulo 6 tem como **objetivo específico** propor aprimoramentos institucionais voltados à criação de mecanismos que assegurem a transparência, a motivação e o controle efetivo das operações de tratamento de dados pessoais realizadas pelo Poder Público em contextos posteriores ao seu recolhimento. Para tanto, discorre-se sobre a relevância dos instrumentos jurídicos formais que regulam o compartilhamento de dados, destacando-se a necessidade de conformidade com os princípios constitucionais e com os parâmetros estabelecidos pela Lei Geral de Proteção de Dados Pessoais (LGPD). Nesse contexto, apresenta-se o Princípio da Única Vez (*Once-Only Principle*) como uma possibilidade estratégica de racionalização administrativa, capaz de promover eficiência sem comprometer os direitos fundamentais à privacidade e à proteção de dados. A análise pondera, ainda, sobre os limites jurídicos e as garantias de legitimidade que devem orientar o compartilhamento de dados pessoais pelo Estado, especialmente no exercício de funções administrativas que envolvem interoperabilidade entre sistemas e bases de dados.

Por fim, no capítulo de conclusão, são sistematizados os principais achados da investigação, com destaque para as contribuições teóricas e práticas que emergem da análise crítica do tratamento de dados pessoais pelo Poder Público. A pesquisa evidencia a complexidade normativa e institucional que envolve o tema, propondo uma leitura integrada entre os fundamentos constitucionais, os parâmetros jurisprudenciais e os instrumentos infralegais de regulação. Ressalta-se ainda, a importância da construção de mecanismos institucionais que assegurem a legitimidade, a transparência e o controle das operações de tratamento de dados, especialmente em contextos de uso secundário. Nesse sentido, o estudo contribui para o aprimoramento do debate acadêmico e para o fortalecimento de práticas administrativas compatíveis com os direitos fundamentais e com os valores democráticos que estruturam o Estado de Direito.

1.2 JUSTIFICATIVA

> Tais preocupações são particularmente relevantes no contexto do Poder Público, dada a natureza assimétrica, não facultativa e continuada das relações entre indivíduos e Estado (Wimmer, 2021).

A motivação para a presente investigação foi instigada por uma provocação teórica formulada pela Professora Miriam Wimmer que, em artigo publicado na Revista Brasileira de Políticas Públicas (Wimmer, 2021), destacou a escassez de produção acadêmica nacional sobre o uso secundário de dados pessoais no âmbito do Poder Público. A autora concluiu que a definição de critérios concretos para a realização legítima e segura desse tipo de tratamento de dados, à luz da Lei Geral de Proteção de Dados Pessoais (LGPD) e da Constituição Federal, ainda constitui um desafio normativo e doutrinário a ser enfrentado.

Aquele estímulo acadêmico encontrou ressonância prática no ano de 2022, quando, no exercício da função de Assessoria Jurídica, surgiu um caso concreto a ser enfrentado: o Conselho Nacional de Justiça (CNJ), por meio do Ofício-Circular n.º 30/2022 – SG, encaminhou para Tribunal Regional Federal da 5ª. Região o Ofício n.º 15/2022/SE/SECAD/DECAU/CGAP/MC, oriundo da Secretaria Nacional do Cadastro Único (SECAD), integrante do então Ministério da Cidadania. O referido documento solicitava autorização para uso da base de dados do Poder Judiciário para qualificação do Cadastro Único para Programas Sociais do Governo Federal (Processo Administrativo SEI n. º 0002746-39.2022.4.05.7000).

A SECAD argumentou que o compartilhamento da base de dados dos servidores do Poder Judiciário seria uma boa prática administrativa, apta a subsidiar o processo de averiguação

cadastral e a detecção de inconsistências nos registros do Cadastro Único. Alegou, ainda, que tal compartilhamento encontrava respaldo no caput do art. 15 do Decreto n. º 10.046, de 9 de outubro de 2019, bem como nas disposições da Lei n. º 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), e da Lei n. º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD). Por fim, comprometeu-se a resguardar o sigilo e a proteger os dados pessoais envolvidos, limitando seu uso à finalidade expressamente indicada.

Diante da demanda por parecer jurídico sobre a legalidade e a legitimidade daquela solicitação, foi realizada uma análise da literatura jurídica nacional pertinente ao uso secundário de dados pessoais pelo Poder Público, o que serviu de ponto de partida para a presente pesquisa.

2 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS: REFERENCIAIS TEÓRICOS

> Os dados pessoais chegam a fazer às vezes da própria pessoa em uma série de circunstâncias nas quais a sua presença física seria outrora indispensável (Doneda, 2011).

A consagração do direito à proteção de dados pessoais como direito fundamental na Constituição Federal brasileira, por meio da Emenda Constitucional nº 115/2022, representou um marco normativo e simbólico na consolidação da cidadania digital. O inciso LXXIX integrado ao artigo 5º estabelece que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais", conferindo densidade constitucional a uma demanda que já vinha sendo reconhecida pela doutrina e jurisprudência como direito fundamental implícito e derivado de outros direitos correlatos.

Os referenciais teóricos que sustentam esse direito fundamental revelam-se multifacetados, articulando diferentes perspectivas que se complementam e dialogam para oferecer uma visão abrangente dos desafios e proteções necessárias na sociedade digital contemporânea. Nessa senda, três visões aqui merecem destaque: a fundamentação jusfilosófica e jurídica, o devido processo informacional e a autodeterminação informativa:

a) **A Fundamentação jusfilosófica e jurídica:**

Sob a ótica do constitucionalismo brasileiro, a proteção de dados foi inicialmente concebida como uma extensão dos direitos à intimidade, à vida privada, à honra e à imagem, previstos nos incisos X e XII do artigo 5º da Constituição Federal, bem como do sigilo das comunicações[17]. Esta compreensão foi atualizada e ampliada pela doutrina, destacando-se o trabalho de Danilo Doneda, que defendia a proteção de dados como um direito fundamental autônomo, intrinsecamente ligado à autodeterminação informacional e à dignidade da pessoa humana. Em sua obra *Da privacidade à proteção de dados pessoais* (Doneda, 2019), argumenta que os dados pessoais representam projeções da personalidade, de modo que sua tutela jurídica deve ser vista como extensão dos direitos de personalidade, exigindo proteção específica e autônoma.

Complementarmente, Sarlet e Saavedra (2020) aprofundam essa fundamentação jusfilosófica, articulando as teorias de Hegel, Axel Honneth e Daniel Solove. Inspirando-se em

[17] Danilo Doneda (2019) destacou que, no contexto brasileiro, a ambivalência entre a proteção de dados pessoais e o direito à privacidade funcionou como um elemento de continuidade entre uma tradição jurídica que reconheceu, regulou e atualizou o direito à privacidade, culminando na formulação de um marco regulatório específico para a proteção de dados.

Hegel, reconhecem que o direito é uma expressão da vontade livre, situando a proteção de dados como condição essencial para o exercício da liberdade concreta na sociedade digital. Honneth contribui com a teoria do reconhecimento, que vincula a proteção de dados à justiça social e à inclusão, enquanto Solove propõe uma abordagem contextual da privacidade, focada na autonomia informacional e considerando os múltiplos riscos decorrentes do tratamento de dados na modernidade.

A confluência dessas abordagens revela que o direito à proteção de dados transcende a tradicional noção de privacidade como "direito de estar só" (Warren e Brandeis, 1890), assumindo uma importância estrutural para a democracia e para o exercício pleno dos direitos fundamentais na sociedade informacional.

A perspectiva jusfilosófica e jurídica, conforme delineada por Doneda, Sarlet e Saavedra, reflete a dimensão da liberdade, dignidade e reconhecimento jurídico do indivíduo, cuja constitucionalização não somente avança no plano normativo, mas também reafirma eticamente a centralidade da pessoa humana frente aos desafios tecnológicos e informacionais contemporâneos.

b) **O devido processo informacional:**

O termo devido processo informacional designa um conjunto de garantias, procedimentos e controles destinados a assegurar que o tratamento de dados pessoais pelo Estado ocorra de forma transparente, legal, justa e racional. Esse conceito abrange o direito do titular à observância dos princípios da finalidade, necessidade, adequação, transparência e segurança no tratamento de suas informações pessoais. Integra, ainda, direitos essenciais como o contraditório, a ampla defesa, o direito à contestação e à retificação dos dados, bem como a responsabilização integral pelos atos de tratamento. Assim, o devido processo informacional constitui a expressão procedimental dos direitos de proteção de dados, funcionando como salvaguarda contra arbitrariedades e como instrumento de efetivação da dignidade da pessoa humana e dos direitos fundamentais.

Segundo Sarlet e Sales Sarlet (2022), o devido processo informacional transcende um legado do constitucionalismo liberal, configurando-se como exigência estruturante do Estado Democrático de Direito. Diante das assimetrias radicais, da pervasividade das tecnologias digitais e das práticas abusivas que comprometem a autonomia dos indivíduos — e até mesmo dos agentes estatais —, impõe-se a adoção de instrumentos normativos e procedimentais capazes de estabelecer limites efetivos ao tratamento de dados pessoais. Dentre esses instrumentos, destacam-se as garantias do contraditório e da ampla defesa, condições

indispensáveis ao livre desenvolvimento da personalidade e à proteção dos direitos fundamentais.

Importa destacar que o direito fundamental à proteção de dados pessoais não se restringe à sua dimensão subjetiva, como direito individual de defesa contra abusos estatais, mas incorpora uma dimensão jurídico-objetiva que impõe ao Estado o dever de proporcionar confiabilidade, integridade e segurança às infraestruturas informacionais sob sua responsabilidade. A ausência dessas garantias representa proteção insuficiente e potencial vulneração dos direitos dos titulares.

Ao enfatizar a absoluta incompatibilidade do direito fundamental à proteção de dados pessoais com práticas estatais que promovam ou permitam o tratamento indiscriminado de informações pessoais, os mesmos autores salientam que o devido processo informacional articula-se com o princípio da separação informacional de poderes. Ambos os princípios operam como mecanismos fundamentais de contenção dos riscos e das assimetrias impostos pela revolução digital, garantindo um controle democrático sobre o fluxo e uso dos dados no âmbito estatal.

Por sua vez, o princípio da separação informacional impõe limites e barreiras entre os entes e órgãos públicos, com o objetivo de impedir a concentração excessiva e o compartilhamento indiscriminado de dados pessoais. Inspirado na lógica clássica da separação dos poderes, esse princípio projeta-se sobre o domínio informacional, exigindo que o tratamento de dados ocorra de forma descentralizada, controlada e com finalidades específicas, prevenindo a formação de bases unificadas que ampliem os riscos de abusos e violações à privacidade.

Além disso, o princípio da separação informacional se alinha diretamente com direitos constitucionais como a privacidade e a intimidade, consagrados na Constituição Federal de 1988 e reforçados posteriormente pela Lei Geral de Proteção de Dados Pessoais (LGPD). Sua emergência responde à necessidade imperativa de proteger os indivíduos contra o tecnovigilantismo estatal — isto é, o uso intrusivo e desproporcional da tecnologia para monitorar e controlar os cidadãos (Ribeiro, 2024).

Sarlet e Sales Sarlet (2022) sustentam ser possível extrair, a partir da interpretação sistemática dos artigos 1º, *caput*, inciso III e parágrafo único, bem como do artigo 2º da Constituição Federal, aqueles dois princípios implícitos e estruturantes da atuação estatal no contexto informacional: o devido processo informacional e a separação informacional de poderes.

Em síntese, enquanto a separação informacional configura uma estrutura preventiva e normativa que limita a circulação e o compartilhamento de dados entre os órgãos públicos, o

devido processo informacional engloba um conjunto de direitos e procedimentos que asseguram a proteção efetiva dos dados ao longo de todo o seu ciclo de tratamento. Ambos os princípios atuam complementarmente para preservar direitos no ambiente informacional público e assegurar o equilíbrio entre o poder estatal e a proteção dos direitos fundamentais no Estado Democrático de Direito.

c) **A Autodeterminação informativa**:

A autodeterminação informativa confere ao indivíduo o controle ativo e consciente sobre seus dados pessoais, abrangendo decisões relativas à coleta, ao tratamento, ao compartilhamento e à correção dessas informações. Trata-se da expressão da autonomia privada no contexto da sociedade da informação, assegurando ao titular o direito de exigir transparência quanto ao uso de seus dados e de revogar consentimentos ou solicitar sua exclusão, quando cabível.

Como pilar do Estado Democrático de Direito na era digital, esse direito não se limita à relação vertical entre indivíduo e Estado, estendendo-se às relações horizontais entre particulares. Impõe que o tratamento de dados pessoais observe princípios constitucionais como a dignidade da pessoa humana e o livre desenvolvimento da personalidade, além de exigir do Estado a garantia da segurança, integridade e confiabilidade das infraestruturas informacionais.

A teoria da autodeterminação informativa foi desenvolvida pelo Tribunal Constitucional Federal Alemão no julgamento do caso do recenseamento de 1983 (*Volkszählungsurteil)*, constituindo um marco na evolução dos direitos fundamentais frente aos desafios da sociedade digital. No Brasil, Laura Schertel Mendes (2018) destaca que essa teoria desloca o eixo da proteção da privacidade da esfera íntima para o reconhecimento do controle ativo do indivíduo sobre o fluxo de seus dados pessoais.

A autora sustenta que o direito à autodeterminação informativa pode ser extraído da Constituição Federal de 1988 por meio de uma interpretação sistemática que articula a inviolabilidade da intimidade e da vida privada (art. 5º, X), o habeas data (art. 5º, LXXII) e o princípio da dignidade da pessoa humana (art. 1º, III). Essa leitura integrada permite reconhecer que o controle sobre os próprios dados é expressão direta da proteção constitucional da personalidade.

Laura Mendes propõe que o habeas data e a autodeterminação informativa sejam compreendidos como duas faces de uma mesma moeda: o primeiro como garantia processual de acesso e retificação de dados; o segundo como direito material de controle sobre sua coleta, uso e circulação. Ela também demonstra que o direito à proteção de dados possui dupla

dimensão: subjetiva, ao conferir ao titular poder decisório sobre seus dados; e objetiva, ao impor ao Estado deveres de proteção, regulação e fiscalização, inclusive nas relações privadas.

A autora demonstra que o direito à proteção de dados possui dupla dimensão: subjetiva, ao conferir ao titular dos dados o poder de decidir sobre a coleta, uso e circulação de suas informações pessoais, com base no consentimento ou em fundamento legal legítimo; e objetiva, porque impõe ao Estado deveres de proteção, regulação e fiscalização, inclusive nas relações privadas, reconhecendo a eficácia horizontal dos direitos fundamentais.

Importante destacar que esse direito não é absoluto, podendo ser limitado por outros direitos ou interesses públicos, desde que respeitados os princípios da legalidade, proporcionalidade e necessidade. A proteção de dados, nesse sentido, é essencial para a efetividade de diversos outros direitos fundamentais, como igualdade, liberdade de expressão, livre exercício profissional e não discriminação.

Ingo Wolfgang Sarlet e Gabriele Sales Sarlet (2022) apresentam a autodeterminação informativa como eixo estruturante da proteção de dados pessoais e do direito à privacidade na sociedade informacional. Para os autores, esse direito confere ao indivíduo controle sobre suas informações frente ao Estado e à coletividade, exigindo práticas de governança que respeitem a autonomia informacional e impeçam a formação de “unidades informacionais” estatais concentradoras.

Eles vinculam a autodeterminação informativa à necessidade de limites claros ao uso e compartilhamento de dados entre os poderes e órgãos públicos, ampliando a clássica separação de poderes para abarcar sua dimensão informacional. Nesse contexto, a autodeterminação impulsiona a exigência por transparência, ética e responsabilidade na gestão de dados, consolidando instrumentos como o devido processo informacional e o princípio da separação informacional de poderes.

A proteção de dados pessoais como direito fundamental articula-se, portanto, com a centralidade do titular dos dados, a proteção da privacidade e os desafios do ambiente digital. Sua consagração constitucional, pela Emenda Constitucional nº 115/2022, representa uma resposta sofisticada aos riscos da sociedade da informação, deslocando o foco da intimidade para a titularidade ativa sobre os dados.

Esse novo paradigma normativo confere à proteção de dados papel estruturante na promoção da dignidade humana, na garantia da liberdade informacional e na efetivação da cidadania digital. A constitucionalização do direito impõe um compromisso substancial aos operadores jurídicos, ao Estado e à sociedade civil na construção de uma governança informacional que respeite os direitos fundamentais.

Nesse cenário, legisladores, reguladores e tribunais são convocados a desenvolver uma proteção eficaz, proporcional e contextualizada, capaz de harmonizar direitos individuais com interesses coletivos e os imperativos da inovação tecnológica. A proteção de dados deve ser compreendida como instrumento de afirmação da autonomia pessoal, da liberdade de expressão e do reconhecimento social do indivíduo.

Cumpre ainda mencionar a proposta de Sarlet e Sales Sarlet (2022) de interpretar o direito à proteção de dados à luz da teoria do constitucionalismo digital, fundamentada nos apontamentos de Ilton Norberto Robl Filho (2022). Segundo essa perspectiva, o constitucionalismo digital revisa criticamente a estrutura do constitucionalismo tradicional, propondo novos parâmetros interpretativos para os direitos fundamentais no ciberespaço.

Mendes e Fernandes (2020) defendem que o constitucionalismo digital constitui uma ideologia normativa voltada à afirmação e proteção de direitos fundamentais em ambientes digitais, oferecendo diretrizes para a atuação jurisdicional, especialmente no controle de constitucionalidade de normas que regulam a internet e o tratamento de dados.

Nesse prisma, o direito à proteção de dados é considerado um direito estrutural, condicionante do exercício de outros direitos constitucionais. A atuação das plataformas digitais, com poderes normativos e adjudicativos sobre os dados dos usuários, desafia a clássica relação Estado-indivíduo, exigindo a efetivação da eficácia horizontal dos direitos fundamentais nas relações privadas digitais.

O artigo de Mendes e Fernandes (2020) destaca a necessidade de a jurisdição constitucional brasileira reconhecer a reterritorialização da internet, considerando a circulação transnacional dos dados e os conflitos jurídicos que transcendem fronteiras estatais. A proteção de dados, nesse contexto, demanda soluções jurídicas que conciliem soberania nacional, governança global e responsabilidade dos intermediários digitais.

O Marco Civil da Internet (Lei nº 12.965/2014) é apresentado como exemplo paradigmático de legislação infraconstitucional de natureza proto-constitucional, ao garantir princípios como proteção à privacidade (art. 3º, II) e liberdade de expressão (art. 3º, I). A interpretação constitucional desses dispositivos deve incorporar os valores do constitucionalismo digital, especialmente em casos complexos envolvendo acesso transnacional a dados, responsabilidade de plataformas e uso de algoritmos com potencial discriminatório.

Assim, o constitucionalismo digital oferece base teórica para a afirmação do direito à proteção de dados como direito fundamental, exigindo dos tribunais constitucionais uma postura ativa, inovadora e responsiva às transformações tecnológicas. Longe de ser mera

prerrogativa individual, esse direito constitui elemento estruturante da cidadania digital e da democracia informacional.

O direito à proteção de dados deve, portanto, ser concebido como um direito em permanente construção, cuja efetividade depende de uma interpretação constitucional dinâmica e aberta às transformações sociais e tecnológicas. Essa perspectiva reforça a necessidade de um comprometimento com a justiça informacional, a equidade no acesso e uso de dados, e a proteção dos direitos humanos em um contexto globalizado, no qual a informação se configura simultaneamente como recurso estratégico e vetor de riscos à liberdade e à personalidade.

2.1 DOS DIREITOS FUNDAMENTAIS

Fundamental é mesmo o amor (Wave, 1976).

Já aqui ressaltado que a matéria objeto da presente reflexão — a proteção de dados pessoais — foi alçada à condição de **direito fundamental** no ordenamento jurídico brasileiro com a promulgação da Emenda Constitucional nº 115, em 10 de fevereiro de 2022. Essa emenda introduziu uma importante modificação no artigo 5º da Constituição da República Federativa do Brasil, ao reconhecer expressamente o direito à proteção de dados pessoais, inclusive nos meios digitais, como um direito fundamental autônomo.

Além de promover o reconhecimento constitucional da proteção de dados, reforçando sua centralidade no sistema de garantias individuais e ampliando a segurança jurídica no tratamento de informações pessoais, a Emenda Constitucional nº 115 também estabeleceu que cabe privativamente à União legislar sobre proteção e tratamento de dados pessoais, o que se configurou como medida relevante para evitar a fragmentação normativa e conflitos de competência entre entes federativos.

O direito fundamental à proteção de dados pessoais, embora dotado de autonomia e de um âmbito de proteção próprio, não se apresenta de forma isolada no ordenamento jurídico. Ao contrário, revela-se intrinsecamente conectado a outros direitos e princípios constitucionais – notadamente com o direito à privacidade – bem como, em uma perspectiva ampliada e característica dos Estados constitucionais abertos, ao direito internacional dos direitos humanos. Essa interconexão reforça sua natureza híbrida, simultaneamente como direito fundamental e direito humano, o que, por sua vez, não exclui a possibilidade de tensões e conflitos normativos em contextos diversos (Sarlet, 2023).

A normatização infraconstitucional, conferida pela Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD), desempenha papel essencial na concretização daquele conteúdo constitucional, ao delimitar o escopo de proteção do direito, definir sua titularidade e os sujeitos obrigados, além de estabelecer parâmetros organizacionais, procedimentais e restritivos.

Releva destacar que a LGPD, embora forjada fora do contexto europeu, adota como fundamento a autodeterminação informativa – instituto jurídico desenvolvido a partir de uma decisão de 1983 do Tribunal Constitucional alemão – e incorpora diversos institutos do Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia, evidenciando uma simetria normativa relevante, mesmo que o Brasil não esteja formalmente vinculado ao direito daquele continente[18].

Nesse contexto, Ingo Wolfgang Sarlet (2023) ressalta a importância de se compreender a dimensão multinível do direito à proteção de dados pessoais, especialmente no ordenamento jurídico brasileiro, no qual se pode identificar três estratos normativos: as constituições dos Estados americanos, a Convenção Americana de Direitos Humanos (e tratados correlatos), e o sistema universal de proteção dos direitos humanos das Nações Unidas. Para o autor, essa estrutura multinível é característica de um direito constitucional de múltiplos níveis e exige uma abordagem interpretativa sensível à complexidade e à pluralidade das fontes jurídicas envolvidas.

Importa aqui, contudo, refletir sobre o real significado da atribuição do status de direito fundamental à proteção de dados pessoais, bem como sobre os limites e possibilidades de restrição a esse direito no contexto constitucional. A análise crítica dessas questões é essencial para entender o alcance normativo da Emenda Constitucional nº 115 e os desafios que se impõem à sua efetivação no cenário jurídico contemporâneo.

Com base na doutrina de Ronald Dworkin, Sarlet (2023) sustenta que a natureza distintiva dos direitos fundamentais decorre do regime jurídico-constitucional qualificado que os conforma, o qual pode assumir contornos variados conforme as especificidades de cada ordenamento constitucional. Tal regime — composto por garantias institucionais — assegura que os direitos fundamentais se traduzam em posições jurídicas subjetivas, revestidas de eficácia normativa suficiente para serem oponíveis pelo indivíduo ao poder estatal, funcionando, assim, como verdadeiros trunfos frente à vontade da maioria.

---

[18] "O perfil atual da proteção de dados está fortemente ligado aos marcos regulatórios europeus e ao seu desenvolvimento, a ponto de o tema chegar a ser por vezes referido, coloquialmente, como tipicamente europeu." (Doneda, 2023).

A concepção de uma categoria de direitos fundamentais associa-se, em sua origem, à ideia de contenção do arbítrio estatal, tendo como fundamento o Estado de Direito — conquista civilizatória que representa a limitação jurídica do poder político, em contraposição à autoridade ilimitada do Estado Absolutista. Com a incorporação do componente democrático, como ocorre na República Federativa do Brasil, que se constitui como Estado Democrático de Direito, agregam-se os princípios da justiça social e do pluralismo político, os quais atuam como garantidores da eficácia dos direitos fundamentais (art. 1º da CF).

George Marmelstein (2019) ressalta a importância de compreender que denominar um direito como fundamental implica assumir consequências jurídicas relevantes. No ordenamento jurídico brasileiro, isso significa reconhecer: (a) que tais direitos possuem aplicação imediata, sendo, portanto, vinculantes e plenamente exigíveis (art. 5º, § 1º, da CF); (b) que constituem cláusulas pétreas, insuscetíveis de supressão mesmo por emenda constitucional (art. 60, § 4º, da CF); e (c) que detêm uma hierarquia normativa superior, capaz de afastar normas infraconstitucionais ou interpretações que lhes sejam contrárias.

Malgrado o reconhecimento de que uma conceituação suficientemente abrangente dos direitos fundamentais seja tarefa complexa e desafiadora – como já advertia José Afonso da Silva ao afirmar que não é fácil concretizar a riqueza multifária da expressão (Silva, 2006), há caracteres de fundamentalidade[19] formal e material que lhes são distintivos e que permitem delinear sua natureza.

Em primeiro lugar, a sua base axiológica. A categoria dos direitos fundamentais possui como valor intrínseco a dignidade humana, que se traduz não apenas no respeito à vida e à integridade física e moral do indivíduo, mas também na proteção à autonomia da vontade e à garantia do mínimo existencial. Essa primeira característica inicial, portanto, refere-se ao seu conteúdo ético e caracteriza o aspecto moral.

Além disso, há uma segunda e igualmente relevante característica: o reconhecimento das normas pela Constituição de um Estado Democrático de Direito. Nisso consiste o aspecto formal, que lhes confere a supremacia normativa e os eleva à condição de parâmetro de validade das demais normas do ordenamento jurídico.

Todavia, o direito positivo brasileiro prevê a possibilidade de existência de direitos apenas materialmente constitucionais, porquanto permite a abertura a outros direitos fundamentais que, embora não catalogados na Constituição, contém decisões basilares relacionadas à dignidade humana ou à limitação do poder.

[19] Nesse sentido: Marmelstein, 2019; Sarlet, 2004; Alexy, 2008; Canotilho, 1992.

Com base no disposto no art. 5º, § 2º, da Constituição Federal, que estende os direitos e garantias expressamente previstos no texto constitucional àqueles decorrentes do regime e dos princípios por ela adotados — inclusive aos tratados internacionais dos quais a República Federativa do Brasil seja parte —, impõe-se reconhecer que os direitos fundamentais não se restringem àqueles formalmente inseridos na Constituição (fundamentalidade em sentido formal), mas também abrangem os que, embora não expressos, se equiparam pelo conteúdo e pela relevância do bem jurídico protegido (fundamentalidade em sentido material).

Partindo da premissa de que os direitos fundamentais expressam a ordem suprema de valores de coexistência, Luis Aguiar de Luque destaca a dificuldade de delimitar seu objeto e recorda a classificação proposta por Gustavo Zagrebelsky[20], que os agrupa em três grandes categorias, a depender de seu conteúdo: direitos de liberdade negativa (ou direitos de não ser obrigado a...), direitos de liberdade positiva (ou direitos de exercer livremente uma certa atividade) e direitos de prestação (Luque, 1993).

A diversidade dessas categorias evidencia a complexidade conceitual, agravada pela existência de distintas perspectivas históricas, ideológicas, políticas e filosóficas. Tais perspectivas concebem os direitos fundamentais como garantias dos indivíduos e da sociedade frente ao poder estatal, seja por estabelecerem esferas de autonomia protegidas contra interferências, seja por imporem deveres ao Estado, seja ainda por assegurarem a participação política dos cidadãos. Nessa ordem de ideias, a proclamação dos direitos fundamentais se constitui em pedra angular que inspira a convicção da imperiosidade de se prevenirem os abusos no exercício do poder (Branco, 2008)[21].

Cumpre acrescer que os direitos fundamentais não emergiram de forma simultânea nem foram concebidos como um bloco único e estático. Ao contrário, acompanharam — e ainda acompanham — o desenvolvimento da sociedade humana, em um processo histórico evolutivo, o que a doutrina clássica refere por gerações sucessivas, traduzindo uma lógica cumulativa e quantitativa (Bonavides, 2006).

A teoria das três gerações, proposta por Karel Vasak em 1977, organizou os direitos humanos fundamentais em três categorias sequenciais: (1) direitos civis e políticos, (2) direitos econômicos, sociais e culturais, e (3) direitos coletivos ou de solidariedade. No entanto, essa

[20] G. Zagrebelsky. Objeto y alcance de la protección de los derechos fundamentales; el Tribunal Constitucional italiano. *apud* Luque, 1993.

[21] Em sua tese de doutorado, ressalta Paulo Gonet: "Na medida em que ganha força a ideia de que o Poder Público deve ser exercido segundo exigências do postulado do respeito à dignidade da pessoa humana, estabiliza-se a noção de que o Estado, no momento em que legisla ou em que aplica o direito, não pode ser arbitrário" (Branco, 2008).

estrutura tem sido alvo de críticas substanciais, tanto do ponto de vista histórico quanto analítico.

Uma das críticas centrais é a ausência de fundamentação histórica rigorosa. A categorização de Vasak foi construída retrospectivamente, moldando-se a uma narrativa política contemporânea sem considerar adequadamente os contextos históricos e as lutas transnacionais que moldaram os direitos humanos. A tentativa de associar as gerações aos ideais da Revolução Francesa (*Liberté, Égalité, Fraternité*) é apontada como uma reconstrução artificial que ignora a complexidade e diversidade das origens desses direitos.

Além disso, a teoria é criticada por obscurecer a interdependência entre os diferentes tipos de direitos, ao segmentá-los em gerações distintas. Essa divisão sugere uma hierarquia implícita e uma linearidade temporal que não condiz com a realidade dinâmica dos direitos humanos.

Outro ponto problemático é a centralidade eurocêntrica da teoria, que privilegia experiências históricas europeias como paradigmas universais, marginalizando contribuições de outras regiões e culturas, especialmente do Sul Global. Isso resulta em uma narrativa que desconsidera os processos de descolonização e as lutas por direitos em contextos não ocidentais.

A teoria é ainda criticada por desconectar os direitos humanos de suas dimensões políticas e sociais concretas, tratando-os como categorias normativas abstratas, desvinculadas das disputas e transformações históricas que lhes conferem significado (Jensen, 2018).

Apesar das críticas, a teoria das gerações de direitos continua sendo amplamente adotada, inclusive pelo Supremo Tribunal Federal brasileiro como fundamento em suas decisões[22].

No que diz respeito à formulação das leis gerais de proteção de dados, prevalece o entendimento doutrinário de que, em escala global, esse processo também passou por diferentes gerações normativas (Bioni; Oliveira; Monteiro, 2020), a despeito de apresentar nuances distintas da classificação dos direitos fundamentais proposta por Karel Vasak. Nesse sentido, Danilo Doneda (2011) destaca a tipologia evolutiva elaborada por Viktor Mayer-Schönberger, que identifica quatro gerações de legislações sobre proteção de dados. A primeira geração é caracterizada por um enfoque técnico e restritivo, voltado à regulação do uso de dados por órgãos estatais, com foco em normas de caráter tecnocrático. A segunda amplia o escopo para o setor privado, reconhecendo o papel central das empresas na coleta e uso de dados. A terceira geração consolida o protagonismo do titular, embora enfrente críticas quanto à efetividade do

[22] Nesse sentido: Brasil, 2018.

consentimento diante da assimetria informacional. Por fim, a quarta geração busca superar essas limitações, relativizando a centralidade do consentimento e incorporando abordagens estruturais e coletivas, com ênfase na autodeterminação informativa e na atuação de autoridades independentes.

Nesse contexto, a proteção de dados pessoais tem sido progressivamente reconhecida como um direito fundamental associado à quarta geração das legislações sobre proteção de dados, conforme a tipologia proposta por Mayer-Schönberger, cuja emergência está diretamente vinculada às transformações tecnológicas e à crescente complexidade das relações informacionais na sociedade contemporânea (Doneda, 2011).

Enquanto a tipologia evolutiva de Viktor Mayer-Schönberger organiza a proteção de dados pessoais em quatro gerações, refletindo a crescente complexidade e abrangência do direito — que passou de um enfoque técnico e individual para uma proteção coletiva e estrutural, acompanhando a evolução histórica, tecnológica e social da proteção jurídica dos dados pessoais — Lorenzo Dalla Corte (2020) entende que, desde 2011, iniciou-se uma quinta era, na qual o direito à proteção de dados se distancia ainda mais da privacidade, ampliando sua autonomia conceitual em resposta ao progresso técnico e à importância crescente do tratamento de dados pessoais ao longo do tempo.

Essa evolução normativa reflete não apenas uma resposta jurídica aos desafios da era digital, mas também uma reconfiguração do papel do indivíduo frente ao poder informacional exercido por entes públicos e privados.

Todavia, em substituição à teoria geracional, há na doutrina posicionamentos que explicam a evolução dos direitos fundamentais como dimensões, no sentido de que esses direitos, inaugurados com os clássicos direitos de matriz liberal-burguesa, encontram-se em constante transformação. Tal processo culmina com a incorporação, nos catálogos constitucionais e no Direito Internacional, de múltiplas e diferenciadas posições jurídicas, cujo conteúdo é tão dinâmico quanto as transformações sociais, políticas, culturais e econômicas (Sarlet, 2007).

A Constituição da República Federativa Brasileira de 1988 acolheu esse processo evolutivo, refletindo-o em sua diversidade semântica ao empregar expressões como: a) Direitos Humanos (art. 4º, II), b) Direitos e Garantias Fundamentais (epígrafe do Título II, e art. 5º, § 1º), c) Direitos e deveres individuais e coletivos (epígrafe do respectivo capítulo), d) Liberdades

constitucionais (art. 5º, inc. LXXI) e d) Direitos e garantias individuais (art. 60, § 4º, inc. IV) (Sarlet, 2017)[23].

Não obstante o reconhecimento da lógica de cumulatividade entre as chamadas gerações de direitos fundamentais (Mendes; Branco, 2024; Sarlet, 2007), há quem recuse a ideia de gerações de direitos por entender não haver substituição de uma geração por outra, mas complementação entre dimensões objetiva e subjetiva (Souza, 2011). Outros autores, ainda, defendem o abandono da noção de gerações ou dimensões, por considerá-la fragmentária e hierarquizante (Mazzuoli, 2017).

Registra-se, enfim, que reiteradamente surgem diversas ampliações na doutrina, tais como as propostas para classificar em direitos de quarta dimensão aqueles relacionados à globalização, que compreendem o direito à democracia, à informação e ao pluralismo político (Bonavides, 2006) e à normatização do patrimônio genético (Bobbio, 2004); ou a defesa da elevação da paz ao grau de direito fundamental de quinta geração ou dimensão, feita por Paulo Bonavides em conferência proferida no ano de 2006 por ensejo do 9º. Congresso Ibero-Americano de Direito Constitucional, em Curitiba (Bonavides, 2008).

Não é, contudo, o foco do presente estudo aprofundar a discussão classificatória. Interessa, neste ponto, destacar que os direitos fundamentais são valores indivisíveis e interdependentes, exercendo uma função jurídico-objetiva ao limitarem a margem de atuação do Estado, impedindo-o de fazer uso arbitrário de suas competências legislativas, administrativas e jurisdicionais (Pieroth, Schilink, 2012).

Com efeito, desde suas origens históricas e finalidades, evidencia-se uma dimensão subjetiva dos direitos fundamentais, que permite aos titulares exigir comportamentos — positivos ou negativos — do Estado ou de terceiros. Essa dimensão, embora proeminente, não se dissocia da dimensão objetiva, com a qual mantém relação de complementaridade e remissão recíproca (Hesse *apud* Mendes; Branco, 2024).

Em que pese a relevância da dimensão subjetiva, voltada à salvaguarda dos direitos individuais diante da atuação estatal, não se pode desconsiderar que os direitos fundamentais também exercem uma função estruturante no ordenamento jurídico, irradiando efeitos sobre a interpretação e aplicação das normas, inclusive nas relações entre particulares. Essa dimensão objetiva projeta-se sobre os deveres de proteção do Estado, que não apenas deve se abster de

[23] Diante da abrangência conceitual do tema, impõe-se a necessária distinção: a expressão "direitos fundamentais" refere-se aos direitos inerentes à pessoa humana que foram reconhecidos e incorporados ao ordenamento jurídico constitucional de um Estado específico. Por sua vez, o termo "direitos humanos" está vinculado ao âmbito do direito internacional, sendo consagrado em tratados e convenções que transcendem a soberania estatal e independem de positivação em constituições nacionais. Nesse sentido: Sarlet, 2004.

violar direitos fundamentais (dimensão negativa), mas também tem o dever de promovê-los ativamente, inclusive mediante a regulação de relações privadas, a fim de prevenir violações.

O reconhecimento dessa dupla dimensão implica compreender que os direitos fundamentais transcendem a proteção de direitos subjetivos individuais, alcançando a condição de normas que refletem os valores estruturantes da sociedade constitucionalmente organizada. Nesse sentido, constituem a base do ordenamento jurídico de um Estado Democrático de Direito (Mendes, Branco, 2024).

O aspecto específico que interessa à presente investigação diz respeito ao papel que os direitos fundamentais desempenham na ordem constitucional, servindo como instrumento de limitação do poder. Tal limitação designa as restrições impostas não somente ao legislador quando este estabelece fronteiras ao exercício dos direitos fundamentais (Pieroth, Schilink, 2012), mas também ao aplicador do direito.

Assim, adota-se neste trabalho a concepção de que o direito à proteção de dados pessoais, por sua condição de direito fundamental, configura-se como uma estrutura normativa indispensável, cuja função é orientar e limitar o exercício do poder estatal. Tal compreensão decorre do fato de que esse direito expressa um ideal político e social alicerçado na centralidade da dignidade da pessoa humana, constituindo-se em pressuposto essencial para a promoção de uma vida social mais equânime.

2.2 DA PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL DE NATUREZA PROCESSUAL NO ORDENAMENTO JURÍDICO BRASILEIRO

> A inclusão de um direito fundamental à proteção de dados pessoais na Constituição Federal está em linha com as novas tendências do constitucionalismo digital e reflete uma importante inovação no ordenamento jurídico brasileiro (Mendes, 2021).

No contexto jurídico brasileiro contemporâneo, observa-se uma distinção formal entre o direito à privacidade e o direito à proteção de dados pessoais. Em sede constitucional, enquanto o direito à proteção de dados pessoais encontra respaldo no artigo 5º, inciso LXXIX, a fundamentação do direito à privacidade está consagrada no artigo 5º, inciso X, da Constituição Federal de 1988. Embora este último mencione expressamente os termos “intimidade” e “vida privada”, estes são frequentemente interpretados como elementos constitutivos de um conceito mais amplo de privacidade[24].

[24] Nesse sentido: STF ADI 6387; RE 21501.

Ambos são direitos fundamentais que, embora compartilhem raízes comuns e estejam logicamente entrelaçados, apresentam contornos conceituais e normativos próprios. A proteção de dados pessoais, ainda que derivada do direito à privacidade, consolidou-se como um instituto autônomo, cuja normatividade e funcionalidade foram forjadas pela crescente necessidade de os indivíduos gerenciarem suas informações em um cenário marcado por intensas transformações tecnológicas e sociais.

O Brasil seguiu o paradigma europeu de direitos fundamentais em múltiplos níveis, no qual o direito à proteção de dados pessoais — consagrado no artigo 8º da Carta dos Direitos Fundamentais da União Europeia — é formalmente distinto do direito à privacidade, previsto em seu artigo 7º (Corte, 2020). Essa separação normativa reflete uma compreensão mais refinada das especificidades e finalidades de cada direito, permitindo uma tutela mais eficaz diante dos desafios impostos pela sociedade da informação.

Na perspectiva do direito europeu, Corte (2020) invoca a doutrina de Hielke Hijmans, segundo a qual os direitos à privacidade e à proteção de dados integram um arcabouço normativo comum: a privacidade configura-se como um direito substantivo — o "jogo" — ao passo que a proteção de dados assume a função de direito processual — suas "regras". Ambos, portanto, convergem na salvaguarda de um mesmo núcleo de direitos e liberdades fundamentais. O autor sustenta, contudo, que a proteção de dados vem progressivamente se desvinculando da privacidade, delineando-se como um regime jurídico autônomo, *sui generis*, ainda que mantenha com ela uma conexão estrutural.

Sob o prisma normativo brasileiro, enquanto o conceito de dado pessoal abrange qualquer informação relacionada a pessoa natural identificada ou identificável, nos termos do artigo 5º, inciso I, da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), a dimensão do direito à privacidade — especificamente no que tange ao tratamento de dados pessoais — possui um escopo mais restrito. Isso porque a privacidade de dados pressupõe que as informações tratadas sejam, por sua natureza, privadas ou sensíveis. Em síntese, o direito à privacidade não se projeta necessariamente sobre todas as formas de tratamento de dados pessoais, ao contrário do direito à proteção de dados, cujo alcance é mais amplo e normativamente autônomo.

A dicotomia entre privacidade e proteção de dados, no Brasil, também se revela em uma transição paradigmática. A proteção de dados, inicialmente concebida como um desdobramento da privacidade, evoluiu para um instituto jurídico com escopo e finalidades que transcendem a esfera individual.

Trata-se de um direito de natureza processual e auxiliar, que opera como mecanismo de controle sobre o tratamento de informações pessoais, incorporando uma dimensão coletiva e estrutural. Essa evolução reflete a crescente complexidade das relações informacionais e a necessidade de salvaguardas jurídicas que respondam adequadamente aos desafios impostos pela economia de dados.

Efetivamente, no ordenamento jurídico brasileiro, a proteção de dados pessoais configura-se como um direito fundamental de natureza processual e auxiliar, cuja função transcende a mera salvaguarda individual da privacidade. Trata-se de uma estrutura procedimental de controle e regulação do tratamento de informações pessoais, que incorpora uma dimensão coletiva, refletindo a complexidade das relações informacionais na sociedade contemporânea.

Essa compreensão decorre da própria arquitetura normativa da Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD), que não somente assegura direitos subjetivos aos titulares dos dados, mas também institui instrumentos de tutela coletiva, reconhecendo que as violações à proteção de dados podem gerar danos de natureza difusa, coletiva ou individual homogênea. A LGPD estabelece obrigações claras e vinculantes para os agentes de tratamento, sejam eles públicos ou privados, e prevê mecanismos administrativos e judiciais específicos para fiscalização, responsabilização e reparação de danos, reforçando o caráter processual e instrumental do direito à proteção de dados.

A dimensão coletiva do direito à proteção de dados pessoais é ainda evidenciada pela possibilidade de ações coletivas, pela exigência de estruturas de governança e *compliance*, e pela necessidade de transparência e *accountability* como condições para a efetividade da proteção de dados em escala institucional e social.

Embora interligados, os termos governança, transparência, *compliance* e *accountability* possuem conotações distintas e complementares no contexto da administração pública. Segundo o Banco Mundial (1992), governança refere-se à forma pela qual o poder é exercido na administração dos recursos sociais e econômicos de um país visando o desenvolvimento. Trata-se, portanto, de um conceito abrangente que envolve estruturas, processos e práticas voltadas à condução ética, eficiente e responsável das instituições.

A transparência constitui um dos pilares da boa governança, sendo o princípio que impõe à Administração o dever de disponibilizar informações claras, acessíveis e compreensíveis sobre suas ações e decisões aos públicos interessados (*stakeholders*). Ela viabiliza o controle social, fortalece a confiança institucional e permite a fiscalização das atividades públicas e privadas (IBGC, 2023).

O *compliance*, por sua vez, refere-se à adoção de sistemas de conformidade que asseguram o cumprimento das normas legais, regulamentos e políticas internas aplicáveis. Trata-se de uma ferramenta essencial para a prevenção de irregularidades, fraudes e atos de corrupção, contribuindo para a integridade institucional e a governança ética (Blok, 2014).

Já a *accountability* diz respeito ao dever de prestar contas e à obrigação de responder pelos atos e resultados da gestão. Envolve não somente a transparência, mas também a justificação das decisões e a responsabilização por eventuais falhas ou desvios, sendo elemento central na consolidação de uma cultura de integridade e responsabilidade pública (Tribunal de Contas da União, 2020).

A partir de uma leitura sistêmica desses institutos, infere-se que a proteção de dados pessoais não se limita a um direito individual isolado, mas se configura como um direito fundamental funcionalizado, voltado à regulação de práticas informacionais em benefício da coletividade e da preservação da dignidade humana na era digital.

Consoante Danilo Doneda (2019), a proteção de dados pessoais transcende a mera salvaguarda da intimidade individual, configurando-se como um mecanismo normativo de regulação das dinâmicas informacionais contemporâneas. Trata-se de um direito fundamental de nova geração, cuja principal função é assegurar a autodeterminação informativa do sujeito diante do crescente poder de coleta, processamento e uso de dados por agentes públicos e privados. Nesse sentido, a proteção de dados adquire centralidade não somente jurídica, mas também social, econômica e política, refletindo a complexidade das estruturas de poder na sociedade digital.

A distinção entre os dois direitos também é enfatizada por Stefano Rodotà, citado por Doneda (2019), ao afirmar que a privacidade diz respeito à esfera privada do indivíduo, enquanto a proteção de dados se refere ao controle sobre o fluxo e o uso das informações pessoais em ambientes diversos, inclusive públicos. Essa perspectiva é reforçada pela Teoria da Privacidade Contextual, desenvolvida por Helen Nissenbaum (2009), segundo a qual a privacidade deve ser compreendida a partir das normas de fluxo informacional adequadas a cada contexto social.

2.3 DAS RESTRIÇÕES A PARTIR DA TEORIA DOS LIMITES DOS LIMITES

> O limite de limites está contido nos próprios direitos fundamentais (Pieroth; Schilink, 2012).

No tópico "2.1 Dos direitos fundamentais" assentou-se que, no âmbito do Estado Democrático de Direito, os direitos fundamentais ocupam posição de supremacia na estrutura normativa das Constituições modernas e funcionam como instrumentos de contenção e racionalização do poder estatal. Contudo, não se pretende concebê-los como prerrogativas absolutas, imunes a qualquer forma de limitação ou ponderação.

O ordenamento jurídico brasileiro, em consonância com o paradigma do constitucionalismo democrático, não reconhece a existência de direitos fundamentais de natureza absoluta[25]. A Constituição da República admite, em situações excepcionais e fundamentadas em relevantes interesses públicos ou na necessidade de harmonização entre as diversas liberdades, a possibilidade de imposição de restrições a prerrogativas individuais ou coletivas.

Nesse sentido, o sistema constitucional vigente estrutura-se de modo a impedir que qualquer direito se sobreponha de forma irrestrita a outros igualmente protegidos. A convivência harmônica entre os direitos fundamentais exige, portanto, mecanismos de compatibilização, conduzindo à consolidação de um entendimento doutrinário majoritário: os direitos fundamentais não são absolutos[26] e, por conseguinte, não se admite o exercício ilimitado das prerrogativas que deles decorrem (Barroso, 2004).

A concepção de relatividade dos direitos fundamentais reconhece que estes são passíveis de intervenções legítimas — sejam elas restritivas ou limitativas — diante de outros valores constitucionais igualmente relevantes. A restrição a um direito fundamental configura, em essência, uma delimitação de sua esfera de proteção ou uma modificação de seus pressupostos fáticos. Definir limites ao exercício de determinado direito decorre da necessidade de compatibilizá-lo com outros bens jurídicos constitucionalmente tutelados, bem como com as circunstâncias concretas reconhecidas pelo ordenamento jurídico (Aragão, 2011).

A restrição implica, portanto, uma intervenção externa e pontual no exercício de um direito fundamental, geralmente justificada pela necessidade de proteger outro direito ou

---

[25] Inobstante, Paulo Gonet ressalta a ponderação de Norberto Bobbio, para quem seria absoluto o direito de não ser escravizado e acresce a previsão do direito a não ser submetido a penas cruéis, conforme prevê o art. 5º, XLVII, e, da CF (Mendes; Branco, 2024).

[26] Nesse sentido: (Zouein, 2023).

interesse público relevante. Tais restrições devem observar os princípios da legalidade, da proporcionalidade e da preservação do núcleo essencial do direito afetado (Sarlet, 2004).

Essas restrições podem ser sistematizadas em três categorias: constitucionais, quando expressamente previstas no texto constitucional; legais, quando estabelecidas por normas infraconstitucionais autorizadas pela Constituição; e implícitas, que, embora não expressamente previstas, decorrem da necessidade de harmonização entre direitos fundamentais ou entre estes e outros valores constitucionais, como a segurança pública, a saúde coletiva e a ordem pública (Farias, 2000).

Trata-se de decorrência da compreensão de que os direitos fundamentais, embora dotados de supremacia formal e material, não podem ser instrumentalizados para legitimar práticas ilícitas, tampouco podem ser utilizados para eximir indivíduos de responsabilidades civis. Sua aplicação não autoriza a supressão de outros direitos igualmente assegurados pela ordem constitucional, nem a negação de prerrogativas de terceiros. Ao contrário, devem ser interpretados e aplicados de forma harmônica e integradora, respeitando o equilíbrio entre os diversos bens jurídicos tutelados.

A realização plena do Estado Democrático de Direito pressupõe um ambiente plural, marcado pela convivência de distintas culturas, ideologias, crenças e opiniões. A premissa de que não existem direitos fundamentais absolutos, tampouco hierarquia entre normas constitucionais, não elimina as controvérsias que emergem da diversidade de valores presentes na sociedade. Ao contrário, essa pluralidade frequentemente dá origem a conflitos resultantes em colisões entre direitos fundamentais — como nos casos em que se contrapõem o preceito da liberdade de expressão e a vedação à propagação de discursos de ódio ou de manifestações contrárias à ordem constitucional e ao próprio Estado de Direito[27].

Credita-se, ainda, a ampliação das possibilidades de atritos entre direitos fundamentais à própria extensão da Constituição, à natureza aberta de sua linguagem e ao seu caráter compromissório, que incorpora normas inspiradas em ideologias e visões de mundo frequentemente divergentes (Sarmento; Souza Neto, 2014).

A colisão entre direitos fundamentais configura um fenômeno jurídico intrínseco à estrutura principiológica que os fundamenta no ordenamento constitucional. Ao contrário das regras, que operam sob uma lógica binária, os princípios jurídicos — forma predominante de positivação dos direitos fundamentais — impõem mandamentos de otimização, cuja concretização depende das múltiplas possibilidades fáticas e jurídicas do caso concreto.

[27] Nesse sentido: AP 1044 DF (Supremo Tribunal Federal, 2024).

Princípios em conflito não se anulam mutuamente; ao contrário, exigem um processo de ponderação que considere o peso específico de cada um, diante das circunstâncias particulares, a fim de alcançar a máxima realização possível de ambos (Alexy, 2008).

As soluções para essas colisões são complexas e exigem uma ponderação que, respeitando o equilíbrio entre os diversos bens jurídicos tutelados, pode culminar na imposição de medidas restritivas. Nesse contexto, destaca-se o princípio da proporcionalidade como instrumento normativo que confere racionalidade e legitimidade à ponderação.

Princípio estruturante do controle de restrições a direitos fundamentais, o princípio da proporcionalidade atua como critério de legitimidade das medidas restritivas, sendo composto por três dimensões analíticas: (a) adequação, que exige que a medida adotada seja idônea para alcançar um fim constitucionalmente legítimo; (b) necessidade, que impõe a escolha da alternativa menos gravosa entre as possíveis; e (c) proporcionalidade em sentido estrito, que demanda um juízo de equilíbrio entre os custos da restrição e os benefícios decorrentes da proteção do bem jurídico contraposto. Essa última etapa, também denominada controle de sintonia fina (*Stimmigkeitskontrolle*), visa aferir a justeza da solução adotada, evitando excessos ou insuficiências na proteção dos direitos fundamentais (Mendes; Branco, 2024).

Vê-se, portanto, que a proteção dos direitos fundamentais não se realiza isoladamente, mas sim dentro de um sistema de garantias interdependentes, no qual a efetividade de um direito pressupõe o respeito aos limites impostos pelos demais. Essa compreensão é essencial para a consolidação de uma ordem jurídica justa, plural e democrática.

Dessa forma, percebe-se que o conceito de restrição aos direitos fundamentais não é problemático, ao contrário, revela-se como uma decorrência natural da convivência entre direitos em tensão. O verdadeiro desafio reside na definição do conteúdo e da extensão admissível dessas restrições (Alexy, 2008). A relativização dos direitos fundamentais, longe de fragilizá-los, é justamente o que assegura sua efetiva proteção em uma sociedade plural e democrática.

Nesse contexto, duas correntes teóricas, ambas inspiradas nos estudos acerca do abuso de direito, são apresentadas como capazes de resolver conflitos e permitir convivência entre os direitos fundamentais potencialmente colidentes entre si: a teoria interna (também referida por teoria dos limites imanentes) e a teoria externa dos limites[28].

A primeira, ainda chamada de concepção estrita, sustenta que os direitos fundamentais contêm limites imanentes, definidos no momento de sua positivação normativa. Assim,

[28] Nesse sentido: Pereira, 2006; Sarmento; Souza Neto, 2014; Mendes, Branco, 2024.

qualquer restrição adicional não criaria novos limites, mas somente concretizaria as balizas previamente estabelecidas no conteúdo do direito. Por outro lado, a teoria externa entende que os limites são extrínsecos ao conteúdo normativo e podem ser legitimamente impostos para proteger outros direitos fundamentais ou interesses públicos relevantes (Souza, 2011).

A teoria dos limites dos limites, ao estabelecer que nenhuma restrição pode atingir o núcleo essencial dos direitos fundamentais, atua como um mecanismo de contenção na lógica da teoria externa dos limites. Esta última admite que os direitos fundamentais podem ser restringidos por fatores extrínsecos, tais como a proteção de outros direitos ou a salvaguarda de interesses públicos relevantes, conferindo flexibilidade à sua aplicação e permitindo a ponderação em contextos de colisão.

Contudo, é precisamente nesse espaço de abertura que a teoria dos limites dos limites se impõe como cláusula de salvaguarda, impedindo que a ponderação se converta em erosão. Ela não nega a validade da teoria externa, mas a qualifica, impondo-lhe um limite estrutural: o respeito intransigente ao núcleo essencial dos direitos. Essa articulação revela uma tensão produtiva entre flexibilidade e rigidez, entre ponderação e proteção, que constitui o cerne da hermenêutica constitucional contemporânea.

Tópico abordado na conferência proferida por Karl August Bettermann, o artigo 19, § 2º da Lei Fundamental da República Federal da Alemanha (*Das Grundgesetz für die Bundesrepublik Deutschland*), de 23 de maio de 1949, estabelece que, mesmo nas hipóteses em que um direito fundamental possa ser restringido por ou em virtude de uma lei, não poderá ser violado o seu conteúdo essencial. O direito positivo germânico, portanto, estabelece expressamente as barreiras que devem ser observadas pelos poderes Legislativo e Executivo quando pretendem restringir o exercício de direitos fundamentais ou intervir em posições jurídicas protegidas.

Com base naquela constituição, Robert Alexy, em sua *Teoria dos Direitos Fundamentais*, afirma que a restringibilidade dos direitos fundamentais somente é admissível quando, no caso concreto, se atribui um peso maior ao princípio colidente (Alexy, 2008) e aduz que o referido art. 19, § 2. º da Lei Básica alemã impõe um limite adicional à restrição, ao proibir que os direitos fundamentais sejam afetados em seu conteúdo essencial.

Embora a Constituição da República Federativa do Brasil de 1988 não contenha disposição expressa sobre a proteção do núcleo essencial dos direitos fundamentais, sua arquitetura normativa revela afinidade substancial com a teoria dos limites dos limites. A vedação de emendas constitucionais tendentes a abolir os direitos e garantias individuais (art. 60, §4º, IV) funciona como um limite material absoluto, inclusive ao poder de reforma,

sinalizando que certos conteúdos são juridicamente indisponíveis, mesmo diante da vontade do legislador constituinte derivado.

Essa cláusula pétrea, ao preservar a essência dos direitos fundamentais, reforça a existência de um espaço normativo intangível, que não pode ser suprimido nem relativizado por razões de conveniência política ou funcionalidade estatal. Assim, ainda que o texto constitucional não mencione expressamente o "núcleo essencial", a lógica garantista adotada pelo constituinte de 1988 consagra, de forma implícita, porém inequívoca, a ideia de que há limites para os próprios limites, assegurando a integridade mínima dos direitos frente a qualquer tentativa de esvaziamento normativo.

Esse ponto central da dogmática dos direitos fundamentais foi analisado no âmbito do Supremo Tribunal Federal por ensejo do julgamento do Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.407/DF[29]. Na ocasião, o relator, ministro Gilmar Mendes, reiterou sua defesa da tese de que a definição do âmbito de proteção constitui pressuposto primário para o desenvolvimento de qualquer direito fundamental.

O relator ali prosseguiu a afirmar que os chamados limites imanentes, ou "limites dos limites", balizam a atuação do legislador ao restringir direitos individuais. Aduziu que decorrem diretamente da Constituição e dizem respeito tanto à necessidade de proteção do núcleo essencial do direito fundamental, quanto à observância de critérios como clareza, determinação, generalidade e proporcionalidade das restrições impostas.

A compreensão dessa noção de essencialidade aproxima-se, metaforicamente, das concepções do atomismo de Leucipo e Demócrito, para os quais o átomo seria uma partícula indivisível e imutável[30]. De modo análogo, o núcleo essencial de um direito fundamental representa uma dimensão inatingível, sobre a qual não se admitem modificações ou restrições de qualquer natureza (Santiago, 2011).

Complementarmente, o princípio da proporcionalidade funciona como instrumento de controle da legitimidade das restrições. A Lei Geral de Proteção de Dados Pessoais (LGPD), por exemplo, incorpora esse princípio ao exigir que o tratamento de dados pessoais seja adequado, necessário e proporcional em sentido estrito. Isso significa que o Poder Público deve demonstrar que a coleta ou o compartilhamento de dados atende a uma finalidade legítima,

---

[29] Este Acórdão teve por objeto uma discussão sobre cobrança de tarifa de cheque especial. Apesar de uma aparente simplicidade da matéria em debate, seu exame revela-se extremamente valioso para os estudiosos do direito constitucional por dois temas ali tratados: a) a fungibilidade entre ações diretas (Arguição de Descumprimento de Preceito Fundamental conhecida como Ação Direta de Inconstitucionalidade); e b) a análise sobre âmbito de proteção de um direito fundamental.

[30] Embora o significado original do termo átomo correspondesse a uma partícula indivisível, no contexto científico contemporâneo o átomo é constituído por várias partículas subatômicas (Encyclopaedia Britannica, [*s.d.*]).

constitui o meio menos invasivo possível e não impõe sacrifícios desproporcionais à privacidade do titular (Duque; Nascimento, 2018).

A relação entre esses dois paradigmas é de complementaridade funcional. A teoria dos limites dos limites atua como uma barreira normativa de contenção, impedindo que o legislador ou o aplicador do direito esvaziem o conteúdo essencial do direito à proteção de dados. Por sua vez, o princípio da proporcionalidade atua como instrumento analítico, permitindo avaliar, caso a caso, se uma restrição específica é justificável e equilibrada. Juntos, esses mecanismos asseguram que o tratamento de dados pelo Estado seja não apenas legal, mas também legítimo sob a ótica constitucional.

Nesse contexto, insere-se também o debate em torno das teorias absoluta e relativa sobre o núcleo essencial dos direitos fundamentais, que contribuem para a delimitação dos contornos da atuação estatal.

Com base na doutrina de Bodo Pieroth e Bernhard Schlink (2012), depreende-se que, sob a ótica da teoria absoluta (*Absolute Theorie*), existe um núcleo substancial autônomo (*Substantieller Wesenskern*) dos direitos fundamentais que se revela inviolável e imune à intervenção estatal. Em contraposição, a teoria relativa (*Relative Theorie*) concebe o núcleo essencial como uma construção casuística, a ser delineada conforme as particularidades de cada situação concreta, mediante a aplicação do princípio da proporcionalidade como critério de aferição.

A teoria absoluta sustenta que esse núcleo é intangível, não podendo ser restringido sob nenhuma hipótese, nem mesmo diante de conflitos com outros direitos ou interesses públicos. Já a teoria relativa admite que o núcleo essencial pode ser flexibilizado, desde que a restrição seja proporcional, necessária e justificada. Essa distinção é crucial para compreender os limites da atuação estatal: enquanto a teoria absoluta impõe uma barreira rígida, a teoria relativa permite uma ponderação mais dinâmica, desde que submetida a critérios rigorosos de controle constitucional.

A relação entre os paradigmas — teoria externa, teoria dos limites dos limites, proporcionalidade e as teorias absoluta e relativa — revela uma arquitetura normativa complexa e interdependente. A teoria dos limites dos limites funciona como uma barreira normativa de contenção, impedindo que o conteúdo essencial do direito seja violado, mesmo sob a lógica da teoria externa. Já a proporcionalidade atua como filtro analítico, permitindo avaliar, caso a caso, se uma restrição específica é justificável e equilibrada.

A teoria relativa, por sua vez, encontra respaldo nesse modelo, ao passo que a teoria absoluta impõe um limite intransponível à ponderação. Essa articulação revela uma tensão

produtiva entre flexibilidade e rigidez, entre ponderação e proteção, que constitui o cerne da hermenêutica constitucional contemporânea.

Nesse contexto, a atuação estatal deve ser orientada por critérios de legalidade, finalidade, minimização e responsabilidade. A exigência de relatórios de impacto à proteção de dados, prevista na Lei Geral de Proteção de Dados Pessoais (LGPD), é exemplo concreto da aplicação desses princípios, ao exigir uma avaliação prévia dos riscos e da proporcionalidade das medidas adotadas.

Em síntese, o tratamento de dados pessoais pelo Poder Público exige a conjugação de quatro vetores constitucionais: a distinção entre limites internos e externos aos direitos fundamentais, a contenção do poder estatal por meio da preservação do núcleo essencial dos direitos (limites dos limites), a racionalização das restrições por meio da proporcionalidade e a definição do grau de intangibilidade do núcleo essencial conforme as teorias absoluta ou relativa. Essa estrutura assegura que o avanço tecnológico e a eficiência administrativa não se sobreponham às garantias fundamentais do cidadão.

2.3.1 O direito à proteção de dados pessoais como cláusula pétrea

> No meio do caminho tinha uma pedra (Andrade, 1979).

A análise atenta dos processos históricos revela que, com frequência, momentos de crise aguda funcionam como catalisadores para o fortalecimento de mecanismos de proteção institucional. Essa dinâmica manifesta-se em diversas esferas da vida social, como se observa, por exemplo, no reforço das políticas de segurança pública após episódios de violência extrema ou atentados de grande repercussão. Tais respostas, embora reativas, são também preventivas e dotadas de valor normativo, ao visarem impedir que as gerações futuras sejam submetidas às mesmas vulnerabilidades enfrentadas pelas anteriores. É nesse contexto que se insere a gênese das chamadas cláusulas pétreas nas constituições modernas — dispositivos que incorporam conquistas civilizatórias inegociáveis e que, por sua natureza, exercem uma força normativa absoluta, inibindo qualquer tentativa legislativa, explícita ou implícita, de retrocesso.

Outra justificativa relevante para a previsão de cláusulas pétreas nas constituições — que, de certo modo, complementa a função de proteção intergeracional — reside na necessidade de conter eventuais investidas do Poder Executivo sobre as competências dos demais Poderes. Essa concepção confere destaque ao papel das cláusulas de imutabilidade como barreiras institucionais à concentração de poder.

Um exemplo paradigmático dessa lógica encontra-se na Constituição dos Estados Unidos, promulgada em 1787. À época, as treze colônias recém-independentes da Inglaterra buscavam proteger-se tanto de uma possível reconquista britânica quanto de conflitos internos que culminassem em guerra civil. Nesse contexto de autodefesa federativa, instituiu-se a cláusula que veda a alteração da representação paritária dos Estados no Senado Federal, para preservar o equilíbrio entre as unidades federadas.

Embora o exemplo norte-americano tenha relevância histórica inegável, foi no cenário pós-Segunda Guerra Mundial que o instituto da limitação material ao poder de reforma constitucional ganhou maior densidade normativa e simbólica. A Lei Fundamental de 1949 da República Federal da Alemanha (*Grundgesetz für die Bundesrepublik Deutschland*), elaborada após o colapso da República de Weimar e a ascensão do regime nazista, incorporou a chamada cláusula de eternidade (*Ewigkeitsklausel*), que foi concebida como um mecanismo de defesa constitucional, destinado a impedir a repetição dos eventos autoritários que marcaram o passado recente alemão.

A preocupação em resguardar a integridade das normas oriundas do poder constituinte derivado reformador, prevenindo desvios de finalidade e abusos de poder, encontra expressão contundente na Constituição da República Federativa do Brasil de 1988. No contexto de reconstrução democrática e reafirmação do Estado de Direito, após um prolongado período de regime autoritário, o constituinte originário consagrou, no artigo 60, § 4º, o núcleo intangível do texto constitucional, como salvaguarda dos valores fundamentais da ordem jurídica.

Cumpre salientar que a Constituição de 1988 não foi pioneira na introdução do instituto das cláusulas pétreas no ordenamento jurídico brasileiro. As constituições republicanas anteriores já continham, em maior ou menor grau, dispositivos que configuravam um núcleo normativo insuscetível de supressão. Contudo, dois aspectos distintivos merecem especial atenção: primeiramente, a peculiaridade de a atual Constituição não vedar a possibilidade de alteração da forma republicana de governo — ao contrário, previu expressamente a realização de um plebiscito em 1993, conferindo ao povo a prerrogativa de optar entre a Monarquia e a República. Em segundo lugar, destaca-se o ineditismo do texto constitucional de 1988 ao estabelecer, de forma explícita, a proteção dos direitos e garantias individuais contra eventuais tentativas de abolição ou esvaziamento[31].

[31] "A eficácia das regras jurídicas produzidas pelo poder constituinte (redundantemente chamado de "originário") não está sujeita a nenhuma limitação normativa, seja de ordem material, seja formal, porque provém do exercício de um poder de fato ou suprapositivo. Já as normas produzidas pelo poder reformador, essas têm sua validez e eficácia condicionadas à legitimação que recebam da ordem constitucional. Daí a necessária obediência das emendas constitucionais às chamadas cláusulas pétreas". (ADI 2.356).

A cláusula pétrea, ao proteger o núcleo essencial dos direitos fundamentais contra supressões ou esvaziamentos, não obsta o legislador reformador de ampliar o catálogo dessas garantias. Contudo, a incorporação de novos direitos não os torna, automaticamente, imunes à reforma constitucional. Prevalece na doutrina constitucional brasileira o entendimento de que somente o poder constituinte originário — dotado de autoridade superior ao poder de emenda — possui legitimidade para instituir cláusulas pétreas. Assim, os direitos fundamentais criados por emenda não gozam da mesma intangibilidade conferida àqueles consagrados originalmente pela Constituição de 1988[32].

Em 10 de fevereiro de 2022, com a promulgação da Emenda Constitucional nº 115, o direito à proteção de dados pessoais foi alçado à condição de direito fundamental, integrando o rol do artigo 5º, inciso LXXIX, da Constituição da República. Tal avanço normativo representou não somente o reconhecimento da centralidade da privacidade na era da informação, mas também um impulso decisivo à consolidação de uma cultura de proteção de dados no Brasil. A imprensa, ao noticiar a medida, ressaltou que a segurança das informações pessoais dos cidadãos brasileiros fora incorporada ao texto constitucional como uma cláusula pétrea, ou seja, insuscetível de supressão por emenda constitucional (Rádio e TV Justiça, 2022).

Em princípio, o direito fundamental à proteção de dados pessoais não foi contemplado pela Constituição originária de 1988, razão pela qual não poderia, à primeira vista, ser enquadrado como cláusula pétrea. Isso porque a introdução de um novo direito fundamental por meio de emenda constitucional não impede, em tese, sua posterior revogação por outra emenda, uma vez que não integra o núcleo intangível originalmente delimitado pelo poder constituinte originário (Mendes; Branco, 2024).

No entanto, o direito à proteção de dados pessoais apresenta uma peculiaridade relevante: mesmo antes da promulgação da Emenda Constitucional nº 115/2022, o Supremo Tribunal Federal já havia reconhecido sua natureza de direito fundamental. Em maio de 2020, no julgamento conjunto das Ações Diretas de Inconstitucionalidade nºs 6387, 6388, 6389, 6390 e 6393, o Plenário da Corte Suprema assegurou a tutela da autodeterminação informativa, suspendendo os efeitos da Medida Provisória nº 954/2020, que determinava o repasse, pelas operadoras de telefonia, de dados pessoais identificáveis de usuários ao IBGE.

Ao analisar esse precedente paradigmático, Laura Schertel Mendes (2020c) destacou que a tônica do julgamento residiu na centralidade da proteção de dados pessoais como

[32] Assim, a inclusão na Carta de um novo direito fundamental não encontrará nas cláusulas pétreas explicitadas embaraço para a sua abolição posterior por outra emenda (Branco, 2022).

elemento estruturante da democracia constitucional, evidenciando o papel desse direito na salvaguarda das liberdades individuais frente ao poder informacional do Estado[33].

Dessa forma, conclui-se que esse direito específico, embora tenha sido formalmente alçado à condição de direito fundamental por meio da atuação do constituinte derivado, subsome-se à categoria de cláusula pétrea. Isso porque, em rigor, a Emenda Constitucional nº 115/2022 não instituiu um novo direito, mas fortaleceu a proteção de um direito já reconhecido implicitamente pela Constituição originária, cuja essência foi previamente afirmada pela jurisprudência do Supremo Tribunal Federal.

2.4 DO NÚCLEO ESSENCIAL DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

> Embora omissa no texto constitucional brasileiro, a ideia de um núcleo essencial decorre do próprio modelo garantístico utilizado pelo constituinte (Mendes; Branco, 2024).

Com a promulgação da Emenda Constitucional nº 115/2022, o direito à proteção de dados pessoais foi elevado à condição de direito fundamental autônomo, integrando expressamente o rol do artigo 5º da Constituição Federal. Esse reconhecimento normativo reforça, de um lado, a centralidade da autodeterminação informativa no Estado Democrático de Direito, consolidando-a como vetor estruturante da proteção da dignidade humana na era digital.

No entanto, a concepção da proteção de dados pessoais exclusivamente sob a ótica da autodeterminação informacional — tal como delineada na paradigmática decisão do Tribunal Constitucional Alemão no caso do Censo de 1983 — incorre no risco de uma interpretação reducionista, segundo a qual qualquer forma de tratamento de dados seria presumivelmente ilegítima, salvo se precedida de consentimento expresso do titular (Corte, 2020). Essa leitura, embora historicamente relevante, revela-se insuficiente diante da complexidade das dinâmicas informacionais contemporâneas, nas quais o consentimento não pode ser o único critério legitimador da intervenção estatal ou privada sobre dados pessoais.

Em contraponto, a compreensão de que a proteção de dados pessoais se configura como o direito fundamental a um sistema normativo que regula o tratamento de informações impõe ao Poder Público e aos entes privados o dever de observar os contornos invioláveis desse direito,

[33] Como decorrência, tem-se o reconhecimento de um direito autônomo à proteção de dados pessoais e o seu duplo efeito sobre os deveres do Estado (um dever negativo de não interferir indevidamente no direito fundamental e um dever positivo de adotar medidas positivas para a proteção desse direito) (Mendes, 2020c).

sobretudo no que tange à preservação de seu núcleo essencial. Trata-se de uma abordagem que transcende a lógica do consentimento e se ancora em princípios estruturantes como finalidade, necessidade, transparência e responsabilidade.

Esse núcleo essencial representa o conteúdo mínimo e inderrogável do direito à proteção de dados, cuja violação compromete a própria legitimidade constitucional do tratamento de informações pessoais. Nele se inserem garantias como o consentimento livre, informado e inequívoco, a finalidade legítima e específica do tratamento, a transparência e o acesso à informação, bem como o direito à retificação, exclusão e portabilidade dos dados. Tais prerrogativas não são meras formalidades procedimentais, mas expressões concretas da dignidade da pessoa humana e da liberdade individual no contexto da sociedade da informação.

O cerne do direito à proteção de dados pessoais, portanto, ultrapassa a concepção tradicional que o vincula exclusivamente à privacidade, afirmando-se como um direito fundamental de caráter processual e regulatório. Sua lógica primordial não reside na proibição, mas na habilitação do tratamento de dados pessoais, desde que submetido a um arcabouço normativo estruturado. Nesse sentido, Lorenzo Dalla Corte (2020) ressalta que a distinção entre privacidade — compreendida como um instrumento de opacidade voltado à limitação do poder — e proteção de dados — entendida como um mecanismo de transparência que orienta e legitima o compartilhamento informacional — é crucial para a compreensão aprofundada da natureza e da função desse direito no contexto contemporâneo.

Diferentemente de um direito de natureza proibitiva, a proteção de dados pessoais não tem por finalidade obstar o tratamento de informações, mas assegurar que este se realize sob parâmetros normativos bem definidos. Os princípios insculpidos no Art. 6º da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) - a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a prestação de contas - compõem o arcabouço jurídico que estrutura o núcleo essencial desse direito, oferecendo salvaguardas concretas sem inviabilizar o uso legítimo dos dados.

Essa concepção, conforme defendido por Corte (2020) no contexto do direito europeu, reforça a natureza eminentemente processual do direito à proteção de dados, cujo valor reside na existência de um sistema regulatório que disciplina o tratamento informacional, independentemente de sua vinculação direta à privacidade ou ao sigilo. Trata-se, assim, de um verdadeiro "direito à normatividade procedimental"[34], cuja fundamentação se aproxima dos

[34] Uma tradução literal da doutrina de Corte (2020) seria "o direito a uma regra" *(A Right to a Rule).*

princípios do devido processo legal e da tutela jurisdicional efetiva, distanciando-se de uma mera proteção da esfera íntima.

Desse modo, o núcleo essencial do direito à proteção de dados — que há de ser observado como limite dos limites — expressa uma escolha normativa coletiva que legitima o tratamento de informações pessoais, desde que submetido a um conjunto plural de princípios e garantias fundamentais que operam como instrumentos regulatórios estruturantes. Essa arquitetura procedimental, marcada por um sistema de freios e contrapesos, traduz uma transformação jurídica e sociocultural que progressivamente dissocia a proteção de dados da lógica clássica da privacidade, consolidando-a como um direito fundamental autônomo, cuja essência reside na governança equilibrada, transparente e responsável dos fluxos informacionais na sociedade digital contemporânea.

Essa abordagem é coerente com os fundamentos da Lei Geral de Proteção de Dados Pessoais (LGPD), a qual não estabelece uma vedação ao tratamento de dados, mas exige que ele ocorra em parâmetros normativos rigorosos que assegurem a proteção dos direitos e das liberdades fundamentais. Ao articular inovação tecnológica, transparência institucional e respeito à dignidade humana, a LGPD consagra um modelo regulatório orientado pela responsabilidade e pela governança ética dos fluxos informacionais.

A Lei Geral de Proteção de Dados Pessoais — LGPD, ao regulamentar o direito fundamental à proteção de dados, estabelece em seu artigo 6º um conjunto de princípios que devem orientar toda e qualquer atividade de tratamento de dados pessoais. Esses princípios constituem os parâmetros normativos indispensáveis para a concretização desse direito no plano infraconstitucional.

Sob a perspectiva de que a proteção de dados pessoais se configura como um direito fundamental processual, a efetiva aplicação da LGPD não pode ocorrer de forma a comprometer aquele conjunto de princípios, que deve orientar toda e qualquer atividade de tratamento de dados pessoais, núcleo essencial do direito à proteção de dados pessoais. Contudo, também não pode ocorrer de forma a comprometer o núcleo essencial do direito à privacidade e à autodeterminação informativa. A restrição ao exercício de qualquer desses direitos deve ser submetida a um rigoroso teste de proporcionalidade, observando-se os critérios de necessidade, adequação e razoabilidade, sob pena de inconstitucionalidade.

Esse foi o entendimento afirmado pelo Supremo Tribunal Federal na Ação Direta de Inconstitucionalidade nº 6.387, em que se reconheceu a proteção de dados pessoais como direito fundamental autônomo, exigindo que qualquer forma de tratamento de dados — especialmente pelo poder público — observe estritamente os princípios constitucionais e seja submetida ao

controle de proporcionalidade. Conforme ali destacou a Ministra Rosa Weber, relatora da ação, eventuais restrições devem ser justificadas por critérios rigorosos de necessidade e adequação, sob pena de violação ao núcleo essencial do direito à privacidade.

Assim, o núcleo essencial do direito à proteção de dados pessoais constitui uma barreira constitucional intransponível, que impede a instrumentalização do indivíduo em nome de interesses econômicos, políticos ou administrativos. Trata-se, em última instância, de um limite ético-jurídico ao poder, cuja observância é condição para a preservação da liberdade e da democracia na era digital.

Nesse cenário, a atuação da Agência Nacional de Proteção de Dados (ANPD) revela-se estratégica, não somente como órgão regulador, mas como garante institucional da integridade do núcleo essencial desse direito. A proteção de dados, portanto, não se resume à legalidade formal do tratamento, mas exige sua legitimidade material, fundada na supremacia dos direitos fundamentais e na limitação substancial do poder de controle sobre as informações pessoais.

Assim, com base na proposição de Corte (2020) acerca da perspectiva do direito europeu comunitário, revela-se cabível, também no contexto jurídico brasileiro, a compreensão da proteção de dados pessoais como um direito fundamental vinculado à normatividade procedimental. Sob essa ótica, refletimos sobre os limites intransponíveis que se impõem, mesmo diante de hipóteses de restrição legal.

A teoria dos limites dos limites, ao estabelecer barreiras normativas contra restrições arbitrárias aos direitos fundamentais, revela-se especialmente pertinente quando aplicada ao direito à proteção de dados pessoais — um direito que, embora frequentemente associado à privacidade e à autodeterminação informacional, possui natureza própria e autonomia conceitual. Mais do que uma simples extensão da esfera privada, a proteção de dados configura-se como um direito fundamental à normatividade procedimental, isto é, um direito a que o tratamento de informações pessoais seja regido por regras claras, transparentes, previsíveis e controláveis — o devido processo informacional, como adrede comentado.

Nesse sentido, a proteção de dados aproxima-se do devido processo legal, não somente como garantia formal, mas como exigência substancial de que qualquer interferência no ciclo de vida dos dados — coleta, armazenamento, uso, compartilhamento ou eliminação — esteja submetida a um procedimento normativo legítimo, proporcional e sujeito a controle. Trata-se, portanto, de um direito à existência de regras e procedimentos que assegurem o tratamento justo e não discriminatório das informações pessoais, independentemente do conteúdo sensível ou da expectativa de privacidade envolvida.

A teoria dos limites dos limites reforça essa dimensão procedimental ao impor obstáculos normativos que impedem o Poder Público (e, por extensão, os entes privados com função pública ou relevância social) de tratar dados pessoais sem base legal clara, finalidade legítima e respeito ao núcleo essencial do direito. A exigência de legalidade estrita, a vedação ao desvio de finalidade, o controle jurisdicional e a proporcionalidade são instrumentos que garantem que o tratamento de dados não se converta em mecanismo de vigilância, discriminação ou manipulação social.

Portanto, a proteção de dados pessoais não se esgota na defesa da intimidade ou na liberdade de decidir sobre o uso das próprias informações. Ela se consolida como um direito à existência de um regime normativo procedimental robusto, que assegure previsibilidade, transparência e responsabilização no uso de dados — valores centrais em uma sociedade digital democrática. Nesse contexto, os obstáculos postos pela teoria dos limites dos limites não apenas protegem o indivíduo contra abusos, mas também estruturam o próprio funcionamento legítimo do Estado e do mercado de dados, reafirmando o compromisso com o Estado de Direito e com a dignidade humana.

2.5 O COMPARTILHAMENTO DE DADOS PESSOAIS COMO ATIVIDADE ADMINISTRATIVA

Salus populi suprema lex esto.[35]

Nos tópicos anteriores, foram analisados aspectos da doutrina dos direitos fundamentais, sustentáculos do referencial teórico adotado pela pesquisa.

Todavia, considerando que o presente estudo se debruça sobre o compartilhamento e uso secundário de dados pessoais no âmbito do Poder Público, o foco recai sobre atos relacionados ao tratamento de dados pessoais praticados por órgãos ou entidades dos entes federativos (União, Estados, Distrito Federal e Municípios) e dos três Poderes (Executivo, Legislativo e Judiciário). Incluem-se, ainda, as Cortes de Contas e o Ministério Público; todos no exercício de suas funções institucionais, como a prestação de serviços e a implementação de políticas públicas, e a atuação fiscalizatória e jurisdicional.

Trata-se, portanto, de uma análise do tratamento de dados pessoais no exercício da atividade administrativa, considerando que essa prática envolve a utilização estratégica dessas

[35] "Que o bem-estar do povo seja a lei suprema". Aforismo atribuído a Cícero no seu livro "*De Legibus*".

informações na gestão jurídica de bens e interesses qualificados da coletividade[36], atuação que exige conformidade com os princípios estruturantes do Direito Administrativo — como legalidade, finalidade, motivação e proporcionalidade — e com os direitos fundamentais assegurados pela Constituição Federal.

Nessa perspectiva, destacam-se as contribuições de Sarlet e Sales Sarlet (2022), que, ao abordar o compartilhamento de dados pessoais pelo Poder Público, indicam que tal prática configura atividade administrativa e, como tal, deve submeter-se ao regime jurídico próprio da atuação estatal. Os autores ampliam o debate para além da proteção de dados pessoais, inserindo o compartilhamento informacional no paradigma do Direito Administrativo, e ressaltam a imprescindibilidade da observância dos princípios da legalidade, finalidade, transparência e motivação, bem como do controle jurisdicional e administrativo.

Sarlet e Sales Sarlet fundamentam essa concepção no voto da Ministra Cármen Lúcia proferido no julgamento sobre o compartilhamento de dados e informações pela Agência Brasileira de Inteligência (ABIN), no qual se enfatizou a natureza administrativa do ato de compartilhamento informacional no âmbito estatal. A ministra destacou a necessidade de delimitação clara das competências e responsabilidades dos órgãos envolvidos, bem como o respeito aos direitos e garantias fundamentais previstos na Constituição.

Vê-se ainda que aqueles autores referenciam expressamente a Lei nº 9.784/1999, que regula o processo administrativo federal, reafirmando que tanto o tratamento quanto o compartilhamento de dados pessoais pelo Poder Público devem observar os procedimentos e garantias próprios dos atos administrativos, com especial atenção ao devido processo legal.

À luz dos fundamentos constitucionais, o Direito Administrativo orienta-se pela busca de estabilidade entre dois valores historicamente tensionados: a liberdade individual e a autoridade estatal. A realização do equilíbrio entre esses vetores encontra expressão nos princípios da legalidade e da supremacia do interesse público sobre o interesse privado que, embora não exclusivos deste ramo jurídico — pois permeiam todo o Direito Público — assumem nele papel estruturante (Di Pietro, 2012).

Além desses, o Direito Administrativo também se submete aos princípios da impessoalidade, moralidade, publicidade e eficiência, conforme preconiza o Art. 37 da Constituição da República Federativa do Brasil de 1988. É a partir deles que se ergue a

[36] "...foi o Estado que por primeiro se encontrou na posição de utilizar largamente informações pessoais. Os motivos são razoavelmente claros: um pressuposto para uma administração pública eficiente é o conhecimento tão acurado quanto possível da população" (Doneda, 2021).

arquitetura normativa e axiológica que sustenta e orienta a atuação administrativa, conferindo-lhe legitimidade, racionalidade e controle jurídico à atividade estatal.

Complementarmente, o regime jurídico administrativo é informado por princípios específicos essenciais para o desempenho equilibrado das atividades estatais, promovendo a harmonização entre os direitos dos administrados e as prerrogativas da Administração Pública. Entre esses princípios destacam-se a motivação, a razoabilidade, a proporcionalidade e a moralidade, que atuam como diretrizes normativas e éticas para a atuação administrativa, orientando a tomada de decisões e a condução dos processos administrativos.

O princípio da motivação impõe à Administração o dever de explicitar os fundamentos de fato e de direito que embasam suas decisões, assegurando a transparência e possibilitando o controle jurisdicional. Já a razoabilidade e a proporcionalidade atuam como instrumentos de controle da adequação e da necessidade das medidas adotadas, vedando excessos e garantindo que os meios empregados sejam compatíveis com os fins públicos perseguidos. O princípio da moralidade, por sua vez, exige que a Administração atue segundo padrões éticos, de boa-fé e probidade, assegurando a legitimidade social e o respeito aos valores democráticos (Meirelles, 1988).

Esses princípios específicos são reconhecidos pela doutrina administrativista de escol como fundamentos essenciais da atuação estatal, integrando-se ao conjunto de valores constitucionais. Segundo Di Pietro (2012), tais princípios orientam a conformação dos atos e procedimentos administrativos. No âmbito federal, encontram-se expressamente previstos no artigo 2º da Lei nº 9.784, de 29 de janeiro de 1999, que regula o processo administrativo no âmbito da Administração Pública Federal.

A incorporação desses princípios ao regime jurídico-administrativo não apenas legitima as prerrogativas conferidas à Administração Pública para a salvaguarda do interesse coletivo, mas também estabelece balizas normativas e instrumentos de controle que condicionam o exercício do poder estatal à observância dos direitos fundamentais, dos valores constitucionais e da promoção do bem comum. Essa tessitura normativa, complexa e articulada, revela-se essencial para fortalecer a confiança social nas instituições públicas e assegurar uma atuação administrativa pautada pela legalidade, pela justiça e pela efetividade.

Inserida nessa estrutura normativa, a atividade administrativa compreende o conjunto de ações concretas e imediatas realizadas pelo Estado, por meio de seus órgãos e agentes, com vistas à realização do interesse público, sob o regime jurídico-administrativo. Nesse contexto, considerando que essa atuação administrativa exige o acesso a informações adequadas, conclui-

se que a efetivação do princípio constitucional da eficiência está intrinsecamente vinculada à capacidade de gestão dessas informações (Gasiola; Machado; Mendes, 2021).

Embora seja exercida, em caráter típico, pelo Poder Executivo, a atividade administrativa também se manifesta nos Poderes Legislativo e Judiciário, sempre que atuam na gestão de seus próprios serviços internos. Essa compreensão decorre da teoria da tripartição dos poderes, segundo a qual cada Poder possui funções típicas e atípicas.

A partir da premissa de que não há uma teoria única da separação de Poderes, que seja universalmente aplicável às diferentes realidades institucionais, Marçal Justen Filho (2005) adverte que, no contexto brasileiro, todos os Poderes desempenham, em alguma medida, funções de natureza administrativa, ainda que com diferentes graus de intensidade e escopo.

Com a dupla finalidade de limitar o poder estatal e, ao mesmo tempo, instrumentalizá-lo para a realização de necessidades coletivas, a atuação do Estado é regida pelo regime jurídico de Direito Administrativo e orienta-se para a consecução de seus fins essenciais: a preservação da ordem pública, a promoção do bem-estar individual dos cidadãos e o avanço do progresso social[37].

Com base na doutrina de Garrido Falla, para quem o Direito Administrativo se ergue sobre o binômio "prerrogativas da Administração — direitos dos administrados", Celso Antônio Bandeira de Mello (2008) leciona que é o entrosamento destes dois termos que lhe delineia a fisionomia, que poderá variar de um para outro sistema jurídico positivo, de modo a apresentar uma feição mais autoritária ou, opostamente, um caráter mais obsequioso aos valores democráticos.

Na contemporaneidade digital do Estado brasileiro, o atingimento dos fins estatais exige a coleta, o armazenamento, a gestão e a utilização de informações, ocorrendo, em grande medida, a partir de bases de dados pessoais, amplamente empregadas nos diversos setores da atuação estatal. Tais dados são essenciais para a execução de múltiplas atividades administrativas, como a seleção e inclusão de famílias de baixa renda em programas federais de assistência social; a garantia do acesso universal e equitativo às ações e serviços de saúde no âmbito do Sistema Único de Saúde (SUS); a viabilização de pagamentos judiciais, como os precatórios; e o aprimoramento dos mecanismos de controle tributário.

Ao realizar ações como coleta, armazenamento e compartilhamento de dados pessoais necessários à viabilização de suas diversas funções, o Poder Público exerce, em sentido amplo,

[37] Nesse sentido: Meirelles, 1988; Justen Filho, 2005.

a administração pública[38]. Trata-se da gestão de interesses coletivos, orientada pela legalidade e finalidade pública.

Com base na doutrina alemã, Gasiola, Machado e Mendes (2021) referem-se à noção de um "direito administrativo da proteção de dados", voltado às regras que autorizam e controlam o tratamento de dados pessoais por órgãos e entes públicos no exercício de suas funções institucionais[39]. Embora esse ramo específico ainda não tenha se consolidado como uma especialidade autônoma no Direito Administrativo brasileiro, é imprescindível que a presente pesquisa se apoie no referencial teórico do regime jurídico-administrativo, a fim de conferir densidade normativa e coerência sistemática à análise proposta.

A atividade administrativa do Poder Público no Estado brasileiro está submetida a um conjunto normativo específico, denominado regime jurídico administrativo, que consiste em um conjunto de prerrogativas que lhes são conferidas para a realização do interesse público e, ao mesmo tempo, de sujeições que impõem limites rigorosos à sua atuação, em conformidade com os direitos fundamentais e com o princípio da legalidade.

A expressão "regime jurídico administrativo" é aqui utilizada em sentido técnico e delimitado[40], referindo-se ao arcabouço normativo de direito público que confere identidade própria ao Direito Administrativo. Esse regime estabelece um conjunto de prerrogativas que posicionam o Poder Público em situação de superioridade jurídica nas suas relações com os administrados, ao mesmo tempo em que impõe restrições rigorosas destinadas a assegurar que sua atuação permaneça orientada pela busca contínua do interesse coletivo.

Elemento estruturante desse regime, o interesse coletivo constitui o núcleo teleológico da atuação do Poder Público. É ele que fundamenta tanto as prerrogativas conferidas ao Estado

---

[38] Alinha-se a pesquisa à advertência feita por Meirelles (1988) no sentido de que a expressão – administração pública – registrada com minúsculas, alude à atividade administrativa em si mesma, enquanto que – Administração Pública -, com maiúsculas, refere-se a pessoas e órgãos administrativos.

[39] Asseveram os autores que há na Alemanha o crescente reconhecimento de um direito administrativo da proteção de dados, como parte do direito administrativo geral. Remetem à doutrina de REIMER, Philipp. Verwaltungsdatenschutzrecht: Das neue Recht für die behördliche Praxis. Baden-Baden: Nomos, 2019. p. 16-17.

[40] No desempenho de suas atividades, a Administração Pública pode se submeter tanto ao regime de direito privado quanto ao regime de direito público. A expressão "Regime Jurídico da Administração" tem sentido genérico, abrangendo os dois regimes jurídicos a que se submete o Poder Público. Diferentemente, a expressão "Regime jurídico administrativo" tem sentido restrito, servindo para designar o regime jurídico de direito público aplicado à Administração (Alexandre; Deus, 2018).

quanto as limitações que lhe são impostas, assegurando que atue como gestor de interesses que não lhe pertencem, mas sim à coletividade, sempre orientado pela realização do bem comum.

O interesse coletivo, também denominado interesse público primário, refere-se às necessidades e aspirações da sociedade como um todo. Ele se distingue do interesse público secundário, que diz respeito aos interesses da própria Administração enquanto pessoa jurídica (como ocorre na arrecadação de tributos ou na gestão patrimonial)[41]. No âmbito do regime jurídico administrativo, é o interesse coletivo que legitima a atuação estatal, conferindo-lhe poderes especiais como o de promover desapropriações, exercer o poder de polícia e a rescindir unilateralmente contratos administrativos.

A concepção prevalente na doutrina brasileira é a de que o regime jurídico administrativo é construído sobre dois pilares fundamentais[42]: de um lado, **a supremacia do interesse público[43]**, que legitima a atribuição de prerrogativas ao Poder Público; de outro, **a indisponibilidade** desse mesmo interesse, que exige a imposição de limites jurídicos à sua atuação. Esses dois princípios estruturantes — frequentemente denominados supraprincípios[44] — constituem o ponto de partida indispensável para a compreensão aprofundada do regime jurídico administrativo e de sua função no Estado Democrático de Direito.

O primado do interesse público traduz-se na primazia dos interesses coletivos sobre os interesses individuais, assegurando que o bem comum prevaleça nas decisões e ações do Estado. Em decorrência direta desse princípio, emerge a indisponibilidade do interesse público, que estabelece a impossibilidade de renúncia, transação ou disposição desses interesses por parte do Poder Público, uma vez que não lhe pertencem, mas sim à coletividade que representa.

No âmbito do regime jurídico-administrativo, a supremacia do interesse público fundamenta a concessão de prerrogativas especiais à Administração em relação aos particulares, legitimando, por exemplo, atos unilaterais e medidas coercitivas. Contudo, tais prerrogativas são contrabalançadas por limites rigorosos, como a observância dos direitos fundamentais, o

[41] A distinção entre interesse público primário e secundário tem origem na doutrina italiana de Renato Alessi e foi difundida no Brasil por Celso Antônio Bandeira de Mello. Nesse sentido: Mello, 2009; Justen Filho, 2005.

[42] Nesse sentido: Mello, 2009; Borges, 2011; Justen Filho, 2005.

[43] Relevante aqui ressaltar que o princípio da supremacia do interesse público não é princípio setorial, típico, específico do direito administrativo, porque é comum a todo o direito público, em seus diferentes desdobramentos, já que se encontra na base de toda processualística, bem como na raiz do direito penal e do constitucional (Cretella Júnior, 1968).

[44] Nesse sentido: Mazza, 2018; Alexandre, Deus, 2018.

controle e a responsabilidade objetiva do Estado, assegurando o equilíbrio entre autoridade estatal e proteção dos direitos individuais.

Ao sublinhar o caráter exorbitante do regime jurídico-administrativo em relação ao direito comum aplicável às relações entre particulares, Edmir Netto de Araújo (2005) enfatiza que não se admite a atuação do Poder Público dissociada do interesse público concretamente identificado. A prerrogativa estatal, portanto, encontra seus limites na própria finalidade que a legitima: a promoção do bem coletivo, sob pena de desvio de finalidade e violação de princípios constitucionais.

Apesar de sua relevância, o princípio da supremacia do interesse público sobre o interesse privado não possui caráter absoluto, sobretudo quando confrontado com outros princípios constitucionais. Nessa perspectiva, o próprio sistema jurídico prevê hipóteses em que direitos e garantias fundamentais asseguram a prevalência de interesses individuais, inclusive diante da atuação estatal, reafirmando o compromisso do Estado de Direito com a proteção da dignidade da pessoa humana e o equilíbrio entre os valores públicos e privados[45].

De todo modo, a relevância do interesse público se manifesta no reconhecimento de que qualquer ato administrativo que dele se afaste será, necessariamente, inválido (Mello, 2008). Não obstante sua centralidade no Direito Administrativo, a dificuldade de delimitação precisa do seu conteúdo confere ao interesse público a natureza de conceito jurídico indeterminado — ou seja, um termo jurídico cujo significado não é fixo, preciso e previamente delimitado, exigindo interpretação e concretização no caso específico (Justen Filho, 2005). Sua aplicação, portanto, demanda uma valoração contextual, realizada pelo intérprete ou pelo administrador, com base em critérios jurídicos, éticos, sociais e políticos.

Em razão de sua formulação imprecisa, é recorrente a utilização estratégica do princípio da supremacia do interesse público por parte dos detentores do poder político como mecanismo de blindagem institucional, com o objetivo de evitar o efetivo controle ou o eventual desfazimento de atos administrativos eivados de vícios, ainda que em afronta a garantias constitucionais fundamentais. Nesse contexto, revela-se particularmente pertinente a crítica de Marçal Justen Filho (2005), ao advertir que a ausência de um instrumento jurídico capaz de

[47] É o caso da inadmissibilidade da utilização de provas obtidas por meios ilícitos, nos termos do art. 5º, inciso LVI, da Constituição Federal, em que o interesse público na obtenção da verdade cede passo ao direito ao devido processo legal.

delimitar com precisão o conteúdo efetivo do interesse público propicia a ocorrência de problemas jurídicos de difícil superação[46].

Em manifestação apresentada na Ação Direta de Inconstitucionalidade nº 6649, a Advocacia-Geral da União sustentou que o Decreto nº 10.046/2019 promove o aprimoramento do sistema de compartilhamento de dados na Administração Pública, com vistas à realização do interesse público. Considerando, contudo, a natureza indeterminada desse conceito e, sob a perspectiva de um Estado Democrático de Direito, impõe-se a necessidade de examinar como se configura, concretamente, o interesse público em questão.

2.5.1 O necessário controle das atividades administrativas

> Toda a disciplina da atividade administrativa tem de ser permeada pela concepção democrática, que sujeita o administrador à fiscalização popular e à comprovação da realização democrática dos direitos fundamentais (Justen Filho, 2005).

O Direito Administrativo configura-se, em essência, como um instrumento jurídico de contenção e fiscalização democrática das estruturas estatais incumbidas da função administrativa, assegurando à sociedade civil mecanismos de controle sobre o exercício do poder político.

O controle da atividade administrativa, elemento estruturante do Estado Democrático de Direito, consiste no conjunto de mecanismos destinados a assegurar que o Poder Público atue em conformidade com os princípios legais, constitucionais e éticos. A doutrina administrativista de escol apresenta distintas classificações para os tipos de controle[47].

Para os fins desta pesquisa, adota-se a classificação em três esferas:

a) **Controle interno**, exercido pelo próprio Poder Público, por meio de suas corregedorias, ouvidorias e unidades de auditoria;

---

[48] Passados vinte anos de sua publicação, continua atual a advertência: “Na atualidade, o exercente do poder político refugia-se no princípio da supremacia do interesse público para evitar o controle ou o desfazimento de atos defeituosos, violadores de garantias constitucionais. ” (Justen Filho, 2005).

[47] A título de exemplificação:
Hely Lopes Meirelles (1988): controle hierárquico, controle finalístico, controle interno, controle externo, controle prévio ou preventivo, controle concomitante, controle subsequente, controle de legalidade ou legitimidade, controle de mérito.
Marçal Justen Filho (2005): controle do Legislativo, controle do Judiciário, controle do Executivo, controle do Tribunal de Contas, controle do Ministério Público.
Maria Sylvia Zanella di Pietro (2012): controle administrativo, legislativo ou judicial; controle prévio, concomitante ou posterior; controle interno ou externo; controle de legalidade ou de mérito.

b) **Controle externo**, realizado por órgão estranho à estrutura do ente controlado, como, por exemplo, o exercido pelo Tribunal de Contas da União sobre as contas dos administradores e demais responsáveis por dinheiros, bens e valores públicos da administração direta e indireta, incluídas as fundações e sociedades instituídas e mantidas pelo Poder Público federal (art. 71, II, da Constituição Federal);

c) **Controle social**, promovido pela sociedade civil, especialmente por meio de instrumentos como a Lei de Acesso à Informação (Lei nº 12.527/2011), que fortalece a transparência e a participação cidadã.

A expressão "controle da atividade administrativa do Estado" encerra um conteúdo conceitual multifacetado, abrangendo tanto a identificação dos órgãos constitucional ou legalmente incumbidos da função de controle, quanto os instrumentos jurídicos por meio dos quais essa função se concretiza (Araújo, 2005). Para além de sua dimensão institucional e normativa, o termo também se refere à própria prática material do controle, enquanto atividade efetiva de fiscalização, orientação e correção da atuação administrativa, revelando-se, assim, como categoria complexa e essencial à preservação da juridicidade e da legitimidade no exercício do poder público.

A clássica doutrina de Hely Lopes Meirelles (1988) destaca que o controle consiste na faculdade de vigilância, orientação e correção da atividade administrativa, podendo ser exercido em todas as esferas e por todos os Poderes do Estado. Essa concepção amplia a compreensão do controle como instrumento de equilíbrio institucional e de garantia da juridicidade e da legitimidade dos atos administrativos.

Sob a perspectiva do Direito Administrativo, o controle da atividade administrativa transcende a mera aferição da legalidade formal — a qual, por sua natureza, exige critérios mais rigorosos do que aqueles aplicáveis às condutas dos particulares —, abrangendo também a análise da legitimidade, da moralidade, da eficiência, da conveniência e da oportunidade dos atos administrativos. Trata-se de um controle multifacetado, que incorpora a verificação da conformidade da atuação estatal com os princípios constitucionais e administrativos, assegurando que o exercício da função pública se oriente não apenas pela estrita legalidade, mas também pela realização concreta do interesse público em sua dimensão substancial.

Toda a conformação normativa da atividade administrativa deve estar imbuída de uma perspectiva democrática substancial, que impõe ao gestor público não apenas a sujeição à fiscalização social, mas também a obrigação de demonstrar, de forma transparente e efetiva, que sua atuação contribui para a concretização dos direitos fundamentais em um ambiente de legitimidade democrática.

Nesse contexto, o compartilhamento de dados pessoais por órgãos e entidades do Poder Público deve ser compreendido como uma manifestação concreta da atividade administrativa. Com a entrada em vigor da Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD), o tratamento de dados pessoais, inclusive no setor público, passou a ser regulado por um regime jurídico específico, que impõe limites e condições para a coleta, o uso e o compartilhamento dessas informações.

A LGPD permite que o Poder Público compartilhe dados pessoais sem o consentimento do titular, desde que tal prática seja necessária para a execução de políticas públicas previstas em leis e regulamentos (art. 7º, III, e art. 23). No entanto, essa autorização legal não é absoluta: o compartilhamento deve observar os princípios da finalidade, necessidade, adequação, transparência, segurança e responsabilização, entre outros previstos na própria LGPD.

Importa destacar que a observância dos princípios setoriais da LGPD não exime o Poder Público do dever de respeitar, de forma simultânea e integrada, os princípios constitucionais que regem a Administração Pública. Assim, o compartilhamento de dados pessoais deve também estar em consonância com os princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência, previstos no caput do art. 37 da Constituição Federal.

Todavia, a invocação de conceitos jurídicos indeterminados — como o interesse público — ou de fundamentos institucionais, como a eficiência administrativa e a autonomia dos Poderes, não pode servir como escudo para afastar o exercício do controle sobre a atividade administrativa. O controle, longe de representar uma afronta à autonomia funcional dos entes estatais, constitui instrumento essencial de legitimação democrática, ao garantir que os agentes públicos, no exercício de competências delegadas pelo Estado, não atuem de forma arbitrária ou em descompasso com os direitos fundamentais e os valores constitucionais.

Essa dupla observância — dos princípios da proteção de dados e dos princípios constitucionais da Administração — é essencial para garantir que o compartilhamento de dados pessoais não se converta em instrumento de arbítrio, discricionariedade desmedida ou violação de direitos fundamentais. O controle da atividade administrativa, nesse cenário, assume papel central: cabe aos órgãos de controle interno, ao Poder Judiciário, à sociedade civil e à Agência Nacional de Proteção de Dados (ANPD) fiscalizar e coibir práticas abusivas, assegurando que o tratamento de dados pelo Estado se realize com transparência, proporcionalidade e respeito à dignidade da pessoa humana.

Portanto, o compartilhamento de dados pessoais pelo Poder Público deve ser compreendido como uma atividade administrativa sujeita a um regime jurídico próprio, que exige a harmonização entre os princípios da LGPD e os pilares constitucionais da

Administração Pública. Essa integração normativa é condição necessária para a construção de uma cultura institucional de respeito à privacidade, à legalidade e à *accountability* no setor público.

2.6 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E A IMPERIOSA REGULAÇÃO DO COMPARTILHAMENTO PELO PODER PÚBLICO COMO LIMITE LEGÍTIMO

> Aliás, ousaria dizer que os parâmetros de proteção dos direitos fundamentais devem ser permanentemente abertos à evolução tecnológica.[48]

O reconhecimento constitucional do direito fundamental à proteção de dados pessoais impõe ao Estado não apenas o dever de abstenção frente a práticas abusivas, mas também a obrigação positiva de estruturar mecanismos normativos e institucionais que regulem rigorosamente o compartilhamento de dados no âmbito público. Essa regulação configura limite legítimo à atuação estatal, especialmente diante da crescente complexidade das tecnologias de coleta, armazenamento e análise de dados, que potencializam riscos à privacidade, à liberdade informacional e à dignidade humana.

Os parâmetros de proteção dos direitos fundamentais não podem ser concebidos como estáticos, devendo permanecer abertos à evolução tecnológica e às transformações sociais, sob pena de se tornarem insuficientes frente às novas formas de vigilância, discriminação algorítmica e concentração informacional. Isso, contudo, não implica abdicar de uma regulação do compartilhamento de dados pelo Poder Público, mas sim, reconhecer que tal regulação deve ser orientada por uma hermenêutica constitucional dinâmica, capaz de preservar o núcleo essencial dos direitos fundamentais em um ambiente digital em constante mutação.

Diante do exposto, a legitimação constitucional do direito fundamental à proteção de dados pessoais evidencia um progresso normativo que reitera a centralidade da dignidade da pessoa humana e da autonomia informativa na atual sociedade digital (Doneda, 2019). Ademais, dados e informações se configuram como recursos essenciais para a concepção, execução e análise de políticas públicas (Gasiola; Machado; Mendes, 2021). Assim, é imprescindível que o sistema jurídico defina orientações claras e precisas para o intercâmbio de dados pessoais no contexto da Administração Pública.

---

[48] Gilmar Ferreira Mendes, ADI 6649.

Essa normatização deve contemplar não apenas critérios objetivos de permissibilidade e restrição, mas também incorporar mecanismos eficazes de rastreabilidade, controle e transparência, como forma de garantir a efetividade do direito e prevenir práticas abusivas ou incompatíveis com os princípios constitucionais da legalidade, finalidade e proporcionalidade. A proteção de dados, nesse contexto, não se limita à tutela da privacidade individual, mas se projeta como instrumento de governança democrática e de contenção dos excessos informacionais do Poder Público.

A doutrina contemporânea dos direitos fundamentais oferece importante aporte para compreender que este direito, assim como os demais direitos de mesma natureza, não possui caráter absoluto, mas é passível de limitações legítimas (Sarlet e Sales Sarlet, 2022). A teoria da relatividade dos direitos fundamentais reconhece que deles pode decorrer a imposição de restrições legítimas sempre que houver a proteção concorrente de outros bens jurídicos constitucionalmente relevantes ou a necessidade de compatibilização entre valores constitucionais distintos.

Nesse contexto, a exigência de atos normativos específicos para disciplinar o compartilhamento de dados pessoais pelo Poder Público configura um legítimo limite necessário ao exercício do direito fundamental à proteção de dados, sempre balizado pelos princípios do Estado Democrático de Direito — especialmente legalidade, proporcionalidade e preservação do núcleo essencial do direito (Sarlet, 2004).

Essa limitação se justifica pela imperiosa necessidade de compatibilizar a proteção da privacidade e da autodeterminação informativa com valores constitucionais como a eficiência administrativa, a segurança pública, a saúde coletiva e outros interesses sociais relevantes, que demandam o intercâmbio legítimo e transparente de informações pessoais. Contudo, tal limitação não é compatível com a dispensa da celebração de convênios, acordos de cooperação técnica ou instrumentos congêneres para a efetivação do compartilhamento de dados entre órgãos públicos, uma vez que a ausência desses mecanismos compromete a rastreabilidade das operações de tratamento de dados pessoais. Essa lacuna pode acarretar sérios riscos à proteção dos direitos fundamentais, especialmente em contextos de formulação e implementação de políticas públicas que envolvam o tratamento de dados pessoais sensíveis.

Imagine-se, por exemplo, o caso de uma base de dados de saúde contendo informações sobre pacientes com doenças infectocontagiosas, compartilhada entre órgãos governamentais sem registro adequado de acesso e finalidade. Sem rastreabilidade, não seria possível identificar quais agentes públicos acessaram os dados, com que propósito, e se houve desvio de finalidade ou exposição indevida. Isso poderia resultar em discriminação institucional, negativa de acesso

a serviços, ou até mesmo em vazamentos que comprometam a reputação e a integridade dos indivíduos afetados. E a inexistência de trilhas auditáveis inviabiliza a responsabilização dos envolvidos e fragiliza o controle democrático, transformando o compartilhamento legítimo em uma potencial fonte de violação de direitos.

Cabe ainda refletir que, embora os serviços de armazenamento de dados de instituições do Executivo federal sejam predominantemente realizados pelo Serviço Federal de Processamento de Dados (SERPRO) — empresa pública vinculada ao Ministério da Fazenda —, existe a possibilidade de que entes públicos, pertencentes a qualquer dos Poderes, necessitem recorrer, em alguma etapa do ciclo de tratamento de dados, a serviços prestados por agentes privados.

Por essa razão, impõe-se uma regulação adequada que contemple tanto o controle estatal sobre o tratamento e o compartilhamento de dados pessoais quanto a delimitação da atuação dos agentes privados envolvidos, em conformidade com a eficácia horizontal dos direitos fundamentais. Essa eficácia ultrapassa a tradicional relação bilateral entre Estado e indivíduo, estendendo-se às relações entre particulares, conforme sustentado por Doneda (2019), Mendes e Fernandes (2020).

Segundo o SERPRO, os dados, isoladamente, não geram valor público significativo sem o suporte de uma estrutura sólida de governança, segurança da informação e garantias efetivas de privacidade e proteção dos cidadãos[49]. Esses elementos, considerados pela estatal como indispensáveis para a construção de um ecossistema digital confiável e eficiente — especialmente diante dos desafios impostos pela crescente digitalização dos serviços públicos — somente se mostram plenamente alcançáveis mediante uma conformação normativa adequada do compartilhamento de dados pessoais, que deve convergir para a promoção da rastreabilidade das informações compartilhadas, assegurando transparência, controle e responsabilidade no tratamento de dados.

Essa rastreabilidade consiste na capacidade técnica e jurídica de registrar, monitorar e auditar o fluxo de dados pessoais nas redes institucionais públicas e privadas. Isso permite identificar quem acessou, quando, com qual finalidade e sob quais condições os dados foram acessados ou transferidos. Tal funcionalidade revela-se indispensável para garantir a responsabilização dos agentes de tratamento, prevenir abusos, possibilitar auditorias eficazes e assegurar o cumprimento dos princípios da transparência, da prestação de contas e da segurança

[49] Consoante pronunciamento no 16º Seminário de Proteção à Privacidade e aos Dados Pessoais, promovido pelo CGI.br e NIC.br.

jurídica, sendo pilares estruturantes do controle democrático e da governança pública de dados (Constituição Federal, art. 5º, LXXIX; LGPD, art. 50).

Do ponto de vista constitucional e normativo, a rastreabilidade configura-se como um instrumento indispensável para assegurar a legalidade, a proporcionalidade e a segurança jurídica no tratamento e compartilhamento dos dados pessoais, aspectos que viabilizam o controle do titular dos dados e das autoridades reguladoras sobre possíveis usos indevidos ou excessivos (Sarlet; Saavedra, 2020). Sem esse mecanismo, a proteção efetiva dos direitos à privacidade e à autodeterminação informativa fica comprometida, pois o controle sobre os dados se torna abstrato, dificultando a reparação de danos e a responsabilização dos agentes públicos e privados envolvidos.

Também merece reflexão o fato de que a ausência de instrumentos adequados de rastreabilidade compromete não apenas a proteção individual dos titulares de dados, mas igualmente a integridade e a legitimidade das políticas públicas respaldadas em dados, expondo o Estado e a sociedade a riscos sistêmicos, violações estruturais e déficits significativos de prestação de contas informacional.

Ademais, a rastreabilidade fortalece o princípio da governança responsável de dados, fundamental no constitucionalismo digital ao permitir compatibilizar o compartilhamento legítimo e necessário de dados — para a eficiência administrativa, segurança pública e interesses sociais — com a proteção dos direitos individuais, respeitando os limites constitucionais que fundamentam essa regulação. Essa capacidade de monitoramento também opera em conformidade com a eficácia horizontal dos direitos fundamentais, ao controlar interações complexas entre entes públicos e privados que compartilham dados no ambiente digital (Doneda, 2019).

Percebe-se, portanto, que a exigência de rastreabilidade integra a dimensão procedimental da proteção de dados pessoais, garantindo que o direito fundamental não permaneça apenas em um plano abstrato, mas se traduza em práticas administrativas responsáveis, transparentes e auditáveis, essenciais para a confiança cidadã e para a legítima construção da cidadania digital.

Esse cenário impõe a necessidade de marcos normativos estruturados, capazes de assegurar elevados padrões de transparência, segurança jurídica e responsabilidade institucional. Revela-se, portanto, incompatível com normas que dispensam a celebração de convênios, acordos ou instrumentos congêneres uma vez que registros precisos e eficazes têm como finalidade prevenir vulnerabilidades sistêmicas, práticas discriminatórias e danos sociais

de natureza estrutural, decorrentes do uso inadequado, desproporcional ou opaco dos dados pessoais.

A conformação desses instrumentos jurídicos deve estar alinhada aos princípios constitucionais da legalidade, finalidade, necessidade e proporcionalidade, bem como aos parâmetros internacionais de proteção de dados, de modo a garantir a tutela efetiva dos direitos fundamentais na esfera digital e a integridade das políticas públicas baseadas em dados.

Portanto, à luz da dogmática dos direitos fundamentais, a exigência de atos normativos específicos para disciplinar o compartilhamento de dados pessoais no âmbito do Poder Público — com vistas à garantia da rastreabilidade — não se limita a um imperativo técnico-jurídico. Trata-se, sobretudo, da afirmação de um limite legítimo e necessário ao exercício do próprio direito fundamental à proteção de dados, conforme delineado pela Constituição Federal (art. 5º, LXXIX) e pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Esse limite é essencial para compatibilizar a inovação tecnológica e a governança digital com os princípios estruturantes do Estado Democrático de Direito, especialmente no contexto da sociedade informacional. Em suma, a rastreabilidade, nesse sentido, opera como instrumento de *accountability*, de modo a permitir a fiscalização do ciclo de vida dos dados e a responsabilização dos agentes públicos e privados, em consonância com os princípios da finalidade, necessidade, transparência e prestação de contas (Sarlet; Saavedra, 2020; Mendes, 2018).

3 DA PROTEÇÃO DE DADOS PESSOAIS.

> Nesse sentido, entende-se fundamental a compreensão da disciplina de proteção de dados pessoais como meio de tutela da personalidade do cidadão, garantindo tanto a autonomia das suas escolhas como a sua proteção contra situações potencialmente discriminatórias (Mendes, 2014).

Um dos traços mais distintivos da sociedade contemporânea é a intensa circulação de informações pessoais, impulsionada pela digitalização e pelo avanço acelerado das tecnologias de análise de dados e de vigilância[50], que promovem uma interconectividade global sem precedentes.

Essa conjuntura propicia ganhos expressivos financeiros e de produtividade no setor privado e aprimora a eficiência das instituições públicas. Contudo, tais avanços tecnológicos também intensificam as preocupações com a salvaguarda da privacidade individual, sobretudo diante do crescente fluxo transnacional de dados pessoais.

Laura Schertel Mendes (2014) destaca o fenômeno da ubiquidade computacional (*ubiquitous computing* ou *"ubicomp"*), característico da revolução das tecnologias da informação e comunicação no século XX, no qual a computação se torna pervasiva e sensível ao contexto do usuário. Embora essa integração tecnológica amplie significativamente as capacidades de ação e expressão dos indivíduos, também intensifica riscos como a exposição indevida, o controle social, a discriminação e as restrições à liberdade individual. Diante desse novo cenário, impõem-se abordagens regulatórias e jurídicas inovadoras, capazes de responder aos desafios complexos decorrentes da presença constante e difusa das tecnologias digitais na vida cotidiana.

Nesse modelo de sociedade da informação, os dados pessoais operam como mediadores essenciais entre o indivíduo e o tecido social, em múltiplas dimensões — econômica, filosófica, jurídica, sociológica e tecnológica — que revelam a profundidade e a complexidade dessa mediação.

Com frequência, destaca-se a dimensão econômica[51]. Os dados pessoais intermediam o acesso a bens, serviços e oportunidades, influenciando desde algoritmos de recomendação de

---

[50] O instigante diálogo entre Bauman e Lyon (2017) evidencia que a vigilância constitui uma dimensão central da modernidade. Embora inicialmente associada à segurança — como nos controles de passaporte em aeroportos —, essa prática estende-se a outras esferas, como a das onipresentes mídias sociais. Nesse contexto, os autores observam que "a cada dia o Google anota nossas buscas, estimulando estratégias de marketing customizadas", revelando como a coleta de dados pessoais se tornou um instrumento sofisticado de monitoramento e influência comportamental.

[51] Sobre a dimensão econômica, popularizou-se a metáfora segundo a qual "os dados são o novo petróleo", atribuída ao matemático britânico Clive Humby, em 2006. Tal comparação, contudo, revela-se inadequada sob diversos aspectos: os dados são infinitamente replicáveis, ao passo que o petróleo é um recurso finito e exaurível; o valor dos dados depende do contexto e da interpretação, e não apenas de sua "extração"; além disso, os dados não se esgotam com o uso — ao contrário, podem gerar valor de forma contínua (Marr, 2018).

compras até decisões de crédito, o que os torna elementos estruturantes da economia digital contemporânea.

Em uma dimensão identitária, os dados pessoais não são meramente registros administrativos; eles expressam aspectos da identidade do sujeito. Nome, gênero, histórico de saúde, preferências e comportamentos digitais compõem uma narrativa sobre quem a pessoa é — ou como é percebida socialmente. Tal representação impacta diretamente a dimensão relacional, uma vez que a forma como os dados são coletados, compartilhados e interpretados condiciona as relações sociais, afetando desde o acesso a serviços até a participação política.

O controle sobre os dados pessoais insere-se, ainda, em uma dimensão política, na medida em que envolve a capacidade do indivíduo de exercer sua autonomia informacional. A gestão desses dados configura-se como um campo de disputa simbólica e normativa, no qual se joga o equilíbrio entre liberdade individual e poder institucional. A crescente assimetria informacional entre cidadãos e grandes plataformas digitais — ou mesmo o Estado — ameaça essa autonomia, comprometendo direitos fundamentais e a própria noção de cidadania digital[52].

Nesse cenário, a proteção de dados pessoais afirma-se como um direito fundamental estruturante, não apenas à salvaguarda da dignidade humana e à promoção da autonomia individual, mas também à própria sustentabilidade da confiança nas dinâmicas sociais, econômicas e políticas da sociedade digital contemporânea.

Em perspectiva global, a matriz normativa da proteção de dados pessoais remonta à Declaração Universal dos Direitos Humanos (DUDH), proclamada em 1948, cujo artigo 12 veda interferências arbitrárias na vida privada, no domicílio e na correspondência. Embora não trate diretamente de dados pessoais nos moldes atuais, a DUDH estabelece os princípios universais de privacidade, honra e reputação que fundamentam as legislações subsequentes (UNICEF, s.d.).

As primeiras legislações especificamente voltadas à proteção de dados pessoais surgiram na década de 1970, em resposta às crescentes preocupações com o uso de tecnologias computacionais para o armazenamento e processamento de informações. O marco inaugural foi a promulgação da lei do Estado de Hesse, na Alemanha, em 1970[53] — considerada a primeira norma específica sobre o tema —, seguida por iniciativas semelhantes em países como Suécia e França. Essas legislações pioneiras refletiam a necessidade de se estabelecer limites jurídicos ao poder informacional do Estado e das corporações, especialmente após os abusos históricos de regimes autoritários.

---

[52] A cidadania digital configura-se como a expressão contemporânea da participação ética, consciente e responsável dos indivíduos no espaço virtual, englobando um conjunto de direitos, deveres e condutas que asseguram sua atuação plena na sociedade digital (Cavalcanti *et al*., 2022).

[53] Em comunicado oficial, a Universidade Goethe Frankfurt am Main reconhece Spiros Simitis como o autor da primeira lei de proteção de dados do mundo, promulgada no estado de Hesse em 1970. Destaca ainda sua atuação como Comissário de Proteção de Dados por 15 anos e sua contribuição decisiva na elaboração da Diretiva Europeia de Proteção de Dados de 1995, consolidando seu papel como figura central na construção do direito à autodeterminação informativa (IDW, 2025).

Bioni e Mendes (2021) observam que, na sequência, houve uma padronização normativa internacional que desempenhou papel estruturante na formação das leis gerais de proteção de dados pessoais, sendo indissociável de sua própria gênese. A atuação de organismos como a OCDE e o Conselho da Europa, por meio da formulação de diretrizes e convenções internacionais desde a década de 1980, estabeleceu fundamentos comuns que favoreceram uma notável convergência regulatória entre os diversos ordenamentos jurídicos, conferindo à proteção de dados um caráter transnacional e sistematizado.

A partir desse movimento inicial, consolidou-se uma agenda internacional voltada à normatização da proteção de dados, culminando na criação de instrumentos jurídicos de grande relevância. Destaca-se, nesse percurso, **a Convenção 108 do Conselho da Europa (1981)**, primeiro tratado internacional juridicamente vinculante sobre proteção de dados pessoais. Posteriormente, a **Diretiva 95/46/CE da União Europeia (1995)**, que estabeleceu um marco regulatório robusto, consolidou os direitos dos titulares e os deveres dos responsáveis pelo tratamento de dados. Esse processo evolutivo culminou no **Regulamento Geral sobre Proteção de Dados (GDPR, 2018),** legislação abrangente e rigorosa, com aplicação direta nos Estados-membros da União Europeia e influência normativa global.

No ordenamento jurídico brasileiro, a proteção de dados pessoais já encontrava amparo normativo, ainda que de forma fragmentada e setorial, desde a promulgação da Constituição Federal de 1988. Nesse marco constitucional, o *habeas data*[54] foi instituído como instrumento para assegurar o direito de acesso e de retificação de informações pessoais constantes de registros ou bancos de dados de entidades governamentais ou de caráter público (art. 5º, LXXII, CF/88), sendo posteriormente regulamentado pela Lei nº 9.507/1997.

Na mesma direção, em setembro de 1990, foi publicado o Código de Defesa do Consumidor (Lei nº 8.078/1990), que introduziu importantes garantias relacionadas à proteção de dados, especialmente no que tange ao tratamento de informações pessoais em cadastros e bancos de dados. O artigo 43 assegura ao consumidor o direito de acesso às informações registradas em seu nome, bem como a possibilidade de correção de dados inexatos, representando um embrião do princípio da autodeterminação informativa.

No contexto da transparência da administração pública, foi sancionada a Lei de Acesso à Informação (Lei nº 12.527/2011). Embora seu objetivo principal seja garantir maior transparência e controle social sobre as ações governamentais, essa norma também contempla dispositivos que resguardam a privacidade dos indivíduos. O artigo 31, por exemplo, estabelece que informações pessoais relativas à intimidade, vida privada, honra e imagem têm acesso restrito, salvo consentimento expresso do titular ou previsão legal.

---

[54] Conforme destacam Arnoldo Wald e Rodrigo Fonseca, a inserção do habeas data na Constituição Federal de 1988 foi impulsionada por um contexto político específico: a existência do Sistema Nacional de Informações (SNI), um extenso banco de dados mantido pelo regime militar (1964–1985), que concentrava informações detalhadas sobre os cidadãos brasileiros. Tal mecanismo de vigilância estatal evidenciou a necessidade de um instrumento jurídico que assegurasse o direito de acesso, retificação e controle sobre os dados pessoais armazenados por órgãos públicos. (Wald; Fonseca, 1998).

Na sequência, foi instituído o Marco Civil da Internet (Lei nº 12.965/2014), que introduziu princípios e garantias fundamentais para o uso da rede mundial de computadores, incluindo a proteção da privacidade e dos dados pessoais. Essa lei estabelece que o tratamento de dados deve observar o consentimento do titular, além de prever a guarda e proteção de registros de acesso. O Decreto nº 8.771/2016, que regulamenta o Marco Civil, detalha medidas de segurança e boas práticas para o tratamento de dados no ambiente digital.

Além das legislações mencionadas, outras normas também contribuíram para oferecer proteção jurídica aos titulares de dados pessoais, ainda que indiretamente. O Código Civil (Lei nº 10.406/2002), por exemplo, protege os direitos da personalidade, incluindo a privacidade. Normas setoriais, como o Código de Ética Médica (Resolução CFM nº 2.217/2018), que disciplina o sigilo médico, também desempenharam papel relevante na proteção de informações sensíveis.

Todavia, o marco normativo fundamental para a assimilação, no ordenamento jurídico brasileiro, de um novo direito de matriz informacional — alinhado aos parâmetros regulatórios internacionalmente consagrados para o tratamento de dados pessoais (Doneda, 2023) — consolidou-se com a Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018.

Importa ressaltar que, embora o direito à proteção de dados pessoais mantenha uma relação intrínseca com o direito à privacidade e com a autodeterminação informativa, esses institutos foram expressamente previstos na LGPD como fundamentos estruturantes da disciplina, conforme dispõe o art. 2º, incisos I e II.

Essa disposição normativa evidencia a autonomia conceitual do direito à proteção de dados, cuja definição mais adequada o caracteriza como um sistema normativo composto por regras e princípios voltados à regulação do tratamento de dados pessoais, em razão de seus impactos potenciais sobre os indivíduos e sobre a ordem social (Corte, 2020).

Sob essa perspectiva ampliada, o direito à proteção de dados pessoais passa a ser compreendido como a consagração de um direito fundamental à normatividade procedimental, isto é, à existência de um arcabouço jurídico deliberadamente construído para autorizar, de forma consciente e coletiva, o tratamento de dados pessoais em razão dos benefícios sociais, econômicos e institucionais que dele podem advir. Tal normatividade, contudo, não se reduz a um aparato técnico ou burocrático: trata-se de um mecanismo estrutural de governança informacional, voltado à contenção dos riscos inerentes à coleta e ao uso massivo de dados, assegurando o equilíbrio entre inovação tecnológica, transparência institucional e a salvaguarda dos direitos fundamentais, com especial destaque para a preservação da dignidade humana e da confiança social nas instituições.

Corte (2020) ressalta que é crucial distinguir a existência de dois tipos de interferência no direito à proteção de dados: a interferência ordinária e aquela que compromete a própria essência do direito. Esta última ocorre quando atos ou omissões desestabilizam a arquitetura

normativa que regula o tratamento de dados pessoais, afetando seus fundamentos estruturais. Esse sistema, concebido como um mecanismo de freios e contrapesos, reflete uma escolha coletiva de permitir o processamento de dados em função de seus benefícios sociais, desde que submetido a regras claras, proporcionais e protetivas dos direitos fundamentais. Quando essa estrutura essencial é violada, a gravidade do ato em si torna-se secundária diante do verdadeiro prejuízo: a erosão da legitimidade e da base normativa que sustenta o próprio direito. Trata-se, portanto, de uma ameaça ao núcleo do direito à proteção de dados e à confiança social que o legitima.

Por outro lado, a interferência ordinária, ou regular, diz respeito a violações ou falhas que, embora possam ser graves em termos concretos, não comprometem a integridade do sistema de proteção de dados. São situações que desafiam aspectos específicos da regulação, como descumprimento de normas, falhas na segurança ou abusos pontuais, mas que podem ser corrigidas no próprio marco jurídico por meio de fiscalização institucional, aplicação de sanções e aprimoramento normativo. Essas interferências não ameaçam a legitimidade democrática do direito à proteção de dados nem o Estado de Direito, pois o sistema continua funcional e capaz de garantir a proteção dos titulares.

A distinção proposta por Corte (2020) evidencia que o direito à proteção de dados não constitui um conjunto isolado de normas, mas sim um ecossistema normativo complexo (Doneda, 2019), cuja essência deve ser preservada para assegurar a confiança, a transparência e a legitimidade no tratamento de dados pessoais na sociedade contemporânea. A violação dessa essência representa um risco de natureza sistêmica e estrutural, ao passo que a interferência regular configura um desafio de ordem operacional e jurídica, passível de enfrentamento sem comprometer os fundamentos do direito.

De fato, a compreensão da proteção de dados como um ecossistema complexo envolve a visão de um conjunto heterogêneo de regras e normas que abrangem desde princípios constitucionais e legais fundamentais até normas infralegais, diretrizes técnicas e procedimentos administrativos. Essa complexa rede normativa, interdependente e articulada, exige uma compreensão sistêmica e integrada para que sua aplicação seja efetiva e coerente com os objetivos de tutela dos direitos fundamentais na sociedade da informação (CGI.br, 2023).

A limitação do direito fundamental à proteção de dados pessoais demanda a observância de critérios estritos de legitimidade constitucional. Conforme destacam Mendes, Rodrigues Junior e Fonseca (2023), tal restrição somente se justifica quando fundada em base jurídica sólida, acompanhada de finalidade clara e específica quanto ao tratamento dos dados. Essa clareza é essencial para aferir o grau de intervenção no direito fundamental em questão. Além disso, a medida deve ser proporcional, adequada e necessária ao fim pretendido, exigindo-se ainda a adoção de mecanismos preventivos mínimos, de natureza procedimental e organizacional, voltados à proteção dos titulares e à mitigação de riscos aos seus direitos da

personalidade. Quanto mais intensa for a restrição imposta, mais robustas devem ser as justificativas e salvaguardas adotadas, sob pena de se institucionalizar intervenções arbitrárias na esfera privada, amparadas em finalidades genéricas ou necessidades coletivas abstratas.

Em essência, a proteção de dados pessoais reflete o compromisso coletivo com uma governança informacional ética e responsável na era digital. Sua legitimidade repousa no respeito ao Estado de Direito e aos princípios democráticos, que asseguram que o processamento de dados seja sempre orientado por normas claras, transparentes e justas. Qualquer ataque à essência desse sistema não representa apenas uma violação a um direito fundamental isolado, mas uma ameaça às bases mais profundas da ordem jurídica e à confiança social que a sustenta. Compreender essa distinção, portanto, é essencial para a preservação e o fortalecimento do direito à proteção de dados como um dos pilares da democracia digital.

3.1 DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

> A despeito do nome de Lei Geral de Proteção de Dados Pessoais – o principal objetivo da LGPD não é proteger dados, mas sim proteger pessoas (Andrade, [s/d]b.).

A Lei nº 13.709/2018 (LGPD) estabelece diretrizes específicas para o tratamento de dados pessoais por entes públicos, reconhecendo as peculiaridades da atuação estatal e a necessidade de compatibilização entre prerrogativas administrativas e os direitos fundamentais dos titulares de dados.

A partir da constatação de que a intensificação da digitalização da sociedade e da economia impulsiona, correlatamente, a transformação digital do Estado, Wimmer (2023) destaca que a atividade de tratamento de dados pessoais dos cidadãos configura-se como componente essencial das funções estatais, constituindo condição indispensável para a realização de suas missões institucionais.

A avaliação crítica das ações de tratamento de dados conduzidas pelo setor público[55] exige uma atenção especial ao compartilhamento e uso secundário de informações pessoais por

[55] O art. 1º da LGPD é expresso quanto à aplicação da lei às pessoas jurídicas de direito público. O parágrafo único do mesmo artigo esclarece que as normas gerais contidas na LGPD "são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios". Já o art. 23, ao regulamentar o tratamento de dados pessoais pelo Poder Público, menciona as "pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ". Este dispositivo, por sua vez, se refere aos "órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público" (ANPD, 2023).

órgãos e entidades vinculadas aos entes federativos — União, Estados, Distrito Federal e Municípios — e aos três Poderes da República: Executivo, Legislativo e Judiciário.

O "uso compartilhado de dados" é instituto definido no art. 5º, XVI, da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), nos seguintes termos:

> [...] comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

No âmbito da Lei Geral de Proteção de Dados Pessoais, o tratamento de dados pessoais pelo Poder Público também compreende a reutilização de informações previamente coletadas, armazenadas e processadas por instituições estatais no exercício de suas funções administrativas, regulatórias, jurisdicionais ou de prestação de serviços públicos.

Essa prática envolve a gestão de dados que, muitas vezes, possuem natureza sensível ou estratégica, exigindo conformidade com os princípios constitucionais da legalidade, finalidade, necessidade, proporcionalidade, segurança, transparência e responsabilização. A análise jurídica dessa atuação estatal demanda a delimitação precisa dos contornos normativos que autorizam ou restringem o uso subsequente de dados pessoais, especialmente quando se trata de finalidades distintas daquelas que motivaram a coleta original.

Sob esse recorte, o grande desafio enfrentado pelo Poder Público consiste em realizar o tratamento de dados pessoais de forma a harmonizar a busca por celeridade e eficiência na implementação de políticas públicas[56] e na prestação de serviços com a observância rigorosa dos direitos fundamentais à privacidade e à proteção de dados (ANPD, 2023), assegurando que a atuação administrativa não comprometa garantias individuais constitucionalmente asseguradas.

No contexto da sociedade digital contemporânea, o Estado figura como um dos principais protagonistas no tratamento de dados pessoais de indivíduos, exercendo essa função desde o instante em que estes adquirem personalidade civil, com o nascimento, até a extinção dessa personalidade, com a morte (Vale; Oliveira, 2025). Nesse cenário, o compartilhamento de dados revela-se como instrumento indispensável à efetivação das funções administrativas ordinárias do Estado, legitimando-se como meio necessário à realização do interesse público.

[56] A ANPD (2023) recomenda que o conceito de política pública seja interpretado amplamente, de modo a abranger qualquer programa ou ação governamental formalmente definido em instrumento oficial.

Conforme destacado por Cardoso (2020), o tratamento de dados pessoais pelo Poder Público possui caráter eminentemente instrumental, significando que os dados coletados e processados constituem ferramentas essenciais para a atuação estatal em benefício dos próprios titulares dessas informações. O exercício da função pública não se dá em benefício próprio do Estado, mas visa atender às necessidades da coletividade. Por essa razão, o uso de dados pessoais deve estar estritamente vinculado à finalidade pública legítima atribuída a cada órgão ou entidade governamental.

Essa concepção instrumental acarreta consequências jurídicas relevantes, especialmente no que diz respeito à exigência de observância rigorosa dos princípios da proporcionalidade e da razoabilidade nas operações de tratamento de dados pessoais. A coleta e o processamento devem restringir-se ao estritamente necessário para o desempenho da função pública específica, vedada a obtenção ou utilização de dados adicionais que não sejam imprescindíveis ao cumprimento das competências legais da Administração. Tal restrição é fundamental para prevenir abusos e assegurar que a tutela da privacidade e da dignidade dos titulares seja respeitada em todas as fases do tratamento.

Dessa forma, a perspectiva instrumental do tratamento de dados impõe que qualquer análise sobre o uso de informações pessoais pelo Poder Público seja orientada por essas premissas, garantindo que o exercício do poder estatal ocorra nos limites constitucionais e legais, com transparência e respeito aos direitos fundamentais. Essa abordagem reforça a necessidade de equilíbrio entre a eficiência administrativa e a proteção dos direitos dos cidadãos, consolidando a proteção de dados pessoais como elemento central da governança pública responsável e democrática.

Em virtude desse papel central na coleta, processamento e compartilhamento de dados pessoais — atividades essenciais à formulação de políticas públicas e ao cumprimento de suas competências institucionais — o Estado ocupa posição de protagonismo no ecossistema informacional contemporâneo. Reconhecendo essa especificidade, a Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece, em seu Capítulo IV (arts. 23 a 32), um regime jurídico próprio[57] para o tratamento de dados pessoais pelo Poder Público, disciplinando suas obrigações, limites e finalidades de forma compatível com os princípios constitucionais da legalidade, finalidade e proporcionalidade.

[57] Cumpre ressaltar que estão excluídas do regime jurídico da LGPD as atividades de tratamento de dados pessoais realizadas pelo Poder Público para fins exclusivamente relacionados à segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, conforme dispõe o art. 4º, inciso III, da Lei nº 13.709/2018.

Uma interpretação adequada do Capítulo IV da LGPD percebe que o tratamento de dados pessoais pelo Poder Público não se limita às bases legais previstas no artigo 7º[58] — ou, no caso de dados sensíveis, às hipóteses específicas delineadas no artigo 11[59] — como ocorre ordinariamente quando os agentes de tratamento são privados. Ao contrário, esse tratamento deve observar, de forma integrada, os critérios adicionais estabelecidos no artigo 23, que introduz exigências específicas para a atuação estatal.

Observa-se, ainda, que o tratamento de dados pelo Poder Público deve ser formalizado, registrado e justificado mediante a indicação clara da base legal aplicável, da finalidade específica e da duração do tratamento. Contudo, o rol das bases legais sofre temperamentos relevantes. Nesse sentido, a dispensa do consentimento do titular é admitida quando o tratamento decorre de previsão legal, regulamentos, contratos, convênios ou instrumentos congêneres, quando forem rigorosamente observados os princípios norteadores da LGPD, especialmente os da finalidade, necessidade, transparência e segurança.

O Art. 23 da LGPD impõe ao Poder Público a obrigação de publicar informações claras e atualizadas sobre os procedimentos de tratamento de dados, preferencialmente em seus sítios eletrônicos, garantindo o livre acesso e a transparência. Além disso, é obrigatória a designação de um encarregado pelo tratamento de dados pessoais, que atuará como canal de comunicação entre o controlador, os titulares e a Agência Nacional de Proteção de Dados.

A atuação da ANPD é central na regulação do setor público, podendo realizar auditorias, solicitar relatórios de impacto à proteção de dados pessoais e recomendar boas práticas. A agência detém competência exclusiva para aplicar sanções administrativas, que incluem advertência, publicização da infração, bloqueio ou eliminação dos dados, sem prejuízo das

---

[58] Referem-se por bases legais às hipóteses autorizativas que legitimam o tratamento de dados pessoais, conforme elencadas no art. 7º da Lei nº 13.709/2018 — LGPD. São elas: o consentimento do titular; o cumprimento de obrigação legal ou regulatória pelo controlador; a execução de políticas públicas pela administração pública; a realização de estudos por órgão de pesquisa, com anonimização sempre que possível; a execução de contrato ou de procedimentos preliminares a pedido do titular; o exercício regular de direitos em processo judicial, administrativo ou arbitral; a proteção da vida ou da incolumidade física do titular ou de terceiro; a tutela da saúde, em procedimentos realizados por profissionais ou serviços de saúde; a proteção do crédito; e os interesses legítimos do controlador ou de terceiro, desde que não prevaleçam os direitos e liberdades fundamentais do titular.

[59] Nos termos do art. 11 da Lei nº 13.709/2018, o tratamento de dados pessoais sensíveis — aqueles que dizem respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico — somente poderá ocorrer mediante o consentimento específico e destacado do titular, ou, sem consentimento, nas hipóteses em que for indispensável para: *(i)* cumprimento de obrigação legal ou regulatória pelo controlador; *(ii)* execução de políticas públicas pela administração pública; *(iii)* realização de estudos por órgão de pesquisa, com anonimização sempre que possível; *(iv)* exercício regular de direitos, inclusive em contrato e em processos judiciais, administrativos ou arbitrais; *(v)* proteção da vida ou da incolumidade física do titular ou de terceiro; (vi) tutela da saúde, exclusivamente por profissionais ou serviços de saúde ou autoridade sanitária; e (vii) prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação em sistemas eletrônicos, desde que não prevaleçam os direitos e liberdades fundamentais do titular.

sanções previstas em outras normas, como a Lei de Improbidade Administrativa e o Estatuto do Servidor Público.

Isso significa que a atividade estatal de tratamento de dados pessoais exige uma leitura que transcenda a aplicação literal das bases legais, demandando uma hermenêutica sistemática e finalística que incorpore os parâmetros normativos próprios da atuação pública. A LGPD, nesse contexto, não apenas especifica as condições sob as quais órgãos e entidades públicas podem tratar dados pessoais, mas também opera como um verdadeiro mecanismo de conformação jurídica, orientando a atuação estatal segundo os princípios da legalidade, finalidade, necessidade e transparência.

Ademais, o artigo 23 da LGPD não se limita a complementar os fundamentos legais do tratamento de dados, mas impõe balizas normativas que condicionam a legitimidade da atuação pública. Exige-se, por exemplo, que o tratamento esteja vinculado à execução de políticas públicas previstas em leis e regulamentos, ao exercício de competências legais ou à prestação de serviços públicos. Essa vinculação funcional é essencial para assegurar que o uso de dados pessoais pelo Estado ocorra com finalidade legítima, proporcionalidade e respeito aos direitos fundamentais dos titulares, especialmente no que tange à autodeterminação informativa e à proteção da privacidade.

A harmonização entre o exercício das funções estatais e a salvaguarda dos direitos fundamentais à privacidade e à proteção de dados impõe ao Poder Público uma conduta estritamente alinhada aos ditames legais e aos princípios consagrados na LGPD. Tal exigência se torna ainda mais premente no contexto da implementação de políticas públicas e do intercâmbio de dados entre os diversos entes federativos, demandando atuação transparente, justificada e juridicamente fundamentada (ANPD, 2023).

Importa, contudo, ressaltar que o compartilhamento de dados pessoais pelo Poder Público é disciplinado pela Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente em seus artigos 25 e 26, que estabelecem os parâmetros necessários para assegurar a legalidade, a transparência e a segurança dessas operações no âmbito estatal. O artigo 25 impõe o dever de manter os dados pessoais em formato estruturado e interoperável, de modo a viabilizar a execução eficiente de políticas públicas, a prestação de serviços, a descentralização da atividade administrativa e o acesso à informação pela sociedade. Cardoso (2020) pontua que essa previsão reforça o caráter instrumental do tratamento de dados pelo Estado, ao assegurar que os dados coletados sejam úteis e adequados à consecução de finalidades públicas legítimas.

O artigo 26 da LGPD complementa o arcabouço normativo aplicável ao setor público ao permitir o uso compartilhado de dados pessoais entre órgãos e entidades públicas, desde que

estritamente vinculado a finalidades específicas relacionadas à execução de políticas públicas ou decorrentes de atribuição legal. Tal compartilhamento não pode ocorrer indiscriminadamente, devendo observar rigorosamente os princípios fundamentais da proteção de dados previstos no artigo 6º da LGPD, como a finalidade, a necessidade, a transparência, a segurança e a responsabilização. Dessa forma, o uso compartilhado deve respeitar os limites legais e constitucionais, garantindo que os dados pessoais sejam tratados de maneira proporcional e razoável, prevenindo excessos e abusos que comprometam os direitos dos titulares.

Por vezes, o compartilhamento de dados pessoais entre entidades públicas, ainda que de forma excepcional, pode demandar a intermediação de entes privados, especialmente em contextos de execução descentralizada de políticas públicas. Nos termos do art. 26, § 1º, da LGPD, tal transferência é permitida apenas nas restritas hipóteses expressamente previstas, como: *(i)* execução descentralizada de atividade pública, exclusivamente para finalidade específica e determinada; *(ii)* quando os dados forem acessíveis publicamente, observadas as disposições da LGPD; *(iii)* mediante previsão legal ou instrumento contratual, convênio ou congênere; ou *(iv)* quando necessária à prevenção de fraudes, à proteção da integridade do titular ou à garantia da segurança pública, vedado o tratamento para outras finalidades.

Em síntese, o compartilhamento de dados pessoais entre órgãos públicos não constitui prática vedada; ao contrário, é expressamente previsto e autorizado pela LGPD, desde que estritamente vinculado a finalidades públicas legítimas e fundamentado em bases legais específicas. A transparência emerge, nesse contexto, como princípio estruturante dessa dinâmica: os entes públicos responsáveis pela transferência de dados devem explicitar, de forma clara e acessível, quais informações estão sendo compartilhadas, com quais destinatários e para quais propósitos. Por sua vez, os órgãos receptores devem justificar o acesso com base na execução de atividades ou políticas públicas específicas e previamente definidas, observando os deveres de prestação de contas e segurança da informação.

Sob essa ótica, o compartilhamento de dados pessoais pelo Poder Público configura-se como ato administrativo[60] e, como tal, deve observar rigorosamente os princípios constitucionais e administrativos aplicáveis, notadamente os princípios da legalidade,

[60] Ainda que, isoladamente considerado, determinado compartilhamento de dados pessoais não produza efeitos jurídicos imediatos, não se trata de ato material de simples execução, segundo a classificação doutrinária de Maria Sylvia Zanella Di Pietro (2012). Conforme leciona a autora, trata-se de ato preparatório ou acessório ao ato principal, que, embora não autônomo, integra o procedimento administrativo ou constitui condição de eficácia do ato principal, razão pela qual não pode ser excluído da noção de ato administrativo.

impessoalidade, moralidade, publicidade e eficiência, insculpidos no *caput* do artigo 37 da Constituição Federal.

O ato administrativo, entendido como a manifestação unilateral de vontade da Administração Pública com efeitos jurídicos imediatos, exige a instauração de processo administrativo, análise técnica e jurídica, decisão fundamentada e registro detalhado, seja por meio de contrato, convênio ou ato normativo interno, submetendo-se, ainda, aos mecanismos de controle e fiscalização[61].

Em consonância com a Lei Geral de Proteção de Dados Pessoais — LGPD e com as orientações da Agência Nacional de Proteção de Dados — ANPD (2023), o compartilhamento de dados pessoais pelo Poder Público reafirma sua natureza de ato administrativo, uma vez que demanda formalização e registro[62], decisão motivada com indicação clara do objeto e da finalidade[63], além da observância aos princípios da transparência e da responsabilização[64].

A compreensão dessa natureza jurídica é essencial para assegurar que o tratamento de dados pessoais — que envolve direitos fundamentais dos titulares — seja conduzido com a devida formalidade, motivação e controle jurídico, em consonância com o Estado Democrático de Direito.

Assim, esse compartilhamento deve estar vinculado a uma finalidade pública específica e compatível com a finalidade original da coleta, garantindo transparência e a adoção de medidas técnicas e administrativas aptas à prevenção de incidentes de segurança. Essa estrutura normativa confirma a evidência de que o compartilhamento de dados pessoais pelo Poder Público não se reduz a uma mera execução material, mas constitui decisão administrativa complexa, sujeita a controle de legalidade, motivação e publicidade — elementos imprescindíveis à proteção dos direitos dos titulares e à legitimidade da atuação estatal.

Portanto, o reconhecimento do compartilhamento de dados pessoais como ato administrativo reforça a necessidade de rigor técnico-jurídico e transparência, alinhando-se aos princípios constitucionais e legais que regem a Administração Pública e a proteção de dados pessoais no Brasil.

Impende ainda ressaltar que, em virtude de sua natureza jurídica, o tratamento de dados pessoais pelo Poder Público configura-se como um ato administrativo sujeito a controle jurídico

---

[61] Nesse sentido: Meirelles, 1988; Di Pietro, 2012.

[62] A ANPD (2023) recomenda a instauração de processo administrativo, do qual constem os documentos e as informações pertinentes, incluindo análise técnica e jurídica, conforme o caso, que exponham a motivação para a realização do compartilhamento e a sua aderência à legislação em vigor, bem como, que o ato formal, a exemplo de contratos, convênios ou instrumentos congêneres firmados entre as partes.

[63] Art. 26 da LGPD.

[64] Art. 6º, VI da LGPD.

em múltiplos níveis. Internamente, esse controle se dá por meio de mecanismos de governança e fiscalização administrativa, enquanto que externamente está submetido ao controle judicial e à supervisão da Agência Nacional de Proteção de Dados — ANPD. Esta última, na qualidade de órgão central para a interpretação da Lei Geral de Proteção de Dados — LGPD e responsável pelo estabelecimento de normas e diretrizes para sua implementação (art. 55-K da LGPD), exerce papel fundamental na fiscalização do cumprimento da legislação pelo setor público. A atuação da ANPD assegura que o tratamento e o compartilhamento de dados pessoais respeitem integralmente os direitos fundamentais dos titulares, em especial no que tange à proteção da privacidade e à salvaguarda dos dados pessoais, garantindo, assim, a legitimidade e a confiança no uso dessas informações pela administração pública.

Além dos princípios administrativos de matriz constitucional, o compartilhamento deve também se submeter às disposições específicas da Lei Geral de Proteção de Dados Pessoais — LGPD. Isso implica que a transferência de dados entre órgãos e entidades públicas deve estar vinculada a finalidades legítimas, como a execução de políticas públicas e o cumprimento de atribuições legais, conforme previsto no art. 26 da LGPD. E ainda, essa atividade deve ser pautada pela boa-fé e pelos princípios expressamente elencados no art. 6º da referida norma: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Todo o conjunto de regras obrigatórias para os agentes de tratamento, incluindo o Poder Público, conforme estabelecido no Guia Orientativo sobre o Tratamento de Dados Pessoais pelo Poder Público (ANPD, 2023), tem por objetivo regulamentar o tratamento de dados pessoais de modo a garantir o livre desenvolvimento da personalidade e a dignidade da pessoa humana.

Essa perspectiva coaduna-se com a concepção teórica de Lorenzo Dalla Corte (2020), que compreende a teoria do direito à proteção de dados como um "direito a uma regra" — aqui interpretado como um **direito à normatividade procedimental** — conduzindo à conclusão de que o tratamento de dados pessoais pelo Poder Público deve ser realizado de modo a respeitar o núcleo essencial desse direito fundamental.

Isso significa que, embora o Estado possa — e deva — tratar dados pessoais para fins legítimos, essa atuação está condicionada à observância de um conjunto mínimo inderrogável de garantias normativas que assegurem a transparência, a previsibilidade, o controle e a proteção efetiva dos direitos dos titulares. A violação desse núcleo essencial comprometeria não apenas a legitimidade do tratamento, mas também a confiança social no exercício do poder estatal, configurando uma interferência estrutural no direito à proteção de dados.

A seguir essa linha de raciocínio, compreende-se que o compartilhamento de dados pelo Poder Público não pode ser visto como um ato meramente técnico ou burocrático, mas como um ato administrativo qualificado, que deve ser praticado com observância rigorosa das normas legais e princípios constitucionais, sujeito a controle judicial e administrativo. A responsabilidade do Estado, nesse cenário, é dupla: garantir a efetividade das políticas públicas e, simultaneamente, proteger os direitos fundamentais relacionados aos dados pessoais, assegurando que o tratamento seja legítimo, transparente e proporcional.

Em suma, a Lei Geral de Proteção de Dados Pessoais, ao disciplinar o tratamento de dados pessoais pelo Poder Público, materializa a teoria de Dalla Corte (2020) ao estruturar um sistema normativo complexo que equilibra o interesse público com a salvaguarda dos direitos individuais. Consolida-se, assim, a proteção de dados como um direito fundamental autônomo e de natureza procedimental, cuja preservação é condição indispensável para a realização da democracia e da dignidade da pessoa na sociedade digital contemporânea.

Nessa perspectiva, o compartilhamento de dados pessoais pelo Poder Público, nos moldes previstos pela LGPD, deve ser compreendido como uma atividade administrativa complexa, inserida em um sistema normativo multifacetado, que articula os princípios constitucionais da administração pública com as regras específicas da legislação de proteção de dados. Essa integração é essencial para assegurar que o tratamento de dados pessoais seja legítimo, transparente, proporcional e eficiente, preservando o núcleo essencial do direito fundamental à proteção de dados e fortalecendo a confiança da sociedade nas instituições públicas.

Cumpre ainda ressaltar que a Agência Nacional de Proteção de Dados, no intuito de auxiliar entidades e órgãos públicos nas atividades de adequação e de implementação da LGPD, estabeleceu no mencionado Guia Orientativo Tratamento de dados pessoais pelo Poder Público (ANPD, 2023) os principais requisitos que devem ser observados nos processos de compartilhamento de dados pessoais pelo Poder Público, visando assegurar a conformidade com a Lei Geral de Proteção de Dados (LGPD) e a proteção dos direitos fundamentais dos titulares.

Em primeiro lugar, destaca-se a necessidade de formalização e registro do compartilhamento, que deve ser precedido de processo administrativo detalhado, contendo análise técnica e jurídica que justifique a operação, bem como sua aderência à legislação vigente. Essa formalização deve se concretizar em atos formais, como contratos, convênios ou instrumentos congêneres, garantindo transparência e responsabilidade.

Quanto ao objeto e finalidade, o Guia orienta que os dados pessoais compartilhados sejam indicados de forma objetiva e restrita ao estritamente necessário para o cumprimento das finalidades específicas, que devem ser claramente definidas, vinculadas a políticas públicas ou atribuições legais. Ademais, é imprescindível avaliar a compatibilidade entre a finalidade original da coleta e a finalidade do compartilhamento, respeitando o princípio da necessidade previsto na LGPD.

Outro requisito fundamental é a definição clara da base legal que legitima o compartilhamento, conforme os artigos 7º e 11 da LGPD, devendo o ato autorizativo explicitar essa fundamentação jurídica, como a execução de políticas públicas específicas. A duração do tratamento deve ser limitada ao período necessário para atingir a finalidade estabelecida, evitando a retenção indevida dos dados.

O guia também enfatiza a importância da transparência e da observância dos direitos dos titulares, recomendando que estes sejam informados sobre o compartilhamento, suas finalidades e os meios para exercer seus direitos, fortalecendo a confiança e o controle social. No âmbito da prevenção e segurança, são exigidas medidas técnicas e administrativas robustas para proteger os dados contra acessos indevidos, vazamentos e usos indevidos, incluindo a adoção preferencial de técnicas como pseudonimização e anonimização quando possível.

Por fim, o documento ressalta a necessidade de observância de outros requisitos, como a vedação ao compartilhamento indiscriminado, a necessidade de avaliar riscos e impactos, e a garantia de governança adequada, com mecanismos de controle e responsabilização. Essas diretrizes, conforme sistematizadas pela ANPD, visam orientar a atuação estatal de forma compatível com os princípios da LGPD.

3.2 LIMITES AO USO SECUNDÁRIO DE DADOS PESSOAIS PELO PODER PÚBLICO À LUZ DA CONSTITUIÇÃO DA REPÚBLICA

> Talvez o mais impressionante sobre o direito à privacidade é que ninguém parece ter uma ideia muito clara do que ele é (Thomson *apud* Solove, 2017).

Em consonância com a doutrina de Sarlet (2023), reconhece-se que o direito fundamental à proteção de dados pessoais, embora dotado de elevada estatura normativa, não se reveste de caráter absoluto. Está sujeito a restrições legítimas, as quais, contudo, devem observar os denominados “limites aos limites” dos direitos fundamentais — mecanismos de contenção que operam como garantias contra excessos e distorções interpretativas. Dentre os

freios constitucionais, destacam-se a exigência de reserva legal simples, a observância do princípio da proporcionalidade e a intangibilidade do núcleo essencial do direito.

Esse núcleo essencial do direito à proteção de dados pessoais transcende a tradicional vinculação à esfera da privacidade. Conforme observou Doneda (2021), a disciplina de proteção de dados pessoais se origina na necessidade de funcionalização da proteção da privacidade, consolidando-se, assim, a percepção de que se cuida de um direito fundamental de natureza processual e regulatória, voltado à tutela da autodeterminação informacional e à conformação jurídica das práticas de tratamento, tanto no âmbito público quanto no privado.

De maneira elucidativa, Andrade (s/d) distingue a privacidade como um conceito de natureza subjetiva[65], ancorado na esfera individual, ao passo que a proteção de dados pessoais se configura como uma noção objetiva, voltada à salvaguarda de interesses coletivos. Embora distintos em sua essência, tais conceitos não se excluem; ao contrário, revelam-se complementarmente indispensáveis à efetivação dos direitos fundamentais à liberdade, à privacidade e ao livre desenvolvimento da personalidade. A conjugação desses institutos, sempre que possível, fortalece o arcabouço normativo voltado à dignidade da pessoa humana na sociedade da informação.

E a correta compreensão dessa desvinculação é de suma importância, posto que a confusão conceitual entre proteção de dados pessoais e privacidade pode gerar sérios desvirtuamentos, como por exemplo, quando o pretexto genérico da "proteção de dados" é indevidamente invocado como subterfúgio para restringir o acesso a informações públicas de interesse coletivo.

Essa problemática foi evidenciada pelo Acórdão 506/2025 do Tribunal de Contas da União — TCU, que analisou mais de 580 mil pedidos de informação feitos a órgãos públicos, entre 2019 e 2023, e constatou que 30,8% foram equivocadamente classificados como "restritos" sob a justificativa genérica de observância da LGPD, sem a devida fundamentação específica exigida pela legislação. A partir dessa constatação, Bruno Dantas (2025) destacou o necessário equilíbrio da relação entre privacidade e transparência: de um lado, a tutela dos dados pessoais constitui expressão dos direitos fundamentais da personalidade; de outro, a publicidade dos atos governamentais é indispensável para evitar abusos.

Com base na doutrina de Corte (2020), compreendemos que a mencionada expressão dos direitos fundamentais da personalidade se dá em uma dimensão coletiva e em caráter procedimental, posto que, na precisa definição de Andrade (s.d.), a proteção de dados pessoais representa a dimensão positiva que assegura e estrutura a liberdade negativa da privacidade.

---

[65] No julgamento da Ação Direta de Inconstitucionalidade nº 6.389 (Caso IBGE), o Ministro Gilmar Mendes reconheceu a existência de um "devido processo informacional" (*informational due process privacy right*) como corolário da dimensão subjetiva do direito fundamental à proteção de dados pessoais, voltado a conferir ao indivíduo o direito de evitar exposições de seus dados sem possibilidades mínimas de controle, sobretudo em relação a práticas de tratamento de dados capazes de sujeitar o indivíduo a julgamentos preditivos e peremptórios.

Nesse mesmo sentido e direção, Danilo Doneda (2021) ressaltou que, no âmbito da proteção de dados pessoais, a tutela jurídica não se limita à salvaguarda da privacidade, mas visa, de forma mais abrangente, à salvaguarda da pessoa humana frente às múltiplas formas contemporâneas de controle social, tecnológico e discriminatório. Trata-se de assegurar a integridade de dimensões essenciais da liberdade individual, promovendo um ambiente normativo que garanta a autodeterminação informacional e a dignidade da pessoa humana em sua plenitude.

A reflexão sobre o direito fundamental à proteção de dados pessoais, especialmente no contexto da atuação do Poder Público, ganha densidade teórica quando se considera a formulação proposta por Laura Schertel Mendes (2014), que concebe esse direito em uma dupla dimensão jurídica que revela tanto sua natureza defensiva quanto sua função promocional. De um lado, configura-se como liberdade negativa, assegurando ao indivíduo um espaço de autonomia informacional imune à intervenção arbitrária do Estado — trata-se da dimensão subjetiva do direito, que opera como limite ao poder público. De outro lado, impõe-se ao Estado um dever positivo de proteção, exigindo a implementação de políticas públicas, estruturas normativas e mecanismos institucionais que garantam o exercício efetivo desse direito — expressão de sua dimensão objetiva.

Essa compreensão dual, conforme destacam Mendes, Rodrigues Junior e Fonseca (2023), é essencial para consolidar a proteção de dados como um pilar da ordem constitucional contemporânea, especialmente em contextos marcados pela intensificação do tratamento automatizado de informações pessoais. A concepção assim amplia o alcance do direito à proteção de dados, ao vinculá-lo não apenas à ideia de privacidade, mas também à liberdade e à dignidade da pessoa humana, exigindo do Estado tanto abstenções, quanto ações positivas para assegurar a transparência, a segurança e a governança dos dados sob sua custódia.

Assim, à luz da dogmática constitucional contemporânea, é imperioso reconhecer que o direito fundamental à proteção de dados pessoais — consagrado expressamente no ordenamento jurídico brasileiro por meio da Emenda Constitucional nº 115/2022 — não se apresenta como um direito absoluto, tampouco pode ser objeto de restrições arbitrárias ou desproporcionais. A atuação normativa sobre esse direito deve ser cuidadosamente distinguida entre a legítima conformação normativa e a restrição inconstitucional. A configuração ocorre quando o legislador, no exercício de sua competência, estabelece parâmetros técnicos e procedimentais que viabilizam o exercício do direito, sem comprometer sua substância. Já a restrição, por sua vez, implica limitação do âmbito de proteção do direito e, por isso, deve submeter-se a um controle rigoroso de constitucionalidade.

No caso específico da proteção de dados pessoais, qualquer medida restritiva — seja por meio de legislação infraconstitucional, seja por atos administrativos — deve respeitar, intransigentemente, os limites impostos pelo núcleo essencial do direito e os critérios da proporcionalidade. O núcleo essencial compreende, nesse contexto, a garantia da

autodeterminação informativa, a transparência no tratamento de dados, a finalidade legítima e a segurança da informação. A supressão ou desfiguração desses elementos, sob o pretexto de regulamentação, configura violação direta ao núcleo essencial do direito fundamental e, por consequência, à própria Constituição e compromete a própria dignidade da pessoa humana, fundamento do Estado Democrático de Direito.

Além disso, a proporcionalidade, em sua tríplice dimensão — adequação, necessidade e proporcionalidade em sentido estrito —, impõe-se como critério hermenêutico e normativo para a aferição da legitimidade de qualquer restrição. Assim, uma norma que autorize o tratamento de dados pessoais deve ser adequada ao fim constitucional que se propõe a atingir, necessária na ausência de meios menos gravosos, e proporcional em sentido estrito, de modo que o sacrifício imposto ao titular dos dados não seja desmedido em relação ao benefício público ou coletivo almejado.

Em síntese, qualquer intervenção normativa que ultrapasse os contornos da configuração legítima e adentre o campo da restrição sem observar os limites do núcleo essencial e os parâmetros da proporcionalidade será, de forma inequívoca, materialmente inconstitucional. No âmbito da proteção de dados pessoais, isso significa que o Estado não pode instrumentalizar o tratamento de informações capazes de identificar os cidadãos como meio de controle social, vigilância indevida ou discriminação, sob pena de subverter os fundamentos constitucionais da liberdade, da privacidade e da dignidade humana.

4 REFLEXÕES NECESSÁRIAS

A visibilidade é uma armadilha (Foucault, 1987).

Ao examinar a tramitação legislativa da Lei Geral de Proteção de Dados Pessoais, Lucas Borges de Carvalho (2023) destaca o veto ao art. 28, que previa a obrigação de transparência ao determinar que "a comunicação ou o uso compartilhado de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade, nos termos do inciso I do caput do art. 23 desta Lei". O autor ressalta que esse veto se fundamentou no argumento de que a "publicidade irrestrita" prevista poderia tornar inviável o exercício regular de atividades públicas essenciais, como fiscalização, controle e polícia administrativa (Brasil, 2018).

É preciso, contudo, ressaltar que a opacidade no tratamento de dados pessoais é juridicamente inadmissível, sobretudo considerando que o compartilhamento de dados pelo Poder Público deve se restringir à finalidade legítima de execução de políticas públicas e ao cumprimento de competências legais, conforme estabelece a Lei Geral de Proteção de Dados Pessoais (LGPD). Em razão da prevalência do interesse coletivo, impõe-se criar instrumentos normativos e operacionais que assegurem a efetividade dos direitos dos titulares, promovam a transparência institucional e viabilizem o controle social sobre as práticas de tratamento de dados realizadas por entes estatais.

Desse modo, o compartilhamento deve observar os princípios basilares da proteção de dados, entre eles finalidade, necessidade, transparência e segurança, vedando a transferência indiscriminada a entes privados, evidenciando a importância dos contratos, convênios e mecanismos formais para assegurar controle e responsabilidade jurídica no uso compartilhado.

Frente a esse cenário normativo e institucional, marcado por vetos legislativos que fragilizam a transparência e por exigências legais que delimitam o compartilhamento de dados à estrita finalidade pública, revela-se pertinente a reflexão crítica sobre os contornos e implicações dessa prática no contexto contemporâneo. A análise deve considerar, sobretudo, os desafios impostos pela tecnovigilância e pelo crescente poder informacional do Estado, bem como deve também ponderar a respeito do necessário equilíbrio entre a eficiência administrativa e a salvaguarda dos direitos fundamentais à privacidade e à proteção de dados pessoais.

O fenômeno do tecnovigilantismo (Ribeiro, 2024) refere-se ao uso crescente de tecnologias digitais para monitoramento e fiscalização das atividades públicas, trazendo ganhos potenciais de eficiência, transparência e controle social. Todavia, a adoção dessas tecnologias

revela desafios éticos e jurídicos ao potencializar formas de vigilância estatal e perigos à privacidade dos cidadãos, exigindo a observância dos princípios de proporcionalidade, razoabilidade e proteção contra abusos.

O poder informacional do Estado pode ser compreendido como a sua capacidade institucional de estruturar e mobilizar fluxos de dados e informações estratégicas com vistas à conformação de condutas, à regulação social e ao exercício da autoridade pública. Essa forma de poder, que se consolida na era digital, articula mecanismos de coleta, processamento, difusão e uso de informações como instrumentos de governança e influência. Nas palavras de Laura Schertel Mendes (2022), trata-se do "poder oriundo do tratamento de informações e do conhecimento gerado a partir delas", evidenciando a centralidade da informação como vetor de transformação do modelo estatal e como fundamento para novas formas de controle e atuação administrativa.

Bioni e Zanatta (2020) destacam que o poder informacional do Estado não é um fenômeno exclusivo da era digital, mas que sua centralidade foi significativamente ampliada pela convergência entre inovações tecnológicas e processos sociais como a datificação. Esse processo, caracterizado pela transformação de aspectos da vida social em dados quantificáveis, intensifica a capacidade estatal de monitoramento, previsão e intervenção, ampliando sua influência sobre a dinâmica contemporânea da sociedade e da economia.

Esse poder se estrutura sobre o controle dos fluxos informacionais e sobre o uso sistemático da informação para conformar condutas, orientar decisões políticas, legitimar práticas administrativas e consolidar a confiança na gestão estatal. Trata-se de uma forma de poder que articula dimensões coercitivas e persuasivas, representando uma inflexão paradigmática no exercício da autoridade estatal na era digital. A esse respeito, Ribeiro (2012) observa que a transição do modelo burocrático tradicional para um Estado informacional implica uma reconfiguração das estruturas de autoridade, agora assentadas na gestão estratégica da informação e na adoção de políticas de inteligência voltadas ao domínio dos fluxos informacionais.

Essa transformação não apenas redefine o papel do Estado, mas também impõe novos desafios normativos e institucionais, sobretudo no que se refere à proteção de dados pessoais, à transparência e à responsabilização. O discurso da eficiência e da inovação tecnológica, embora legítimo, não pode obscurecer a necessidade de salvaguardas jurídicas robustas que limitem o poder informacional do Estado e garantam os direitos fundamentais dos cidadãos.

O poder informacional do Estado configura-se como legítimo quando orientado à promoção do interesse público, à eficiência administrativa e à proteção dos direitos dos

cidadãos. No entanto, quando esse poder se converte em tecnovigilância — isto é, em práticas sistemáticas de monitoramento, coleta massiva de dados e controle social por meio de tecnologias digitais — ele pode ultrapassar os limites da legalidade e da proporcionalidade, configurando uma disfunção institucional.

O avançar dessa reflexão conduz ao debate sobre o *trade-off* entre o princípio constitucional da eficiência na administração pública e a proteção de dados pessoais. Aponta-se que a suposta oposição entre eficiência e proteção é, muitas vezes, um falso dilema, visto que a proteção dos dados pessoais é essencial para conferir legitimidade, transparência e controle democrático, além de evitar desvios de finalidade, discriminação e abusos tecnológicos (Vaz; Ângelis, 2021). Portanto, a eficácia da administração pública depende de um equilíbrio jurídico rigoroso que não sacrifique direitos fundamentais em nome da eficácia.

4.1 UMA REFLEXÃO SOBRE O PODER INFORMACIONAL DO ESTADO.

> Oportuno lembrar que a efetividade do direito fundamental à proteção de dados pessoais é incompatível com medidas que visam ou oportunizem o tratamento indiscriminado de dados pessoais pelos órgãos estatais (Sarlet; Sarlet, 2023).

Na contemporaneidade, a utilização integrada e interoperável de grandes volumes de dados configura-se como elemento fundamental para a entrega eficiente de serviços públicos e para a formulação de políticas públicas eficazes. Tal prática representa um instrumento estratégico de governança, segurança e desenvolvimento, sendo essencial para a modernização do Estado e para a promoção do interesse coletivo. Nesse contexto, o Estado assume a condição de um ator informacional, cuja capacidade de coletar, processar e utilizar dados confere-lhe um poder singular, que transcende as formas tradicionais de exercício da autoridade estatal.

Inserida no campo das ciências sociais aplicadas, esta investigação demanda a reflexão sobre o conceito de poder, elemento estruturante para a análise das dinâmicas sociais e institucionais relacionadas ao poder informacional estatal. À luz da metáfora proposta por Bertrand Russell[66], o poder constitui um eixo teórico e analítico central para as ciências sociais, assim como a energia é princípio fundamental para a física, sendo indispensável para interpretar as relações e transformações sociais que permeiam o objeto deste estudo.

Conforme destacado por Frazão, Carvalho e Milanez (2022), o poder derivado dos dados e da informação possui natureza marcadamente plástica e dinâmica, o que o torna

[66] Russel *apud* Silveira, 2000.

suscetível a múltiplas formas de manifestação e instrumentalização. Os autores reforçam essa perspectiva ao citar Carissa Véliz, que, assim como Bertrand Russell, recorre à analogia com a energia para ilustrar a maleabilidade dos dados, ressaltando sua capacidade de conversão entre diferentes formas de poder. Essa plasticidade explica a estreita correlação entre o poder informacional e os domínios econômico, político e social, evidenciando que o controle e a manipulação de dados pessoais transcendem a esfera técnica, constituindo-se como vetor estratégico de influência e dominação nas sociedades contemporâneas.

Embora a análise exaustiva das múltiplas manifestações do poder enquanto fenômeno social extrapole os limites desta pesquisa, é oportuno recorrer às ideias de Alvin Toffler, que destaca o conhecimento e a informação como os novos recursos estratégicos e a forma mais poderosa de poder. Segundo Toffler (1991), o poder se manifesta principalmente por meio da violência, da riqueza e do conhecimento, sendo este último o mais sutil e crescente, capaz de influenciar decisões e reconfigurar as relações de poder por meio do que denomina "*powershift*" — uma mudança no equilíbrio de poder em que o conhecimento supera a força física e o capital econômico.

A partir dessa perspectiva, o poder informacional do Estado emerge como uma nova dimensão do poder estatal, oriunda do tratamento de informações e do conhecimento gerado a partir delas (Mendes, 2022). Trata-se da capacidade estatal de coletar, processar, armazenar, controlar e utilizar informações como forma de exercer poder político, social e econômico, com impactos diretos na organização e funcionamento das instituições públicas.

A Lei Geral de Proteção de Dados Pessoais (LGPD) reporta-se a vinte espécies de operações para caracterizar o tratamento de dados[67]. Todavia, para fins desta análise, o poder informacional estatal pode ser compreendido em três modos principais: a coleta de dados — que abrange censos, registros civis, dados fiscais, informações de saúde, educação e segurança pública; o processamento e análise — que envolve o uso de *big data*, inteligência artificial e algoritmos para transformar dados brutos em conhecimentos estratégicos; e o uso e disseminação — que consiste na aplicação efetiva dessas informações na formulação de políticas públicas, prevenção de crimes e comunicação institucional, entre outras finalidades.

[67] Lei nº 13.709/2018:
"Art. 5º Para os fins desta Lei, considera-se:
[...]
X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração"

Inúmeros benefícios decorrentes do poder informacional estatal são amplamente divulgados. Por exemplo, segundo notícia publicada pela Agência Gov (Brasil, 2024), o compartilhamento de dados via plataforma "Conecta GOV.BR" gerou uma economia de R$ 2,41 bilhões para a administração pública e cidadãos entre janeiro e outubro de 2024. Destaca-se a Plataforma de Governança Territorial do Instituto Nacional de Colonização e Reforma Agrária (Incra), que utiliza bases do CPF e CNPJ para validação automática de dados, facilitando serviços como a regularização fundiária. Similarmente, o Ministério da Saúde informa que a Rede Nacional de Dados em Saúde (RNDS), principal rede de interoperabilidade do SUS, permite o acesso ao histórico clínico do paciente em tempo real, evitando exames repetidos e promovendo um cuidado mais ágil e qualificado (Brasil, [2025]).

Esses avanços indicam uma redefinição do Estado, que se afasta do modelo burocrático analógico para assumir, sob o paradigma digital, o papel de gestor de fluxos informacionais. Contudo, essa transformação traz consigo riscos e desafios significativos. A coleta massiva de dados pode comprometer a privacidade dos cidadãos, especialmente quando realizada sem consentimento ou transparência adequados. A centralização de informações em grandes bases pode ensejar usos indevidos, como vigilância política, perseguição de opositores e manipulação da opinião pública, ameaçando a própria democracia.

Laura Schertel Mendes (2022), ao analisar os limites constitucionais do compartilhamento de dados pessoais na Administração Pública, alerta que o poder informacional é legítimo quando exercido para alcançar objetivos legais do Estado, de forma supervisionada, transparente e procedimentalizada. Entretanto, seu uso para subjugar indivíduos por meio de vigilância contínua e decisões arbitrárias representa a subversão do Estado de Direito.

E, com base na formulação de Lucas Borges de Carvalho (2023), é possível compreender que o cidadão ocupa uma posição estruturalmente vulnerável na relação com o Estado no que se refere ao tratamento de seus dados pessoais. Essa vulnerabilidade decorre do caráter compulsório da coleta de informações pelo Poder Público, impedindo o titular de exercer plenamente sua autonomia sobre o fornecimento de dados. Em um cenário de assimetria informacional e de poder, a ausência de salvaguardas adequadas pode converter o aparato estatal em instrumento de práticas abusivas, como a discriminação algorítmica ou a vigilância massiva.

Em consonância, Ingo Wolfgang Sarlet e Gabrielle Sarlet (2023) enfatizam que a concentração excessiva do poder informacional e a ausência de limites claros ao

compartilhamento de dados pessoais colocam em risco não apenas o direito fundamental à proteção de dados, mas também a ordem democrática e o Estado de Direito.

No âmbito do Direito Administrativo, os poderes da Administração Pública são instrumentos essenciais para a consecução dos objetivos estatais. Tradicionalmente, esses poderes — hierárquico, disciplinar, regulamentar e de polícia — são bem delimitados e fundamentados em normas constitucionais e infraconstitucionais. O poder informacional, embora não possa ser formalmente classificado entre os poderes administrativos clássicos, representa uma dimensão transversal que potencializa o exercício desses poderes e reconfigura a atuação estatal na sociedade digital. Com a transformação digital, a coleta, análise e compartilhamento de dados subsidiam decisões administrativas, políticas públicas preditivas e ações de segurança, consolidando a informação como recurso estratégico e uma nova dimensão do poder estatal.

Nesse cenário, o exercício do poder informacional pelo Estado deve ser pautado por contenção, fundamentação jurídica e respeito aos direitos fundamentais, a fim de evitar abusos e práticas incompatíveis com o Estado Democrático de Direito. A relevância desse tema foi reconhecida no julgamento da Ação Direta de Inconstitucionalidade nº 6.649, proposta pelo Conselho Federal da Ordem dos Advogados do Brasil contra o Decreto nº 10.046/2019, que instituiu o Cadastro Base do Cidadão (CBC) e o Comitê Central de Governança de Dados (CCGD). O CBC, ao consolidar dados de múltiplos órgãos federais em uma megabase integrada, ampliou significativamente o poder informacional do Estado, permitindo o compartilhamento de dados pessoais sem a exigência de convênios ou acordos formais (Anastácio *et al.,* 2020).

Tal estrutura normativa suscitou preocupações quanto à ausência de salvaguardas adequadas, à compatibilidade com os princípios da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e à proteção dos direitos dos titulares. O Supremo Tribunal Federal, ao analisar a matéria, assentou que o compartilhamento de dados pessoais pela Administração Pública deve observar os princípios da legalidade, finalidade legítima, necessidade, proporcionalidade e transparência, exigindo mecanismos de controle, responsabilização e participação social. Assim, a ADI 6.649 reafirma que o poder informacional estatal, embora legítimo em sua finalidade, deve ser exercido em limites constitucionais estritos, sob pena de se converter em instrumento de vigilância indevida e erosão das garantias fundamentais.

A Associação Data Privacy Brasil, atuando como *amicus curiae* no julgamento da ADI nº 6.649, criticou a ausência de mecanismos que garantissem o tratamento adequado, seguro e transparente dos dados, especialmente em relação aos usos secundários, que podem transformar

o CBC em instrumento de vigilância estatal (Vergili; Zanatta, 2022). O parecer técnico apresentado ao STF alertou para o potencial do decreto em criar uma infraestrutura estatal de vigilância de alta complexidade, capaz de integrar dados biométricos e comportamentais, ampliando o risco de identificação automatizada e vigilância contínua dos cidadãos (Ferreira, 2020).

O poder informacional estatal, quando instrumentalizado positivamente, pode fomentar políticas públicas eficazes; contudo, seu uso desvirtuado pode alimentar práticas autoritárias, como vigilância sistemática, censura e segregação social. Exemplos emblemáticos ilustram esses riscos: de acordo com Chapman (2024), o programa de vigilância PRISM da Agência de Segurança Nacional dos Estados Unidos da América — NSA, revelado por Edward Snowden, expôs a coleta massiva de dados sem mandados judiciais, afetando milhões de cidadãos; o relatório "Algoritmos del Silencio" do IPYS Venezuela (2024) denunciou bloqueios e repressão à liberdade de expressão digital; e a crise humanitária em Mianmar evidenciou o papel das plataformas digitais na amplificação do discurso de ódio contra a minoria Rohingya, conforme documentado pela Anistia Internacional (Amnesty International, 2022).

Necessário ainda recordar os exemplos históricos da Gestapo e da Stasi, citados por Gustavo Gil Gasiola (2019), que ilustram como o poder informacional pode ser instrumentalizado para fins repressivos e autoritários, reforçando a necessidade de limites constitucionais e democráticos claros para o exercício desse poder na sociedade contemporânea.

Por tudo aqui reflexionado, percebe-se que o poder informacional do Estado, ao conferir-lhe a capacidade singular de coletar, processar e utilizar dados pessoais em larga escala, representa uma dimensão essencial e transversal do exercício da autoridade estatal na contemporaneidade. Essa potência confirma o entendimento de que o compartilhamento de dados pessoais pelo Poder Público não pode ser compreendido como mera atividade técnica ou burocrática, mas sim como um ato administrativo vinculado, sujeito a formalidades, motivação adequada e controle. Deve, portanto, observar estritamente os princípios constitucionais e legais que regem o tratamento de dados pessoais, em especial os previstos na Lei Geral de Proteção de Dados (LGPD), que impõe limites claros quanto à finalidade, adequação, necessidade e transparência.

Desse modo, a proteção ao núcleo essencial do direito fundamental à proteção de dados pessoais revela-se imperativa para evitar que o poder informacional se converta em instrumento de abuso, vigilância indevida ou discriminação, ameaçando a dignidade da pessoa humana e a integridade do Estado Democrático de Direito. A legitimidade do poder informacional estatal

requer um equilíbrio entre a eficiência administrativa e a salvaguarda dos direitos fundamentais, especialmente os previstos nos incisos X, XII e LXXIX do artigo 5º da Constituição Federal.

Para tanto, o compartilhamento de dados pessoais pelo Poder Público deve ser precedido de ato administrativo formal, devidamente motivado, que observe os princípios da legalidade, finalidade, necessidade, proporcionalidade e transparência. Além disso, é imprescindível haver compatibilidade entre a finalidade original da coleta e a finalidade do uso secundário, bem como a adoção de medidas técnicas e administrativas que assegurem a minimização dos dados e a responsabilização dos agentes envolvidos.

Somente por meio dessa conjugação será possível consolidar uma governança de dados ética, responsável e constitucionalmente legítima, capaz de promover o interesse público sem sacrificar os direitos individuais, preservando os fundamentos do Estado de Direito e a dignidade da pessoa humana.

4.2 UMA REFLEXÃO SOBRE O *TRADE-OFF* ENTRE O PRINCÍPIO DA EFICIÊNCIA E A PROTEÇÃO DE DADOS PESSOAIS PELO PODER PÚBLICO

> Assim, a fim de conter os riscos de desvios de finalidade, a busca pela eficiência e pela inovação no setor público deve ser compatibilizada com as garantias de transparência, participação da sociedade civil, definição de finalidades específicas e motivação de decisões administrativas (Carvalho, 2023).

No contexto jurídico, o conceito de *trade-off* representa uma dinâmica de tensão e escolha entre valores, princípios ou direitos que, embora legítimos e constitucionalmente protegidos, podem entrar em conflito no caso concreto.

Trata-se de uma noção oriunda da economia[68]. Do ponto de vista econômico, o *trade-off* está relacionado à análise do custo de oportunidade, — ou seja, àquilo que se renuncia ao optar por determinada alternativa em detrimento de outra. Esse fenômeno manifesta-se em múltiplos níveis decisórios, desde as finanças pessoais até a formulação de políticas públicas, exigindo uma ponderação cuidadosa das vantagens e desvantagens relativas, com vistas à maximização do benefício conforme o contexto e as prioridades envolvidas.

[68] No campo da economia, o conceito de *trade-off* tem sido objeto de investigação desde a década de 1960, com contribuições pioneiras de Skinner (1969; 1974), seguidas por importantes desenvolvimentos teóricos e empíricos em estudos como os de Corbett e Wasenhove (1993), Hayes e Pisano (1996), Silveira e Slack (2001), Boyer e Lewis (2002) e Teng e Cummings (2002). Esses trabalhos convergem na análise da necessidade de as organizações definirem critérios competitivos coerentes como condição para a sustentação de estratégias genéricas eficazes, perspectiva também adotada por Mauss e Magalhães (2007).

No Direito, essa lógica de renúncia parcial ou total a determinado bem ou interesse em favor da maximização de outro é transposta para situações nas quais o ordenamento jurídico não oferece soluções absolutas, exigindo do intérprete uma atuação pautada pela ponderação e pela busca de equilíbrio. A tensão entre direitos ou princípios igualmente válidos impõe ao julgador o dever de realizar escolhas justificadas, com base em critérios de proporcionalidade, razoabilidade e adequação ao caso concreto.

Contudo, essa ponderação não é ilimitada: deve respeitar os contornos estabelecidos pela teoria dos limites dos limites dos direitos fundamentais, segundo a qual nem mesmo em situações de colisão é admissível a supressão do núcleo essencial de um direito. Conforme argumenta Alexy (2008), os direitos fundamentais possuem uma estrutura de princípios que admite restrições, mas essas restrições devem ser justificadas por razões igualmente fundamentais, submetendo-se a um teste de proporcionalidade em sentido estrito. Silva (2007), por sua vez, reforça que a teoria dos limites dos limites funciona como uma cláusula de contenção contra abusos interpretativos, assegurando que o conteúdo mínimo de cada direito permaneça inviolável, mesmo diante de interesses públicos relevantes.

Percebe-se assim que essa relação de conflito na escolha, em que se sacrifica um aspecto em troca de um ganho em outro, é especialmente evidente em contextos de colisão entre direitos fundamentais. A liberdade de expressão, por exemplo, pode entrar em choque com o direito à honra ou à privacidade, exigindo do julgador uma análise que transcenda a literalidade normativa e que se concentre na função social e na hierarquia circunstancial desses direitos. De modo semelhante, políticas públicas frequentemente demandam escolhas complexas entre interesses igualmente legítimos, como ocorre na tensão entre desenvolvimento econômico e proteção ambiental, ou entre segurança pública e garantias individuais.

Para lidar com essas situações, o Direito recorre a princípios estruturantes como o da proporcionalidade e o da razoabilidade. Esses princípios funcionam como instrumentos metodológicos que orientam a decisão jurídica, permitindo avaliar se a restrição imposta a determinado direito é adequada, necessária e se respeita o núcleo essencial do direito afetado. Essa fórmula procedimental revela-se particularmente desafiadora quando se trata da atuação do Poder Público diante da colisão entre o princípio da eficiência administrativa e o direito fundamental à proteção de dados pessoais.

A eficiência, insculpida no *caput* do artigo 37 da Constituição Federal, impõe à Administração Pública o dever de atuar com celeridade, economicidade e resultados. Por outro lado, a proteção de dados pessoais, reconhecida pelo Supremo Tribunal Federal como direito fundamental autônomo, impõe limites objetivos ao tratamento de informações dos cidadãos,

exigindo finalidades legítimas, transparência e segurança. A tensão entre esses dois polos se intensifica na era digital, onde a coleta e o processamento massivo de dados são frequentemente apresentados como instrumentos de modernização dos serviços públicos.

Conforme já delineado em capítulo anterior, o compartilhamento de dados pessoais entre entes e órgãos públicos não configura, por si só, prática vedada pelo ordenamento jurídico brasileiro. Ao contrário, encontra respaldo na Lei Geral de Proteção de Dados Pessoais — LGPD, que, em seu artigo 26, autoriza o uso compartilhado de dados pessoais pelo Poder Público, desde que tal tratamento esteja vinculado a uma finalidade legítima, específica e determinada, voltada à execução de políticas públicas previstas em normas legais ou regulamentares. Trata-se, portanto, de uma hipótese de tratamento lícito, condicionada à observância dos princípios da finalidade, necessidade, transparência e segurança, que conformam o regime jurídico protetivo dos dados pessoais no âmbito estatal.

Entretanto, como observa Carvalho (2023), a legitimidade do compartilhamento de dados pelo Poder Público pode ser controversa. Em muitos casos, a finalidade pública invocada pode entrar em tensão com outros direitos fundamentais igualmente protegidos, ou mesmo com outras finalidades públicas concorrentes. Além disso, surgem dúvidas quanto à extensão das competências institucionais para acessar ou tratar determinadas informações pessoais, sobretudo quando a legislação aplicável é ambígua, as justificativas apresentadas são frágeis ou o risco de desvio de finalidade e de impactos negativos aos titulares se mostra elevado. Tais incertezas reforçam a necessidade de uma interpretação estrita e fundamentada das hipóteses legais de compartilhamento, sob pena de se comprometer a integridade do direito fundamental à proteção de dados.

Nesse contexto, a taxonomia proposta por Custers e Ursic (2017) oferece uma contribuição analítica relevante para a compreensão dos diferentes graus de afastamento da finalidade original no uso secundário de dados pessoais. Sob a ótica do controlador, os autores distinguem três categorias: a reciclagem de dados, que corresponde à reutilização para o mesmo propósito inicial, ainda que em novo contexto; o reaproveitamento de dados, que envolve finalidades distintas, mas ainda relacionadas ao escopo original; e a recontextualização de dados, que representa o uso em contextos completamente diversos daquele que justificou a coleta.

Essa classificação revela-se particularmente útil para avaliar práticas estatais como o cruzamento de bases de dados para fins de controle antifraude, fiscalização ou gestão de benefícios sociais. Nessas hipóteses, a identificação do grau de afastamento da finalidade original permite aferir com maior precisão os riscos à conformidade com os princípios da

LGPD, especialmente os da finalidade, necessidade e transparência. Ainda que o uso secundário não seja, por si só, vedado, sua legitimidade pode depender da adoção de salvaguardas adicionais, como a elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), conforme previsto na própria legislação.

No plano jurisprudencial, o Supremo Tribunal Federal tem desempenhado papel central na consolidação do direito fundamental à proteção de dados pessoais como um instrumento de contenção de excessos administrativos e de salvaguarda da esfera privada dos cidadãos frente ao poder estatal. A Corte afirma que a proteção de dados não apenas limita práticas de vigilância indevida, mas também reforça os pilares da transparência e da legitimidade na atuação pública.

Um marco emblemático dessa construção jurisprudencial foi o julgamento da Ação Direta de Inconstitucionalidade nº 6387, no qual o STF suspendeu os efeitos da Medida Provisória que autorizava o compartilhamento de dados de usuários de telefonia com o IBGE durante a pandemia de COVID-19. Apesar da alegada finalidade pública legítima — a formulação de políticas emergenciais —, o Tribunal entendeu que a medida violava direitos fundamentais como a intimidade, a vida privada e o sigilo de dados, por ausência de garantias mínimas de segurança, finalidade específica e controle institucional.

O caso ilustra de forma paradigmática o *trade-off* entre eficiência administrativa e proteção de dados, reafirmando que a busca por resultados na gestão pública não pode se sobrepor, de forma abstrata e desproporcional, às garantias constitucionais. O STF, ao aplicar os princípios da proporcionalidade e da razoabilidade, reiterou que a atuação estatal deve ser simultaneamente eficaz e constitucionalmente legítima — e, sobretudo, compatível com os limites dos limites impostos pela própria Constituição à restrição de direitos fundamentais.

Diante desse panorama, impõe-se reconhecer que o compartilhamento de dados pessoais pelo Poder Público deve, doravante, observar com rigor os parâmetros constitucionais delineados pelo Supremo Tribunal Federal, especialmente no julgamento paradigmático da ADI 6387. A Corte estabeleceu um marco normativo e interpretativo que exige do Poder Público não apenas a invocação genérica de finalidades públicas, mas a demonstração concreta de que o tratamento de dados atende aos princípios da proporcionalidade, da necessidade e da finalidade, sem comprometer o núcleo essencial dos direitos fundamentais envolvidos.

Assim, o *trade-off* entre eficiência administrativa e proteção de dados não pode ser resolvido por meio de soluções automáticas ou que privilegiam tão-somente aspectos técnicos, mas deve ser enfrentado com base em critérios jurídicos estritos, que assegurem a legitimidade democrática da atuação estatal. A internalização dessa lógica decisória pelos entes públicos e

pelas entidades delegatárias de serviços é condição indispensável para a construção de uma cultura institucional de respeito à autodeterminação informacional, à transparência e à responsabilidade no uso de dados pessoais no Brasil.

Nesse cenário, a consolidação de práticas de governança de dados e a institucionalização de mecanismos de *accountability* tornam-se imperativos para assegurar que o compartilhamento de dados pelo Estado ocorra dentro dos marcos constitucionais, promovendo uma cultura pública de respeito à dignidade informacional.

Convém, contudo, destacar que, à luz da doutrina dos Sete Princípios do *Privacy by Design*[69], desenvolvida pela Dr.ª Ann Cavoukian (2009), é possível concluir que a suposta tensão entre o interesse público — especialmente sob a ótica da eficiência administrativa — e a proteção de dados pessoais configura um falso *trade-off*. Trata-se de uma oposição apenas aparente, que não representa um conflito necessário ou irreconciliável, mas que pode ser superada mediante uma compreensão mais sofisticada e integrada da relação entre essas dimensões.

Essa compreensão decorre, em especial, do princípio da Funcionalidade Plena — Soma Positiva, não Soma Zero, segundo o qual a privacidade deve ser concebida como um valor compatível com outros objetivos legítimos, e não como um obstáculo a ser superado. A proposta do *privacy by design* é justamente evitar dicotomias artificiais — como privacidade *versus* segurança ou privacidade *versus* eficiência — sustentando ser possível promover simultaneamente ambos os valores por meio de soluções técnicas e organizacionais adequadas.

Dessa forma, o reconhecimento do falso *trade-off* sustenta uma interdependência dinâmica e complementar entre o interesse público e a proteção de dados pessoais. Ambos são elementos estruturantes para o equilíbrio do poder informacional do Estado. A proteção integral dos dados pessoais, longe de inviabilizar a atuação estatal, contribui para sua legitimidade, transparência e eficácia, consolidando uma administração pública orientada por princípios constitucionais e comprometida com os direitos fundamentais na era digital.

[69] Princípios que serão abordados no capítulo 6.1. Mecanismos de controle da atividade administrativa de compartilhamento de dados pessoais pelo Poder Público.

5 ANÁLISE JURISPRUDENCIAL: PRINCIPAIS CASOS PARADIGMÁTICOS DO SUPREMO TRIBUNAL FEDERAL

> Os riscos inerentes à era digital devem ser considerados na leitura e na aplicação da Constituição Federal de 1988.[70]

Nos tópicos seguintes, são analisados dois julgamentos paradigmáticos do Supremo Tribunal Federal — a ADI nº 6387 e a ADI nº 6649 — que se consolidam como marcos interpretativos fundamentais na definição dos limites constitucionais para o compartilhamento de dados pessoais pelo Poder Público.

Trata-se de decisões que estabelecem o imprescindível equilíbrio entre a proteção dos direitos fundamentais à privacidade e à proteção de dados pessoais, consagrados na Constituição Federal, e as legítimas demandas estatais voltadas à formulação e execução de políticas públicas. A ADI nº 6387, em particular, suspendeu dispositivos da Medida Provisória nº 954/2020, que autorizava o compartilhamento compulsório de dados telefônicos com o IBGE, destacando a centralidade dos princípios da transparência, da finalidade específica e da segurança jurídica no tratamento de dados pessoais. Por sua vez, a ADI nº 6649 aprofunda a discussão sobre os limites constitucionais do uso secundário de dados pelo Estado, reforçando a necessidade de compatibilidade entre finalidades e a observância do devido processo legal.

O exame desses julgamentos permite compreender como o STF tem consolidado parâmetros jurídicos essenciais à legitimação do compartilhamento de dados pessoais pelo Poder Público, reafirmando a proteção ao núcleo essencial do direito fundamental à proteção de dados. Destacam-se, nesse contexto, a delimitação das bases legais, a compatibilidade de finalidades e a observância dos princípios da transparência, da segurança e da proporcionalidade.

Esses precedentes revelam o esforço do Supremo Tribunal Federal em construir uma jurisprudência que harmonize a tutela dos direitos fundamentais dos titulares com a efetividade das políticas públicas, estabelecendo balizas normativas que orientam o tratamento de dados pessoais na atuação administrativa estatal e asseguram a preservação da dignidade, da privacidade e da confiança da sociedade na gestão dos dados pessoais na era digital.

Contudo, antes de examinar os casos paradigmáticos, mister se faz compreender o contexto em que foram forjados.

---

[70] Voto do Ministro Gilmar Ferreira Mendes proferido no julgamento da Ação Direta de Inconstitucionalidade - ADI nº 6.649.

Nesse intuito, mostra-se relevante, inicialmente, reconhecer que, conforme destaca Wimmer (2023), nas últimas décadas, observou-se uma evolução significativa na incorporação de tecnologias digitais pelos governos, acompanhada pela ampliação das capacidades de tratamento, processamento e integração de dados. Esse avanço técnico-científico esteve diretamente associado a uma mudança de paradigma na compreensão do papel da tecnologia na administração pública, marcada pela transição do modelo de Governo Eletrônico — voltado à informatização de processos internos e à eficiência administrativa — para o modelo de Governo Digital. Este novo paradigma, centrado no cidadão, pressupõe a integração sistêmica de processos governamentais e o uso intensivo de tecnologias emergentes, como inteligência artificial e plataformas móveis, com vistas à desburocratização, à transparência e à inovação na prestação de serviços públicos (Oliveira; Marinho, 2023).

Nesse cenário de crescente digitalização e intensificação do uso de dados pessoais pelo Estado, emergiu a necessidade de um marco normativo que assegurasse a proteção dos direitos fundamentais dos titulares. É nesse contexto que se insere a promulgação da Lei nº 13.709/2018 — a Lei Geral de Proteção de Dados Pessoais (LGPD) —, que estabelece princípios, direitos e deveres aplicáveis ao tratamento de dados pessoais no Brasil.

A LGPD representou não apenas uma resposta à complexidade da sociedade da informação, mas também um instrumento essencial para equilibrar a eficiência administrativa promovida pelo Governo Digital com a salvaguarda da privacidade, da autodeterminação informativa e da confiança da sociedade na atuação estatal. Assim, a transformação digital do Estado e a consolidação de uma cultura de proteção de dados caminham de forma indissociável na construção de uma governança pública legítima e orientada por direitos.

A Lei Geral de Proteção de Dados Pessoais — LGPD trouxe, em seu art. 5º, X, o seguinte conceito para tratamento: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Estabeleceu ainda aquela legislação brasileira de proteção de dados pessoais que as atividades de tratamento deverão observar a boa-fé e os princípios que enumera, dentre eles, o da finalidade, que consiste na sua realização para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (art. 6º, I).

Toda essa previsão legislativa entrou em vigor no dia 18 de setembro de 2020, em momento anterior, portanto, à inclusão da proteção de dados pessoais no rol dos direitos e garantias fundamentais (art. 5º, LXXIX, CR).

Aquele acréscimo, decorrente da Emenda Constitucional n.º 115, promulgada em 10 de fevereiro de 2022, fortaleceu o interesse público na observância do atendimento do princípio da finalidade na utilização de informações relacionadas às pessoas naturais, identificadas ou identificáveis.

Verificou-se ali verdadeiramente uma "progressão generacional" (Doneda, 2011) do escopo normativo, com o reconhecimento crescente dos dados pessoais como expressão da personalidade[71]. Esse movimento teve início quando o Estado brasileiro subscreveu a Declaração na XIII Cimeira Ibero-Americana na cidade de Santa Cruz de la Sierra, em 2003, em que os Chefes de Estado e de Governo se declararam conscientes de que a proteção de dados pessoais é um direito fundamental das pessoas e destacaram a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos (Segib, 2003).

Cabe ressaltar que, antes da referida reunião de cúpula, e mesmo anteriormente à promulgação da LGPD, a proteção aos dados pessoais, ou às informações pessoais constantes em bancos de dados, seria possível no Brasil sob a perspectiva da proteção constitucional à privacidade (art. 5º, X).

Além da inviolabilidade garantida à vida privada e à intimidade, também seria possível se pensar em proteção às informações pessoais constantes em bancos de dados, posto que o texto constitucional conferiu proteção ao sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (art. 5º, XII) e instituiu o habeas data como remédio para garantir o acesso a informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados (art. 5º, LXXII).

Ao nível infraconstitucional, a Política Nacional de Informática, disposta pela Lei n º. 7.232/84 já previa o estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas.

Na década de 1990, grande evolução no ordenamento jurídico brasileiro para a tutela dos dados pessoais adveio com o Código de Defesa do Consumidor (CDC), a Lei n º. 8.078/90,

[71] Inspirado pela doutrina de Stefano Rodotá, Danilo Doneda introduziu o conceito de "progressão generacional" das legislações sobre proteção de dados pessoais, recorrendo deliberadamente à terminologia da informática para ilustrar a evolução contínua e incremental dos modelos jurídicos, em busca de maior sofisticação normativa e densidade principiológica.

que garantiu ao consumidor o acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele (art. 43).

Cumpre, contudo, observar que, muito antes da Emenda Constitucional n. º 115/2022, havia posicionamentos doutrinários[72] no sentido de que dados cadastrais — como nome, filiação, endereço e número de inscrição no CPF —, por si sós, não estariam abrangidos pela proteção conferida ao direito à privacidade. Segundo essa corrente, tais dados somente estariam constitucionalmente protegidos quando relacionados a aspectos da vida privada ou da intimidade do indivíduo.

Alinhado àquela interpretação restritiva da garantia de inviolabilidade do sigilo de dados, o Supremo Tribunal Federal havia consolidado entendimento jurisprudencial no sentido de que a proteção prevista no art. 5º, inciso XII, da Constituição Federal referia-se à comunicação de dados — e não aos dados em si mesmos —, ainda que armazenados em sistemas informatizados. Tal distinção evidenciava uma limitação na abrangência da tutela constitucional, especialmente diante do crescente uso de dados pessoais pelo poder público e por entes privados.[73]

As interpretações segundo as quais o texto constitucional conferia proteção apenas à comunicação de dados — e não aos dados em si mesmos — revelavam-se insuficientes diante da complexidade crescente do fenômeno informacional. Como advertiu Doneda (2011), tais leituras não captavam a profundidade das novas formas de controle e vigilância possibilitadas pela manipulação massiva de dados pessoais, que extrapolam o mero conteúdo comunicacional e alcançam dimensões estruturais da vida em sociedade.

Ainda que formuladas em um contexto anterior à promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), aquelas abordagens continuaram a influenciar a interpretação constitucional mesmo após sua entrada em vigor, evidenciando, como observa Mendes (2018), que o arcabouço normativo então vigente permanecia aquém dos desafios impostos pelo tratamento automatizado de informações e pelos efeitos concretos que esse processamento pode gerar sobre os direitos fundamentais dos indivíduos.

Necessário, porém, ter a perspectiva de que, desde a década de 1960 com o surgimento da ARPANET — projeto pioneiro desenvolvido pela Advanced Research Projects Agency (ARPA) agência militar dos Estados Unidos —[74], teve início a chamada Era da Informação,

[72] Ferraz Júnior, 1993.
[73] RE 418.416 / SC; HC 91.867 / PA.
[74] UNITED STATES. DARPA, 2025.

marco fundamental para a transformação global nas formas de comunicação e processamento de dados (Castells, 1999). Originalmente concebida para garantir a troca segura de informações militares em um contexto de Guerra Fria, a ARPANET evoluiu para a base técnica da internet moderna, possibilitando a interconexão de redes de computadores e ampliando exponencialmente a capacidade de tratamento e cruzamento de dados.

Nesse contexto, os dados pessoais passaram a assumir uma importância central — dada a constatação de que qualquer informação que permitisse a identificação, seja ela efetiva ou potencial, poderia ser utilizada para a construção de perfis informacionais detalhados, com impactos profundos na privacidade e na autonomia dos indivíduos (Ferreira; Garcia, 2024). Essa evolução tecnológica não apenas ampliou a coleta e o uso de dados, mas também impulsionou transformações no âmbito da governança pública, que passou a integrar as tecnologias digitais como elementos essenciais para a modernização do Estado e a criação de valor público, configurando uma nova era em que a proteção dos dados pessoais se torna um imperativo jurídico e social.

Venturosamente, consolidou-se no Brasil uma tendência de avanço no processo de transformação cultural, voltada à promoção, no seio da coletividade, da compreensão do direito à proteção de dados pessoais para além de uma mera decorrência da privacidade: trata-se de um direito fundamental autônomo, cujo âmbito de proteção se vincula diretamente à tutela da dignidade e da personalidade dos cidadãos na sociedade da informação (Mendes; Fonseca, 2020a).

Nessa contextualização, cumpre ainda acrescer que, enquanto a sociedade brasileira — especialmente no meio acadêmico — debatia a relevância da consagração da proteção de dados como direito fundamental, expandia-se nacionalmente a utilização da plataforma “gov.br”, portal do governo federal que, ao centralizar diversos canais digitais, inseriu o Brasil no movimento de plataformização dos serviços públicos (Bioni *et al,* 2022).

Esse movimento de plataformização, ao demandar a interconexão de informações entre distintos setores econômicos, públicos e privados, revelou um alinhamento à chamada “Nova Economia”, na qual os dados pessoais deixaram de ser meramente mercadorias e passaram a constituir a base estrutural de um novo modelo de capitalismo (Bouk, 2018). E, em tal cenário, ganha relevo a coleta, análise e o processamento daqueles ativos estratégicos aptos a oferecerem valiosas informações.

O fenômeno da integração entre grandes volumes de informação como ferramenta de negócios, referido na literatura acadêmica e na indústria como *Big Data* (De Mauro; Greco; Grimaldi, 2015), provocou o avanço da coleta e do compartilhamento de dados pessoais, tanto

no âmbito dos agentes de tratamento privados, quanto na esfera do Poder Público, o que também amplificou a geração de riscos de malferir um dos fundamentos da disciplina de proteção de dados pessoais: a autodeterminação informativa dos titulares (art. 2º, inciso II, da Lei nº 13.709/18 – LGPD). A análise da origem desse conceito, gerado na doutrina e jurisprudência constitucional alemãs, evidencia que, nas atuais condições de tratamento automatizado, não há dados insignificantes, pois, o risco não reside no tipo de dado, mas nas finalidades e possibilidades decorrentes de seu tratamento (Mendes, 2020b).

A utilização daqueles dados pessoais coletados é muitas vezes realizada por interoperabilidade, que consiste na capacidade de fluxo de dados e compartilhamento de informações entre sistemas de diversas organizações, conforme disciplina não somente a referida Lei Geral de Proteção de Dados Pessoais (art. 25), mas também a Estratégia Nacional de Governo Digital (ENGD), instituída pela Lei nº 14.129, de 29 de março de 2021 - Lei do Governo Digital (art. 3º, XIV)[75].

Consolidou-se, portanto, um ambiente em que grandes corporações e o Estado concentram poder, recursos e informações em volume desproporcionalmente superior ao dos indivíduos, condição que configura uma acentuada assimetria informacional entre os entes públicos e o cidadão comum, potencializando desequilíbrios de forças nas relações e ampliando a vulnerabilidade dos titulares dos dados.

Nessa conjuntura, o julgamento da ADI nº 6387 representou um marco histórico no ordenamento jurídico brasileiro ao reconhecer, pela primeira vez, o direito fundamental autônomo à proteção de dados pessoais. Essa decisão ampliou a concepção tradicional de privacidade, que se restringia ao "direito de ser deixado só", para incluir o contemporâneo direito à proteção e à autodeterminação informacional.

Naquele julgamento, o Supremo Tribunal Federal estabeleceu parâmetros constitucionais para o tratamento estatal de dados pessoais, impondo a necessidade de mecanismos técnicos e administrativos robustos que garantam a segurança contra acessos indevidos, vazamentos e usos ilícitos. Além disso, o Tribunal enfatizou a observância dos princípios da proporcionalidade e da minimização dos dados coletados.

Assim, a decisão consolidou a proteção de dados pessoais como um direito fundamental no Brasil, influenciando decisivamente a legislação, a jurisprudência e o debate acadêmico

[75] Por sua potencialidade para propiciar amplas condições de troca e interação com os Poderes de diferentes esferas de governo e com a sociedade em geral, o atributo da interoperabilidade é considerado um dos pontos-chave das políticas de governo eletrônico (BRASIL, 2012), e foi incluído dentre os 10 objetivos declarados na Estratégia Nacional de Governo Digital para o período de 2024 a 2027, conforme estabelece o Decreto nº 12.069, de 21 de junho de 2024 e a Portaria SGD/MGI nº 4.248, de 26 de junho de 2024.

sobre o tema. O julgamento promoveu maior segurança jurídica e proteção efetiva aos cidadãos na era digital, sinalizando a importância de equilibrar o avanço tecnológico com a salvaguarda dos direitos fundamentais e configurando um novo paradigma na tutela da dignidade e da autonomia informacional.

5.1 ADI Nº 6387 – CASO DO IBGE

> O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados.[76]

Nesse enfoque, o primeiro caso paradigmático a ser aqui examinado, dirimido pelo Supremo Tribunal Federal, versou sobre a Medida Provisória nº 954/2020. Essa norma previa o compartilhamento de dados pessoais — como nome, telefone e endereço — entre empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado (STFC) e de Serviço Móvel Pessoal (SMP) e a Fundação Instituto Brasileiro de Geografia e Estatística — IBGE, com o objetivo de viabilizar a realização do censo por telefone no contexto da pandemia da Covid-19.

Proposta pelo Conselho Federal da Ordem dos Advogados do Brasil, a ADI nº 6387 alegava a inconstitucionalidade formal da medida provisória impugnada, por inobservância dos requisitos da relevância e da urgência previstos no art. 62 da CF, bem como a sua inconstitucionalidade material, por afronta ao postulado fundamental da dignidade da pessoa humana e às garantias constitucionais da inviolabilidade da intimidade, da vida privada, da honra e da imagem, do sigilo de dados e da autodeterminação informativa (arts. 1º, III, e 5º, X e XII, da Lei Maior).

Contra a referida medida também foram ajuizadas as Ações Diretas de Inconstitucionalidade nº 6388, 6389, 6393 e 6390, por quatro partidos políticos: PSDB, PSB, PSOL e PCdoB, que sustentavam o argumento de que a norma violava princípios constitucionais fundamentais, como a dignidade da pessoa humana, a inviolabilidade da intimidade, da vida privada, da honra e da imagem, bem como o sigilo dos dados e a autodeterminação informativa.

No conjunto das ações, delinearam-se duas correntes argumentativas antagônicas (Mendes; Rodrigues Junior; Fonseca, 2023). De um lado, sustentava-se a necessidade da norma

[76] Acórdão proferido na Ação Direta de Inconstitucionalidade - ADI nº 6387.

como instrumento essencial para a produção estatística nacional, especialmente em um contexto de crise sanitária e social. É dizer, por parte do IBGE, advertiam para o risco de um "apagão estatístico", que comprometeria não somente o controle da pandemia, mas também a formulação de políticas públicas eficazes nos âmbitos fiscal, social e econômico.

De outro lado, os autores das ações diretas de inconstitucionalidade apontavam graves vícios de inconstitucionalidade, centrados em três eixos principais: (a) a vaguidade e generalidade da redação normativa, que autorizava restrições sensíveis a direitos fundamentais sem delimitação clara de escopo e finalidade; (b) a desproporcionalidade entre os dados requisitados e os fins estatísticos alegados, uma vez que a MP exigia a totalidade dos dados pessoais dos usuários, e não apenas amostras estatisticamente representativas; e (c) a ausência de garantias mínimas de segurança da informação, especialmente no que tange à proteção dos dados durante sua transmissão entre as operadoras e o IBGE.

A controvérsia, portanto, revelou a tensão entre a efetividade das políticas públicas em contextos excepcionais e a necessidade de observância estrita aos direitos fundamentais à privacidade e à proteção de dados pessoais, cuja consagração constitucional foi posteriormente reforçada com a positivação autônoma desse direito no ordenamento jurídico brasileiro (Mendes; Rodrigues Junior; Fonseca, 2023).

As ações tramitaram conjuntamente e a decisão proferida na ADI nº 6387, ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil, foi reproduzida nos demais processos. Na sessão plenária de 7 de maio de 2020, o STF confirmou a liminar anteriormente concedida pela ministra Rosa Weber, suspendendo os efeitos da Medida Provisória nº 954/2020.

Aquele julgamento foi amplamente celebrado como histórico[77], sendo considerado um marco na jurisprudência constitucional brasileira. Nele, o Supremo Tribunal Federal firmou entendimento de que, no contexto da sociedade da informação, não há dados pessoais insignificantes ou neutros. Conforme salientado no voto do Ministro Ricardo Lewandowski, a atual capacidade tecnológica de processamento massivo e cruzamento de informações transforma até mesmo dados aparentemente triviais em verdadeiras chaves de acesso a perfis complexos de milhões de indivíduos. Esses dados, embora dotados de elevado potencial para a formulação e execução de políticas públicas, também carregam consigo riscos substanciais de uso indevido, inclusive por meio de práticas dissimuladas e opacas, capazes de comprometer a esfera privada e gerar perturbações concretas na vida cotidiana dos cidadãos.

[77] Um demonstrativo da relevância daquele reconhecimento do direito fundamental à proteção de dados pessoais foi o adjetivo "histórico" então utilizado não somente no ambiente acadêmico, a exemplo: (Mendes; Rodrigues Junior; Fonseca, 2023), mas também por muitos veículos da imprensa especializada, a exemplo: (Krieger, 2021).

Pavimentou-se, ali, o reconhecimento de um direito fundamental autônomo à proteção de dados pessoais e à autodeterminação informacional. O entendimento firmado naquele precedente passou a ser a referência sobre o tratamento de dados pessoais pelo Estado — tanto que foi expressamente mencionado no julgamento da ADI nº 6.649, que será examinada no tópico subsequente.

Diante da relevância do julgamento da ADI nº 6387 para a consolidação do direito fundamental à proteção de dados pessoais no ordenamento jurídico brasileiro, destaca-se que o Supremo Tribunal Federal, sob a relatoria da Ministra Rosa Weber, reconheceu expressamente que informações relacionadas à identificação — efetiva ou potencial — de pessoas naturais integram o escopo de proteção das cláusulas constitucionais que asseguram a liberdade individual, a privacidade e o livre desenvolvimento da personalidade. Assim, o tratamento desses dados deve observar os limites constitucionais, sob pena de violação a direitos fundamentais.

A Corte também apontou a inconstitucionalidade da Medida Provisória nº 954/2020 por não prever mecanismos técnicos ou administrativos adequados à proteção contra acessos indevidos, vazamentos ou usos indevidos dos dados compartilhados, descumprindo, portanto, os deveres constitucionais de proteção à privacidade e à segurança informacional dos cidadãos.

Além disso, o STF enfatizou a desproporcionalidade entre o volume de dados exigidos e a finalidade declarada da medida, agravada pela ausência de garantias mínimas de anonimização ou pseudonimização[78]. Ressaltou-se que o compartilhamento de dados com o IBGE, embora não seja vedado em absoluto, deve ocorrer sob estrita observância das garantias constitucionais, com salvaguardas compatíveis com os direitos fundamentais envolvidos.

Mesmo diante da urgência imposta pela pandemia da COVID-19, o Tribunal foi categórico ao afirmar que a crise sanitária não pode justificar o atropelo de garantias constitucionais. A manutenção dos dados por período superior ao estritamente necessário também foi considerada excessiva, violando o princípio da minimização.

Por fim, o STF assentou que o compartilhamento de dados pessoais por concessionárias de serviço público com entes estatais deve ser acompanhado de mecanismos robustos de proteção e segurança, reafirmando que a excepcionalidade da situação não afasta a necessidade de respeito aos direitos fundamentais.

---

[78] A Lei Geral de Proteção de Dados Pessoais (LGPD) define anonimização como o uso de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (art. 5º, XI). Já a pseudonimização é caracterizada como o tratamento pelo qual o dado perde essa possibilidade de associação, direta ou indireta, exceto mediante o uso de informação adicional mantida separadamente pelo controlador, em ambiente controlado e seguro (art. 13, § 4º).

Porém, ainda que emblemático, o julgamento não esgotou a complexa discussão jurídica sobre o uso secundário de dados pessoais pelo Estado, tema que permanece em evolução no cenário constitucional brasileiro.

5.2 ADI Nº 6649, JULGADA CONJUNTAMENTE COM ADPF Nº 695, RELATIVAS AO DECRETO 10.046/2019 – CASO DO CADASTRO BASE DO CIDADÃO

> O tratamento de dados pessoais pelo Estado é essencial para a prestação de serviços públicos. Todavia, diferentemente do que assevera o ente público, a discussão sobre a privacidade nas relações com a Administração Estatal não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais[79].

Após o julgamento da ADI nº 6387, o tema do compartilhamento de dados pessoais pelo Poder Público para fins secundários — isto é, para finalidades distintas daquelas que motivaram sua coleta original — voltou à pauta do Supremo Tribunal Federal por ocasião do julgamento da Ação Direta de Inconstitucionalidade — ADI nº 6.649, ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), a qual foi apreciada conjuntamente com a Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 695, proposta pelo Partido Socialista Brasileiro (PSB).

Ambas as ações questionavam a constitucionalidade do Decreto nº 10.046/2019, que dispôs sobre a governança no compartilhamento de dados no âmbito da administração pública federal, instituindo o Cadastro Base do Cidadão — CBC e o Comitê Central de Governança de Dados — CCGD[80].

O Decreto nº 10.046/2019 representou uma referência normativa central na consolidação da governança de dados no âmbito da Administração Pública Federal, ao regulamentar o compartilhamento de dados entre órgãos e entidades públicas e instituir mecanismos estruturantes como o Cadastro Base do Cidadão (CBC) e o Comitê Central de Governança de Dados (CCGD). Seu campo de aplicação abrangeu a Administração Pública Federal direta, autárquica e fundacional, bem como os demais Poderes da União, com exclusões

[79] Acórdão proferido na Ação Direta de Inconstitucionalidade - ADI nº 6.649.

[80] Antes da edição do Decreto nº 10.046/2019, o compartilhamento de bases de dados entre órgãos e entidades da administração pública federal era disciplinado pelo Decreto nº 8.789/2016, o qual inovou ao prever, como regra, o acesso automático e preferencial às informações cadastrais, sem a exigência de convênios ou acordos específicos, embora sem revogar os mecanismos voluntários de cooperação já existentes.

expressas que resguardam os conselhos profissionais, o setor privado e os dados protegidos por sigilo fiscal sob a gestão da Receita Federal.

A compreensão sistemática do decreto original pode ser organizada, conforme propõe Pedrazzoli (2023), a partir de cinco eixos temáticos interdependentes. O primeiro eixo (artigos 1º ao 3º) refere-se às disposições introdutórias, que estabelecem os objetivos do compartilhamento de dados, os conceitos fundamentais empregados e as diretrizes gerais que orientam a atuação dos entes públicos. Tais dispositivos inaugurais delineiam o propósito de promover maior eficiência administrativa, melhorar a prestação de serviços públicos e subsidiar a formulação de políticas públicas baseadas em dados confiáveis e integrados.

O segundo eixo (artigos 4º a 15) trata das regras específicas para o compartilhamento de dados, organizadas com base em uma classificação tripartida que considera o grau de confidencialidade das informações. Essa categorização distingue entre o compartilhamento amplo, restrito e específico. O compartilhamento amplo refere-se a dados públicos, acessíveis a qualquer interessado, sem necessidade de autorização prévia. Já o compartilhamento restrito abrange dados protegidos por sigilo, cujo acesso é permitido a todos os órgãos abrangidos pelo decreto, desde que observadas regras simplificadas definidas pelo CCGD. Por fim, o compartilhamento específico diz respeito a dados sigilosos cujo acesso é restrito a determinados órgãos, conforme previsão legal e autorização do gestor dos dados. Importa destacar que o decreto dispensa a celebração de instrumentos formais, como convênios ou acordos, para a efetivação do compartilhamento entre entes públicos, desde que respeitadas as diretrizes da própria norma e da Lei Geral de Proteção de Dados (LGPD).

O terceiro eixo normativo (artigos 16 a 20) é dedicado à criação do Cadastro Base do Cidadão, concebido como uma base integradora de dados cadastrais essenciais dos cidadãos. O CBC tem como finalidade viabilizar a identificação unificada do cidadão perante o Estado, facilitar o intercâmbio de dados entre órgãos públicos e permitir o cruzamento de informações a partir do número de inscrição no CPF. A base integradora do CBC é alimentada inicialmente com dados biográficos do CPF, aos quais se somam, progressivamente, informações provenientes de outras bases temáticas, com atualizações periódicas.

O quarto eixo diz respeito à instituição do Comitê Central de Governança de Dados, órgão colegiado responsável por coordenar a implementação do fluxo de compartilhamento de dados previsto no decreto. O CCGD possui atribuições relevantes, como a definição de diretrizes para a categorização dos dados, a deliberação sobre regras de segurança e sigilo, a compatibilização das políticas de segurança da informação entre os órgãos públicos e a resolução de controvérsias entre gestores e solicitantes de dados. Sua composição inicial incluía

representantes de órgãos estratégicos, como o Ministério da Economia, a Casa Civil, a Controladoria-Geral da União, a Advocacia-Geral da União e o INSS.

Por fim, o quinto eixo compreende as disposições finais e transitórias, que regulam aspectos operacionais e de transição para a plena implementação do modelo de governança de dados instituído. Embora voltado à racionalização administrativa, o Decreto nº 10.046/2019 suscitou importantes controvérsias constitucionais, especialmente no que se refere à proteção de dados pessoais, à autodeterminação informativa e à necessidade de compatibilização com os princípios da LGPD e com os direitos fundamentais consagrados na Constituição Federal, notadamente os previstos nos artigos 5º, X e XII.

Conforme observa Ferreira (2023), os Decretos nº 10.046/2019 e nº 10.047/2019[81] instituíram, no âmbito do Poder Executivo Federal, uma estrutura normativa voltada à criação de uma base de dados unificada — o Cadastro Base do Cidadão —, com o objetivo declarado de facilitar o acesso da população a serviços públicos digitais. Embora a digitalização e a desburocratização da administração pública constituam demandas legítimas da sociedade brasileira, o modelo normativo adotado revelou-se problemático sob a ótica constitucional e legal.

A autora destaca que o Decreto nº 10.046/2019 não especificava claramente as finalidades do compartilhamento de dados nem os critérios técnicos e jurídicos para sua realização, tampouco delimitava os papéis dos diferentes Poderes da República no tratamento dessas informações. Tal omissão normativa colocava em risco a observância dos princípios da legalidade, da finalidade e da proporcionalidade, consagrados na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e na jurisprudência do Supremo Tribunal Federal. Nesse sentido, a autora sustenta que a governança de dados pessoais no setor público deveria ser orientada por um paradigma constitucional apto a assegurar a proteção dos direitos fundamentais dos titulares, mesmo diante das exigências de eficiência administrativa e inovação tecnológica.

O exame da constitucionalidade daquele Decreto nº 10.046/2019 foi realizado em 15 de setembro de 2022, no julgamento da Ação Direta de Inconstitucionalidade nº 6.649, ocasião em que o Supremo Tribunal Federal fixou parâmetros constitucionais a serem observados no compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública. A decisão reafirmou a centralidade dos direitos fundamentais à privacidade e à proteção de dados

[81] Dispõe sobre a governança do Cadastro Nacional de Informações Sociais e institui o programa Observatório de Previdência e Informações, no âmbito do Cadastro Nacional de Informações Sociais.

pessoais no contexto da atuação estatal, consolidando a exigência de conformidade com os princípios da proporcionalidade, da finalidade e da segurança da informação.

Pela relevância de seu impacto sobre a disciplina do tratamento de dados pelo Poder Público, analisa-se aqui detidamente a ADI nº 6.649 e verifica-se que o Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) insurgiu-se contra o Decreto nº 10.046/2019, sustentando em sua exordial que, sob o pretexto de facilitar o acesso da população a serviços públicos federais, o ato normativo instituiu uma estrutura de vigilância estatal de alta complexidade e potencial lesivo. Segundo a argumentação, o referido decreto autorizaria o tratamento e o compartilhamento de um amplo espectro de dados pessoais — incluindo informações sensíveis, dados biométricos e comportamentais — sem as devidas salvaguardas constitucionais e legais, o que configuraria uma ameaça à privacidade e à autodeterminação informativa dos cidadãos.

O Conselho Federal apontou, ainda, a existência de vícios de inconstitucionalidade tanto formais quanto materiais. No plano formal, argumentou-se que o decreto extrapolaria os limites da função regulamentar do Presidente da República, inovando no ordenamento jurídico em afronta ao art. 84, incisos IV e VI, alínea "a", da Constituição Federal. No aspecto material, sustentou-se que o ato normativo violaria diretamente os direitos fundamentais previstos nos arts. 1º, inciso III, e 5º, caput, incisos X, XII e LXXII da Constituição, ao comprometer a dignidade da pessoa humana, a inviolabilidade da intimidade e da vida privada, o sigilo de dados e o direito ao habeas data, especialmente à luz do reconhecimento da proteção de dados pessoais como direito fundamental autônomo, conforme havia sido decidido pelo STF na ADI nº 6.387.

Além disso, o CFOAB destacou a existência de antinomias entre o Decreto nº 10.046/2019 e o arcabouço infraconstitucional vigente. Embora o decreto alegasse fundamentar-se na Lei de Acesso à Informação (Lei nº 12.527/2011), na Lei da Identificação Civil Nacional (Lei nº 13.444/2017) e na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), a análise de seu conteúdo revelaria, segundo a petição, uma incompatibilidade substancial com os dispositivos dessas normas. Em vez de regulamentá-las fielmente, o decreto contrariaria frontalmente seus comandos, especialmente no que tange à finalidade, à transparência e à limitação do tratamento de dados pelo Poder Público.

Diante da relevância constitucional da matéria em debate e da representatividade das entidades postulantes, o Supremo Tribunal Federal admitiu a intervenção de três instituições na qualidade de *amicus curiae*, consoante o permissivo contido no Art. 138. Código de Processo Civil de 2015: a Associação Data Privacy Brasil de Pesquisa, o Laboratório de Políticas

Públicas e Internet (LAPIN) e o Instituto Mais Cidadania. A atuação desses colaboradores processuais teve por finalidade oferecer subsídios técnicos e jurídicos ao órgão julgador, ampliando a pluralidade do debate constitucional.

As manifestações apresentadas por tais entidades enriqueceram a discussão ao trazerem análises críticas sobre os riscos estruturais associados à centralização de dados pessoais em bases unificadas. Destacou-se, nesse contexto, a referência a experiências internacionais, como o emblemático caso do *National Data Bank*, nos Estados Unidos da América, que evidenciam os potenciais abusos decorrentes do uso indiscriminado de informações pessoais em sistemas estatais centralizados, com impactos diretos sobre a privacidade e a autodeterminação informativa dos cidadãos.

A sustentação oral configura-se como expressão qualificada da função essencial da Advocacia, indispensável à administração da justiça, conforme consagrado no art. 133 da Constituição da República. No âmbito da Ação Direta de Inconstitucionalidade nº 6.649, a manifestação oral foi realizada pelo advogado Danilo César Maganhoto Doneda[82], em nome do Conselho Federal da Ordem dos Advogados do Brasil.

Na ocasião, aquela defesa enfatizou a necessidade de que a modernização da administração pública — por meio de práticas de gestão e planejamento baseadas no uso intensivo de dados — seja acompanhada de salvaguardas institucionais capazes de mitigar os riscos decorrentes do tratamento de dados pessoais dos cidadãos. Com esse objetivo, foram propostas medidas concretas voltadas à legitimação do compartilhamento de dados no setor público, entre as quais se destacam:

(i) A verificação efetiva da compatibilidade de finalidades entre os entes envolvidos no compartilhamento;

(ii) A consideração dos riscos inerentes ao tratamento, com a adoção de mecanismos de avaliação de risco e atenção especial aos dados sensíveis;

(iii) A criação de plataformas que promovam a transparência quanto ao uso de dados pessoais e que assegurem ao cidadão o exercício de seus direitos, inclusive a possibilidade de realizar escolhas informadas sobre o tratamento de suas informações.

No âmbito da defesa da constitucionalidade do Cadastro Base do Cidadão (CBC), o Advogado-Geral da União sustentou que tal instrumento não configurava a criação de uma nova

[82] O advogado e professor Danilo Doneda foi, reconhecidamente, o precursor neste país do debate sobre a proteção de dados pessoais. Em 2006, lançou o livro "Da Privacidade à Proteção de Dados Pessoais", fruto da sua tese de doutorado na Universidade do Estado do Rio de Janeiro, distinguido como uma das mais completas obras sobre o tema no Brasil. Nos anos seguintes, se engajou nas discussões pela criação de um Marco Civil da Internet, que viria a se concretizar em 2014. Nesse sentido: (Souza, 2022).

base de dados, mas sim uma plataforma tecnológica voltada à integração e à interoperabilidade de informações já existentes, dispersas entre diversos órgãos da administração pública. A finalidade precípua do CBC, conforme argumentado, residiria na promoção da confiabilidade e da consistência entre os cadastros governamentais, por meio de mecanismos de consulta em tempo real, sem que haja duplicação ou geração autônoma de dados.

Com base em Nota Técnica emitida pelo Ministério da Economia, foi enfatizado que o CBC constituía ferramenta essencial para a autenticação digital, sendo um vetor de modernização administrativa. Destacaram-se, nesse contexto, os benefícios decorrentes de sua implementação, como a simplificação de procedimentos burocráticos, a racionalização de recursos públicos e a elevação da eficiência na prestação de serviços estatais. Ressaltou-se, ainda, que soluções análogas são amplamente adotadas em países da União Europeia, a exemplo dos chamados *Base Registries*, os quais servem de referência internacional em matéria de governança de dados.

No tocante à estrutura de governança do sistema, defendeu-se a legitimidade do Comitê Central de Governança de Dados (CCGD), instituído pelo Decreto nº 10.046/2019. Argumentou-se que a composição do colegiado — integrada por representantes da Advocacia-Geral da União, da Receita Federal, do INSS, da Casa Civil, da Secretaria Especial de Modernização do Estado e da Secretaria Especial de Desburocratização, Gestão e Governo Digital — assegurava uma perspectiva ampla e articulada das necessidades da administração pública, dada a natureza estratégica e transversal das funções desempenhadas por seus membros.

E, em 15 de setembro de 2022, o Supremo Tribunal Federal conheceu da Ação Direta de Inconstitucionalidade nº 6.649 para, no mérito, julgar parcialmente procedentes os pedidos, conferindo interpretação conforme ao Decreto n.º 10.046/2019 para subtrair do campo semântico da norma eventuais aplicações conflitantes com o direito fundamental à proteção de dados pessoais, consagrado no artigo 5º, inciso LXXIX, da Constituição Federal, e regulamentado pela Lei nº 13.709/2018 — Lei Geral de Proteção de Dados — LGPD.

O Tribunal assentou que o compartilhamento de dados pessoais entre órgãos e entidades da administração pública federal somente é legítimo quando pautado por critérios estritos, a saber: *(i)* a definição de propósitos legítimos, específicos e explícitos para o tratamento dos dados; *(ii)* a compatibilidade entre o tratamento e as finalidades previamente informadas; e *(iii)* a limitação do compartilhamento ao mínimo necessário para o cumprimento dessas finalidades. Tais exigências devem ser observadas em consonância com os princípios, garantias e procedimentos estabelecidos na LGPD, naquilo que for compatível com o setor público.

Adicionalmente, o STF reforçou o dever de publicidade previsto no artigo 23, inciso I, da LGPD, determinando que cada entidade governamental mantenha informações claras, atualizadas e acessíveis sobre as hipóteses legais, finalidades, procedimentos e práticas adotadas no tratamento e compartilhamento de dados pessoais. O acesso ao Cadastro Base do Cidadão foi condicionado ao cumprimento integral dessas diretrizes, incumbindo ao Comitê Central de Governança de Dados (CCGD) a implementação de mecanismos rigorosos de controle de acesso, a limitação do uso a órgãos que demonstrem necessidade justificada e a formalização da inclusão de novos dados, sempre sob os princípios da proporcionalidade e da razoabilidade.

No tocante às atividades de inteligência, a Corte reafirmou a necessidade de observância da legislação específica, exigindo medidas proporcionais e necessárias, procedimentos administrativos formais com controle judicial, sistemas eletrônicos de segurança e registro de acessos, além do respeito aos direitos dos titulares previstos na LGPD[83].

O STF também estabeleceu que o tratamento irregular de dados pessoais por entes públicos enseja a responsabilidade civil objetiva do Estado, com possibilidade de ação regressiva contra o agente público nos casos de dolo ou culpa. Ademais, a violação dolosa do dever de publicidade foi qualificada como ato de improbidade administrativa, sujeitando o infrator às sanções legais e disciplinares cabíveis.

Por maioria, o Plenário declarou, com efeitos *pro futuro*, a inconstitucionalidade do artigo 22 do Decreto nº 10.046/2019, mantendo, contudo, a estrutura do CCGD por um prazo de 60 dias, a fim de que o Poder Executivo promovesse sua reestruturação. Essa reconfiguração deveria assegurar ao órgão perfil institucional independente, composição plural e garantias contra interferências indevidas, de modo a fortalecer a transparência e o controle democrático sobre a governança de dados pessoais no âmbito da administração pública federal.

Sem adentrar nas discussões doutrinárias sobre a sua natureza jurídica[84] — se consiste em um mecanismo de controle de constitucionalidade, em uma técnica hermenêutica, em um princípio de conservação das normas ou numa técnica de decisão — verifica-se que a fórmula da interpretação conforme, por se desvincular da lógica binária entre constitucionalidade e

---

[83] Determinou-se ainda que fossem observados os parâmetros fixados no julgamento da ADI nº 6.529, que discutiu o fornecimento de dados à Agência Brasileira de Inteligência — ABIN. Destaca-se da Ementa do Acórdão: O fornecimento de informação entre órgãos que não cumpra os rigores formais do direito nem atenda estritamente ao interesse público, rotulado legalmente como defesa das instituições e do interesse nacional, configura abuso do direito, contrariando a finalidade legítima posta na norma legal.

[87] Para aprofundar: Andrade, 1998; e Sicca, 1999. Ambos os artigos fizeram a análise do tema, incluindo referências a entendimentos de diversos juristas.

inconstitucionalidade, revelou-se um instrumento eficaz para a resolução harmoniosa da controvérsia em torno do Decreto nº 10.046/2019.

Em seu voto, o Ministro Gilmar Mendes fundamentou a adoção da técnica decisória da interpretação conforme à Constituição como medida necessária para evitar os efeitos deletérios da eventual declaração de inconstitucionalidade do Decreto nº 10.046/2019 com efeito repristinatório[85]. Segundo o Ministro, a revogação pura e simples do referido decreto implicaria a revalidação automática do Decreto nº 8.789/2016, o qual, além de impor o compartilhamento compulsório de informações cadastrais entre todos os órgãos da administração pública federal, carecia de qualquer previsão normativa quanto à adoção de salvaguardas institucionais mínimas para a proteção de dados pessoais. Tal cenário, na avaliação do relator, agravaria o quadro de insegurança jurídica e instabilidade institucional, na medida em que restabeleceria um regime normativo ainda mais incompatível com os parâmetros constitucionais de proteção à privacidade, à autodeterminação informativa e à proporcionalidade no tratamento de dados pessoais.

Com essa abordagem interpretativa, o Supremo exerceu autocontenção judicial, respeitando o princípio da separação dos Poderes e evitando a invalidação total do ato normativo. Simultaneamente, assegurou a supremacia da Constituição e impediu desfechos potencialmente inconstitucionais, ao afastar interpretações que pudessem comprometer direitos fundamentais, especialmente o direito à proteção de dados pessoais. Trata-se, portanto, de uma manifestação paradigmática do papel contramajoritário do Judiciário, que, sem usurpar competências legislativas, garante a força normativa da Constituição e a integridade do sistema de direitos fundamentais.

Releva observar que a solução adotada pelo Supremo Tribunal Federal na ADI nº 6.649/DF, ao aplicar a técnica da interpretação conforme a Constituição, configura uma manifestação paradigmática do exercício da função contramajoritária do Poder Judiciário (Barroso, 2015). Tal atuação corresponde ao papel institucional do STF como guardião da Constituição e dos direitos fundamentais, especialmente diante de atos normativos que, embora expressem a vontade da maioria legislativa, revelem-se incompatíveis com os preceitos constitucionais. A interpretação conforme, nesse contexto, não apenas preserva a norma infraconstitucional em sua validade formal, mas também a reconcilia com os valores e

[88] Em reforço de sua argumentação, o Ministro Gilmar Mendes invocou a doutrina de Gustavo Zagrebelsky e Valeria Marcenò, ao afirmar que "a eliminação pura e simples da lei não remediaria a inconstitucionalidade, mas concorreria, paradoxalmente, para produzir resultados de inconstitucionalidade ainda mais grave".

princípios constitucionais, assegurando a supremacia da Constituição e a proteção dos direitos fundamentais frente a eventuais excessos ou omissões do legislador.

O papel contramajoritário do Supremo Tribunal Federal constitui uma das dimensões mais relevantes da jurisdição constitucional contemporânea. Conforme observa Barroso (2015), esse papel, longe de representar uma anomalia democrática, tornou-se amplamente aceito no constitucionalismo moderno, sendo legitimado por dois fundamentos principais: a proteção dos direitos fundamentais — que representam o núcleo ético mínimo e a reserva de justiça de uma comunidade política — e a salvaguarda das regras do jogo democrático, assegurando a integridade dos canais de participação política e impedindo que maiorias circunstanciais comprometam a igualdade de acesso ao processo deliberativo.

Inspirando-se em John Stuart Mill, Barroso (2015) enfatiza que a jurisdição constitucional exerce o papel de sentinela contra a tirania das maiorias, fenômeno pelo qual decisões majoritárias podem, paradoxalmente, comprometer os próprios fundamentos democráticos ao oprimir minorias ou distorcer o processo deliberativo. Nesse sentido, o STF não se opõe à democracia, mas a qualifica, ao garantir que o exercício do poder político se dê nos limites constitucionais e com respeito aos direitos fundamentais.

Essa concepção encontra expressão paradigmática no julgamento da Ação Direta de Inconstitucionalidade nº 6.649/DF, no qual o Supremo Tribunal Federal, ao adotar a técnica da interpretação conforme à Constituição, preservou a norma infraconstitucional, condicionando sua aplicação à observância dos direitos fundamentais à proteção de dados pessoais e à transparência administrativa. A decisão evidencia o exercício responsável do papel contramajoritário do Judiciário: o STF atuou com autocontenção, respeitando a separação de Poderes, mas sem abdicar de sua função de guardião da Constituição.

Ao condicionar a validade do decreto à observância dos princípios da proporcionalidade, da finalidade e da publicidade — nos termos da LGPD —, o Tribunal reafirmou que a democracia não se esgota na vontade da maioria, exigindo também o respeito a direitos fundamentais e a garantias institucionais. Configurou-se, assim, um exemplo de como a jurisdição constitucional pode harmonizar a preservação normativa com a supremacia constitucional, assegurando a integridade do Estado Democrático de Direito.

Com base nos parâmetros fixados no julgamento da ADI nº 6.649/DF, o Supremo Tribunal Federal preservou o núcleo essencial dos direitos fundamentais e reconheceu a constitucionalidade do Decreto nº 10.046/2019, que passou, assim, a exercer papel normativo relevante ao regulamentar, no âmbito da Administração Pública, o compartilhamento de dados

pessoais à luz da Lei Geral de Proteção de Dados (LGPD) e da Lei de Acesso à Informação (LAI).

Além da técnica da interpretação conforme à Constituição, outra ferramenta decisória empregada pelo STF, que merece aqui destaque, foi a modulação dos efeitos da declaração de inconstitucionalidade do artigo 22 do referido decreto. Tal medida encontra respaldo no artigo 27 da Lei nº 9.868/1999[86], que disciplina o processo e julgamento das ações diretas de inconstitucionalidade e das ações declaratórias de constitucionalidade. Esse dispositivo autoriza o Supremo a restringir os efeitos da decisão ou a fixar sua eficácia a partir do trânsito em julgado ou de outro momento, desde que presentes razões de segurança jurídica ou de excepcional interesse social.

Superando o dogma de que lei inconstitucional é lei nula[87], o art. 27 da Lei n.º 9.868/1999 — fortemente inspirado na Constituição Portuguesa de 1976[88] — institucionalizou a ponderação de interesses como fundamento para a modulação temporal dos efeitos em controle de constitucionalidade.

Evidencia-se, nesse contexto, um nítido caráter consequencialista da norma, ao conduzir a aplicação da técnica da modulação de efeitos pelo Supremo Tribunal Federal à consideração dos efeitos práticos e concretos que essa decisão pode gerar na realidade social, política, econômica e jurídica. Trata-se de uma manifestação do constitucionalismo contemporâneo, que busca equilibrar a supremacia da Constituição com a estabilidade institucional e a previsibilidade normativa.

Um exame mais detido da técnica de modulação temporal dos efeitos em sede de controle de constitucionalidade revela sua inserção em uma perspectiva pragmática de decisão judicial. Essa técnica não se limita a um instrumento de ajuste temporal da eficácia das decisões

---

[89] No ano 2000, o Conselho Federal da Ordem dos Advogados do Brasil ajuizou ação direta de inconstitucionalidade contra esse dispositivo da Lei nº 9.868/99, a qual foi julgada nos seguintes termos: "É constitucional a norma contida no art. 27 da Lei nº 9.868/99, que permite a modulação de efeitos, pelo Supremo Tribunal Federal, da decisão que declara a inconstitucionalidade de lei ou ato normativo. " (STF. Plenário. ADI 2154/DF e ADI 2258/DF, Rel. Min. Dias Toffoli, redatora do acórdão Min. Cármen Lúcia, julgados em 03/04/2023 — Info 1089).

[90] Nesse sentido, confira-se o AI 631533/RJ (Brasil, 2007): "O dogma da nulidade da lei inconstitucional pertence à tradição do direito brasileiro. A teoria da nulidade tem sido sustentada por importantes constitucionalistas. Fundada na antiga doutrina americana, segundo a qual *"the unconstitutional statute is not law at all"*, significativa parcela da doutrina brasileira posicionou-se pela equiparação entre inconstitucionalidade e nulidade. Afirmava-se, em favor dessa tese, que o reconhecimento de qualquer efeito a uma lei inconstitucional importaria na suspensão provisória ou parcial da Constituição. Razões de segurança jurídica podem revelar-se, no entanto, aptas a justificar a não-aplicação do princípio da nulidade da lei inconstitucional.

[91] Sobre os efeitos da declaração de inconstitucionalidade, dispõe o artigo 282.º da Constituição da República Portuguesa (Portugal, 2005): "4. Quando a segurança jurídica, razões de equidade ou interesse público de excecional relevo, que deverá ser fundamentado, o exigirem, poderá o Tribunal Constitucional fixar os efeitos da inconstitucionalidade ou da ilegalidade com alcance mais restrito do que o previsto nos n.s. 1 e 2. "

do Supremo Tribunal Federal, mas incorpora, em sua própria estrutura, três elementos fundamentais: o consequencialismo, o antifundacionalismo e o contextualismo.

Conforme argumenta Melo (2021), a modulação de efeitos representa uma ruptura com o dogma da nulidade absoluta da norma inconstitucional, ao admitir sua eficácia residual com base em razões de segurança jurídica ou de excepcional interesse social — evidenciando seu caráter antifundacionalista. Além disso, a autora destaca que sua aplicação exige uma análise atenta do contexto fático, político, econômico e social em que se insere a norma impugnada, o que a aproxima de uma abordagem contextualista. Por fim, a técnica demanda a antecipação dos efeitos concretos da decisão, com vistas à obtenção de um ponto de equilíbrio entre a preservação da ordem jurídica e a proteção dos direitos fundamentais, o que a caracteriza como essencialmente consequencialista.

5.2.1 Do Cadastro Único para Programas Sociais do Governo Federal (CadÚnico).

> O Cadastro Único proporciona uma visão abrangente da parcela mais vulnerável da população brasileira, permitindo que os governos em todos os níveis saibam quem são essas famílias, onde vivem, suas condições de vida e suas necessidades (Brasil, [2025]).

Para melhor perceber a complexidade da controvérsia constitucional submetida ao crivo do Supremo Tribunal Federal na Ação Direta de Inconstitucionalidade nº 6.649, é imprescindível considerar, além do Cadastro Base do Cidadão instituído pelo Decreto nº 10.046/2019, a existência do Cadastro Único para Programas Sociais do Governo Federal (CadÚnico), instrumento igualmente relevante na política de gestão de dados pessoais pelo Estado.

Consoante o exposto na justificativa deste trabalho, no ano de 2022, a Secretaria Nacional do Cadastro Único (SECAD), vinculada à época ao Ministério da Cidadania, solicitava o acesso à base de dados de servidores do Poder Judiciário, com fundamento no Decreto nº 10.046/2019 e sob a justificativa de identificar eventuais inconsistências na qualificação dos beneficiários registrados no CadÚnico.

Instituído pelo art. 6º-F da Lei nº 8.742/1993, incluído pela Lei nº 14.284/2021, o CadÚnico configurava-se, à época do julgamento da ADI nº 6.649, como um registro público eletrônico destinado à coleta, processamento, sistematização e disseminação de informações

georreferenciadas[89], com o objetivo de identificar e caracterizar socioeconomicamente as famílias de baixa renda em todo o território nacional. Tal estrutura, embora voltada à eficiência na promoção de políticas públicas, suscitava relevantes questionamentos quanto à compatibilidade de seus mecanismos de interoperabilidade com os princípios constitucionais da proteção de dados pessoais, da legalidade, da finalidade e da proporcionalidade.

Regulamentado pelo Decreto nº 11.016/2022, o CadÚnico constituiu-se em instrumento essencial para a coleta, o processamento, a sistematização e a disseminação de informações destinadas à identificação e à caracterização socioeconômica das famílias de baixa renda residentes no território nacional. Trata-se de uma base de dados estruturada que subsidia a formulação, a implementação, o monitoramento e a avaliação de políticas públicas nos âmbitos federal, estadual, distrital e municipal, sendo, portanto, um pilar da atuação estatal voltada à redução das desigualdades sociais.

A gestão nacional do CadÚnico é atualmente atribuída ao Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome, em razão de sua competência para coordenar os programas federais de transferência de renda. Ressalte-se, contudo, que se trata de uma política pública de caráter federativo, cuja operacionalização é compartilhada e descentralizada entre a União, os estados, o Distrito Federal e os municípios.

Além dos entes federativos, o sistema é acessado pela Caixa Econômica Federal, na qualidade de agente operador contratado para o processamento dos dados cadastrais, reforçando a complexidade institucional e a necessidade de rigor na governança da informação (Caixa Econômica Federal, 2023).

Conforme informações divulgadas pelo Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome (BRASIL, 2025), o Cadastro Único (CadÚnico) representa o principal instrumento do Estado brasileiro para viabilizar a inclusão de cidadãos em programas de benefícios sociais, como o Programa Bolsa Família, o Pé-de-Meia, a Tarifa Social de Energia Elétrica, o Auxílio Gás e o Programa Minha Casa Minha Vida, entre outros, com interligação *online* de diferentes bases de dados governamentais, voltada à automatização de processos e à maior precisão na identificação dos beneficiários.

Ocorre que, antes do julgamento da Ação Direta de Inconstitucionalidade nº 6.649, em 2022, a interconexão de bases de dados sob a custódia do Poder Público e o uso secundário de dados pessoais — isto é, a utilização dessas informações para finalidades distintas daquelas que

[89] Atualmente, vigora a redação conferida ao art. 6º-F da Lei nº 8.742/1993 pela Lei nº 14.601/2023, a qual suprimiu a exigência de coleta de coordenadas geográficas no âmbito do Cadastro Único para Programas Sociais do Governo Federal (CadÚnico).

motivaram sua coleta original — configuravam tema controverso e objeto de intensos debates jurídicos e doutrinários[90]. Tal controvérsia refletia a crescente complexidade do tratamento de dados pessoais no âmbito da Administração Pública, especialmente diante da ausência de parâmetros normativos e jurisprudenciais claros que delimitassem os contornos e as condições para o compartilhamento legítimo dessas informações.

Entretanto, como já destacado, o Supremo Tribunal Federal (STF) havia reconhecido, ainda antes da promulgação da Emenda Constitucional nº 115/2022, o direito fundamental autônomo à proteção de dados pessoais, conforme decidido no julgamento da ADI nº 6387. Na ocasião, a Corte entendeu que o compartilhamento de dados deve observar os princípios da necessidade, adequação, proporcionalidade e finalidade, além de garantir mecanismos técnicos e administrativos aptos a proteger os dados contra acessos não autorizados e vazamentos.

Posteriormente, no julgamento conjunto da ADI nº 6649 e da ADPF nº 695, o STF firmou entendimento no sentido de que o ordenamento jurídico brasileiro não autoriza o fluxo irrestrito de dados pessoais no âmbito da Administração Pública. A Corte validou o compartilhamento de dados entre órgãos públicos, desde que observados critérios rigorosos, como a existência de propósitos legítimos, específicos e explícitos, a limitação ao mínimo necessário e a adoção de mecanismos de controle e transparência compatíveis com a LGPD.

Assim, o compartilhamento de dados entre órgãos e entidades estatais, especialmente para fins diversos daqueles que justificaram sua coleta, deve observar critérios rigorosos, tais como as expectativas razoáveis do titular, a natureza sensível dos dados tratados e os potenciais prejuízos decorrentes da exposição indevida dessas informações. A conformidade com os princípios constitucionais e legais de proteção de dados é condição indispensável para a legitimidade do tratamento, sob pena de responsabilização civil e administrativa dos agentes públicos envolvidos.

Ademais, destaca-se o princípio da finalidade, previsto no art. 6º, inciso I, da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 — LGPD), o qual se apresenta como desdobramento do princípio da autodeterminação informativa. Esse princípio impõe que o tratamento de dados, inclusive em sua vertente secundária, seja compatível com a finalidade original da coleta, restringindo-se a propósitos legítimos, específicos e explícitos. A inobservância desse parâmetro configura violação aos direitos fundamentais à privacidade, à intimidade e à dignidade da pessoa humana. Dessa forma, a interpretação normativa e jurisprudencial consolidada pela LGPD e pelo STF estabelece um paradigma jurídico que

[90] Nesse sentido: Ferreira, 2020.

orienta a governança pública de dados pessoais, exigindo equilíbrio entre a eficiência administrativa e a proteção efetiva dos direitos dos titulares.

6 ANÁLISE DAS PRÁTICAS DE COMPARTILHAMENTOS DE DADOS PESSOAIS PELO PODER PÚBLICO POSTERIORES AOS PARADIGMAS JULGADOS PELO SUPREMO TRIBUNAL FEDERAL.

> Não obstante, assim como ocorre com as demais operações de tratamento, o uso compartilhado de dados pessoais deve ser realizado em conformidade com a LGPD, notadamente com os princípios, as bases legais, garantia dos direitos dos titulares e outras regras específicas aplicáveis ao Poder Público[91].

Conseguinte a um avanço cultural verificado na sociedade brasileira, verificou-se uma evolução progressiva na jurisprudência do Supremo Tribunal Federal no tocante à proteção de dados pessoais. O entendimento inicialmente restritivo — que limitava a tutela constitucional à comunicação de dados[92] — foi gradualmente superado por uma concepção mais abrangente, segundo a qual toda informação que permita, direta ou indiretamente, a identificação de uma pessoa natural deve ser considerada dado pessoal. Nesse novo paradigma, tais informações passaram a integrar o escopo de proteção das garantias constitucionais voltadas à liberdade individual (art. 5º, caput), à privacidade e ao livre desenvolvimento da personalidade (art. 5º, incisos X e XII), consolidando uma leitura mais coerente com os desafios da sociedade da informação[93].

Nessa trajetória jurisprudencial evolutiva, o julgamento da Ação Direta de Inconstitucionalidade nº 6.387 representou um marco relevante ao afirmar que o compartilhamento de dados pessoais, mesmo quando realizado entre entes públicos e concessionárias de serviço público, deve observar mecanismos vigorosos de proteção e segurança da informação, em estrita consonância com os direitos fundamentais à privacidade, à autodeterminação informativa e à transparência. Essa compreensão foi decisiva para influenciar os fundamentos adotados no julgamento da Ação Direta de Inconstitucionalidade nº 6.649, no qual o Supremo Tribunal Federal consolidou parâmetros constitucionais mais estritos para o compartilhamento de dados pelo Poder Público, produzindo efeitos estruturantes sobre o regime jurídico da governança de dados no setor público.

Integrada na cultura desse ecossistema informacional contemporâneo, a Agência Nacional de Proteção de Dados (ANPD), como órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para a sua implementação[94], por meio de seu Guia

---

[91] Guia Orientativo de Tratamento de dados pessoais pelo Poder público. (ANPD, 2023).
[92] HC 91.867 / PA.
[93] ADI 6387 / DF
[94] Art. 55-K da LGPD.

Orientativo, informa que o compartilhamento de dados pessoais pelo Poder Público deve observar requisitos fundamentais que garantam a conformidade com a Lei Geral de Proteção de Dados (LGPD) e a proteção dos direitos dos titulares (ANPD, 2023). Entre esses requisitos destacam-se a formalização e o registro detalhado do compartilhamento, a delimitação clara e restrita da finalidade vinculada a políticas públicas ou atribuições legais, e a fundamentação em base legal adequada.

Além disso, impõe-se a observância do princípio da necessidade, limitando o tratamento ao mínimo indispensável, a transparência quanto ao compartilhamento e aos direitos dos titulares, bem como a adoção de medidas técnicas e administrativas robustas para assegurar a segurança e a prevenção contra acessos ou usos indevidos. Por fim, o Guia reforça a importância da governança responsável, com mecanismos de controle, avaliação de riscos e responsabilização, consolidando um modelo de compartilhamento legítimo, seguro e respeitoso dos direitos fundamentais na administração pública.

Nessa senda, o Supremo Tribunal Federal (STF), no julgamento da ADI nº 6.649, estabeleceu parâmetros claros e rigorosos para o compartilhamento de dados pessoais entre órgãos e entidades públicas, garantindo a proteção do direito fundamental à privacidade e à proteção de dados. Entre os principais requisitos, destaca-se a necessidade de eleição de propósitos legítimos, específicos e explícitos para o tratamento dos dados, a compatibilidade do uso com as finalidades informadas e a limitação do compartilhamento ao mínimo necessário para atender a essas finalidades, em conformidade com a Lei Geral de Proteção de Dados (LGPD).

Ademais, o compartilhamento deve observar o dever de publicidade previsto no artigo 23 da LGPD, exigindo que as entidades públicas forneçam informações claras e atualizadas sobre as bases legais, finalidades e procedimentos adotados, garantindo transparência e controle social. E o acesso ao Cadastro Base do Cidadão restou condicionado à comprovação da real necessidade e à implementação de mecanismos rigorosos de controle, limitando-se a informações indispensáveis ao interesse público.

O STF também reforçou que o tratamento irregular de dados pessoais pelo Poder Público acarreta responsabilidade civil do Estado e responsabilização administrativa dos agentes públicos, incluindo a possibilidade de sanções por improbidade administrativa em caso de violação dolosa do dever de publicidade.

Por fim, a Corte determinou a reestruturação do Comitê Central de Governança de Dados, visando conferir-lhe perfil independente, plural e garantias contra influências indevidas,

consolidando um marco jurisprudencial que equilibra a eficiência administrativa com a proteção dos direitos fundamentais na sociedade da informação.

Com vistas a sistematizar os principais pontos de convergência entre as orientações da ANPD e os parâmetros firmados pelo STF, apresenta-se, a seguir, um quadro comparativo que evidencia a construção de um arcabouço normativo e jurisprudencial, voltado à legitimação do compartilhamento de dados pessoais no setor público, em estrita observância aos direitos fundamentais e à eficiência administrativa:

Tabela 01 – Comparativo ANPD e Jurisprudência STF

Parâmetros/Requisitos	Guia Orientativo da ANPD	Acórdão do STF na ADI nº 6.649
Formalização e Registro	Exige formalização prévia e registro detalhado do compartilhamento, com análise técnica e jurídica que justifique a operação.	Determina que o compartilhamento deve observar diretrizes claras, com controle rigoroso pelo Comitê Central de Governança de Dados (CCGD).
Objeto e Finalidade	Compartilhamento deve ter finalidade específica, legítima e restrita ao mínimo necessário para o cumprimento do interesse público.	Exige eleição de propósitos legítimos, específicos e explícitos, compatíveis com as finalidades informadas (art. 6º, I e II da LGPD).
Base Legal	Necessária fundamentação legal clara para o compartilhamento, conforme artigos 7º e 11 da LGPD.	Compartilhamento condicionado ao cumprimento integral dos requisitos legais e constitucionais da LGPD, respeitando princípios da proporcionalidade e necessidade.
Duração do Tratamento	Limitação temporal do tratamento, vinculada à finalidade específica, evitando retenção indevida.	Limitação do compartilhamento ao mínimo necessário para a finalidade pública, conforme princípios da LGPD.
Transparência e Direitos dos Titulares	Obrigação de informar os titulares sobre o compartilhamento, suas finalidades e direitos, garantindo controle social.	Determina mecanismos rigorosos de controle de acesso, sistema eletrônico de registro para responsabilização e medidas de segurança compatíveis com a LGPD.
Prevenção e Segurança	Adoção de medidas técnicas e administrativas robustas para proteção contra acessos indevidos, vazamentos e abusos.	Determina mecanismos rigorosos de controle de acesso, sistema eletrônico de registro para responsabilização e medidas de

		segurança compatíveis com a LGPD.
Governança e Responsabilização	Reforça a necessidade de governança adequada, com avaliação de riscos, controle e responsabilização dos agentes.	Estabelece responsabilidade civil do Estado e responsabilização administrativa e penal dos agentes públicos em caso de tratamento irregular ou doloso.
Participação e Independência	Recomenda pluralidade e transparência na governança dos dados públicos, com participação da sociedade civil.	Determina reestruturação do CCGD para perfil independente e plural, com garantias contra influências indevidas, ampliando a participação democrática

Fonte: Autoria própria.

Em resposta aos parâmetros fixados no Acórdão do STF na ADI nº 6.649, foi editado, cerca de dois meses após a publicação da ata de julgamento, o Decreto nº 11.266, de 25 de novembro de 2022, com o objetivo de promover ajustes no Decreto nº 10.046, de 9 de outubro de 2019, de modo a alinhá-lo às exigências delineadas pelo Supremo Tribunal Federal. Posteriormente, o referido decreto foi novamente alterado pelo Decreto nº 11.574, de 2023, especialmente no que se refere à reconfiguração de competências de determinados órgãos responsáveis pela execução das atividades previstas na norma. Como bem observou Pedrazzoli (2023), essa última modificação está diretamente relacionada à reestruturação administrativa decorrente da mudança de gestão no Governo Federal em 2023.

O Decreto nº 10.046/2019, principal diploma que regula a governança no compartilhamento de dados no âmbito da Administração Pública federal, foi substancialmente reformulado para se alinhar aos princípios constitucionais e às diretrizes da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 — LGPD).

A primeira e mais emblemática alteração foi a incorporação expressa dos princípios da finalidade, adequação e necessidade, previstos no artigo 6º da LGPD, ao rol de diretrizes obrigatórias do Decreto, por meio da inclusão dos incisos VII a IX no artigo 3º. Essa medida reforça a exigência de que o compartilhamento de dados entre órgãos públicos observe critérios estritos de proporcionalidade e pertinência, evitando práticas arbitrárias ou desnecessárias.

No tocante à transparência, os §§ 1º e 2º do artigo 5º foram reformulados para assegurar que as operações de compartilhamento sejam publicizadas de forma clara e acessível, promovendo o controle social e a *accountability* administrativa. A exigência de autorização formal do gestor de dados para compartilhamentos em níveis restrito e específico, prevista nos

§§ 3º e 4º do mesmo artigo, introduziu um filtro adicional de legalidade e legitimidade, subordinando tais operações às diretrizes do Comitê Central de Governança de Dados (CCGD), à LGPD, à Lei de Acesso à Informação (Lei nº 12.527/2011), à Lei do Governo Digital (Lei nº 14.129/2021) e às orientações da Agência Nacional de Proteção de Dados (ANPD).

No que se refere ao Cadastro Base do Cidadão (CBC), o artigo 17 passou a prever, em seu § 2º, que o acesso à base deve observar os princípios da LGPD, enquanto o § 3º atribui ao CCGD a competência para estabelecer mecanismos rigorosos de controle de acesso, limitando-o a órgãos que demonstrem necessidade concreta. O § 7º do mesmo artigo exige justificativa formal prévia para a inclusão de novos dados na base, e o artigo 20-A institui sistemas eletrônicos de registro de acesso, com vistas à responsabilização em caso de uso indevido.

A inovação mais relevante em termos de responsabilização estatal foi a introdução do artigo 15-A, que explicita a responsabilidade civil objetiva do Estado por danos decorrentes do tratamento indevido de dados pessoais, com previsão de ação regressiva contra agentes públicos nos casos de dolo ou culpa, em consonância com o artigo 37, § 6º, da Constituição Federal.

Por fim, o redesenho institucional do CCGD, promovido pelos artigos 22 a 25, conforme redação dada pelo Decreto nº 11.574/2023, fortaleceu a governança democrática e plural do sistema. Destacam-se a substituição da Secretaria Especial de Desburocratização por representante do órgão central do SISP, a inclusão de representantes do Ministério da Justiça e de organizações da sociedade civil com atuação comprovada em proteção de dados, selecionados por processo público e com direito a voto, além da participação de membros convidados do CNJ, Senado e Câmara dos Deputados.

Essas alterações, de fato, favoreceram a adoção de um modelo de governança pública orientado por princípios constitucionais, transparência, controle social e responsabilidade institucional.

Percebe-se, contudo, que as alterações promovidas no Decreto nº 10.046/2019 após o julgamento da Ação Direta de Inconstitucionalidade nº 6.649 não conferem a completa aderência àquele Acórdão, tampouco ao Guia Orientativo da ANPD, porquanto evidenciam a persistência de lacunas normativas e desafios institucionais que ainda demandam enfrentamento rigoroso para assegurar a plena efetividade da proteção constitucional de dados pessoais pelo Poder Público.

Embora o Supremo Tribunal Federal tenha conferido interpretação conforme à Constituição à norma impugnada — evitando sua invalidação e preservando a continuidade do programa normativo — subsistem questões relevantes ainda não suficientemente equacionadas, entre as quais se destaca a persistente fragilidade dos mecanismos de segurança do Cadastro

Base do Cidadão (CBC), cuja estrutura técnica e normativa carece de aprimoramentos compatíveis com os padrões exigidos pela LGPD e pelo STF.

Tal preocupação, amplamente debatida no âmbito da ADI, não foi objeto de solução normativa concreta nas alterações subsequentes ao decreto. Essa omissão revela-se particularmente preocupante, uma vez que a segurança da base integradora constitui elemento essencial para a proteção da privacidade e da autodeterminação informacional dos cidadãos. Diante disso, impõe-se ao Comitê Central de Governança de Dados (CCGD) a adoção de medidas técnicas e administrativas robustas, capazes de mitigar riscos de acessos indevidos, vazamentos e usos abusivos de dados, sob pena de comprometimento da legitimidade constitucional do modelo de governança informacional adotado.

Outro ponto crítico, conforme destacado por Pedrazzoli (2023), diz respeito à ausência de clareza normativa quanto à articulação entre as figuras do gestor de dados, prevista no Decreto nº 10.046/2019, e do encarregado pelo tratamento de dados pessoais, instituído pela Lei Geral de Proteção de Dados Pessoais (LGPD). Essa indefinição compromete a delimitação precisa de competências e responsabilidades, gerando insegurança jurídica e operacional no âmbito da Administração Pública federal. Tal ambiguidade pode fragilizar a efetividade da governança de dados e dificultar a responsabilização em casos de violação de direitos.

Soma-se a isso a preocupação com o desenho institucional do Comitê Central de Governança de Dados (CCGD), cuja composição suscita dúvidas quanto à sua independência e pluralidade[95]. Apesar da previsão de participação de dois representantes da sociedade civil, a maioria dos membros é oriunda da própria Administração Pública Federal, e as decisões podem ser tomadas por maioria simples, concentrando o poder decisório nas mãos do Executivo. Essa configuração, como observa a autora, contrasta com modelos mais democráticos e participativos, como o do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, que apresenta composição mais diversificada e mecanismos institucionais mais robustos de controle social e participação plural.

Além daquelas fragilidades institucionais apontadas por Pedrazzoli (2023), subsiste um dos problemas mais graves do Decreto nº 10.046/2019, não obstante as alterações promovidas

[95] Conforme o Art. 22 do Decreto nº 10.046/2019, essa é a Composição do CCGD: Secretaria de Governo Digital, que o preside; Advocacia-Geral da União; Casa Civil da Presidência da República; Secretaria de Transparência e Prevenção da Corrupção da Controladoria-Geral da União; Secretaria Especial da Receita Federal do Brasil; Ministério da Justiça e Segurança Pública; Ministério da Previdência Social; Ministério do Trabalho e Emprego; LAPIN — Laboratório de Políticas Públicas e Internet; GovDados — Governança de dados no setor público; Banco Central do Brasil, na qualidade de membro convidado; Conselho Nacional de Justiça, na qualidade de membro convidado; Senado Federal, na qualidade de membro convidado; e Câmara dos Deputados, na qualidade de membro convidado. Cumpre ressaltar que a indicação dos membros convidados é facultativa, ato discricionário dos órgãos representados.

pelos Decretos nº 11.266/2022 e nº 11.574/2023: a ausência de transparência no compartilhamento de dados pessoais entre entidades públicas. O artigo 5º do Decreto original — não alterado pelas modificações posteriores — continua a dispensar a celebração de convênios, acordos de cooperação técnica ou instrumentos congêneres para viabilizar o compartilhamento, resultando em uma falta de transparência efetiva para o cidadão quanto aos dados compartilhados e os órgãos envolvidos nessa troca. Essa dispensa contrasta, paradoxalmente, com a exigência de observância das diretrizes do artigo 3º do próprio Decreto e da Lei Geral de Proteção de Dados (LGPD), que estabelecem, entre outros princípios, a auditabilidade e a prestação de contas no tratamento de dados pessoais.

A ausência de formalização por meio de instrumentos que registrem e regulamentem o compartilhamento compromete severamente a auditabilidade, dificultando o controle e a fiscalização das operações, além de fragilizar a responsabilização em casos de uso indevido. O princípio da prestação de contas, previsto no artigo 6º, inciso X, da LGPD, impõe ao agente de tratamento o dever de demonstrar o cumprimento das normas de proteção de dados. Tal dever, no entanto, torna-se praticamente inviável diante da inexistência de mecanismos formais que documentem e justifiquem essas operações. Como exemplo, a ausência de registros pode inviabilizar a identificação de responsabilidades em casos de vazamento ou uso indevido de dados sensíveis.

Sob a perspectiva administrativa e constitucional, o compartilhamento de dados pessoais pelo Poder Público configura uma atividade sujeita aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência, conforme estabelece o artigo 37 da Constituição Federal. A ausência de formalização e transparência fere diretamente o princípio da publicidade, dificultando o controle social e institucional sobre o uso dos dados e comprometendo a governança democrática e o respeito aos direitos fundamentais dos titulares.

Nesse contexto, a Agência Nacional de Proteção de Dados (ANPD, 2023) orienta que o uso compartilhado de dados pessoais pelo Poder Público deve ser formalizado, seja em conformidade com as normas gerais que regem os procedimentos administrativos, seja em observância à obrigatoriedade de registro das operações de tratamento, conforme dispõe o artigo 37 da LGPD. Tal formalização é imprescindível para garantir transparência, auditabilidade, responsabilização e, consequentemente, a legitimidade e a segurança jurídica das operações de compartilhamento — protegendo, assim, não apenas a privacidade, mas também a confiança pública na atuação estatal.

Outro problema que remanesce no Decreto nº 10.046/2019, mesmo após as alterações introduzidas pelos Decretos nº 11.266/2022 e nº 11.574/2023, relaciona-se à terminologia

adotada para definir os dados pessoais. O texto normativo continua a utilizar expressões como “atributos biográficos”, “atributos biométricos” e “atributos genéticos”, que divergem não apenas da Lei Geral de Proteção de Dados Pessoais (LGPD), mas também de outras legislações fundamentais do ecossistema informacional brasileiro, como a Lei de Acesso à Informação (Lei nº 12.527/2011) e o Marco Civil da Internet (Lei nº 12.965/2014).

Ocorre que essa escolha terminológica não se limita a uma mera opção semântica, mas implica consequências jurídicas relevantes, porquanto cria uma desconexão conceitual e normativa que pode gerar insegurança jurídica e dificultar a harmonização das normas que regulam o tratamento e a proteção dos dados pessoais no país.

A LGPD, por exemplo, adota definições claras e amplamente reconhecidas internacionalmente para “dados pessoais” e “dados pessoais sensíveis”, englobando informações que identificam ou podem identificar uma pessoa natural, incluindo categorias especiais como dados biométricos e genéticos, com proteção reforçada. Ao substituir esses termos, o Decreto nº 10.046/2019 — não obstante as modificações introduzidas — alarga de forma imprecisa e obscurece o conceito de dados pessoais, ao definir “atributos biográficos” como “dados relativos aos fatos da vida” da pessoa natural, abrangendo uma gama ampla e indeterminada de informações. Essa vagueza pode permitir interpretações extensivas e usos que ultrapassem os limites previstos na LGPD, comprometendo direitos fundamentais como a privacidade, a autodeterminação informativa e a dignidade da pessoa humana.

Além disso, a terminologia adotada pelo Decreto dificulta a interoperabilidade normativa e a aplicação uniforme das regras de proteção de dados, uma vez que órgãos públicos, operadores de dados e titulares podem enfrentar dificuldades para compreender e aplicar os conceitos coerentemente, gerando riscos de tratamentos inadequados ou abusivos.

Assim, não obstante os aprimoramentos normativos realizados no Decreto nº 10.046/2019, constata-se que sua estrutura ainda revela deficiências institucionais e procedimentais que comprometem a plena conformidade com os parâmetros constitucionais delineados pelo Supremo Tribunal Federal, especialmente no julgamento da ADI nº 6649. A Corte Suprema assentou que o compartilhamento de dados pessoais no âmbito da Administração Pública deve observar finalidades legítimas, específicas e explícitas, além de respeitar os princípios da necessidade, da proporcionalidade e da transparência, conforme preconizado pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Portanto, revela-se imprescindível uma nova e criteriosa revisão do Decreto nº 10.046/2019, sob pena de perpetuar um modelo normativo desalinhado com os direitos fundamentais e com os avanços da cidadania digital. Tal revisão deve visar à consolidação de

um modelo de governança de dados públicos que assegure segurança jurídica, pluralismo institucional, controle social efetivo e aderência estrita aos direitos fundamentais à privacidade e à proteção de dados — pilares essenciais da ordem constitucional vigente e da sociedade da informação.

6.1 A POLÍTICA DE GOVERNANÇA DE DADOS

> Governments using data in an ethical way to improve public services quality and increase public value, while strengthening democratic standards and avoiding discrimination, must be the norm. (Organisation for Economic Co-operation and Development, 2019).

Conforme divulgado pelo Ministério da Gestão e da Inovação em Serviços Públicos, na quarta-feira, 23/7/2025, o Governo Federal abriu uma consulta pública para debater com a sociedade a criação da Política de Governança e Compartilhamento de Dados. O principal objetivo da proposta é pautar as políticas e os serviços públicos pelo uso estratégico dos dados, promovendo maior eficiência, transparência e eficácia na administração pública (Brasil, 2025).

Para tanto, foi apresentada para discussão uma minuta de decreto[96], que institui a Política de Governança de Dados no âmbito da administração pública federal direta, autárquica e fundacional. Trata-se de ato normativo destinado a revogar o Decreto nº 10.046, de 9 de outubro de 2019, representando um avanço significativo no ordenamento jurídico brasileiro, especialmente em razão da amplitude e do grau de detalhamento das diretrizes relativas à governança, interoperabilidade e compartilhamento de dados.

O novo decreto representa mais uma iniciativa voltada ao fortalecimento da Infraestrutura Nacional de Dados (IND), com o propósito de orientar os órgãos públicos no uso estratégico de dados, visando à formulação de políticas públicas mais eficazes e à prestação de serviços com maior eficiência, segurança e transparência, inclusive mediante o emprego de tecnologias como a Inteligência Artificial (Brasil, 2025).

Todavia, sob a ótica da observância à Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD), é imprescindível analisar a minuta com olhar crítico para aferir sua adequação, suficiência e segurança jurídica.

---

[96] BRASIL. **Minuta de decreto**. Institui a Política de Governança de Dados, dispõe sobre a interoperabilidade e o compartilhamento de dados e sobre registros de referência no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Disponível em: https://brasilparticipativo.presidencia.gov.br/processes/politicadedados/media. Acesso em: 17 ago. 2025.

A minuta de decreto reconhece expressamente a necessidade de que o compartilhamento de dados se dê em observância aos princípios e parâmetros estabelecidos na LGPD, conforme se confere nos artigos 2º e 24, e consagra como princípio estruturante o tratamento ético dos dados pessoais, com ênfase no respeito aos direitos dos titulares e na observância das diretrizes emanadas da Agência Nacional de Proteção de Dados (ANPD).

Além disso, reforça a aplicação do princípio da necessidade, restringindo o compartilhamento de dados pessoais ao estritamente necessário para o cumprimento das finalidades legítimas dos órgãos e entidades públicas[97], conforme previsto no parágrafo único do artigo 24 do projeto.

Não obstante esse avanço normativo, exige aprimoramentos, especialmente quanto à operacionalização prática desses princípios. No que se refere às bases legais do tratamento, por exemplo, embora a LGPD preveja hipóteses nas quais o consentimento do titular não é exigido, o decreto deveria explicitar com maior clareza os procedimentos de verificação da legitimidade, especificidade e transparência das finalidades públicas, assegurando o cumprimento dos deveres de informação e prestação de contas impostos ao Poder Público.

No tocante à segurança da informação, embora a minuta mencione genericamente a necessidade de garantir a proteção dos dados e da infraestrutura tecnológica (art. 4º, III), carece de normatização mais robusta quanto à adoção de medidas técnicas e administrativas concretas para mitigação de riscos. A ausência de diretrizes específicas sobre práticas como criptografia, anonimização, controle de acesso e auditorias periódicas compromete a efetividade da proteção de dados no contexto da interoperabilidade e do compartilhamento interinstitucional, contrariando não apenas os comandos da LGPD, mas também os padrões internacionais de boas práticas em governança de dados.

Sob o enfoque da governança, o Decreto institui uma estrutura organizacional clara, com papéis bem definidos para o Executivo de Dados, curadores, curadores corporativos, unidades de tecnologia da informação e encarregados de dados (Art. 9º e seguintes). A segregação de funções e a vedação de acúmulo entre o encarregado de dados e executivos/curadores (Art. 20) evidenciam a preocupação com a independência e especialização das atividades relativas à proteção dos dados pessoais.

O capítulo dedicado à interoperabilidade e ao compartilhamento de dados (Capítulo IV) está alinhado ao paradigma da eficiência e inovação na administração pública. São explicitados

[97] Miriam Wimmer esclarece que a finalidade ampla de "atendimento de políticas públicas" não seria compatível com o compartilhamento de dados pessoais, devendo ser apurada à luz das competências específicas de cada órgão (Pernambuco, 2023).

objetivos legítimos do compartilhamento, incluindo o atendimento ao interesse público e a melhoria das políticas públicas.

A minuta promove o reuso dos dados para evitar coleta redundante e privilegia o compartilhamento via interoperabilidade, que deve respeitar requisitos legais e de segurança. No entanto, apresenta lacunas em relação a instrumentos jurídicos suficientes para garantir a conformidade com os princípios da LGPD e outras normas pertinentes, na medida em que dispensa a formalização por convênios ou acordos para o compartilhamento (Art. 27).

A formalização jurídica do compartilhamento de dados entre entes públicos, sobretudo quando envolve dados pessoais ou informações sensíveis, constitui exigência inafastável no Estado Democrático de Direito. O acesso, a disponibilização ou a transferência consensual de dados entre órgãos e entidades ou sistemas de órgãos e entidades, incluído o uso compartilhado de dados pessoais, não pode ser tratado como mera questão técnica ou informal, sob pena de comprometimento da segurança jurídica, da proteção de direitos fundamentais e da legitimidade da atuação administrativa.

A complexidade das obrigações envolvidas impõe que os instrumentos jurídicos delimitem com precisão as finalidades legais do compartilhamento, atribuam responsabilidades específicas aos entes participantes, instituam mecanismos robustos de governança, segurança da informação e *compliance*, e estabeleçam regras claras para o tratamento, armazenamento, controle de acesso e descarte dos dados. Tais instrumentos devem ainda prever cláusulas que viabilizem auditoria, responsabilização e transparência, assegurando *accountability* perante a sociedade e reforçando a legitimidade da gestão pública de dados.

A ausência de formalização conduz a práticas fragmentadas e não padronizadas, que fragilizam a proteção dos titulares e corroem os fundamentos da segurança jurídica. O compartilhamento de dados pessoais pelo Poder Público configura, inequivocamente, ato administrativo, por envolver manifestação de vontade voltada à consecução de finalidades institucionais, nos termos dos artigos 2º e 37 da Constituição Federal. Como tal, deve observar os princípios da legalidade, impessoalidade, finalidade, motivação, publicidade e controle, sendo imprescindível sua submissão a atos normativos específicos que confiram estrutura jurídica e legitimidade à prática. A informalidade nesse contexto não apenas contraria os princípios constitucionais, como compromete a coerência federativa e a proteção dos direitos fundamentais.

A dispensa de instrumentos jurídicos formais acarreta riscos significativos, como a ambiguidade na responsabilização por eventuais violações, a ausência de controle sobre o uso dos dados, a fragilidade das medidas de segurança da informação e a inviabilidade de auditorias

e fiscalização regulatória. Tais vulnerabilidades são incompatíveis com os padrões exigidos pela Lei Geral de Proteção de Dados Pessoais (LGPD), que impõe deveres específicos de transparência, rastreabilidade e responsabilização.

Diante desse cenário, torna-se imprescindível a adoção de protocolos mínimos obrigatórios para cada operação de compartilhamento, formalizados por meio de atos normativos internos, resoluções e portarias emanadas de instâncias centrais de governança, bem como instrumentos jurídicos específicos — como convênios e termos de cooperação — sempre que a complexidade ou sensibilidade dos dados assim o exigir.

Esses dispositivos são essenciais para garantir a harmonização com os princípios da LGPD, instituir padrões mínimos de controle técnico e jurídico, viabilizar responsabilização administrativa e judicial, e assegurar o pleno exercício dos direitos dos titulares, como acesso, retificação e oposição ao uso indevido de seus dados.

Embora seja legítimo o esforço por maior eficiência administrativa, tal objetivo não pode se sobrepor às garantias constitucionais e legais que regem o tratamento de dados pessoais. Protocolos normatizados e formalizados não representam entraves burocráticos, mas sim condições estruturantes para a construção de um ambiente interoperável, confiável e juridicamente seguro. A confiança da sociedade na atuação ética e legal do Poder Público depende da observância rigorosa desses parâmetros.

A dispensa de formalização por convênio ou instrumento jurídico deve ser restrita aos casos nos quais o compartilhamento esteja amparado por protocolos obrigatórios definidos em atos normativos vinculativos, com fundamentação legal e conformidade com os princípios constitucionais do ato administrativo. Tal revisão permitirá conciliar celeridade com segurança jurídica, mitigando riscos e fortalecendo a responsabilidade administrativa na gestão de dados públicos.

Ao prever que fica dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a efetivação do compartilhamento de dados entre os órgãos públicos (Art. 27), o novo decreto diverge do modelo de proteção de dados pessoais adotado no cenário europeu — a despeito de o Brasil integrar, desde 2022, o Comitê Consultivo da Convenção 108 na qualidade de membro observador[98].

A versão atual da Convenção 108 do Conselho da Europa, denominada Convenção 108+, constitui um tratado internacional que visa proteger as pessoas em relação ao tratamento automatizado de dados pessoais (Conselho da Europa, 2018). Essa convenção estabelece

[98] COUNCIL OF EUROPE. **Bureau Meetings**. 2025. Disponível em: https://www.coe.int/en/web/data-protection/bureau-meetings. Acesso em: 17 ago. 2025.

diretrizes para a proteção dos dados pessoais e prevê mecanismos de cooperação internacional, mas não dispensa expressamente a formalização jurídica para o compartilhamento de dados entre entes públicos. Ao contrário, enfatiza a necessidade de garantir níveis adequados de proteção por meio de instrumentos jurídicos, legislação ou acordos normativos que assegurem a legitimidade, a finalidade clara, a segurança e a responsabilização no tratamento e transferência de dados pessoais, inclusive no âmbito transfronteiriço.

O artigo 14 da Convenção 108+ trata especificamente dos fluxos transfronteiriços de dados pessoais e estabelece que as transferências devem ocorrer com base em legislação adequada, instrumentos juridicamente vinculativos, garantias ou consentimento explícito, respeitando sempre os direitos dos titulares e o princípio da proporcionalidade. Isso enfatiza a importância de estruturas formais e acordos claros para legitimar o compartilhamento de dados, mesmo no contexto interno.

Portanto, a Convenção 108+ não justifica, como regra geral, a dispensa da formalização por convênios ou instrumentos jurídicos para o compartilhamento de dados. Ela reforça a necessidade de segurança jurídica, responsabilidade e clareza na transferência, recomendando formalização e controle rigoroso conforme as circunstâncias, o que vai ao encontro da recomendação de que o compartilhamento público de dados pessoais deve ser assentado em bases normativas e protocolos mínimos que assegurem a governança adequada do fluxo de dados pessoais.

Assim, a exigência de formalização e governança rigorosa nos processos de compartilhamento de dados pessoais no contexto da interoperabilidade pública encontra respaldo não apenas na legislação nacional, como a Lei Geral de Proteção de Dados Pessoais (LGPD), mas também em tratados internacionais que estabelecem padrões mínimos de segurança e governança, a exemplo da Convenção 108+ do Conselho da Europa (Conselho da Europa, 2018).

Trata-se de um alinhamento normativo que consolida o imperativo institucional de que o Estado brasileiro observe padrões éticos e de transparência no tratamento de dados pessoais, em conformidade com os princípios constitucionais e internacionais de proteção de dados.

6.2 O COMPARTILHAMENTO DE DADOS PELOS ÓRGÃOS PÚBLICOS FEDERAIS E PELAS PRESTADORAS DE SERVIÇOS PÚBLICOS

O GRANDE IRMÃO ESTÁ VIGIANDO VOCÊ (Orwell, 2021).

O Decreto nº 12.428, de 3 de abril de 2025, que regulamenta o compartilhamento de dados pessoais por órgãos públicos federais e prestadoras de serviços públicos, representa um marco regulatório relevante no cenário jurídico brasileiro, especialmente após o julgamento da Ação Direta de Inconstitucionalidade (ADI) nº 6.649 pelo Supremo Tribunal Federal (STF), que reconheceu a legitimidade do compartilhamento de dados entre entes públicos, desde que observados os princípios da finalidade, necessidade e proporcionalidade, bem como os requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD).

Consoante o Ministério da Gestão e da Inovação em Serviços Públicos, destaca-se a iniciativa denominada "Qualificação de Endereços", um processo automatizado de verificação e validação dos dados de endereço dos cidadãos registrados nas bases de benefícios da seguridade social. Esse procedimento é realizado por meio do cruzamento dessas informações com os dados fornecidos por prestadoras de serviços públicos, como concessionárias de energia elétrica e telecomunicações[99].

Segundo esclarece o referido Ministério, a iniciativa tem respaldo na Lei nº 15.077/2024, que, ao alterar dispositivos da Lei Orgânica da Assistência Social (Lei nº 8.742/1993), estabeleceu, em seu art. 3º, a obrigação das concessionárias de serviços públicos de fornecerem os dados de que sejam detentoras, com vistas à qualificação cadastral e à melhoria da gestão dos benefícios sociais[100].

Com fundamento nesse dispositivo, foi editado o Decreto nº 12.428/2025, posteriormente alterado pelo Decreto nº 12.455/2025, que regulamenta o art. 35, § 2º, da Lei nº 8.742/1993 e o art. 3º da Lei nº 15.077/2024. O novo marco normativo disciplina o compartilhamento de dados entre órgãos públicos e prestadoras de serviços, com ênfase na gestão do Benefício de Prestação Continuada (BPC), assegurando a pseudonimização dos dados e a observância dos princípios da LGPD.

---

[99] BRASIL**. Qualificação de endereços**. Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/qualificacao-de-enderecos. Acesso em: 03 ago. 2025.

[100] "Art. 3º As prestadoras de serviços públicos deverão compartilhar com o Ministério da Gestão e da Inovação em Serviços Públicos, na forma prevista neste Decreto, as informações de base de dados de que sejam detentoras, com a finalidade de aperfeiçoar o processo de verificação de requisitos para a concessão, a manutenção e a ampliação de benefícios da seguridade social, nos termos do disposto no art. 3º da Lei nº 15.077, de 27 de dezembro de 2024. "

Publicado em 3 de abril de 2025 e atualizado pelo Decreto nº 12.455, de 15 de maio de 2025, o referido decreto visa promover a integração e qualificação das informações utilizadas na concessão, manutenção e revisão de benefícios, assegurando maior eficiência, transparência e segurança jurídica na gestão pública.

Um dos elementos centrais do Decreto é a imposição às concessionárias e prestadoras de serviços públicos — incluindo setores essenciais como energia elétrica, água e telefonia — da obrigação de compartilharem dados cadastrais, especialmente os endereços físicos dos usuários, com o Ministério da Gestão e da Inovação em Serviços Públicos (MGI). A medida visa aprimorar a verificação dos critérios de elegibilidade para benefícios sociais, prevenindo fraudes e assegurando que os auxílios públicos sejam destinados às pessoas em situação de vulnerabilidade. O BPC, como instrumento fundamental de proteção social, é o principal foco dessa política integrada.

Entretanto, a obrigatoriedade do compartilhamento de tais dados suscita preocupações relevantes no campo da privacidade e da proteção de dados pessoais. O repasse massivo de informações, como endereços físicos, amplia a exposição dos titulares a riscos de violação de privacidade, facilitando sua identificação e localização, o que pode resultar em usos indevidos, como perseguição, discriminação e fraudes. Mesmo com a aplicação de técnicas de pseudonimização, a ausência de salvaguardas robustas e controles eficazes pode permitir a reidentificação dos titulares, comprometendo a eficácia das medidas protetivas previstas na Lei Geral de Proteção de Dados Pessoais (LGPD).

Além disso, há o risco de desvio de finalidade, uma vez que dados coletados para um propósito específico podem ser utilizados para finalidades diversas e não autorizadas, em violação aos princípios da finalidade e da necessidade — pilares da LGPD e do ordenamento jurídico brasileiro. Esse desvio pode ocorrer tanto por agentes públicos quanto por funcionários das prestadoras, especialmente na ausência de mecanismos rigorosos de controle, auditoria e responsabilização.

Outro aspecto preocupante é o aumento da superfície de ataque para incidentes de segurança da informação. A expansão dos pontos de exposição a riscos cibernéticos compromete a integridade e a confidencialidade dos dados pessoais. A multiplicidade de agentes envolvidos no compartilhamento, com diferentes níveis de maturidade em segurança cibernética, cria vulnerabilidades que podem ser exploradas por agentes maliciosos, expondo um grande volume de dados sensíveis a vazamentos e acessos não autorizados.

No plano jurídico, a insegurança e a falta de transparência perante os titulares dos dados são questões cruciais. A insuficiente comunicação sobre quais dados são compartilhados, com

quais entidades e para quais finalidades, fere o princípio da transparência, dificultando o controle social e a fiscalização. Ademais, a ausência de delimitação clara das bases legais e dos limites para o compartilhamento pode gerar conflitos institucionais e dificultar a responsabilização em caso de abusos ou incidentes.

Há ainda o risco concreto de que o acesso a informações detalhadas sobre endereços físicos seja utilizado para práticas discriminatórias ou excludentes, como a restrição indevida de benefícios sociais, segmentação injusta ou exclusão de grupos vulneráveis, contrariando os princípios constitucionais da igualdade e da não discriminação. Quando cruzados com outros dados sensíveis, esses endereços podem revelar informações sobre o perfil socioeconômico, condições de saúde e outras características pessoais, ampliando o potencial de discriminação e violação de direitos fundamentais.

A imposição desse compartilhamento compulsório, sem a implementação de salvaguardas técnicas, jurídicas e administrativas adequadas, poderia fragilizar direitos fundamentais consagrados na Constituição Federal e na LGPD, como a privacidade, a autodeterminação informativa e a dignidade da pessoa humana. Portanto, é imprescindível que o compartilhamento ocorra estritamente dentro dos parâmetros legais, com mecanismos robustos de governança, transparência, segurança da informação e responsabilização.

As críticas à regulamentação do Decreto nº 12.428/2025, especialmente em sua versão original, concentraram-se em aspectos relacionados à clareza, abrangência e segurança jurídica do compartilhamento de dados pessoais. Entidades como Data Privacy Brasil, InternetLab, IDEC e CEDIS/IDP destacaram o risco de repasse indiscriminado de bases de dados inteiras, o que poderia violar o princípio da minimização e expor um contingente populacional expressivo a riscos excessivos no tratamento dos dados (INT3R4, 2025). Em resposta a essas críticas e em consonância com os parâmetros fixados pelo STF na ADI nº 6.649, a versão atualizada do Decreto reforça os princípios da finalidade legítima, adequação, necessidade e transparência, limitando o compartilhamento ao mínimo necessário para as finalidades públicas específicas, conforme previsto no artigo 6º da LGPD.

Ademais, o Decreto determina que o compartilhamento seja formalizado e controlado, com a adoção de técnicas de proteção como a pseudonimização, preservando a privacidade dos titulares e resguardando a possibilidade de reidentificação apenas em ambiente seguro e controlado. A estrutura institucional prevista atribui ao MGI a responsabilidade pelo

recebimento e tratamento das informações, com a Dataprev[101] como operadora, garantindo mecanismos rigorosos de controle e fiscalização, alinhados às diretrizes de governança recomendadas pelo STF para o Cadastro Base do Cidadão e demais bases integradoras.

Importa destacar que a regulamentação do Decreto nº 12.428/2025 foi precedida de consulta pública promovida pelo Ministério da Gestão e Inovação em Serviços Públicos — MGI[102], o que configurou um avanço significativo em termos de participação social. Essa consulta permitiu que diversos segmentos da sociedade civil, especialistas, entidades representativas e cidadãos contribuíssem com sugestões e críticas, fortalecendo a transparência e a legitimidade do processo normativo. A participação social ampliada contribuiu para o aprimoramento da regulamentação, especialmente no que tange à proteção da privacidade, à segurança da informação e à responsabilização no tratamento de dados pessoais.

A edição do Decreto nº 12.455/2025, que atualizou o Decreto nº 12.428, reforçou a transparência e a clareza sobre os dados efetivamente compartilhados, consolidando as garantias previstas na LGPD e ampliando a participação social por meio de nova consulta pública, em consonância com o princípio da publicidade e o controle social destacados no julgamento da ADI nº 6.649.

Assim, a regulamentação promovida pelo Decreto nº 12.428/2025 e suas atualizações consolida um arcabouço normativo que materializa os parâmetros fixados pelo STF, promovendo um compartilhamento de dados pessoais no setor público pautado na legalidade, transparência, segurança e respeito aos direitos fundamentais, especialmente no âmbito da seguridade social e da prestação de serviços públicos essenciais.

Todavia, permanece a expectativa de que os atos regulamentares subsequentes — que definirão procedimentos, prazos, bases legais específicas e medidas técnicas e administrativas — sejam elaborados com transparência e rigor, a fim de evitar lacunas que comprometam a proteção dos direitos fundamentais. Assim, apesar dos avanços normativos trazidos pelo Decreto nº 12.455/2025, o acompanhamento contínuo por parte da sociedade civil, órgãos reguladores e especialistas é essencial para garantir a efetividade das garantias previstas e mitigar eventuais riscos no compartilhamento de dados pessoais no setor público.

---

[101] A Empresa de Tecnologia e Informações da Previdência (Dataprev) é uma empresa pública vinculada ao Ministério da Gestão e Inovação em Serviços Públicos, com personalidade jurídica de direito privado, patrimônio próprio e autonomia administrativa e financeira.

[102] No âmbito da consulta pública, houve a realização do Webinar — Qualificação de Endereços — Regulamentação do Decreto nº 12.428/2025 (Webinar, 2025).

7 APRIMORAMENTOS NORMATIVOS E TÉCNICOS PARA O COMPARTILHAMENTO DE DADOS PELO PODER PÚBLICO

> Assim, a questão central, quando se discute a necessidade de compartilhamento de dados no âmbito da Administração Pública à luz do princípio da finalidade, diz respeito à definição de quais condições devem ser observadas para o repurposing de dados pessoais custodiados pelo Estado (Wimmer, 2023).

A necessidade de equacionamentos acerca do uso secundário de dados pessoais pelo Poder Público emerge como um dos principais desafios contemporâneos à luz do direito fundamental à proteção de dados e do imperativo constitucional de observância dos princípios que regem a Administração Pública.

Isso porque o compartilhamento de dados pessoais pelo Poder Público se insere em uma zona de tensão normativa que exige a harmonização entre o direito fundamental à proteção de dados pessoais, consagrado no art. 5º, LXXIX, da Constituição Federal, e os princípios constitucionais que regem a Administração Pública, notadamente os da publicidade e da eficiência (art. 37, caput, CF). A conciliação desses polos demanda uma interpretação sistemática e principiológica da ordem constitucional, de modo a assegurar que a transparência e a efetividade da atuação estatal não se sobreponham indevidamente à autodeterminação informativa dos cidadãos.

No capítulo anterior foi mencionado um caso paradigmático que envolve o compartilhamento de dados de endereço físico dos cidadãos por prestadoras de serviços públicos com o Ministério da Gestão e da Inovação em Serviços Públicos, conforme autorizado pelo Decreto nº 12.428/2025. A medida tem como objetivo aperfeiçoar a verificação de requisitos para a concessão e manutenção de benefícios da seguridade social. Todavia, a utilização de dados pseudonimizados, como o CPF mascarado, e a ausência de consentimento explícito dos titulares suscitam dúvidas quanto à proporcionalidade da medida e à suficiência das salvaguardas adotadas para proteger os direitos fundamentais envolvidos.

Outro exemplo emblemático ocorre no âmbito da integração de cadastros sociais para a concessão de benefícios assistenciais, como o Bolsa Família. Essa integração é regulamentada pela Instrução Normativa SAGICAD/MDS nº 2, de 21 de maio de 2025, que estabelece os procedimentos operacionais para a inclusão e atualização de dados no Cadastro Único para Programas Sociais do Governo Federal (CadÚnico), por meio da interoperabilidade com o Cadastro Nacional de Informações Sociais (CNIS) e o Cadastro de Pessoa Física (CPF). Trata-se de medida orientada à eficiência administrativa, ao buscar otimizar a identificação de

beneficiários e prevenir fraudes, promovendo maior racionalidade na execução das políticas públicas. Contudo, a iniciativa também suscita preocupações legítimas quanto à proteção dos dados pessoais dos beneficiários, especialmente diante da ausência de mecanismos que assegurem a transparência, o controle e a participação dos titulares no processo de compartilhamento e reutilização dessas informações.

O exame dos exemplos referidos evidencia que a eficiência administrativa, embora constitucionalmente assegurada, não pode ser instrumentalizada como justificativa para a erosão de direitos fundamentais. A atuação estatal no tratamento secundário de dados pessoais deve ser orientada por uma lógica de equilíbrio, na qual a proteção seja compreendida não como obstáculo, mas como condição de legitimidade e qualidade da ação pública.

Todavia, conforme destacado por Alves e Valadão (2023), a Lei Geral de Proteção de Dados Pessoais (LGPD) não apresenta uma regulamentação sistemática nem suficientemente clara acerca do tratamento secundário de dados pessoais, tanto no âmbito do setor privado quanto do setor público. Essa lacuna normativa pode contribuir para a consolidação de um ambiente de insegurança jurídica, especialmente diante da crescente complexidade das operações de tratamento de dados em contextos interinstitucionais.

A ausência de diretrizes específicas impõe um desafio significativo a operadores jurídicos, gestores públicos e agentes econômicos, que se veem diante da necessidade de compatibilizar a reutilização de dados com os direitos fundamentais dos titulares. O uso de dados pessoais para finalidades diversas daquelas que motivaram sua coleta original exige, portanto, balizas jurídicas claras e legitimadoras, sob pena de violação aos princípios da legalidade, da finalidade e da autodeterminação informativa.

Aduzem Alves e Valadão (2023) que, embora a LGPD não regule expressamente o tratamento secundário de dados pessoais, sua possibilidade decorre implicitamente do princípio da finalidade, consagrado no art. 6º, inciso I, da referida lei, dispositivo que estabelece que o tratamento de dados deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular, vedando-se qualquer tratamento posterior que seja incompatível com essas finalidades.

O princípio funciona como um mecanismo normativo de contenção de abusos, ao limitar a atuação dos agentes de tratamento e preservar a coerência entre a finalidade declarada e a efetiva utilização dos dados. Nesse contexto, assume papel central na estruturação da confiança entre o titular e o agente de tratamento, ao garantir que os dados não sejam utilizados de forma arbitrária ou desproporcional, em prejuízo à privacidade e à autonomia informacional

do titular. Trata-se, portanto, de um instrumento de concretização da necessária transparência, que deve orientar toda a atuação pública no âmbito da proteção de dados pessoais.

E ainda que não trate de forma expressa e específica do tratamento secundário de dados pessoais publicamente disponíveis, a LGPD oferece diretrizes normativas que, interpretadas sistematicamente, indicam a possibilidade de sua realização. O § 3º do art. 7º estabelece que o tratamento de dados pessoais de acesso público deve observar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. O § 4º, por sua vez, dispensa o consentimento do titular para o tratamento de dados tornados manifestamente públicos por ele próprio, desde que resguardados seus direitos e os princípios da Lei. Por fim, o § 7º autoriza o tratamento posterior desses dados para novas finalidades, se forem legítimas e específicas, e que se assegure a preservação dos direitos do titular, bem como a observância dos fundamentos e princípios da LGPD.

É dizer, não obstante a ausência de um regime normativo minucioso sobre o tratamento secundário de dados pessoais, à luz da Lei Geral de Proteção de Dados Pessoais (LGPD), a prática é juridicamente admissível. Ordinariamente, se compreende que essa admissibilidade está condicionada à estrita observância dos limites constitucionais e legais, com destaque para o princípio da finalidade, a compatibilidade da nova finalidade com o contexto original da coleta e o respeito integral aos direitos fundamentais dos titulares.

Nesse cenário, impõe-se à atuação administrativa e jurisdicional o dever de fomentar a elaboração de critérios normativos e parâmetros interpretativos claros, capazes de orientar tanto o Poder Público quanto os agentes privados na adoção de condutas que estejam em consonância com as garantias fundamentais, promovam a legitimidade social das operações de tratamento e previnam abusos, mitigando riscos e fortalecendo a confiança no sistema de proteção de dados.

A partir da reflexão crítica proposta por Alves e Valadão (2023), evidencia-se a necessidade premente de consolidação de normativas infralegais e diretrizes técnicas que supram as lacunas interpretativas atualmente existentes, especialmente no que tange ao tratamento secundário de dados no setor público. Tal consolidação demanda a criação de mecanismos institucionais que assegurem a transparência, a motivação e o controle efetivo das operações de tratamento posterior. Somente mediante esse aprimoramento normativo e institucional será possível à LGPD cumprir sua função protetiva plenamente, sem, contudo, inviabilizar a inovação, a eficiência administrativa e o uso legítimo dos dados, promovendo, assim, o necessário equilíbrio entre os interesses públicos e a salvaguarda dos direitos fundamentais dos cidadãos.

7.1 MECANISMOS DE CONTROLE DA ATIVIDADE ADMINISTRATIVA DE COMPARTILHAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

> Sob esta perspectiva, a proteção de dados pessoais relaciona-se diretamente com a própria preservação da democracia, a fim de impossibilitar que agentes econômicos e políticos possam se utilizar das vulnerabilidades e fragilidades das pessoas para manipulá-las com o objetivo de angariar vantagens indevidas ou mesmo de distorcer o resultado de eleições ou de deliberações (Frazão; Carvalho; Milanez, 2022).

O compartilhamento de dados pessoais pelo Poder Público, enquanto manifestação da atividade administrativa, deve ser compreendido sob uma perspectiva que transcende a mera dimensão técnico-operacional, adentrando o campo dos direitos fundamentais, entre os quais se destaca o direito à proteção de dados pessoais. A concepção teórica desenvolvida por Lorenzo Dalla Corte (2020) oferece uma contribuição inovadora ao caracterizar esse direito não apenas como um direito substantivo autônomo, mas como um "direito a uma regra" — isto é, um direito à existência de um regime normativo procedimental que discipline o tratamento de dados.

Essa abordagem implica que o processamento de informações pessoais pelo Estado deve respeitar o núcleo essencial do direito fundamental, o qual se estrutura a partir de uma escolha coletiva de instituir um sistema de freios e contrapesos voltado à limitação do poder informacional e à proteção da autonomia dos titulares.

Sob esse sistema, o compartilhamento de dados pessoais pelo Poder Público não pode prescindir de mecanismos formais de controle e de *accountability* que assegurem a delimitação clara das finalidades, a legitimidade do uso e a conformidade com os princípios constitucionais da legalidade, da finalidade, da transparência e da proteção aos direitos fundamentais, especialmente o direito à privacidade e à autodeterminação informativa. O núcleo essencial desses direitos, portanto, funda-se em uma estrutura regulatória de natureza procedimental, que garante não apenas o respeito ao conteúdo substantivo do direito, mas também a previsibilidade, a sujeição a normas e a possibilidade de controle externo — elementos indispensáveis para conferir legitimidade jurídica e social ao uso estatal de dados pessoais.

Conforme ressaltam Frazão, Carvalho e Milanez (2022), o debate sobre o controle do tratamento de dados pessoais não se limita a um domínio restrito, mas se insere em um contexto regulatório multifacetado, que abrange tanto a heterorregulação — entendida como a

normatividade estatal coercitiva — quanto formas complementares de regulação, como a autorregulação setorial, as soluções tecnológicas desenvolvidas por atores privados e os mecanismos técnicos incorporados à própria arquitetura dos fluxos informacionais. Para a efetiva preservação dos direitos fundamentais, é imprescindível que a heterorregulação atue como instância mediadora e coordenadora, capaz de assegurar o equilíbrio entre os diferentes níveis regulatórios e de impedir que interesses mercadológicos desordenados ou dinâmicas tecnológicas descontroladas comprometam a integridade do regime jurídico de proteção de dados pessoais.

Essa complexidade regulatória, evidenciada por Frazão, Carvalho e Milanez (2022), reforça a imprescindibilidade de um sistema de governança no qual o Estado exerça com vigor suas funções normativa e fiscalizatória, a fim de evitar a colonização do espaço informacional por agentes econômicos hegemônicos[103]. Essa colonização pode ocorrer diretamente, por meio da imposição de padrões empresariais, ou de maneira indireta, mediante o domínio tecnológico e a manipulação dos fluxos informacionais, comprometendo a efetividade das garantias constitucionais. Esse processo representa uma ameaça concreta à liberdade, à dignidade da pessoa humana e ao direito à autodeterminação informativa, ao passo que fragiliza o ambiente regulatório e esvazia o conteúdo do direito fundamental à proteção de dados em sua dimensão coletiva e social.

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) configura um marco normativo essencial no ordenamento jurídico brasileiro, ao reconhecer o direito à proteção de dados como expressão da dignidade da pessoa humana e da autonomia individual. No entanto, como adverte Dalla Corte (2020), a eficácia desse direito depende intrinsecamente da concretização do chamado "direito a uma regra" — isto é, da existência e da observância de normas procedimentais democráticas, transparentes e previamente estabelecidas, que estruturem de forma legítima o tratamento e o compartilhamento de dados pessoais.

Nesse diapasão, a LGPD deve ser compreendida como condição necessária, porém não suficiente: sua efetividade exige articulação contínua com outras formas de regulação — tecnológicas, setoriais e sociais — a fim de evitar que dispositivos legais sejam esvaziados na prática cotidiana das operações de tratamento de dados, em afronta às garantias constitucionais.

---

[103] O pesquisador Victor Habib Lantyer de Mello esclarece que o termo colonialismo de dados se refere à apropriação massiva de informações pessoais e sociais por corporações e Estados, em analogia às práticas de exploração típicas do colonialismo histórico. Assim como este se apropriava de territórios e recursos humanos, o colonialismo de dados "apropria-se da vida humana para que se possa extrair continuamente dados dela em busca de lucro" (Mello, 2025).

Trata-se de articulação que exige o fortalecimento permanente dos mecanismos institucionais de fiscalização, controle e responsabilização, os quais devem poder acompanhar a evolução das tecnologias e das práticas de tratamento de dados, especialmente no que se refere ao uso secundário de informações pessoais.

É imperativo que a LGPD dialogue ativamente com as demais fontes de regulação, demandando a construção de mecanismos institucionais que zelem pelo cumprimento e atualização do regime protetivo, fiscalizando usos secundários e impondo sanções dissuasórias quando da violação de finalidades. Isso implica que os mecanismos institucionais de fiscalização, controle e responsabilização sejam fortalecidos e estejam em constante evolução para lidar com os novos desafios, especialmente no que tange à segurança no uso secundário de dados pessoais.

O uso seguro de dados pessoais pelo Poder Público impõe, assim, a exigência de motivação e justificação formal dos atos administrativos que autorizem o tratamento secundário dessas informações, submetendo-os ao crivo do controle social e judicial. Nesse sentido, a formalização dos atos relacionados ao compartilhamento e à reutilização de dados deve ser clara, fundamentada e acessível, de modo a assegurar os princípios da legalidade, da transparência e da *accountability*. Essa exigência é condição indispensável para a legitimidade da atuação estatal no âmbito da governança de dados, especialmente diante da assimetria informacional entre o Estado e os titulares. A sujeição desses atos ao controle externo — tanto jurisdicional quanto social — configura salvaguarda essencial para a proteção dos direitos fundamentais, em especial o direito à privacidade e à autodeterminação informativa.

Sob a ótica do regime jurídico administrativo e com base na Lei Geral de Proteção de Dados Pessoais — LGPD e nas diretrizes da Agência Nacional de Proteção de Dados (ANPD, 2023), compreende-se que o uso compartilhado de dados pessoais pelo Poder Público está sujeito a um conjunto de requisitos formais e materiais, que visam assegurar a conformidade com os princípios constitucionais e legais de proteção à privacidade e à autodeterminação informacional.

A partir dessa estrutura normativa, impõem-se requisitos específicos para o compartilhamento de dados pessoais pelo Poder Público, os quais devem ser previamente motivados e formalizados por meio de decisão administrativa do agente de tratamento emissor ou mediante instrumento jurídico específico — como contrato, convênio ou instrumento congênere — firmado entre os agentes envolvidos. Esses atos devem conter, de forma clara e detalhada, a identificação dos agentes de tratamento, a definição de suas respectivas responsabilidades, a descrição dos dados pessoais objeto do compartilhamento, a finalidade

específica da operação, a base legal que a fundamenta, os meios técnicos utilizados, o prazo de duração da atividade, as medidas de segurança adotadas, eventuais restrições ao repasse a terceiros e, sobretudo, a demonstração da compatibilidade entre a finalidade original da coleta e a nova finalidade pretendida.

A observância dessas condições não apenas assegura a conformidade com os princípios da LGPD — como os da finalidade, necessidade e transparência —, mas também reforça os mecanismos de controle institucional, funcionando como salvaguarda contra práticas abusivas ou arbitrárias no tratamento de dados pessoais por parte do Estado.

Portanto, o uso legítimo e seguro dos dados pessoais pelo Poder Público deve estar assentado na formalização clara, na motivação explícita e na sujeição dos atos administrativos autorizativos a mecanismos robustos de controle social e judicial. Tal normatividade processual traduz a essência do direito à proteção de dados, configurando o sistema de freios e contrapesos regulatórios que Dalla Corte destaca como centro do direito fundamental.

Ademais, esse modelo impõe a incorporação dos princípios de *privacy by design* (privacidade desde a concepção) e *privacy by default* (privacidade por padrão) desde a gênese dos sistemas públicos, integrando a proteção de dados à própria arquitetura institucional do Estado. Com isso, assegura-se que a tutela do núcleo essencial do direito à privacidade não seja reduzida a formalidade procedimental, mas reconhecida como princípio estruturante das políticas públicas.

Concebida na década de 1990 pela Dr.ª Ann Cavoukian, então Comissária de Informação e Privacidade da província de Ontário, Canadá, a metodologia do *privacy by design* se constituiu em uma resposta inovadora e proativa aos desafios emergentes da proteção de dados pessoais (Passos, 2023). Essa abordagem rompe com o paradigma tradicional, que tratava a privacidade como um elemento acessório ou uma etapa posterior nos processos tecnológicos e administrativos, propondo, em seu lugar, a integração da proteção de dados desde a fase de concepção de sistemas, produtos e serviços — ou seja, como um componente estrutural e intrínseco ao seu desenvolvimento.

O *privacy by design* estabelece uma nova abordagem técnica ao reconhecer que a privacidade deve ser incorporada de forma sistemática e antecipatória, com o objetivo de prevenir violações antes que ocorram, e não meramente reagir a elas. Essa metodologia é sustentada por sete princípios fundamentais, que orientam sua implementação prática e normativa (Cavoukian, 2009):

Proatividade, não reatividade — Adota medidas preventivas que antecipam riscos e impedem a ocorrência de incidentes relacionados à privacidade.

Privacidade como configuração padrão — Garante que a proteção de dados seja ativada automaticamente, sem necessidade de ação do titular;

Privacidade incorporada ao design — Integra a proteção de dados à arquitetura e às funcionalidades dos sistemas desde sua concepção;

Funcionalidade plena — abordagem de soma positiva — Rejeita a dicotomia entre privacidade e funcionalidade, promovendo soluções que conciliem ambos os interesses;

Segurança de ponta a ponta — Assegura a proteção dos dados pessoais durante todo o seu ciclo de vida, da coleta à eliminação;

Visibilidade e transparência — Promove a auditabilidade e a clareza nos processos de tratamento de dados, reforçando a confiança dos titulares;

Respeito pela privacidade do usuário — Valoriza a autodeterminação informativa, conferindo ao titular controle efetivo sobre seus dados pessoais.

Esses princípios estão expressamente consagrados no artigo 25 do Regulamento Geral sobre a Proteção de Dados — GDPR da União Europeia (2016), que impõe aos agentes de tratamento a obrigação de aplicar, tanto no momento da definição dos meios de tratamento quanto durante o próprio tratamento, medidas técnicas e organizacionais adequadas que assegurem, por padrão, o processamento apenas dos dados pessoais essenciais para cada finalidade específica, evitando, em especial, o acesso não autorizado ou a disponibilização automática a um número indefinido de pessoas.

No contexto brasileiro, a Lei Geral de Proteção de Dados Pessoais (LGPD), embora não adote expressamente os termos, incorpora seus fundamentos de maneira substancial, especialmente no artigo 46. Esse dispositivo impõe aos agentes de tratamento o dever de adotar salvaguardas técnicas e administrativas eficazes para proteger os dados pessoais contra acessos não autorizados, bem como contra eventos acidentais ou ilícitos de destruição, perda, alteração ou divulgação. O § 2º do mesmo artigo explicita que tais medidas devem ser observadas desde a fase de concepção do produto ou serviço até sua plena execução, evidenciando uma aderência normativa aos princípios estruturantes do *privacy by design*.

Correlato, o princípio do *privacy by default* estabelece que as configurações de privacidade concebidas durante o desenvolvimento de produtos e serviços devem ser ativadas automaticamente, sem exigir nenhuma ação adicional por parte do titular (European Commission, [*s.d.*]). Essa configuração padrão assegura um nível elevado de proteção, reduz riscos operacionais e jurídicos, de modo a promover maior confiança nas soluções tecnológicas e administrativas adotadas.

Em termos conceituais, *privacy by design* e *privacy by default* representam uma mudança paradigmática na governança de dados, ao proporem a integração sistemática e antecipada da privacidade em todas as fases dos processos organizacionais e tecnológicos. Essa abordagem normativa não apenas assegura conformidade legal, mas também fortalece a transparência institucional, a responsabilidade dos agentes de tratamento e a autodeterminação informativa dos titulares, em consonância com os princípios constitucionais da dignidade da pessoa humana, da legalidade e da proteção aos direitos fundamentais.

Portanto, a utilização legítima e segura de dados pessoais pelo Poder Público requer a incorporação sistemática dos princípios de *privacy by design* e *privacy by default* como diretrizes estruturantes da atuação estatal. A adoção desses princípios assegura que o tratamento de dados pelo Estado seja planejado e executado com rigor técnico, jurídico e ético, mitigando riscos, assegurando a finalidade legítima e garantindo o pleno exercício dos direitos dos titulares. Assim, sua implementação constitui condição essencial para uma administração pública eficiente, transparente e comprometida com a proteção integral dos direitos fundamentais na sociedade digital contemporânea.

Para a efetiva concretização da normatividade procedimental, impõe-se ainda a participação qualificada dos titulares, da sociedade civil e de órgãos independentes tanto no processo regulatório quanto na fiscalização. Tal arranjo garante o exercício do controle democrático e previne a captura regulatória por interesses econômicos, resguardando o sentido constitucional da proteção de dados. A complexidade do ambiente digital contemporâneo exige, assim, uma governança plural e inclusiva, que reafirma o equilíbrio entre os poderes e a centralidade da pessoa humana.

Em síntese, a incorporação das reflexões de Dalla Corte à análise da governança pública dos dados reafirma que o direito à proteção de dados pessoais configura-se, primordialmente, como um direito fundamental de natureza procedural. Sua essência reside na escolha coletiva por um ordenamento jurídico que institua freios e contrapesos institucionais eficazes ao tratamento estatal de informações.

Apenas sob esse paradigma será possível compatibilizar o uso legítimo e eficiente dos dados pessoais com a salvaguarda intransigente dos direitos fundamentais, preservando a dignidade, a autonomia e a liberdade dos indivíduos em uma sociedade republicana e tecnologicamente orientada.

7.2 DA IMPORTÂNCIA DOS INSTRUMENTOS JURÍDICOS FORMAIS PARA O COMPARTILHAMENTO DE DADOS

> Não é só o indivíduo, mas também a sociedade que carece de defesa (Nabuco, 1997).

A Administração Pública contemporânea configura-se como uma estrutura informacional complexa, cuja eficiência está diretamente vinculada à capacidade de coletar, processar, compartilhar e divulgar dados de forma segura e legítima. Nesse cenário, o compartilhamento de dados entre órgãos públicos não se reduz a uma prática burocrática de rotina, mas representa uma atividade administrativa, que demanda controle jurídico rigoroso — sobretudo quando envolve dados pessoais.

O pleno exercício do direito à informação sobre o desenvolvimento das atividades administrativas é condição indispensável para a efetivação do princípio democrático no âmbito da Administração Pública, cuja concretização se dá, essencialmente, por meio da participação cidadã e do controle social (Motta, 2003).

Como bem apontam Gasiola, Machado e Mendes (2021), a gestão da informação pela Administração Pública está submetida a dois grandes eixos normativos: o dever de transparência, disciplinado pela Lei nº 12.527/2011 (Lei de Acesso à Informação — LAI), e o dever de proteção de dados pessoais, regulado pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados — LGPD). Esses dois regimes jurídicos, embora distintos em sua origem e finalidade, convergem na conformação de um modelo informacional que busca equilibrar o acesso público às informações administrativas com a tutela dos direitos fundamentais dos titulares de dados.

Cumpre ressaltar que a transparência administrativa não se limita ao cumprimento formal do princípio da publicidade dos atos governamentais. Sua efetividade exige medidas que transcendam a mera disponibilização de dados e documentos, demandando que as informações sejam apresentadas de forma clara, inteligível e acessível a todos os segmentos sociais interessados. A transparência, nesse sentido, não se esgota na abertura de canais informativos, mas pressupõe a promoção de uma cultura institucional voltada à *accountability*, à participação cidadã e ao controle democrático da Administração Pública.

A interseção entre os regimes da transparência e da proteção de dados impõe à Administração Pública o desafio de realizar o tratamento de dados pessoais com base em uma leitura sistemática e ponderada. Tal compatibilização exige que o compartilhamento de informações se dê por meio de uma arquitetura normativa que equilibre o exercício das

competências institucionais com a mitigação dos riscos à privacidade, à intimidade e à autodeterminação informativa dos titulares. Trata-se, portanto, de uma operação jurídica que demanda não apenas conformidade legal, mas também aderência aos princípios constitucionais e aos parâmetros de proporcionalidade e necessidade previstos na LGPD.

É nesse contexto que os instrumentos jurídicos formais — como convênios, termos de cooperação e contratos administrativos — assumem papel central. Mais do que formalizar o compartilhamento, esses instrumentos funcionam como garantias procedimentais que viabilizam o controle da legalidade, da finalidade e da proporcionalidade das operações de tratamento de dados.

O compartilhamento de dados entre órgãos públicos, portanto, deve ser compreendido como uma modalidade de tratamento inserida no processo de transformação digital do Estado, voltada à promoção da eficiência administrativa e à melhoria dos serviços públicos. Contudo, essa prática não pode se desenvolver à margem da legalidade, especialmente diante da positivação do direito fundamental à proteção de dados pessoais (art. 5º, LXXIX, CF/88, incluído pela EC 115/2022).

A ascensão da proteção de dados como direito fundamental autônomo revela uma transmutação substancial da ideia de privacidade, movendo-se de uma prerrogativa de opacidade (limites impostos ao poder estatal) para uma garantia de transparência procedimental — ou seja, a existência de um conjunto normativo que determina as condições e requisitos do tratamento e compartilhamento de dados pessoais.

Inspirando-se na doutrina de Lorenzo Dalla Corte (2020), defende-se aqui que o direito à proteção de dados deve ser compreendido como "direito à normatividade procedimental", ou "direito à regra", em tradução literal — ou seja, um direito fundamental que ultrapassa a proteção da privacidade, abarcando a garantia da existência de um sistema normativo que regule, de forma clara e previsível, as condições e os limites do tratamento de dados pessoais.

Essa concepção, que privilegia uma lógica procedimental em detrimento de uma abordagem meramente substancial, é corroborada por Gasiola *et al.* (2021), ao reconhecer que o tratamento de dados pela Administração Pública exige base legal específica, seja para a execução de políticas públicas (art. 7º, III, LGPD), seja para o cumprimento de competências legais (art. 23, LGPD). A formalização por meio de instrumentos jurídicos é, portanto, condição necessária à legitimidade do tratamento e ao controle de mérito e constitucionalidade dos atos administrativos que o autorizam.

Em virtude do princípio da publicidade administrativa, insculpido no art. 37 da Constituição da República e irradiado por todo o texto constitucional como expressão dos princípios republicano e democrático (art. 1º, CF), toda atividade administrativa deve ser compatibilizada com o dever de transparência. Essa compatibilização, no entanto, não pode ignorar os limites impostos pela proteção de dados pessoais, exigindo instrumentos jurídicos que permitam a ponderação entre os interesses públicos e os direitos fundamentais dos titulares.

Convênios e termos de cooperação, quando adequadamente estruturados, cumprem essa função ao estabelecer cláusulas que definem com precisão a finalidade do compartilhamento, a base legal que o autoriza, os mecanismos de segurança da informação, a responsabilidade dos agentes envolvidos e os meios de controle institucional, inclusive por reguladores, como a Agência Nacional de Proteção de Dados (ANPD). Esses elementos, como sustenta Corte (2020), constituem a própria essência do direito à proteção de dados, entendido como um sistema de garantias normativas voltado à regulação legítima do poder informacional.

A exigência de instrumentos jurídicos formais para o compartilhamento de dados pelo Poder Público configura-se, ainda, como verdadeira cláusula de salvaguarda dos direitos fundamentais dos indivíduos. Tais instrumentos não apenas conferem legitimidade ao fluxo informacional entre entes estatais, como também operam como barreiras normativas contra práticas arbitrárias ou ilegítimas. Sua ausência pode comprometer a validade dos atos administrativos fundados em dados obtidos de forma ilegal ou ilícita, violando o princípio da legalidade e do devido processo legal.

Nesse sentido, é a proposição de Paulo Otero (2013) de aplicação, no campo do direito administrativo, de um princípio garantístico cuja origem remonta ao processo penal: o princípio da inadmissibilidade da prova ilícita. Transposto para o domínio da Administração Pública, esse princípio impede que decisões administrativas sejam fundamentadas em elementos informacionais cuja obtenção não tenha observado os requisitos legais e constitucionais, especialmente aqueles relacionados à proteção de dados pessoais. Trata-se, portanto, de uma vedação à utilização de dados obtidos por meios ilegítimos, que comprometeriam não apenas a validade do ato administrativo, mas também a integridade do sistema jurídico como um todo.

Essa perspectiva revela que a regulação do fluxo informacional público não se destina exclusivamente à tutela da esfera privada dos cidadãos, mas também à preservação da integridade democrática, da confiança institucional e da legitimidade da ação estatal. A proteção de dados, nesse contexto, transcende o plano individual e alcança uma dimensão coletiva, na medida em que o uso indevido de informações compromete a transparência e o controle social

sobre a Administração Pública. Desse modo, a ausência de formalização adequada pode comprometer não apenas direitos subjetivos, mas também o interesse público na conformidade, na rastreabilidade e na responsabilização dos atos administrativos.

Assim, os instrumentos jurídicos formais — como convênios, termos de cooperação e contratos administrativos — não apenas estruturam o compartilhamento de dados, mas também operam como garantias procedimentais que asseguram a legalidade, a finalidade e a proporcionalidade do tratamento, em consonância com os postulados do Estado Democrático de Direito. Ao estabelecer parâmetros normativos claros, esses instrumentos viabilizam o controle institucional e social sobre o uso de dados pessoais pela Administração, funcionando como mecanismos de contenção do arbítrio e de promoção da segurança.

7.3 O PRINCÍPIO DA ÚNICA VEZ (*ONCE-ONLY PRINCIPLE)*

> Transformar o governo pelo digital, promovendo a efetividade das políticas, a qualidade dos serviços e reconquistando a confiança dos brasileiros.[104]

Ao longo deste trabalho, foram analisados diversos requisitos que funcionam como limites ao compartilhamento e aos usos secundários de dados pessoais sob a custódia do Poder Público. Neste tópico, destaca-se uma relevante possibilidade de equacionamento: o Princípio da Única Vez (*Once-Only Principle*), concebido como um instrumento estratégico para o tratamento de dados pessoais na esfera estatal. Tal princípio visa simplificar as interações entre o cidadão e o Estado, promovendo simultaneamente a eficiência administrativa e a proteção à privacidade e aos direitos fundamentais.

Esse princípio estabelece que o cidadão deve fornecer seus dados pessoais à Administração Pública apenas uma única vez, eliminando a necessidade de repetição das mesmas informações em diferentes órgãos ou serviços públicos. Por sua vez, os serviços públicos digitais devem assegurar a interoperabilidade das informações, ou seja, a capacidade de compartilhamento seguro e eficiente entre os diversos entes administrativos, sem que haja nova solicitação ao usuário (Portugal, [*s.d.*]).

Na prática, isso significa que, uma vez prestada a informação a um órgão público, os demais entes estatais ficam impedidos de exigir novamente os mesmos dados diretamente do cidadão. Compete a esses órgãos buscar e compartilhar as informações entre si, de forma

[104] Missão da Secretaria de Governo Digital.

segura, eficiente e estritamente vinculada a finalidades legítimas. Esse procedimento evita a redundância burocrática, reduz erros decorrentes da múltipla inserção de dados, diminui custos operacionais e contribui para a modernização do Estado, promovendo um ecossistema digital mais ágil, integrado e centrado no cidadão.

Sob a perspectiva da proteção de dados, o Princípio da Única Vez requer a implementação de mecanismos robustos de segurança, transparência e governança, de modo a garantir que o compartilhamento e a reutilização de dados pessoais entre órgãos públicos ocorram em conformidade com os marcos legais e os direitos fundamentais. Isso implica a observância dos princípios da finalidade, necessidade, minimização e, quando aplicável, do consentimento, além da adoção de salvaguardas tecnológicas e organizacionais aptas a mitigar riscos de vazamento, acesso indevido ou tratamento incompatível com os direitos dos titulares.

O Princípio da Única Vez (*Once-Only Principle*) tem sua origem vinculada à consolidação das políticas de governo digital no âmbito da União Europeia, especialmente a partir do final da década de 2000, como resposta à crescente demanda por eficiência administrativa, interoperabilidade entre sistemas públicos e respeito aos direitos fundamentais dos cidadãos na era digital. Foi formalmente reconhecido no contexto das iniciativas da União Europeia voltadas à construção do Mercado Único Digital, sendo incorporado ao eGovernment Action Plan 2016–2020 (European Commission, 2016), que estabeleceu compromissos para o progresso da modernização das administrações públicas da União Europeia, com ênfase na integração de serviços, na interoperabilidade de sistemas e na centralidade do cidadão, sempre em consonância com os direitos à privacidade e à proteção de dados pessoais, conforme delineado pelo então vigente arcabouço jurídico europeu.

Não obstante tenha sido promovido como um vetor de modernização administrativa e de simplificação das interações entre cidadãos e o Estado, foi também objeto de críticas relevantes no campo da proteção de dados pessoais, especialmente no contexto europeu. Tais críticas concentraram-se na tensão entre a eficiência administrativa e os direitos fundamentais à privacidade e à autodeterminação informativa, conforme delineados pelo Regulamento Geral sobre a Proteção de Dados (GDPR).

Uma das principais preocupações disse respeito ao risco de centralização excessiva de dados. A implementação do princípio poderia levar à criação de grandes repositórios interconectados de informações pessoais, o que ampliaria significativamente a superfície de exposição a incidentes de segurança, como vazamentos, acessos indevidos e usos abusivos. Essa concentração de dados, ainda que tecnicamente viável, exige, portanto, salvaguardas

jurídicas e tecnológicas para não comprometer os direitos dos titulares (European Data Protection Supervisor, 2016).

Além disso, alegou-se que o princípio poderia comprometer o controle do titular sobre seus dados, uma vez que, ao fornecer suas informações a um único órgão, o cidadão poderia não ter clareza ou meios efetivos para acompanhar como, por quem e para quais finalidades esses dados seriam reutilizados por outras entidades públicas. Isso levantou preocupações quanto à transparência e à possibilidade de exercício pleno dos direitos previstos nos artigos 12 a 22 do GDPR, como o direito de acesso, de oposição e de limitação do tratamento (European Data Protection Board, 2020).

Outro ponto criticado refere-se à observância dos princípios da finalidade e da minimização, pilares do regime europeu de proteção de dados. O compartilhamento amplo e automatizado de dados entre órgãos públicos poderia resultar em usos secundários não compatíveis com a finalidade original da coleta, violando o disposto no artigo 5º, inciso 1, alíneas “b” e “c” do GDPR. Por isso, a reutilização de dados deve ser sempre justificada por uma base legal clara, específica e proporcional, sob pena de configurar tratamento ilícito (European Data Protection Supervisor, 2017).

Por fim, os críticos ressaltaram que a interoperabilidade técnica entre sistemas públicos, embora essencial para a efetividade do *Once-Only Principle*, deve ser acompanhada de mecanismos de governança, segurança da informação e prestação de contas. A falta de tais salvaguardas compromete não apenas a conformidade com o GDPR, mas também a confiança dos cidadãos na integridade do ecossistema digital estatal (European Data Protection Supervisor, 2017).

Essas críticas não negam a utilidade do princípio, mas reforçam a necessidade de sua implementação ser cuidadosamente calibrada com os direitos fundamentais à privacidade e à proteção de dados, sob pena de se converter em um instrumento de erosão desses direitos.

Portanto, embora o Princípio da Única Vez represente um instrumento valioso para a promoção da eficiência administrativa e da desburocratização dos serviços públicos, sua implementação não está isenta de riscos significativos à proteção dos direitos fundamentais dos titulares de dados pessoais. A efetividade desse princípio depende da observância estrita dos fundamentos normativos da proteção de dados, exigindo a adoção de medidas técnicas, administrativas e jurídicas vigorosas, tais como a avaliação de impacto à proteção de dados (DPIA), a implementação de mecanismos de segurança da informação, a transparência nos fluxos de dados e a garantia de participação informada dos titulares.

A União Europeia realizou uma escolha estratégica e juridicamente significativa ao adotar o Princípio da Única Vez (*Once-Only Principle*) como elemento central de sua agenda de transformação digital e integração administrativa. Essa decisão representa um *trade-off* normativo e operacional cuidadosamente ponderado entre dois valores fundamentais: de um lado, a busca por maior eficiência, celeridade e interoperabilidade nos serviços públicos; de outro, a preservação dos direitos fundamentais à privacidade e à proteção de dados pessoais, conforme consagrados no Regulamento Geral sobre a Proteção de Dados (GDPR).

Mais do que uma medida de racionalização interna, o Princípio da Única Vez constitui um instrumento de integração transfronteiriça, essencial para a consolidação do Mercado Único Digital europeu. Por meio de sistemas interoperáveis e seguros, as informações fornecidas em um Estado-membro podem ser compartilhadas com autoridades de outros países da União, respeitando os princípios da finalidade, da minimização e da segurança. Essa arquitetura normativa e tecnológica visa facilitar a mobilidade de pessoas e empresas, ampliar o acesso a serviços públicos digitais e fortalecer a competitividade da economia europeia, sem comprometer os direitos dos titulares de dados pessoais (Comissão Europeia, 2020).

Nesse contexto, a União Europeia optou por institucionalizar o Princípio da Única Vez como um compromisso regulado entre eficiência administrativa e proteção de dados, reconhecendo que a construção de um Estado digital moderno, funcional e inclusivo exige soluções que conciliem inovação tecnológica com respeito aos direitos fundamentais. Essa escolha revela uma concepção sofisticada de governança digital, orientada não apenas por metas operacionais, mas por valores constitucionais compartilhados.

Ao adotar esse princípio, a União Europeia realiza um *trade-off* normativo e institucional cuidadosamente calibrado que visa assegurar que os cidadãos não sejam obrigados a fornecer repetidamente as mesmas informações às administrações públicas. Com isso, promove-se a interoperabilidade dos sistemas, a padronização das bases de dados e a integração dos serviços públicos em escala transnacional (Portugal, [*s.d.*]).

No plano administrativo, essa diretriz reflete um compromisso com a modernização da gestão pública, a racionalização de recursos e a redução de custos e prazos processuais, sem comprometer os pilares do Estado de Direito. A conectividade transfronteiriça e a digitalização dos serviços são concebidas como instrumentos para a realização de uma administração pública mais responsiva, transparente e centrada no usuário.

No plano jurídico, o *trade-off* encontra fundamento nos princípios estruturantes da ordem jurídica da União Europeia, especialmente a legalidade, a proporcionalidade e a proteção dos direitos fundamentais.

O referido princípio internacional de transformação digital também foi incorporado pelo ordenamento jurídico e pelas políticas públicas brasileiras, com o objetivo de tornar o compartilhamento de dados entre os órgãos da Administração Pública não apenas uma possibilidade técnica, mas uma obrigação institucional pautada pela transparência, pela finalidade legítima e pela proteção dos direitos dos titulares.

O Governo Brasileiro declarou oficialmente a adoção do Princípio da Única Vez (*Once-Only Principle*) como diretriz estruturante de sua estratégia de transformação digital, conforme divulgado pelo Ministério da Gestão e da Inovação em Serviços Públicos (Brasil, 2021). A opção por aderir a esse princípio orienta-se pela lógica de que o cidadão deve fornecer determinados dados pessoais apenas uma única vez à Administração Pública, sendo vedada a exigência reiterada das mesmas informações por diferentes órgãos estatais. Sua operacionalização, por sua vez, está diretamente vinculada ao Cadastro Base do Cidadão, programa que visa consolidar dados essenciais em uma base única, permitindo que os demais entes e entidades da administração pública federal acessem essas informações de forma segura, eficiente e interoperável.

O Princípio da Única Vez também se alinha aos objetivos da Estratégia Nacional de Governo Digital — ENGD, prevista na Lei nº 14.129, de 29 de março de 2021 — Lei do Governo Digital. Essa norma estabelece, entre outras diretrizes, a implementação de uma identificação única e nacional e o reuso ético e estruturado de dados públicos para qualificar a tomada de decisões e a oferta de serviços públicos digitais. Trata-se, portanto, de uma política pública orientada à eficiência administrativa, à desburocratização e à promoção de uma governança digital centrada no cidadão, sem descurar da observância aos princípios da legalidade, da finalidade e da proteção de dados pessoais, conforme exigido pela Lei Geral de Proteção de Dados Pessoais — LGPD.

É inegável que a transformação digital do Estado contribui para a simplificação de procedimentos e para a melhoria da qualidade dos serviços públicos. No entanto, tais benefícios somente se concretizam de forma legítima e sustentável quando são universalmente acessíveis e implementados com pleno respeito aos direitos fundamentais dos cidadãos, especialmente no que se refere à proteção de seus dados pessoais.

Diante do desafio de conciliar a celeridade da transformação digital com a salvaguarda da privacidade, o Brasil tem avançado em iniciativas normativas e institucionais voltadas à modernização da administração pública. Essas ações incluem a integração de bases de dados, o desenvolvimento de sistemas interoperáveis e a adoção de soluções tecnológicas orientadas à eficiência e à desburocratização. Todavia, tais medidas devem ser acompanhadas

de garantias jurídicas, de modo a assegurar que a inovação digital não se dê em detrimento dos direitos dos titulares, mas sim como instrumento de sua efetivação.

7.4 OBSERVÂNCIA DE LIMITES E GARANTIAS DE LEGITIMIDADE NO COMPARTILHAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

> Ainda que essas finalidades não tenham sido enunciadas de modo expresso, as expectativas legítimas e razoáveis que o titular tinha ou poderia ter, no momento da coleta, quanto à utilização desses dados, devem ser preservadas na realização do tratamento secundário (Alves; Valadão, 2023).

O Brasil tem registrado avanços expressivos em sua trajetória de transformação digital da administração pública, consolidando-se como uma referência regional e internacional em governo digital. De acordo com levantamento promovido pelo Ministério da Gestão e da Inovação em Serviços Públicos[105], aproximadamente 90% dos serviços públicos federais já se encontram disponíveis em formato digital, e mais de 160 milhões de cidadãos possuem contas ativas na plataforma GOV.BR. Esses indicadores evidenciam não apenas a amplitude da digitalização dos serviços, mas também o grau de adesão da população às soluções digitais oferecidas pelo Estado, refletindo um cenário de crescente maturidade institucional e tecnológica no setor público brasileiro (Brasil, 2025).

Considerando que o acesso a plataformas digitais governamentais pressupõe, em regra, a utilização de dados pessoais, o estudo *"Uso de Serviços Digitais — um retrato do Brasil"* evidencia que o compartilhamento dessas informações constitui elemento essencial para o exercício pleno da cidadania e para a fruição de direitos fundamentais no contexto digital brasileiro. A disponibilização de serviços públicos por meio de canais digitais depende, necessariamente, da circulação legítima e segura de dados entre os diversos órgãos públicos, exigindo um arcabouço normativo que concilie eficiência administrativa com proteção de direitos.

Nesse contexto se insere a Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD), que não tem por finalidade obstar o compartilhamento de dados pessoais pelo Poder Público, mas sim discipliná-lo de forma a garantir que esse tratamento ocorra com base

[105] Esse estudo, intitulado "*Uso de serviços digitais — um retrato do Brasil"*, foi realizado pelo Banco Interamericano de Desenvolvimento (BID), e teve o apoio do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), com o objetivo declarado de produzir evidências empíricas que subsidiem a qualificação das iniciativas de transformação do Estado.

em fundamentos legais claros, respeitando os princípios da finalidade, necessidade, segurança, transparência e responsabilização.

A LGPD, portanto, viabiliza a prestação de serviços públicos digitais de maneira simplificada, acessível e segura, ao mesmo tempo em que assegura a proteção dos direitos dos titulares e promove a confiança da sociedade na atuação estatal. Trata-se de um marco regulatório que busca equilibrar a inovação tecnológica com a preservação da dignidade da pessoa humana no ambiente digital.

Com fundamento no disposto no § 6º do art. 23 da LGPD, a transparência no uso compartilhado de dados pessoais pelo Poder Público constitui um dever jurídico essencial à proteção dos direitos dos titulares e à legitimidade do tratamento de dados na esfera estatal. A norma impõe aos agentes de tratamento da Administração Pública a obrigação de disponibilizar, em seus sítios eletrônicos oficiais, informações claras, adequadas e ostensivas, em local de destaque e de fácil acesso, sobre o uso compartilhado de dados pessoais.

Ademais, para garantir o exercício do direito à informação, previsto no art. 9º da LGPD, e reforçar os mecanismos de *accountability* e controle social sobre a atuação estatal, necessário se faz o fácil acesso às seguintes informações:

a) Identificação dos agentes de tratamento envolvidos no compartilhamento, permitindo a rastreabilidade e a responsabilização por eventuais violações;

b) Descrição dos dados pessoais objeto do compartilhamento, bem como a finalidade específica que justifica tal uso, em consonância com os princípios da finalidade, adequação e necessidade (art. 6º, I a III);

c) Data de início e término do uso compartilhado, acompanhada da justificativa da razoabilidade do prazo e da indicação do período de conservação dos dados, conforme previsto no art. 16 da LGPD;

d) Definição das responsabilidades de cada agente de tratamento, inclusive no que se refere à garantia dos direitos dos titulares, como forma de assegurar a responsabilização solidária ou subsidiária, conforme o caso;

e) Avaliação da compatibilidade entre a finalidade original da coleta e a nova finalidade do uso compartilhado, nos termos do art. 8º, assegurando que não haja desvio de finalidade ou ampliação indevida do escopo do tratamento;

f) Os canais de comunicação disponibilizados para o exercício dos direitos dos titulares, como acesso, correção, exclusão, portabilidade e oposição, conforme previsto nos arts. 18 e seguintes da LGPD.

Essa publicidade do compartilhamento de dados pessoais pelo Poder Público não constitui mera faculdade administrativa, mas sim um dever jurídico de natureza constitucional e infraconstitucional, diretamente vinculado aos princípios da transparência, da legalidade e da eficiência, bem como ao exercício do controle social.

Sob a ótica da Constituição Federal, o caput do art. 37 impõe à administração pública direta e indireta, de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios, a observância obrigatória ao princípio da publicidade. Esse dispositivo consagra a transparência administrativa como um pressuposto essencial do regime democrático, ao assegurar que a sociedade possa acompanhar, fiscalizar e influenciar a atuação do Estado. O controle social, nesse contexto, configura-se como uma das expressões mais concretas do princípio democrático consagrado no *caput* do art. 1º da Constituição, ao permitir que o povo exerça, de forma contínua, a soberania popular por meio da fiscalização da gestão pública.

No plano infraconstitucional, a Lei nº 12.527/2011 — Lei de Acesso à Informação (LAI) — reforça esse dever ao estabelecer, em seu art. 3º, inciso I, que a publicidade é a regra e o sigilo, a exceção. O inciso V do mesmo artigo explicita como diretriz a promoção do desenvolvimento do controle social da administração pública, impondo à Administração o dever de disponibilizar informações de forma ativa e acessível. Ademais, o art. 7º, inciso II, da LAI, dispõe que o direito de acesso à informação abrange dados contidos em registros ou documentos produzidos ou acumulados por órgãos públicos, ainda que não arquivados formalmente, incluindo, por evidente, os dados pessoais tratados e compartilhados no exercício de funções públicas.

Nesse contexto, o compartilhamento de dados pessoais pelo Poder Público, por configurar um ato administrativo complexo, deve observar os princípios da transparência e da motivação, sendo obrigatória a sua publicização, especialmente quando envolver múltiplos entes estatais e finalidades diversas. A ausência de transparência nesse processo compromete não apenas a legalidade do ato, mas também a confiança da sociedade na integridade do ecossistema digital estatal.

Adicionalmente, cumpre reforçar que, por se tratar de divulgação formal de ato administrativo, o uso compartilhado de dados pessoais entre órgãos e entidades do Poder Público deve ser formalizado por meio de processo administrativo, contrato, convênio ou instrumento congênere, reforçando a exigência de documentação, motivação e controle institucional sobre tais práticas. Essa formalização assegura a legalidade do tratamento e se constitui em um instrumento de *accountability* institucional, permitindo a rastreabilidade das decisões administrativas e a responsabilização dos agentes públicos envolvidos.

7.5 O COMPARTILHAMENTO DE DADOS PESSOAIS SOB CUSTÓDIA DO CONSELHO NACIONAL DE JUSTIÇA.

O que se não apaga é o futuro (Assis, 1872).

O Conselho Nacional de Justiça (CNJ), em consonância com os preceitos constitucionais brasileiros e com o marco regulatório da proteção de dados pessoais, aprovou a Resolução nº 647, de 26 de setembro de 2025, que estabelece diretrizes específicas para o acesso e o compartilhamento de dados pessoais sob sua custódia. O normativo revela um compromisso institucional com os direitos fundamentais à privacidade, à proteção de dados e à transparência pública, harmonizando esses valores por meio de princípios jurídicos e técnicos detalhados, em sintonia com os avanços da governança digital.

A Resolução parte do reconhecimento do direito constitucional à proteção de dados pessoais como direito fundamental, consagrado no art. 5º, inciso LXXIX, da Constituição Federal, e o contrapõe, equilibradamente, ao princípio da publicidade dos atos processuais, previsto no art. 5º, inciso LX. Essa dualidade impõe um desafio hermenêutico e operacional: o de compatibilizar a transparência institucional com o resguardo da intimidade dos indivíduos. Tal tarefa é conduzida sob os fundamentos da Lei Geral de Proteção de Dados Pessoais (LGPD — Lei nº 13.709/2018) e da Lei de Acesso à Informação (LAI — Lei nº 12.527/2011), que, longe de serem antagônicas, convergem para a construção de uma transparência qualificada e responsável.

Nos artigos 1º e 2º, a Resolução estabelece que os dados pessoais sob custódia do CNJ podem ser acessados pelo próprio titular, por instituições públicas e privadas, e por pessoas naturais, desde que observadas as hipóteses legais previstas na LGPD, especialmente os princípios da finalidade, boa-fé e interesse público. O acesso deve ser estritamente necessário ao desempenho de funções legais e regulamentares, vedando qualquer forma de tratamento inadequado, desproporcional ou desvinculado da finalidade declarada.

Especificamente para o compartilhamento, a Resolução impõe a obrigatoriedade de instrumentos jurídicos formais, como contratos ou convênios, que definam com clareza a finalidade, o escopo, o tipo de dado e as responsabilidades das partes envolvidas, excetuando-se apenas os casos de obrigação legal ou cumprimento de decisão judicial (art. 10). Destaca-se, ainda, a previsão de reciprocidade no compartilhamento, sempre que possível, como forma de beneficiar as atividades institucionais do CNJ.

As finalidades do compartilhamento são expressamente delimitadas no art. 11, abrangendo: simplificação da oferta de serviços públicos, formulação e avaliação de políticas públicas, melhoria da qualidade dos dados, eficiência administrativa, promoção do benefício social, garantia da publicidade processual e desenvolvimento tecnológico, especialmente no uso de inteligência artificial para sistematização da produção jurídica dos tribunais. Para tanto, o art. 12 impõe diretrizes rígidas de adequação, segurança da informação, não discriminação e responsabilização institucional.

A proteção dos dados é assegurada por mecanismos técnicos e administrativos robustos, incluindo controles de acesso, criptografia, trilhas de auditoria e gestão de vulnerabilidades, inclusive para dados biométricos (arts. 3º e 4º). O tratamento interno de dados exige avaliação prévia, com participação do Encarregado pelo Tratamento de Dados Pessoais e dos comitês especializados, consolidando uma estrutura de governança informacional alinhada às melhores práticas internacionais (art. 6º).

A Resolução reforça o compromisso com a transparência ativa, disponibilizando instrumentos jurídicos e dados públicos no portal do CNJ, conforme as premissas da LAI, observando, entretanto, a proteção dos dados pessoais e os princípios da LGPD (arts. 25 e 26). A governança de dados, coordenada pela Presidência do CNJ e apoiada por comitês técnicos, assegura a avaliação contínua da qualidade, integridade e segurança das informações (art. 27).

No campo da pesquisa acadêmica, o CNJ permite o tratamento de dados pessoais, inclusive sensíveis, desde que garantida a anonimização, o controle rigoroso de acesso e a restrição do uso às finalidades autorizadas, observando critérios éticos e legais que impedem a exposição indevida dos titulares (Capítulo III). A divulgação dos resultados deve preservar integralmente a privacidade, e o órgão de pesquisa assume responsabilidade pela segurança da informação e pela reparação de danos decorrentes de uso indevido.

Em caso de incidentes de segurança envolvendo dados compartilhados, os parceiros privados devem comunicar imediatamente o CNJ, apresentar análise de impacto e arcar com as medidas de mitigação e remediação (art. 20), exigência que reforça a cultura de responsabilidade e conformidade, essencial no atual contexto regulatório.

Esse arcabouço normativo demonstra como o CNJ, enquanto controlador de dados pessoais no âmbito do Poder Judiciário, institui um modelo de tratamento e compartilhamento pautado na razoabilidade, legalidade, transparência e segurança jurídica. Trata-se de uma resposta institucional moderna aos desafios da proteção de dados em um ambiente complexo, que envolve a proteção dos direitos individuais sem abrir mão do controle social e da eficiência administrativa.

Cuida-se de um equilíbrio normativo que, sem dúvida, é um marco de referência para o direito público digital brasileiro, contribuindo para a construção de uma governança de dados robusta, ética e transparente no sistema judiciário, alinhada aos padrões internacionais de direitos humanos e proteção de dados pessoais.

Nesse contexto, é incontornável a reflexão comparativa entre a Resolução CNJ nº 647/2025 e o Decreto nº 10.046/2019, que trata da governança de dados na administração pública federal. Enquanto o Decreto estabelece diretrizes gerais para o compartilhamento de dados, com foco no Cadastro Base do Cidadão e na gestão centralizada por comitê, a Resolução do CNJ avança ao detalhar instrumentos jurídicos específicos, exigindo formalização rigorosa e controle técnico do compartilhamento.

O Decreto prevê princípios relevantes — como privacidade, compartilhamento mínimo e transparência — mas não exige, expressamente, a celebração de instrumentos jurídicos como condição para o compartilhamento, salvo nos casos de obrigação legal ou decisão judicial. Já a Resolução do CNJ impõe essa exigência como regra, fortalecendo a segurança jurídica, promovendo rastreabilidade efetiva e assegurando transparência no fluxo de dados, mitigando riscos de uso indevido.

Além disso, a Resolução prioriza mecanismos técnicos e administrativos seguros, com participação de comitês especializados e do encarregado pelo tratamento, refletindo maior aderência às disposições da LGPD. Conclui-se, portanto, que a Resolução nº 647/2025 do CNJ representa um modelo progressista e detalhista, que reconhece a complexidade e a sensibilidade dos dados pessoais no âmbito do Judiciário, adotando medidas concretas para garantir transparência qualificada, segurança reforçada e rastreabilidade precisa.

Essa comparação evidencia a maturidade normativa da Resolução do CNJ, consolidando sua posição como referência para ações de proteção e governança de dados pessoais pelo Poder Público, e contribuindo para o fortalecimento da confiança institucional e da cultura de proteção de dados no Brasil.

A Resolução nº 647/2025 do Conselho Nacional de Justiça representa, portanto, um avanço normativo e institucional que transcende o mero cumprimento da legislação vigente. Ao estabelecer um modelo de compartilhamento de dados pessoais pautado na legalidade, na transparência e na segurança, o CNJ reafirma seu papel como guardião da confiança pública e como agente de inovação regulatória no sistema de justiça.

Mais do que um instrumento técnico, a Resolução é expressão de uma visão de futuro: um Poder Judiciário que respeita os direitos fundamentais, promove a governança ética da informação e se abre ao controle social sem abdicar da proteção da dignidade dos indivíduos.

Nesse sentido, a norma não apenas organiza o presente, mas projeta um horizonte de maturidade institucional e de responsabilidade democrática.

A Resolução nº 647/2025 é, portanto, uma aposta no futuro — um futuro no qual o compartilhamento de dados não será fonte de vulnerabilidade, mas de fortalecimento da cidadania, da justiça e da confiança nas instituições. Ao reconhecer que o dado pessoal é expressão da pessoa humana, o CNJ inscreve na arquitetura normativa do Estado brasileiro um compromisso que não se apaga: o de proteger o que há de mais sensível e permanente na vida democrática.

8 CONCLUSÕES

> É você que ama o passado e que não vê que o novo, o novo sempre vem (Como [...], 1976).

Este capítulo tem por finalidade apresentar a síntese conclusiva da pesquisa, respondendo à indagação central: "Quais são os limites e as possibilidades para o compartilhamento e uso secundário de dados pessoais no âmbito do Poder Público? "

A investigação demonstrou que o compartilhamento de dados entre entes públicos é juridicamente admissível, e mais do que isso, expressamente previsto e regulado pela Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD). Contudo, sua legitimidade está condicionada à observância de critérios rigorosos, tais como legalidade, finalidade, necessidade, transparência e proporcionalidade.

Partindo-se do reconhecimento do direito à proteção de dados pessoais como direito fundamental constitucional (art. 5º, LXXIX, da Constituição Federal), estrutural e normativo, que reflete um ideal político e social vinculado à dignidade da pessoa humana, compreende-se que ultrapassa a mera garantia de privacidade para configurar, fundamentalmente, o direito à existência de um regime normativo e procedimental que assegure previsibilidade, transparência e efetividade. Esse regime deve limitar o poder informacional estatal e permitir a construção legítima e democrática das operações de tratamento de dados pelo Estado.

Desse modo, o uso secundário de dados pelo Poder Público deve respeitar os direitos fundamentais dos titulares, configurando-se como ato administrativo sujeito a mecanismos de controle, responsabilização e prestação de contas.

A atividade administrativa de compartilhamento de dados, ao envolver dimensões complexas e assimetrias informacionais entre Estado e cidadãos, exige uma governança informacional ética, responsável e constitucionalmente legítima. Essa governança deve integrar, simultaneamente, os pilares da legalidade, da eficiência, da publicidade e da moralidade (art. 37 da Constituição Federal) e o cumprimento rigoroso dos comandos da Lei Geral de Proteção de Dados Pessoais, especialmente no que diz respeito à compatibilidade de finalidades, minimização de dados e responsabilização dos agentes públicos envolvidos.

A análise empreendida revelou que o compartilhamento de dados no setor público exige finalidades públicas legítimas, nos termos do artigo 26 da Lei Geral de Proteção de Dados Pessoais (LGPD). Além disso, essa prática deve ser formalizada por meio de instrumentos jurídicos adequados — como convênios, termos de cooperação ou contratos administrativos — sempre fundamentados na transparência ativa. Ressalta-se que a compatibilidade entre a

finalidade original da coleta e o uso secundário é requisito imprescindível, sob pena de configurar desvio de finalidade, em afronta ao princípio da autodeterminação informativa e à segurança jurídica do tratamento.

Reconhece-se, contudo, que há hipóteses em que se pode admitir o reaproveitamento de dados pessoais. O cruzamento de bases de dados administrativas para fins de controle antifraude constitui exemplo emblemático de uso secundário que, embora represente uma recontextualização informacional, não deve ser automaticamente interpretado como vedado pelo ordenamento jurídico. Ao contrário, tal prática pode ser juridicamente admissível, desde que observados os princípios e requisitos estabelecidos pela Lei Geral de Proteção de Dados Pessoais, especialmente no que tange à compatibilidade de finalidades, à minimização de dados e à responsabilização dos agentes públicos.

Sob essa perspectiva, a LGPD não deve ser concebida como entrave à eficiência administrativa, mas sim como vetor normativo que promove a interoperabilidade responsável, segura e auditável entre os entes públicos. A dialética entre proteção de dados e eficiência estatal não revela antagonismo, mas sim uma relação de complementaridade normativa, na medida em que a LGPD impõe a adoção de instrumentos jurídicos formais e práticas institucionais que assegurem a integridade, a transparência e a legitimidade democrática dos fluxos informacionais no âmbito da Administração Pública.

A interoperabilidade entre sistemas e bases de dados públicos permite a troca automática e segura de informações entre os órgãos da administração pública, evitando que o cidadão precise reapresentar dados já constantes nas bases governamentais. Por essa razão, configura-se como elemento estruturante da transformação digital do Estado, promovendo a ampliação do acesso a serviços públicos com qualidade, segurança e celeridade. Trata-se de um mecanismo que transcende a mera integração tecnológica, assumindo papel estratégico na conformação de uma Administração Pública orientada por princípios de eficiência, transparência e controle social.

Vê-se, por exemplo, que em duas edições do Concurso Público Nacional Unificado (CPNU), a integração das bases de dados nas inscrições permitiu assegurar aos estudantes de baixa renda o direito à isenção da taxa de inscrição por meio da consulta automática e segura às informações do Cadastro Único (CadÚnico). Conforme evidenciam essas iniciativas conduzidas pelo Ministério da Gestão e da Inovação em Serviços Públicos (Brasil, 2025), a articulação sistêmica entre diferentes esferas governamentais, viabilizada por soluções interoperáveis, fortalece a soberania digital nacional ao assegurar que o tratamento de dados

ocorra em infraestrutura segura, confiável e sob governança estatal, em consonância com os marcos normativos da proteção de dados e da segurança da informação.

Essa dinâmica de interoperabilidade permite a superação da fragmentação institucional e informacional que historicamente caracteriza a prestação de serviços públicos no Brasil, contribuindo para a mitigação da burocracia e dos entraves administrativos tradicionais. Ao viabilizar a troca segura, controlada e eficiente de dados entre órgãos e entidades da Administração Pública, a interoperabilidade gera efeitos concretos como a desburocratização dos processos, a redução dos tempos de resposta ao cidadão, o aprimoramento da qualidade dos serviços prestados. Esses elementos são estruturantes para a legitimidade democrática e para a eficiência administrativa, conformando um modelo de governança pública orientado por princípios constitucionais e pelas diretrizes da transformação digital do Estado.

Todavia, em situações dessa natureza, diante da complexidade e sensibilidade envolvidas, recomenda-se a adoção de salvaguardas adicionais, como a elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), conforme previsto nos artigos 5º, inciso XVII, e no artigo 50, § 2º, "d" da LGPD, como medida de governança e mitigação de riscos. Esses relatórios permitem avaliar previamente as ameaças, justificar a necessidade do tratamento e assegurar a conformidade com os direitos fundamentais dos titulares. Essa medida reforça a governança informacional responsável e contribui para a legitimidade democrática das práticas administrativas de tratamento de dados.

Recomenda-se, ainda, o fortalecimento e implementação de instrumentos jurídicos formais como garantias procedimentais centrais, capazes de promover a rastreabilidade, delimitar competências e responsabilidades, além de viabilizar o controle social efetivo e a *accountability*. Tais instrumentos devem ser claros, detalhados e amparados por mecanismos institucionais permanentes de fiscalização e auditoria, permitindo o controle interdisciplinar e a participação qualificada da sociedade civil, do Poder Judiciário e da Agência Nacional de Proteção de Dados (ANPD).

A exigência de instrumentos jurídicos formais para o compartilhamento de dados pessoais no âmbito do Poder Público representa uma cláusula essencial de salvaguarda dos direitos fundamentais. Esses instrumentos não apenas conferem legitimidade ao fluxo informacional entre entes estatais, mas igualmente funcionam como mecanismos normativos de contenção contra práticas arbitrárias, abusivas ou ilegítimas. Sua ausência pode comprometer a validade dos atos administrativos que se fundamentem em dados obtidos irregularmente, em afronta direta aos princípios da legalidade, da finalidade e do devido processo legal.

Consolida-se, assim, um princípio garantístico de elevada densidade normativa, que impõe à Administração Pública o dever de assegurar que toda decisão baseada em dados pessoais esteja respaldada por procedimentos legalmente previstos e constitucionalmente adequados. A observância desses requisitos é especialmente relevante diante da necessidade de preservar a integridade dos direitos fundamentais à privacidade, à autodeterminação informativa e à proteção de dados pessoais, conforme reconhecido pelo Supremo Tribunal Federal e pela Emenda Constitucional nº 115/2022.

Ademais, é crucial superar assimetrias de poder existentes entre órgãos públicos no tratamento compartilhado de dados. Para isso, recomenda-se a adoção de modelos alternativos e inovadores de governança institucional que promovam a descentralização da custódia dos dados, a cooperação horizontal equilibrada entre agentes e a participação plural e independente nos processos decisórios. Essa governança plural deve contribuir para impedir a concentração excessiva do poder informacional, mitigando o risco do "colonialismo de dados" e assegurando o respeito à autonomia dos titulares e à integridade democrática da gestão pública.

À luz do Princípio da Única Vez (*Once-Only Principle*), destaca-se o desafio e a oportunidade de reconciliar eficiência administrativa e proteção dos direitos fundamentais, mediante interoperabilidade técnica combinada a rigorosos mecanismos de governança, transparência e prestação de contas. A incorporação sistemática dos princípios de *privacy by design* e *privacy by default* desde a concepção dos sistemas públicos deve garantir que a proteção dos dados pessoais não seja encarada como mero formalismo, mas como linha mestra das políticas públicas digitais, assegurando segurança, minimização e controle dos titulares.

Esse modelo normativo-procedimental deve ainda ser complementado por uma participação efetiva dos titulares e da sociedade civil em processos regulatórios e de fiscalização, instituindo mecanismos de controle democrático e prevenção contra captura regulatória por interesses privados ou políticos. A efetividade do direito à proteção de dados repousa em uma decidida escolha coletiva por um sistema jurídico e institucional que imponha freios e contrapesos substanciais à atuação estatal no espaço informacional, protegendo a dignidade, a liberdade e a autonomia individual no contexto da era digital.

A jurisprudência do Supremo Tribunal Federal, especialmente nas Ações Diretas de Inconstitucionalidade (ADIs) nº 6387 e nº 6649, reforça a necessidade de observância de balizas constitucionais, como o devido processo legal, a proporcionalidade e a proteção da privacidade, para que o compartilhamento e o uso de dados pessoais pelo Estado se mantenham nos limites da legalidade e da legitimidade democrática. Nesse contexto, a atuação da Agência Nacional de Proteção de Dados (ANPD) revela-se essencial para o estabelecimento de diretrizes

interpretativas e operacionais que assegurem a conformidade do setor público com os parâmetros legais e constitucionais vigentes.

Conclui-se, portanto, que o desafio atual não é apenas construir uma arquitetura regulatória eficiente, mas assegurar que o avanço tecnológico e a busca por eficiência administrativa caminhem em harmonia com a salvaguarda intransigente dos direitos fundamentais, refletindo uma concepção sofisticada de Estado Democrático de Direito, onde o controle democrático, a transparência e a responsabilidade institucional são os fundamentos que legitimam o uso legítimo e socialmente aceitável dos dados pessoais do cidadão.

Embora não esgote a complexidade do tema, o estudo identifica que, no atual contexto digital, novas perspectivas emergem e se interconectam. Como sugestão para pesquisas futuras, destaca-se a necessidade de aprofundar a análise sobre o papel da inteligência artificial e da automação no uso secundário de dados pessoais, com especial atenção aos riscos de discriminação algorítmica, opacidade decisória e impactos sobre os direitos fundamentais.

Em suma, reafirma-se que o compartilhamento e o uso secundário de dados pessoais pelo Poder Público são juridicamente possíveis, porém não ilimitados. Submetem-se a um regime jurídico estrito, que exige a harmonização entre a busca por eficiência administrativa e a proteção integral dos direitos fundamentais. A LGPD, a jurisprudência constitucional e as diretrizes da ANPD constituem um tripé normativo essencial, que impõe transparência, proporcionalidade e responsabilidade como condições indispensáveis para a legitimidade do tratamento de dados na esfera estatal.

Uma perspectiva promissora se delineia no horizonte normativo e institucional inaugurado pela Resolução nº 647/2025 do Conselho Nacional de Justiça, que estabelece diretrizes para o tratamento e o compartilhamento de dados pessoais sob a custódia do órgão, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e com a Emenda Constitucional nº 115/2022.

Trata-se de normativo que, ao prever que o compartilhamento de dados pessoais requer a celebração de instrumento jurídico adequado para efetivação do tratamento, converge para uma Administração Pública digital mais integrada, transparente e legitimada pela confiança social, construída sobre os pilares do respeito rigoroso aos direitos fundamentais, da observância dos princípios constitucionais da publicidade, eficiência e legalidade, e da contínua inovação regulatória. E, ao condicionar o acesso e o uso de dados pessoais à demonstração de propósitos legítimos, específicos e proporcionais, a Resolução reforça a centralidade da governança informacional como instrumento de qualificação da transparência e de fortalecimento da soberania digital do Estado brasileiro.

Em um cenário marcado pela intensificação do governo digital e pela transformação tecnológica acelerada, a proteção dos dados pessoais no âmbito do Poder Público revela-se não apenas uma exigência legal, mas um imperativo democrático inadiável.

Essa pesquisa contribui para consolidar um modelo de Administração Pública que não se prende às amarras do passado, mas avança com coragem rumo ao novo — um modelo que alia eficiência tecnológica à integridade ética, reafirmando o compromisso inegociável com a dignidade humana, a legalidade rigorosa e a gestão transparente e responsável dos dados. Na era digital, é a confiança da sociedade que guia a inovação pública.

REFERÊNCIAS

ALEXANDRE, Ricardo; DEUS, João de. **Direito Administrativo**. São Paulo: Método, 2018.

ALEXY, Robert. **Teoria dos Direitos Fundamentais.** Trad. Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

ALVES, Fabricio; VALADÃO, Rodrigo. **Regime Jurídico do Tratamento Secundário de Dados Pessoais Pelo Poder Público.** *In*: LIMA, Ana; ALVES, Fabricio da Mota (coord.). Comentários aos Regulamentos e Orientações da ANPD. São Paulo: Revista dos Tribunais, 2023. Disponível em: https://www.jusbrasil.com.br/doutrina/comentarios-aos-regulamentos-e-orientacoes-da-anpd-ed-2023/1823974791. Acesso em: 16 jul. 2025.

AMNESTY INTERNATIONAL. **The social atrocity: Meta and the right to remedy for the Rohingya**. Londres: Amnesty International, 2022. Disponível em: https://www.amnesty.org/en/documents/asa16/5933/2022/en/. Acesso em: 17 maio 2025.

ANASTÁCIO, Kimberly; SANTOS, Bruna; VARON, Joana (coord.). **Cadastro Base do Cidadão**: a megabase de dados. Rio de Janeiro: Coding Rights, 2020. Disponível em: https://codingrights.org/docs/megabase.pdf. Acesso em: 14 jul. 2025.

ANASTÁCIO, Kimberly; SANTOS, Bruna; VARON, Joana. **Cadastro base do cidadão:** a megabase de dados. Rio de Janeiro: Coding Rights, 2020. Disponível em: https://codingrights.org/docs/megabase.pdf. Aceeso em: 13 jun. 2025.

ANDRADE, André Gustavo C. de. Dimensões da interpretação conforme a Constituição. **Revista da Emerj**, Rio de Janeiro, 1998.

ANDRADE, Carlos Drummond de. No meio do caminho. Rio de Janeiro: Record, 1979.

ANDRADE, Walmar. **A diferença entre privacidade e proteção de dados pessoais.** Disponível em: https://walmarandrade.com.br/diferenca-entre-privacidade-e-protecao-de-dados-pessoais/. Acesso em: 30 jun. 2025. [s.d.]

ANDRADE, Walmar. **O principal objetivo da LGPD não é a proteção de dados pessoais.** Disponível em: https://walmarandrade.com.br/principal-objetivo-da-lgpd/. Acesso em: 06 jul. 2025.

ARAGÃO, João Carlos Medeiros de. Choque entre direitos fundamentais: consenso ou controvérsia?. **Revista de Informação Legislativa**, Brasília, v. 48, n. 189, p. 259-268, jan./mar. 2011.

ARAÚJO, Edmir Netto de. **Curso de direito administrativo**. São Paulo: Saraiva, 2005.

ASSIS, Machado de. Ressurreição. Rio de Janeiro: Garnier, 1872.

BARROSO, Luís Roberto. A razão sem voto: o Supremo Tribunal Federal e o governo da maioria. **Revista Brasileira de Políticas Públicas**, Brasília, v. 5, n. 2, 2015. Disponível em: https://bibliotecadigital.tse.jus.br/server/api/core/bitstreams/a5a196ff-5a8d-4e2d-b121-149c41622819/content. Acesso em: 10 jul. 2025.

BARROSO, Luís Roberto. Liberdade de Expressão e Limitação a Direitos Fundamentais. Ilegitimidade de Restrições à Publicidade de Refrigerantes e Sucos. **Revista de Direito Público da Economia**, Belo Horizonte, v. 2, n. 7, jul./set. 2004.

BARROSO, Luís Roberto. **O Novo Direito Constitucional Brasileiro**: contribuições para a construção teórica e prática da jurisdição constitucional no Brasil. Belo Horizonte: Fórum, 2014.

BAUMAN, Zygmunt; LYON, David. **Vigilância líquida.** Rio de Janeiro: Zahar, 2013.

BIONI, Bruno R.; MENDES, Laura Schertel. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. *In*: BIONI, Bruno R. (org.). **Lei Geral de Proteção de Dados**: comentários à Lei nº 13.709/2018. São Paulo: Revista dos Tribunais, 2021. p. 157–180. Disponível em: https://observatoriolgpd.com/wp-content/uploads/2021/08/1629122407livro-LGPD-Bruno-Bioni-completo-internet-v2.pdf. Acesso em: 26 ago. 2025.

BIONI, Bruno R.; ZANATTA, Rafael A. F. **Direito e economia política dos dados**: um guia introdutório. *In*: DOWBOR, Ladislau (org.). Sociedade vigiada: como a invasão da privacidade por grandes corporações e estados autoritários ameaça instalar uma nova distopia. São Paulo: Autonomia Literária, 2020. p. 123–125.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BIONI, Bruno Ricardo; OLIVEIRA, Rafael Zanatta de; MONTEIRO, Renata Ávila. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. **Revista Brasileira de Políticas Públicas**, v. 10, n. 2, p. 733–758, 2020. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/6405. Acesso em: 10 jun. 2025.

BIONI, Bruno; GARROTE, Marina; MEIRA, Marina; PASCHOALINI, Nathan. **Entre a visibilidade e a exclusão**: um mapeamento dos riscos da Identificação Civil Nacional e do uso de sua base de dados para a plataforma gov.br. Associação Data Privacy Brasil de Pesquisa, 2022. Disponível em: https://brunobioni.com.br/blog/2022/11/14/entre-a-visibilidade-e-a-exclusao-um-mapeamento-dos-riscos-da-identificacao-civil-nacional-e-do-uso-de-sua-base-de-dados-para-a-plataforma-gov-br/ Acesso em: 14 set. 2025.

BLOK, Marcella. A Nova Lei Anticorrupção e o Compliance. **Revista de Direito Bancário e do Mercado de Capitais**, [*s. l.*], v. 65, p. 263, jul. 2014. Disponível em: https://emd-public.nyc3.digitaloceanspaces.com/eusouempreendedor-uploads/RT-Marcella-Blok-Nova-lei-anticorrup%C3%A7%C3%A3o-e-compliance-.pdf. Acesso em: 14 set. 2025.

BOBBIO, Norberto. **A Era dos Direitos.** 7. ed. Rio de Janeiro: Elsevier, 2004.

BONAVIDES, P. A quinta geração de direitos fundamentais. **Revista Brasileira de Direitos Fundamentais & Justiça**, [*s. l.*], v. 2, n. 3, p. 82–93, 2008. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/534. Acesso em: 4 jun. 2025.

BONAVIDES, Paulo. **Curso de Direito Constitucional.** 19. ed. São Paulo: Malheiros, 2006.

BORGES, Alice Gonzalez. **Supremacia do interesse público**: desconstrução ou reconstrução?. Salvador: Academia Baiana de Letras Jurídicas, 2011. Disponível em: https://www.academia.edu/29222291. Acesso em: 11 jun. 2025.

BOUK, Dan. **The National Data Center and the Rise of the Data Double.** Historical Studies in the Natural Sciences, vol. 48, no. 5, 2018, pp. 627–36. JSTOR2. Disponível em:<< https://www.jstor.org/stable/26616643>>

BRANCO, Paulo Gustavo Gonet. **Cláusulas pétreas.** *In*: ENCICLOPÉDIA JURÍDICA DA PUC-SP. São Paulo: PUC-SP, 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/21/edicao-2/clausulas-petreas. Acesso em: 12 jun. 2025.

BRANCO, Paulo Gustavo Gonet. **Juízo de ponderação na jurisdição constitucional:** pressupostos de fato e teóricos reveladores do seu papel e de seus limites. 2008. Tese (Doutorado em Direito)-Universidade de Brasília, Brasília, 2008. Disponível em: https://repositorio.unb.br/handle/10482/5128. Acesso em: 09 jun. 2025.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 25 maio 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. **Biometria e reconhecimento facial:** Estudos preliminares. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/radar-tecnologico-biometria-anpd-1.pdf. Acesso em: 25 maio 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo**: tratamento de dados pessoais pelo Poder Público. Versão 2.0. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 25 maio 2025.

BRASIL. Conselho Nacional de Justiça. **Resolução nº 647, de 26 de setembro de 2025**. Dispõe sobre o acesso a dados pessoais constantes dos sistemas informatizados do Conselho Nacional de Justiça. Brasília, DF: CNJ, 26 set. 2025. Disponível em: https://www.cnj.jus.br. Acesso em: 1 out. 2025.

BRASIL. **Decreto n. 10.046, de 9 outubro 2019.** 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. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 12 jul. 2025.

BRASIL. **Decreto n. 10.047, de 9 outubro 2019.** Dispõe sobre a governança do Cadastro Nacional de Informações Sociais e institui o programa Observatório de Previdência e Informações, no âmbito do Cadastro Nacional de Informações Sociais. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10047.htm. Acesso em: 12 jul. 2025.

BRASIL. **Decreto nº 12.428, de 3 de abril de 2025.** Regulamenta o art. 35, § 2º, da Lei nº 8.742, de 7 de dezembro de 1993, e o art. 3º da Lei nº 15.077, de 27 de dezembro de 2024, para dispor sobre o compartilhamento de dados pelos órgãos públicos federais e pelas prestadoras de serviços públicos. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12428.htm. Acesso em: 14 jul. 2025.

BRASIL. **Decreto nº 12.455, de 15 de maio de 2025.** Altera o Decreto nº 12.428, de 3 de abril de 2025, que regulamenta o art. 35, § 2º, da Lei nº 8.742, de 7 de dezembro de 1993, e o art. 3º da Lei nº 15.077, de 27 de dezembro de 2024, para dispor sobre o compartilhamento de dados pelos órgãos públicos federais e pelas prestadoras de serviços públicos. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12455.htm. Acesso em: 14 jul. 2025.

BRASIL. Governo Federal. **Princípio "Once Only".** Governo Digital, 13 abr. 2021. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/outros-eventos/seminario-internacional-de-protecao-de-dados/principio-once-only. Acesso em: 19 jul. 2025.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponivel em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 set. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 22 maio 2025

BRASIL. **Lei nº 9.868, de 10 de novembro de 1999**. Dispõe sobre o processo e julgamento da ação direta de inconstitucionalidade e da ação declaratória de constitucionalidade perante o Supremo Tribunal Federal. Brasília, DF: Presidência da República, 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9868.htm. Acesso em: 26 maio 2025.

BRASIL. **Medida Provisória nº 954, de 17 de abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações com a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública decorrente do coronavírus (COVID-19). Brasília, DF: Presidência da República, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 18 maio 2025.

BRASIL. **Mensagem nº 451, de 14 de agosto de 2018**. Veto parcial ao Projeto de Lei nº 53, de 2018, que dispõe sobre a proteção de dados pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Msg/VEP/VEP-451.htm. Acesso em: 2 set. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Uso de serviços digitais – um retrato do Brasil.** Brasília: MGI, 2025. Disponível em: https://www.gov.br/gestao/pt-

br/assuntos/noticias/2025/abril/pesquisa-revela-que-77-dos-brasileiros-consideram-facil-o-acesso-a-servicos-publicos-digitais/usodeservicosdigitais_bid.pdf. Acesso em: 19 jul. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos**. Governo abre consulta pública sobre a criação da Política de Governança e Compartilhamento de Dados.** Brasília, DF: Portal Gov.br, 23 jul. 2025. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/noticias/2025/julho/governo-abre-consulta-publica-sobre-a-criacao-da-politica-de-governanca-e-compartilhamento-de-dados. Acesso em: 16 ago. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Do eletrônico ao digital:** linha do tempo da governança digital no Brasil**.** Brasília, DF: Governo Federal, 2024b. Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital. Acesso em: 3 jun. 2025.

BRASIL. Ministério da Saúde. **Rede Nacional de Dados em Saúde – RNDS.** Brasília, DF, 2025c. Disponível em: https://www.gov.br/saude/pt-br/composicao/seidigi/rnds. Acesso em: 14 jul. 2025.

BRASIL. Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome. **Cadastro Único.** Disponível em: https://www.gov.br/mds/pt-br/acoes-e-programas/cadastro-unico. Acesso em: 12 jul. 2025.

BRASIL. Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome. **Instrução Normativa SAGICAD/MDS nº 2, de 21 de maio de 2025.** Estabelece regras e procedimentos operacionais relativos ao processo de inclusão e atualização de dados no Cadastro Único para Programas Sociais do Governo Federal. Disponível em: https://www.gov.br/mds/pt-br/acesso-a-informacao/legislacao/instrucoes/instrucao-normativa-sagicad-mds-no-2-de-21-de-maio-de-2025. Acesso em: 16 jul. 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n. 2.356 MC/DF e Ação Direta de Inconstitucionalidade n. 2.362 MC/DF**. Relator: Min. Néri da Silveira. Brasília, DF, julgado em 25 nov. 2010. Disponível em: https://stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI2362CM.pdf. Acesso em: 12 jun. 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade 6.407 MC-Ref / DF**. Referendo na medida cautelar na ação direta de inconstitucionalidade. Relator(a): min. Gilmar mendes. Julgamento: 30 nov. 2020. Publicação: 10 dez. 2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur438110/false. Acesso em: 18 maio 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade 6.649/DF.** Relator(a): Min. Gilmar Mendes. Julgamento: 15 set. 2022. Publicação: 19 jun. 2022. Órgão julgador: Tribunal Pleno. Disponível em: << https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false >> Acesso em: 18/05/2025.

BRASIL. Supremo Tribunal Federal. **AI 631533/RJ**. Relator: Min. Gilmar Mendes. Julgado em: 12 mar. 2007. Publicado em: 18 abr. 2007. Disponível em: https://portal.stf.jus.br/constituicao-supremo/leis-infraconstitucionais/verlegislacao.asp?item=346. Acesso em: 27 maio 2025.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário n. 888.815, Rio Grande do Sul**. Relator: Ministro Luís Roberto Barroso. Brasília, DF, julgado em 12 set. 2018. Disponível em: https://stf.jus.br/arquivo/cms/bibliotecaConsultaProdutoBibliotecaPastaFachin/anexo/RE888815.pdf. Acesso em: 4 jun. 2025.

BRASIL. Tribunal de Contas da União . **Acórdão nº 506, de 12 mar. 2025**. Disponível em: https://pesquisa.apps.tcu.gov.br/doc/acordao-completo/506/2025/Plenário. Acesso em: 29 jun. 2025.

BRASIL. Tribunal de Contas da União. **Acórdão nº 2591/2024** – Plenário. Relator: Ministro Aroldo Cedraz. Brasília, DF, 4 dez. 2024. Processo nº 010.781/2022-6. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/NUMACORDAO%253A2591%2520ANOACORDAO%253A2024%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0. Acesso em: 24 maio 2025.

BRASIL. Tribunal de Contas da União. **Referencial básico de governança aplicável a organizações públicas e outros entes jurisdicionados ao TCU.** 3. ed. Brasília: TCU, 2020.

CAIXA ECONÔMICA FEDERAL. **Manual do Sistema de Cadastro Único.** Brasília: CAIXA, 2023. Disponível em: https://www.caixa.gov.br/Downloads/cidades-cadastramento-unico-manuais/Manual_Cadastro_Unico.pdf. Acesso em: 12 jul. 2025.

CARDOSO, André Guskow. **O regime e uso compartilhado de dados pessoais pela Administração Pública no âmbito da LGPD**. Informativo Justen, Pereira, Oliveira e Talamini. Curitiba, nº 163, setembro de 2020. Disponível em: http://www.justen.com.br. Acesso em: 13 jul. 2025.

CARVALHO, Lucas Borges de. O poder público e a proteção de dados pessoais no Brasil: novos desafios, velhas práticas administrativas. **Revista de Direito Administrativo**, [*s. l.*], v. 282, n. 2, p. 133–162, 2023. Disponível em: https://periodicos.fgv.br/rda/article/view/89347. Acesso em: 18 jul. 2025.

CARVALHO, Salo de. **Como NÃO se faz um trabalho de conclusão**: provocações úteis para orientadores e estudantes de Direito. 2. ed. São Paulo: Saraiva, 2013.

CASTELLS, Manuel. **A era da informação**: economia, sociedade e cultura. Tradução: Roneide Venâncio Majer. 6. ed. São Paulo: Paz e Terra, 1999. (v. 1).

CAVALCANTI, Ana Elizabeth Lapa Wanderley *et al.* **Cartilha Cidadania Digital.** São Paulo: Faculdades Metropolitanas Unidas, 2022. Disponível em: https://justica.sp.gov.br/wp-content/uploads/2022/11/CartilhaCidadaniaDigital2022FMUSJC.pdf. Acesso em: 28 jun. 2025.

CAVOUKIAN, Ann. **Privacy by Design: The 7 Foundational Principles.** Ontario: Information and Privacy Commissioner of Ontario, 2009. Disponível em: https://www.datatilsynet.no/globalassets/global/bilder/rettigheter-og-plikter/innebygd-personvern/7foundationalprinciples_anncavoukian2.pdf. Acesso em: 18 jul. 2025.

CHAPMAN, Samuel. Edward Snowden & the NSA PRISM Program: What You Need to Know in 2025. **Privacy Journal**, [*s. l.*], 21 nov. 2024. Disponível em: https://www.privacyjournal.net/edward-snowden-nsa-prism/. Acesso em: 14 jul. 2025.

CÍCERO, Marco Túlio. **De Legibus.** The Latin Library, [s. d.]. Disponível em: https://www.thelatinlibrary.com/cicero/leg3.shtml. Acesso em: 13 jun. 2025.

COMISSÃO EUROPEIA. **The Once Only Principle system**: a breakthrough for the EU's Digital Single Market. Bruxelas, 5 nov. 2020. Disponível em: https://commission.europa.eu/news-and-media/news/once-only-principle-system-breakthrough-eus-digital-single-market-2020-11-05_en. Acesso em: 19 jul. 2025.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Personal data protection:** perceptions and attitudes of Internet users. São Paulo: CETIC.br, 2023. Disponível em: https://cetic.br/media/docs/publicacoes/6/20230727104238/iso-year-xv-n-2-personal-data-protection.pdf. Acesso em: 23 jun. 2025. (ICT Households Survey, Year XV, n. 2).

COMITÊ GESTOR DA INTERNET NO BRASIL. Por uma internet melhor para os brasileiros. **Revista .br**, São Paulo, v. 15, n. 22. Disponível em: https://www.cgi.br/media/docs/publicacoes/3/20250523115905/revistabr-ano-15-2025-edicao22.pdf. Acesso em: 23 maio 2025.

COMO nossos pais. Intérprete: Belchior. *In:* ALUCINAÇÃO. Intérprete: Belchior. Universal Music, 1976.

COMPARTILHAMENTO de dados gera economia de R$ 2,41 bilhões entre janeiro e outubro de 2024. Agência Gov, [*s. l.*], 4 dez. 2024. Disponível em: https://agenciagov.ebc.com.br/noticias/202412/compartilhamento-de-dados-gera-economia-de-r-2-41-bilhoes-entre-janeiro-e-outubro-de-2024. Acesso em: 14 jul. 2025.

CONSELHO DA EUROPA. **Convenção 108+**: Convenção para a proteção das pessoas relativamente ao tratamento de dados de caráter pessoal. Elsinore: Conselho da Europa, 2018. Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. Acesso em: 17 ago. 2025.

CORTE. Lorenzo Dalla. A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection. *In*: HALLINAN, Dara; LEENES, Ronald; GUTWIRTH, Serge; DE HERT, Paul (ed.). **Data Protection and Privacy.** (v. 12).

CRETELLA JÚNIOR, José. Princípios informativos do direito administrativo. **Revista de Direito Administrativo,** Rio de Janeiro, v. 93, out. 1968.

CUSTERS, Bart; URSIC, Helena. Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection. **SSRN Electronic Journal**, [*s. l.*], 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3046774. Acesso em: 30 maio 2025.

DANTAS, Bruno. Transparência ou opacidade? Como a má aplicação da LGPD ameaça a democracia. **Atricon**, Brasília, DF, 19 mar. 2025. Disponível em: https://atricon.org.br/transparencia-ou-opacidade-como-a-ma-aplicacao-da-lgpd-ameaca-a-democracia/. Acesso em: 29 jun. 2025.

DE MAURO, Andrea; GRECO, Marco; GRIMALDI, Michele. **What is big data?** A consensual definition and a review of key research topics. AIP Conference Proceedings, 2015. Disponível em: https://www.semanticscholar.org/venue?name=AIP%20Conference%20Proceedings

DI PIETRO, Maria Sylvia Zanella. **Direito administrativo.** São Paulo: Atlas, 2012.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Joaçaba**, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://doneda.net/a-protecao-dos-dados-pessoais-como-um-direito-fundamental/. Acesso em: 21 jun. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: DONEDA, Danilo *et al.* (org.). **Tratado de Proteção de Dados Pessoais.** 2. ed. Rio de Janeiro: Forense, 2023.

DUQUE, M. S.; NASCIMENTO, I. M. A. do. O princípio da proporcionalidade à luz da teoria dos limites dos limites: critérios de análise de restrições a direitos fundamentais. **Revista Estudos Institucionais**, [*s. l.*], v. 4, n. 2, p. 949–968, 2018. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/308. Acesso em: 8 jun. 2025.

ENAP, Fundação Escola Nacional de Administração Pública. **Governo Integrado**: como construí-lo?. 2023. Disponível em: https://www.escolavirtual.gov.br/curso/935. Acesso em: 14 out. 2025.

ENCYCLOPAEDIA BRITANNICA. **Subatomic particle.** Encyclopaedia Britannica. Disponível em: https://www.britannica.com/summary/subatomic-particle. Acesso em: 8 jun. 2025.

EUROPEAN COMMISSION. **What does data protection 'by design' and 'by default' mean?.** Brussels: European Commission. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en. Acesso em: 18 jul. 2025.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 07/2020 on the concepts of controller and processor in the GDPR.** Brussels: EDPB, 2020. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en. Acesso em: 18 jul. 2025.

EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 1/2017 on the proposal for a European Interoperability Framework**. Brussels: EDPS, 2017. Disponível em: https://edps.europa.eu/data-protection/our-work/publications/opinions/european-interoperability-framework_en. Acesso em: 18 jul. 2025.

EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 8/2016 on the coherent enforcement of fundamental rights in the age of big data.** Brussels: EDPS, 2016. Disponível em: https://edps.europa.eu/data-protection/our-work/publications/opinions/coherent-enforcement-fundamental-rights-age-big-data_en. Acesso em: 18 jul. 2025.

FALEIROS JÚNIOR, José Luiz de Moura. Democracia digital, consensualização e o Estado brasileiro: reflexões à luz da Lei nº 14.129/2021. **Revista Digital de Direito Administrativo**, São Paulo, v. 10, n. 2, p. 1–19, 2023. Disponível em: https://revistas.usp.br/rdda/article/view/200794. Acesso em: 22 maio 2025.

FARIAS, Edilsom. Restrição de direitos fundamentais. **Seqüência Estudos Jurídicos e Políticos**, Florianópolis, v. 21, n. 41, p. 67–82, 2000. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/15416. Acesso em: 10 jun. 2025.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, São Paulo, v. 88, p. 439–459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231.. Acesso em: 29 jul. 2024.

FERREIRA DA SILVA, Carlos Bruno. **Proteção de dados e cooperação transnacional:** teoria e prática na Alemanha, Espanha e Brasil. Belo Horizonte: Arraes, 2014.

FERREIRA, Lucia Maria Teixeira. Parecer sobre a legalidade dos Decretos 10.046/2019 e 10.047/2019 em face das normas que disciplinam os direitos fundamentais à proteção de dados e à privacidade no ordenamento jurídico brasileiro. **Revista do Ministério Público do Estado do Rio de Janeiro**, Rio de Janeiro, n. 75, p. 258-259, jan./mar 2020.

FERREIRA, Lucia Maria Teixeira. Repercussões do julgamento da ADI nº 6.649 e da ADPF nº 695: separação informacional de poderes e limites do compartilhamento de dados pessoais. *In*: **MENDES, Laura Schertel** *et al.* **(orgs.). Direitos fundamentais na era digital**: Anuário 2023 das Comissões Especiais de Proteção de Dados (CEPD) e de Direito Digital (CEDD). Porto Alegre: Fundação Fênix, 2023.

FERREIRA, Lucia Maria Teixeira; GARCIA, Matheus. Responsabilidade civil por vazamento de dados pessoais: análise da decisão proferida no AREsp n.2.130.619/SP. **Civilistica.com**, Rio de Janeiro, v. 13, n. 2, 2024. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/1038/805. Acesso em: 13 jan. 2025.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. 25. ed. Petropolis: Vozes, 1987.

FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovana. **Curso de proteção de dados pessoais**: fundamentos da LGPD. Rio de Janeiro: Forense, 2022.

GASIOLA, Gustavo Gil. Criação e desenvolvimento da proteção de dados na Alemanha. **JOTA**, [*s. l.*], 29 maio 2019. Disponível em: https://www.jota.info/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha. Acesso em: 18 maio 2025.

GASIOLA, Gustavo Gil. MACHADO, Diego. MENDES, Laura Schertel. O tratamento de dados pessoais pela administração pública : transparência, bases legais e limites constitucionais. *In*: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio (org.). **A Lei Geral de Proteção de Dados Pessoais**: aspectos práticos e teóricos **relevantes** no setor público e privado – LGPD. São Paulo: Revista dos Tribunais, 2021. p. 137-161.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.

GOMES, Gilvaneide Francisca; OLIVEIRA, Katyeudo Karlos Sousa; SOUZA, Ricardo André Cavalcante. Competências da cidadania digital: especificação e avaliação de uma proposta de experiência de ensino-aprendizagem. **Gestão.Org**, Recife, v. 19, n. 2, p. 1–25, jul./dez. 2021. Disponível em: https://periodicos.ufpe.br/revistas/gestaoorg/article/view/252647. Acesso em: 23 jun. 2025.

HARARI, Yuval Noah. **Nexus:** Uma breve história das redes de informação, da Idade da Pedra à inteligência artificial. São Paulo: Companhia das Letras, 2024.

IDW – Informationsdienst Wissenschaft. Studie zeigt Nutzen von molekularer Tumoranalyse. 28 maio 2025. Disponível em: https://nachrichten.idw-online.de/2025/05/28/studie-zeigt-nutzen-von-molekularer-tumoranalyse. Acesso em: 14 jun. 2025.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das Melhores Práticas de Governança Corporativa**. 6. ed. São Paulo: IBGC, 2023. Disponível em: https://setrerj.org.br/wp-content/uploads/2023/08/2023_Código-das-Melhores-Práticas-de-Governança-Corporativa_6a-Edição.pdf. Acesso em: 14 set. 2025.

INSTITUTO PRENSA Y SOCIEDAD. **Algoritmos del silencio:** Reporte anual de Derechos Digitales 2023. Disponível em: https://ipysvenezuela.org/2024/05/16/algoritmos-del-silencio-reporte-anual-de-derechos-digitales-2023/. Acesso em: 17 maio 2025.

INT3R4. **Entidades cobram limites ao uso de dados do cidadão em benefícios sociais.** Int3r4, 10 jun. 2025. Disponível em: https://www.int3r4.com.br/2025/06/10/entidades-cobram-limites-ao-uso-de-dados-do-cidadao-em-beneficios-sociais/. Acesso em: 14 jul. 2025.

IPYS VENEZUELA. **Algoritmos del silencio**: reporte anual de derechos digitales 2023. Caracas: Instituto Prensa y Sociedad Venezuela, 2024. Disponível em: https://ipysvenezuela.org/wp-content/uploads/2024/05/IPYS_ReporteDerechosDigitales-2023.pdf. Acesso em: 17 maio 2025.

JENSEN, Steven L. B. **Putting to rest the Three Generations Theory of Human Rights.** Universal Rights Group**,** 21 fev. 2018. Disponível em: https://www.universal-rights.org/putting-rest-three-generations-theory-human-rights/. Acesso em: 4 jun. 2025.

JENSEN, Steven L. B.; SIMON, Hendrik. **Against the Historiographical Hierarchization of Human Rights**: Towards New Political Histories of International Human Rights Law. An Interview with Steven L. B. Jensen, Part 1. Völkerrechtsblog, 12 fev. 2024. Disponível em: https://voelkerrechtsblog.org/against-the-historiographical-hierarchization-of-human-rights/. Acesso em: 4 jun. 2025.

JUSTEN FILHO, Marçal. **Curso de direito administrativo**. São Paulo: Saraiva, 2005.

KRIEGER, Ana Luiza. Decisão histórica: STF reconhece direito autônomo à proteção de dados. **Migalhas**, São Paulo, 26 out. 2021. Disponível em: https://www.migalhas.com.br/depeso/353697/decisao-historica-stf-reconhece-direito-autonomo-a-protecao-de-dados. Acesso em: 8 jul. 2025.

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET. **Nota Técnica "10 Recomendações para a Interoperabilidade de Dados na Administração Pública".** 2021. Disponível em: https://lapin.org.br/2021/05/18/nota-tecnica-interoperabilidade-de-dados-na-administracao-publica/. Acesso em: 17 jul. 2025.

LAMARÃO NETO, Homero; QUEIROZ, Marina Moraes Diniz de Oliveira. Teoria dos limites dos limites e as restrições de liberdades individuais na pandemia de COVID-19 no Brasil. **Cadernos Ibero-Americanos de Direito Sanitário**, [*s. l.*], v. 12, n. 2, p. 25–35, 2023. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/977. Acesso em: 17 jul. 2025.

LUQUE, Luis Aguiar de. Los limites de los derechos fundamentales. **Revista del Centro de estudios Constitucionales**, [*s. l.*], n. 14, enero-abr. 1993.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD**: Lei geral de proteção de dados pessoais: comentada. 3. ed. São Paulo: Revista dos Tribunais, 2021.

MARMELSTEIN, George. **Curso de direitos fundamentais.** 8. ed. São Paulo: Atlas, 2019.

MARR, Bernard. Here's why data is not the new oil. **Forbes**, [*s. l.*], 5 mar. 2018. Disponível em: https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/. Acesso em: 15 jun. 2025.

MAZZA, Alexandre **Manual de direito administrativo.** 8. ed. São Paulo : Saraiva Educação, 2018.

MAZZUOLI, Valério de Oliveira. **Curso de direitos humanos.** 4. ed. Rio de Janeiro: Forense, 2017.

MEIRELLES, Hely Lopes. **Direito Administrativo brasileiro**. 13 ed. São Paulo: Revista dos Tribunais, 1988.

MELLO, Ana Paula Pessoa; MESQUITA, Hudson; VIEIRA, Carlos Eduardo. **Introdução à Interoperabilidade (ePING).** Brasília: Escola Nacional de Administração Pública (ENAP), 2015. Disponível em: https://repositorio.enap.gov.br/handle/1/2398. Acesso em: 23 maio 2025.

MELLO, Victor Habib Lantyer de. Colonialismo de dados: a geopolítica da informação. **Migalhas**, São Paulo, 5 maio 2025. Disponível em: https://www.migalhas.com.br/depeso/429396/colonialismo-de-dados-a-geopolitica-da-informacao. Acesso em: 16 jul. 2025.

MELO, Teresa. Modulação temporal de efeitos: técnica pragmatista de decisão e parâmetros para sua aplicação. **Revista de Direito Brasileira**, Florianopolis, v. 29, n. 11, p. 184–198, 2021. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/6067. Acesso em: 27 maio. 2025.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 19. ed. São Paulo: Saraiva, 2024.

MENDES, Laura S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. Rio de Janeiro: Saraiva, 2014. (Série IDP - Linha de pesquisa acadêmica). Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788502218987/. Acesso em: 11 mai. 2025. *E-book.*

MENDES, Laura Schertel *et al.* **(org.). Direitos fundamentais na era digital**: Anuário 2023 das Comissões Especiais de Proteção de Dados (CEPD) e de Direito Digital (CEDD). Porto Alegre: Fundação Fênix, 2023. (Série Direito, 87).

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, v. 25, n. 4, 2020 Disponível em: https://ojs.unifor.br/rpen/article/view/10828. Acesso em: 04 ago. 2024.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. **Direitos Fundamentais & Justiça**, Belo Horizonte, v. 12, n. 39, p. 185-216, jul./dez. 2018.

MENDES, Laura Schertel Ferreira; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento. Tendências contemporâneas de materialização. **Revista Estudos Institucionais**, Rio de Janeiro, v. 6, n. 2, p. 507-533, maio/ago. 2020b.

MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. **JOTA**, [*s. l.*], 10 maio 2020c. Disponível em: https://www.jota.info/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais. Acesso em: 12 jun. 2025.

MENDES, Laura Schertel. Democracia, poder informacional e vigilância: limites constitucionais ao compartilhamento de dados pessoais na Administração Pública. **O Globo**, [*s. l.*], 13 ago. 2022. Disponível em: https://oglobo.globo.com/blogs/fumus-boni-iuris/post/2022/08/laura-schertel-democracia-poder-informacional-e-vigilancia.ghtml. Acesso em: 15 maio 2025.

MENDES, Laura Schertel; GASIOLA, Gustavo Gil. Compartilhamento de dados no setor público. **Consultor Jurídico**, São Paulo, 14 set. 2022. Disponível em: https://www.conjur.com.br/2022-set-14/schertel-gasiola-compartilhamento-dados-setor-publico/. Acesso em: 25 maio 2025.

MENDES, Laura Schertel; RODRIGUES JUNIOR, Otávio Luiz; FONSECA, Gabriel Campos Soares da. O Supremo Tribunal Federal, a proteção constitucional dos dados pessoais e a positivação superveniente de um direito fundamental autônomo. *In*: DONEDA, Danilo *et al.* (org.). **Tratado de Proteção de dados pessoais**. 2. ed. Rio de Janeiro: Forense, 2023. p. 174–195.

MOTTA, Fabrício. Notas sobre publicidade e transparência na Lei de Responsabilidade Fiscal no Brasil. **Revista de Direito Administrativo & Constitucional**, Belo Horizonte, v. 3, n. 11, jan./mar. 2003.

NABUCO, Joaquim. Um estadista do Império. v. 2. Rio de Janeiro: Topbooks, 1997.

NAKAMURA, André Luiz dos Santos. Restrições aos direitos fundamentais. **Revista Direitos Humanos Fundamentais**, Osasco, v. 16, n.2, p. 153-166, jul./dez. 2016.

NASCIMENTO, Francisco Paulo do. **Metodologia da Pesquisa Científica**: teoria e prática – como elaborar TCC. Brasília: Thesaurus, 2016.

NISSENBAUM, Helen. **Privacy in context: technology, policy, and the integrity of social life.** Stanford: Stanford University Press, 2009. Disponível em: https://www.amazon.com/dp/B005M43916. Acesso em: 21 jun. 2025.

NOBRE JUNIOR, Edílson Pereira. A autoridade nacional de proteção de dados e o dever estatal de sua tutela: anotações em torno da independência do órgão regulador. *In*: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (coord.). **LGPD & Administração Pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020. p. 559–584.

NUNES, D. H.; MONTES NETTO, C. E.; SILVEIRA, S. S. A aplicação da teoria dos limites dos limites aos direitos fundamentais pelo Supremo Tribunal Federal. **Revista Direitos Culturais**, [*s. l.*], v. 16, n. 39, p. 275-297, 9 set. 2021.

OLIVEIRA, Joana D'Arc de; MARINHO, Sidnei Vieira. A trajetória do governo eletrônico ao digital: um ensaio teórico sobre a transformação digital no setor público brasileiro. *In*: SEMINÁRIOS EM ADMINISTRAÇÃO, 26., 2023, São Paulo. **Anais** [...]. São Paulo: Universidade de São Paulo, 2023. Disponível em: https://login.semead.com.br/26semead/anais/arquivos/1855.pdf. Acesso em: 8 jul. 2025.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **The Path to Becoming a Data-Driven Public Sector**. Paris: OECD Publishing, 2019. Disponível em: https://doi.org/10.1787/059814a7-en. Acesso em:11 maio 2025.

ORWELL, George. **1984**. Jandira: Principis, 2021.

OTERO, Paulo. **Manual de Direito Administrativo**. Coimbra: Almedina, 2013.

PASSOS, Matheus. **Uma introdução ao Privacy by Design**. DPO na Prática, 22 fev. 2023. Disponível em: https://dponapratica.com.br/2023/02/introducao-privacy-by-design/. Acesso em: 18 jul. 2025.

PEDRAZZOLI, Marcela Gaspar. Compartilhamento de dados pessoais no âmbito da administração pública: uma análise da ADI 6.649 e de suas repercussões normativas. **Revista da Procuradoria-Geral do Estado de Mato Grosso do Sul**, Campo Grande, n. 19, 2023. Disponível em: https://www.pge.ms.gov.br/wp-content/uploads/2023/12/Revista-PGE-19-marcela.pdf. Acesso em: 12 jul. 2025.

PEREIRA, Jane Reis Gonçalves. **Interpretação Constitucional e Direitos Fundamentais:** uma contribuição ao estudo das restrições aos direitos fundamentais na perspectiva da teoria dos princípios. Rio de Janeiro: Renovar, 2006.

PERNAMBUCO. Tribunal Regional Federal (5. Região). **Cartilha de Segurança e Proteção de Dados Pessoais.** Recife: TRF5, 2023. Disponível em: https://issuu.com/trf5/docs/cartilha_protecao_de_dados. Acesso em: 25 ago. 2025.

PIEROTH, Bodo; SCHILINK, Bernhard**. Direitos Fundamentais**. Trad. SOUSA, António Francisco de. FRANCO, Antonio. São Paulo: Saraiva, 2012.

PORTUGAL. Agência para a Modernização Administrativa. **Princípio 5:** Peça novas informações uma única vez. Mosaico. Disponível em: https://mosaico.gov.pt/principios/5. Acesso em: 18 jul. 2025.

PROTEÇÃO de dados pessoais passa a ser direito fundamental. Rádio e TV justiça. [*S. l.*:*s. n.*], 4 de mar. de 2022. 1 vídeo (8 min). Disponível em: https://www.youtube.com/watch?v=CjTGdiWHc4E. Acesso em: 12 jun. 2025.

PULLIDO, Carlos Bernal. **El principio de proporcionalidad y los derechos fundamentales:** el principio de proporcionalidad como criterio para determinar el contenido de los derechos fundamentales vinculantes ao legislador. Madrid: Centro de Estudios Politicos y Constitucionales, 2003.

QUARANTINI LEITE, C.; BARREIROS DE CARVALHO FONSECA, A. Compartilhamento de dados pessoais sensíveis entre os órgãos da administração pública: uma análise do decreto nº 10.046/2019 à luz da relatoria da ADPF 695 E ADI 6649/DF. **Revista Conversas Civilísticas**, Salvador, v. 4, n. 1, p. 39–67, 2024. Disponível em: https://periodicos.ufba.br/index.php/conversascivilisticas/article/view/60763. Acesso em: 27 maio. 2025.

RIBEIRO, M. S. **Do Tecnosolucionismo ao Tecnovigilantismo**: um estudo sociológico sobre os usos de emergentes tecnologias pelas forças de segurança do Ceará. 2024. Tese (Doutorado em Sociologia) – Universidade Federal do Ceará, Fortaleza, 2024.

ROBL FILHO, Ilton Norberto. Alguns apontamentos sobre o constitucionalismo digital. **Consultor Jurídico**, São Paulo, 22 jan. 2022. Disponível em: https://www.conjur.com.br/2022-jan-22/observatorio-constitucional-alguns-apontamentos-constitucionalismo-digital. Acesso em: 27 ago. 2025.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SANTIAGO, Denny Mendes. **As limitações aos direitos fundamentais**: os limites dos limites como instrumento de proteção ao núcleo essencial destes direitos. 2012. Dissertação (Mestrado em Direito) - Universidade Federal de Minas Gerais, Belo Horizonte, 2012.

SANTIAGO, Denny Mendes. O Atomismo de Leucipo e Demócrito: sua possibilidade de atuação como ferramenta interpretativa acerca do núcleo essencial dos direitos fundamentais. **Revista de Direitos e Garantias Fundamentais**, Vitória, n. 9, p. 143-164, jan./jun. 2011.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais**. 4. ed. Porto Alegre: Livraria do Advogado, 2004.

SARLET, Ingo Wolfgang. Conceito de direitos e garantias fundamentais. *In*: **CAMPILONGO, Celso Fernandes; GONZAGA, Alvaro de Azevedo; FREIRE, André Luiz** (coord.). **Enciclopédia jurídica da PUC-SP.** São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/67/edicao-1/conceito-de-direitos-e-garantias-fundamentais. Acesso em: 15 jul. 2025.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: DONEDA, Danilo *et al.* (org.). **Tratado de Dados Pessoais**. 2. ed. Rio de Janeiro: Forense, 2023.

SARLET, Ingo Wolfgang; SAAVEDRA, Bruno. **Direitos fundamentais e proteção de dados pessoais**: fundamentos filosóficos e jurídicos. Porto Alegre: Livraria do Advogado, 2020.

SARLET, Ingo Wolfgang; SALES SARLET, Gabriele. **Separação informacional de poderes no direito constitucional brasileiro.** São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022.

SARLET, Ingo Wolfgang; SARLET, Gabrielle Bezerra Sales. Notas sobre os limites do compartilhamento de dados pessoais e a separação informacional de poderes no Brasil. *In*: **MENDES, Laura Schertel** *et al.* **(org.). Direitos fundamentais na era digital**: Anuário 2023 das Comissões Especiais de Proteção de Dados (CEPD) e de Direito Digital (CEDD). Porto Alegre: Fundação Fênix, 2023.

SARMENTO, Daniel; SOUZA NETO, Cláudio Pereira de. **Teoria dos direitos fundamentais.** 2. ed. São Paulo: Malheiros, 2014.

SCHWAB, Klaus. **A Quarta Revolução Industrial.** Tradução Daniel Moreira Miranda. São Paulo: Edipro, 2019.

SECRETARIA-GERAL IBERO-AMERICANA. Declaração de Santa Cruz de la Sierra. XIII Cúpula Ibero-Americana de Chefes de Estado e de Governo, Santa Cruz de la Sierra, Bolívia, 14-15 nov. 2003. Madrid: Secretaria-Geral Ibero-Americana, 2003. Disponível em: https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf. Acesso em: 6 jul. 2025.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. Serpro defende governança e segurança de dados públicos em evento nacional sobre privacidade. Brasília: Serviço Federal de Processamento de Dados, 28 ago. 2025. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2025/seminario-ccgibr-nicbr. Acesso em: 28 ago. 2025.

SICCA, Gerson dos Santos. A interpretação conforme à Constituição – Verfassungskonforme Auslegung – no direito brasileiro. **Revista de Informação Legislativa**, Brasília, DF, v. 36, n. 143, jul./set. 1999.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** 26. ed. São Paulo: Malheiros, 2006.

SILVA, Virgílio Afonso da. **Direitos fundamentais**: conteúdo essencial, restrições e eficácia. São Paulo: Malheiros, 2007.

SILVEIRA, Henrique Flávio Rodrigues da. Um estudo do poder na sociedade da informação. **Ciência da Informação**, [*s. l.*], v. 29, n. 3. 2000. Disponível em: https://revista.ibict.br/ciinf/article/view/875. Acesso em: 14 out. 2025.

SOLOVE, Daniel J. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. **San Diego Law Review**, v. 44, p. 745, 2007. Disponível em: https://ssrn.com/abstract=998565. Acesso em: 14 out. 2025.

SOUZA, Carlos Affonso de. Da privacidade à proteção de dados: o legado de Danilo Doneda. **UOL**, São Paulo, 5 dez. 2022. Coluna Tilt. Disponível em: https://www.uol.com.br/tilt/colunas/carlos-affonso-de-souza/2022/12/05/da-privacidade-a-protecao-de-dados-o-legado-de-danilo-doneda.htm. Acesso em: 8 jul. 2025.

SOUZA, Marcos Sampaio de. **O conteúdo essencial dos direitos sociais no constitucionalismo brasileiro.** Dissertação (Mestrado em Direito) - Universidade Federal da Bahia, Salvador, 2011.

SUPREMO TRIBUNAL FEDERAL (Brasil). **Liberdade de expressão, democracia e novas tecnologias.** Brasília: STF, 2024. (Cadernos de Jurisprudência do STF: Concretizando Direitos Humanos, v. 6). Disponível em: https://www.stf.jus.br/arquivo/cms/publicacaoCatalogoProdutoProduto/anexo/Cadernos_STF_LiberdadeExpressaoeNovasTecnologias.pdf. Acesso em: 4 jun. 2025.

TALLINN Declaration on eGovernment. Tallin: EU2017.EE, 2017. Disponível em: https://www.newsd.admin.ch/newsd/message/attachments/49838.pdf. Acesso em: 14 maio 2025.

TAVARES, André Ramos. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2010.

TEPEDINO, G. Editorial. **Revista Brasileira de Direito Civil**, [*s. l.*], v. 24, n. 2, 2020. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/587. Acesso em: 18 maio. 2025.

TOFFLER, Alvin. **Powershift**: conhecimento, riqueza e violência nas vésperas do século XXI. Rio de Janeiro: Record, 1991.

TREDESTINAÇÃO (ou Uso Secundário) no Tratamento de Dados Pessoais pelo Poder Público. HISTÓRIA E DADOS, por Rodrigo Valadão. [*S. l.: s. n.*], 16 dez. 2021. 1 vídeo (34 min). Disponível em: https://www.youtube.com/watch?v=4aiP5Zmffro. Acesso em: 14 jun. 2025.

UNIÃO EUROPEIA. Ministerial Declaration on eGovernment: the Tallinn Declaration. Tallinn, 6 out. 2017. Disponível em: https://interoperable-europe.ec.europa.eu/sites/default/files/document/2018-04/eGovernmentMinisterialDeclarationsignedinTallinnon6October2017.pdf. Acesso em: 3 jun. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados – GDPR). Disponível em: https://gdpr-info.eu/. Acesso em: 18 jul. 2025.

UNICEF. **Declaração Universal dos Direitos Humanos.** Brasília: UNICEF Brasil. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 14 jun. 2025.

UNITED STATES. **Defense Advanced Research Projects Agency (DARPA).** Innovation timeline. Arlington, VA: DARPA, [2025]. Disponível em: https://www.darpa.mil/about/innovation-timeline. Acesso em: 6 jul. 2025.

VALE, Luís Manoel Borges do; OLIVEIRA, Rafael Carvalho Rezende. **LGPD na Administração Pública.** Rio de Janeiro: Forense, 2025.

VAZ, Wesley; ÂNGELIS, Virgínia de. **O falso paradoxo entre proteção de dados e eficiência no setor público.** LGPD Brasil, 10 nov. 2021. Disponível em: https://lgpdbrasil.com.br/o-falso-paradoxo-entre-protecao-de-dados-e-eficiencia-no-setor-publico/. Acesso em: 2 set. 2025.

VERGILI, Gabriela; ZANATTA, Rafael. **Os problemas do Cadastro Base do Cidadão e a ADI 6.649.** São Paulo: Data Privacy Brasil, 2022. Disponível em: https://www.dataprivacybr.org/documentos/os-problemas-do-cadastro-base-do-cidadao-e-a-adi-6-649/. Acesso em: 14 jul. 2025.

WAVE. Intérprete: João Gilberto. Compositor: Antônio Carlos Jobim. *In:* AMOROSO. Intérprete: João Gilberto. Rhino/Warner RecordsWave, 1976. Faixa 5.

WEBINAR - Qualificação de Endereços - Regulamentação do Decreto nº 12.428/2025. Ministério da gestão e inovação. [*S. l.: s. n.*], 3 abr. 2025. 1 vídeo (48 min). Disponível em: https://www.youtube.com/watch?v=Z3kjUXJtMiM. Acesso em: 14 jul. 2025.

WESTIN, Alan F. **Privacy and Freedom**. New York: Atheneum, 1967.

WIMMER, Miriam. Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia. **Revista Brasileira de Políticas Públicas**, Brasília, v. 11, n.1, p. 122/142, 2021. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/7136 .

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. *In*: DONEDA, Danilo *et al.* (org.). **Tratado de Proteção de Dados Pessoais.** 2. ed. Rio de Janeiro: Forense, 2023.

WORLD BANK. **Governance and development**. Washington, DC, 1992.

ZOUEIN, Luís Henrique Linhares. **Manual de Direitos Fundamentais à luz do Direito Internacional dos Direitos Humanos.** Belo Horizonte: CEI, 2023.