Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP
Curso de Direito

O vácuo regulatório na proteção de dados pessoais no setor público brasileiro: a desejável unificação de diretrizes específicas

Ana Vitória Gomes Nogueira

Brasília-DF
2025

ANA VITÓRIA GOMES NOGUEIRA

O vácuo regulatório na proteção de dados pessoais no setor público brasileiro: a desejável unificação de diretrizes gerais

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Direito pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP.

Sob orientação da Prof(a). Luísa Lacerda.

Brasília-DF

2025

Banca Examinadora

Prof(a). Luísa Lacerda
Orientadora

Prof(a). Janete Ricken Lopes de Barros
Examinadora

Prof(a). Teresa Cristina de Melo Costa
Examinadora

Ao meu avô, Joaquim de Oliveira, *in memorian.*
Homem simples, alegre e de coração bom.
Rico de história, generoso em silêncio,
mestre em viver com pouco.
Fez da inteligência um legado e da simplicidade um valor.
Minha maior referência — o mais próximo de Jesus que já conheci.

O vácuo regulatório na proteção de dados pessoais no setor público brasileiro: a desejável unificação de diretrizes gerais

Ana Vitória Gomes Nogueira

SUMÁRIO: 1. INTRODUÇÃO 2. UMA ANÁLISE PRINCIPIOLÓGICA DA PROTEÇÃO DE DADOS NO SETOR PÚBLICO 2.1 FINALIDADE, ADEQUAÇÃO E NECESSIDADE 2.2 LIVRE ACESSO/QUALIDADE DOS DADOS/TRANSPARÊNCIA; 2.3 DIREITOS DOS TITULARES: SEGURANÇA, PREVENÇÃO, RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS (ACCOUNTABILITY) 2.4 NÃO DISCRIMINAÇÃO 3. ANÁLISE DA APLICAÇÃO DAS BASES LEGAIS DA LGPD NO SETOR PÚBLICO 3.1 BASES LEGAIS: CONSENSO, OBRIGAÇÃO LEGAL E LEGÍTIMO INTERESSE 3.2 SUPREMACIA DO INTERESSE PÚBLICO E HARMONIZAÇÃO COM DIREITOS FUNDAMENTAIS 4. CONFLITO ENTRE TRANSPARÊNCIA/PUBLICIDADE E PROTEÇÃO DE DADOS NO SETOR PÚBLICO 5. COMPARTILHAMENTO DE DADOS PELO PODER PÚBLICO E PARÂMETROS CONSTITUCIONAIS: ANÁLISE DA ADI 6649, MP 954/2020 E ADPF 695 6. CONCLUSÃO

- **Resumo:**

A Lei Geral de Proteção de Dados Pessoais (LGPD) trouxe um marco regulatório fundamental para a proteção de dados no Brasil, incluindo normas específicas para o setor público. No entanto, a ausência de regulamentação detalhada gera insegurança jurídica, dificultando a implementação eficaz da legislação. Este trabalho investiga os impactos dessa lacuna normativa, analisando a necessidade de diretrizes mais claras para equilibrar transparência e privacidade na administração pública. Para isso, são consideradas abordagens

adotadas em diferentes países, bem como a relevância da jurisprudência do STF no julgamento da ADI n º 6649. Os resultados apontam para a necessidade de uma regulamentação mais precisa, garantindo segurança jurídica e efetividade na proteção dos dados pessoais.

Palavras-chave: LGPD; proteção de dados; setor público; segurança jurídica; transparência.

Abstract:

The General Data Protection Law (LGPD) established a regulatory framework for data protection in Brazil, including specific rules for the public sector. However, the lack of detailed regulation creates legal uncertainty, hindering the effective implementation of the legislation. This study examines the impacts of this regulatory gap, analyzing the need for clearer guidelines to balance transparency and privacy in public administration. To this end, approaches adopted in different countries are considered, as well as the relevance of the Brazilian Supreme Court's ruling in ADI No. 6649. The findings highlight the need for more precise regulations to ensure legal certainty and effectiveness in data protection.

Keywords: LGPD; data protection; public sector; legal certainty; transparency.

1 INTRODUÇÃO

A proteção de dados pessoais foi consagrada na Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), em vigor desde 18 de setembro de 2020. A norma representou um avanço regulatório ao alinhar o país a padrões internacionais incorporando a autodeterminação informativa como princípio orientador do tratamento de dados pessoais, ainda que a privacidade já fosse reconhecida como direito fundamental desde o artigo 5º, X, da Constituição Federal de 1988.

A Lei Geral de Proteção de Dados Pessoais foi impulsionada pela crescente digitalização e pelo uso massivo de dados pessoais por empresas e órgãos públicos. A necessidade de um marco regulatório se intensificou com escândalos como o da Cambridge Analytica, que utilizou dados de usuários do Facebook sem consentimento para influenciar a campanha de Donald Trump em 2016. Esse episódio expôs globalmente os riscos da coleta e do tratamento indiscriminado de dados.

No Brasil, a proteção de dados tem raízes constitucionais, no direito à intimidade e à vida privada, e em leis específicas, como a Lei nº 9.296/1996, interceptações telefônicas, e a Lei nº 12.527/2011, Lei de Acesso à Informação (LAI).[1] Esta última reforçou a transparência, mas também gerou tensões com a proteção de dados no setor público. O Marco Civil da Internet, Lei nº 12.965/2014, contribuiu com princípios voltados à privacidade e proteção de dados.

Além das demandas internas, fatores externos impulsionaram a criação da LGPD. O Regulamento Geral de Proteção de Dados (RGPD) da União Europeia (Comissão Europeia, 2018), com sua eficácia extraterritorial e rigor na transferência internacional de dados, pressionou países a adotarem normas similares. Para se alinhar a esse contexto, o Brasil sancionou a LGPD em 2018, após audiências públicas (Coutinho, 2017) que garantiram participação social. Inspirada no RGPD, a LGPD estabeleceu regras claras para o tratamento de dados pessoais e criou a Autoridade Nacional de Proteção de Dados (ANPD) com competência para fiscalizar sua aplicação.[2]

---

[1] "... em um plano mais abstrato, o conflito em questão é apenas aparente, pois, se bem compreendidas, a LGPD e a LAI expressam princípios, normas e propósitos similares, que se complementam e se reforçam mutuamente, seja no que concerne à promoção do princípio da transparência, seja quanto à proteção de informações pessoais." (Carvalho, 2020).

[2] Destaca-se que não foi objeto deste estudo analisar as relações políticas e de poder nesses mecanismos que visam aumentar a participação popular durante a implementação de uma lei, por exemplo. Mas vale ressaltar a importância de estudos no sentido de averiguar se o Direito é apenas mais um veículo consagrador do "estado da relação de forças entre os grupos" ou se, de fato, atua como vocalizador de demandas, inclusive das partes menos favorecidas ou subrepresentadas, como as minorias. Como ressalta, por exemplo, o sociólogo Bourdieu: "o direito

Apesar de representar um avanço, a LGPD ainda enfrenta obstáculos no setor público. A ausência de diretrizes uniformes permite interpretações divergentes e dificulta a definição de responsabilidades institucionais. Embora a transformação da ANPD em autarquia tenha conferido mais autonomia, a falta de regulamentação específica segue como um entrave à efetividade da lei.

A ausência de regulamentação específica para o setor público é um desafio, especialmente após o julgamento da Ação Direta de Inconstitucionalidade (ADI) nº 6649, que questiona o Decreto nº 10.046/2019, relativo à governança no compartilhamento de dados no âmbito da administração pública federal. A decisão evidenciou lacunas e incertezas que comprometem a efetividade e a segurança jurídica na aplicação da proteção de dados pelo poder público.

O avanço de novas tecnologias e dispositivos móveis de comunicação levou a uma rápida escalada na coleta, análise e compartilhamento de dados pessoais entre atores públicos e privados. Esses acontecimentos reacenderam o debate sobre os limites do tratamento de dados pelo setor público, especialmente sobre os critérios para o seu compartilhamento e uso secundário, ou seja, a utilização de dados pessoais para finalidades diferentes das que justificaram sua coleta inicial (Wimmer, 2021). Diante disso, torna-se urgente refletir sobre os impactos da indefinição normativa e a necessidade de diretrizes claras que assegurem a efetiva aplicação da LGPD no setor público.

Esse cenário é agravado pela fragmentação do ordenamento jurídico. O excesso de normas, por vezes contraditórias, dificulta a harmonização entre transparência e proteção de dados pessoais. A ausência de um guia unificado amplia a margem de subjetividade e pode resultar em práticas administrativas desiguais.

A questão central desta pesquisa é a ampla permissão concedida ao setor público para o tratamento de dados pessoais, sem regulamentação suficientemente clara. Ainda que essa flexibilidade se fundamente no princípio da supremacia do interesse público, ela pode gerar

---

limita-se a consagrar simbolicamente, por um registro que eterniza e universaliza, o estado da relação de forças entre os grupos e as classes que produz e garante praticamente o funcionamento de tais mecanismos" (Bourdieu, 2004). Questões relacionadas à assimetria da informação, à capacidade discursiva e ao poder de argumentação são alguns dos aspectos a serem considerados, especialmente quando os mecanismos utilizados são virtuais. Sob esse aspecto, destaca-se, também, pesquisa realizada em 2015 sobre o processo de participação popular no canal e-Democracia, da Câmara dos Deputados, para discussão do então projeto de lei que tratava do Marco Civil da Internet (tema que recebeu o maior número de contribuições em relação aos demais temas já disponibilizados no canal). De acordo com pesquisa realizada, "o perfil dos usuários está muito aquém de representar os vários grupos políticos e estratos sociais existentes no Brasil, especialmente entre os usuários de iniciativas de participação política digital criadas e coordenadas por órgãos governamentais" (Freitas, 2016).

insegurança jurídica e relativizar o direito fundamental à proteção de dados, previsto no artigo 5º, inciso LXXIX, da Constituição Federal.

A hipótese deste estudo é que a ausência de unificação normativa e diretrizes específicas para o tratamento de dados pelo setor público dificulta a aplicação da LGPD, criando um ambiente jurídico e operacional confuso e inseguro. Este trabalho defende a necessidade de maior clareza e uniformidade nas normas que regulam o tratamento de dados pessoais pelo poder público, com o objetivo de garantir a proteção adequada e o cumprimento dos direitos dos titulares de dados. A relevância da pesquisa reside no impacto direto que a ausência de regulamentação provoca na vida dos titulares de dados, vulnerabilizando os direitos fundamentais.

A metodologia será a revisão bibliográfica de natureza qualitativa e descritiva, baseada em obras doutrinárias, artigos científicos, legislação e jurisprudência.

2 UMA ANÁLISE PRINCIPIOLÓGICA DA PROTEÇÃO DE DADOS NO SETOR PÚBLICO

A LGPD surgiu em resposta ao crescimento exponencial do processamento de dados e à necessidade de garantir um tratamento ético e responsável. Com a digitalização e o uso cada vez mais amplo de informações pessoais em diversos setores, a LGPD passou a ser um instrumento essencial para proteger a privacidade[3] e os direitos fundamentais dos titulares de dados pessoais. Para isso, a legislação estabelece princípios que orientam sua aplicação de forma segura e transparente, garantindo o respeito à dignidade dos indivíduos.

A adoção do modelo europeu como parâmetro para a legislação brasileira, no entanto, apresenta algumas divergências. De acordo com Doneda (2006), a doutrina da privacidade passou por um processo evolutivo, inicialmente centrado no individualismo e no direito de ser deixado só, como defendido por Warren e Brandeis. No entanto, com o avanço da tecnologia e o aumento dos fluxos de dados, a privacidade passou a ser entendida não apenas como um direito individual, mas também como um direito que está intimamente ligado ao funcionamento da sociedade democrática. A evolução tecnológica permitiu a coleta de dados em escala antes impensável, fenômeno que Doneda denomina “vontade da técnica”, em que a capacidade

[3] Canotilho, j. J.; Machado, Jónatas E. M. (2003) identificam duas facetas do direito à intimidade: a prerrogativa de barrar o acesso de terceiros a informações sobre a esfera privada e familiar e a proteção contra a divulgação indevida desses dados. Por sua vez, a doutrina alemã adota a "teoria das três esferas", que distingue a "vida íntima", caracterizada por aspectos totalmente reservados ao indivíduo; a "vida privada", compartilhada apenas com um círculo restrito de pessoas; e a "vida pública", que diz respeito à interação do indivíduo com a coletividade.

técnica de tratar dados passou a ditar a intensidade da vigilância informacional (Gonçalves, 2019).

No entendimento de Doneda (2019), a proteção da privacidade não se restringe mais à garantia de "isolamento e segredo", mas foi expandida para uma perspectiva de controle da circulação e do uso que outras pessoas fazem das informações pessoais do titular. Essa perspectiva reforça a compreensão da proteção de dados como direito fundamental vinculado à dignidade humana, nos termos do artigo 1º, inciso III, da Constituição Federal.

Os princípios fundamentais da LGPD – finalidade, adequação, necessidade, transparência, livre acesso, qualidade dos dados, segurança, prevenção, não-discriminação e responsabilização – servem como diretrizes para o tratamento de dados em diferentes esferas. O objetivo da LGPD é prevenir abusos, garantir boas práticas e proteger os direitos dos titulares de dados pessoais.

No setor público, a aplicação da LGPD apresenta desafios próprios, que vão além da simples conformidade legal. De acordo com o artigo 23 da LGPD, o tratamento de dados realizado pelo poder público deve atender a finalidades específicas relacionadas ao interesse público e à execução de políticas governamentais. Assim, os órgãos públicos devem seguir não apenas os princípios gerais da proteção de dados, previstos no artigo 6º,[4] mas também garantir que o uso das informações seja conduzido de forma ética e transparente, sem comprometer os direitos dos titulares de dados pessoais.

A análise desses princípios evidencia que a proteção de dados pessoais na administração pública não se limita ao cumprimento da legislação, sendo um pilar para uma gestão ética, transparente e voltada ao indivíduo. Mais do que orientações normativas, os princípios da LGPD promovem uma cultura de respeito à privacidade, fortalecendo a confiança nas instituições públicas.

Ao equilibrar a execução de políticas públicas com a proteção da privacidade, o setor público reforça o compromisso com a democracia e os direitos fundamentais. A adoção de práticas de tratamento de dados responsáveis e transparentes não apenas garante segurança jurídica, mas também contribui para uma administração pública mais eficiente, confiável e alinhada ao interesse social.

[4] A teoria da ponderação de Robert Alexy apresenta conexão intrínseca com os direitos fundamentais, ao estabelecer critério para resolver colisões entre direitos no caso concreto. Como os princípios jurídicos são mandamentos de otimização, um direito prevalece sobre outro quando tem peso maior na situação. Apesar de sua ampla adoção no direito constitucional, há críticas quanto à falta de precisão metodológica e ao risco de decisões subjetivas.

Para a aplicação da LGPD no setor público, os princípios de proteção de dados podem ser organizados de acordo com 4 funções principais (Wimmer, 2021).

(1) Finalidade/adequação/necessidade;

(2) Livre acesso/qualidade dos dados/transparência;

(3) Segurança/ prevenção/responsabilização/prestação de contas;

(4) Não-discriminação.

A seguir, são explorados cada um desses grupos com foco nas peculiaridades do setor público, suas implicações e os desafios envolvidos.

2.1 FINALIDADE, ADEQUAÇÃO E NECESSIDADE

Os princípios da finalidade, adequação e necessidade orientam diretamente a forma como os dados devem ser tratados no setor público, assegurando que a coleta e o uso de dados pessoais sejam proporcionais e justificados. No contexto da administração pública, esses princípios impõem limitações rigorosas sobre o uso de dados, que devem ser vinculados a finalidades públicas claras e legítimas.[5]

O princípio da finalidade, conforme o artigo 6º, inciso I, da LGPD, estabelece que o tratamento de dados pessoais deve ocorrer para propósitos específicos, legítimos e informados ao titular. No setor público, esse princípio assume uma importância ainda maior, pois o tratamento de dados deve estar diretamente relacionado à prestação de serviços e ao cumprimento das obrigações legais.

Um município pode coletar dados pessoais, como nome, endereço e telefone, para cadastrar cidadãos em um programa de assistência social, como o Bolsa Família. Esses dados devem ser usados exclusivamente para gerenciar os benefícios do programa. Se o município utilizar esses dados para campanhas publicitárias ou outros fins não relacionados, isso violaria o princípio da finalidade, pois o titular não foi informado sobre tais usos. Nesse caso, seria necessário obter novo consentimento ou uma base legal específica.[6]

[5] É fundamental examinar as implicações organizacionais da aplicação dos princípios da finalidade, adequação e necessidade no setor público. Esses princípios determinam que o tratamento de dados pessoais deve estar alinhado às atribuições do órgão responsável e à justificativa específica para sua coleta, o que restringe a circulação dessas informações dentro da administração estatal. Assim, essa limitação contrapõe-se à noção de que o Estado funcionaria como uma "unidade informacional", na qual os dados poderiam ser livremente compartilhados entre diferentes órgãos governamentais. Nesse sentido, a concepção de divisão informacional de poderes tem sido utilizada para fundamentar o entendimento de que a coleta e o tratamento de dados pessoais por órgãos públicos devem estar estritamente limitados às suas competências legais (Simitis, 1987; Maranhão; Campos, 2019).

[6] Exemplo adaptado com base nas orientações da ANPD (2023).

Além disso, esse princípio é essencial para preservar a confiança dos indivíduos nas instituições. Ao garantir que os dados pessoais fornecidos para um objetivo específico não serão utilizados para outros fins sem o consentimento do titular, a finalidade reforça a transparência e a responsabilidade no uso de dados, prevenindo possíveis abusos e promovendo a boa-fé entre o poder público e os indivíduos.

A compatibilidade de finalidades, essencial ao uso secundário de dados, é reafirmada por autoridades de proteção de dados ao redor do mundo. Algumas recorrem, inclusive, ao conceito de "integridade contextual" (Nissenbaum, 2010). A autora destaca a importância de respeitar as expectativas razoáveis dos indivíduos sobre o tratamento e compartilhamento de seus dados. A partir de uma perspectiva brasileira, Bruno Bioni também adota o conceito de "privacidade contextual" para examinar o uso secundário de dados pessoais, defendendo que a elasticidade dessa abordagem, alinhada às expectativas legítimas dos indivíduos e às especificidades do vínculo entre o titular e o controlador, é crucial para regular os usos de dados que não podem ser previamente definidos ou rigidamente controlados (Bioni, 2019).

No setor público, há o dever de especificar, de forma clara e legítima, o motivo pelo qual cada conjunto de dados será tratado, sempre em consonância com o interesse público. Essa exigência decorre da necessidade de transparência e de respeito aos direitos dos titulares. Um dos principais desafios está no uso posterior dessas informações para outros propósitos que não estavam previstos no momento da coleta. A LGPD proíbe esse tipo de reencaminhamento sem base legal adequada, como restrições indevidas de direitos ou uso indevido em outras esferas administrativas. A secretaria municipal de saúde realiza a coleta de informações referentes a indivíduos diagnosticados com determinada doença infecciosa, com o objetivo de planejar, executar e acompanhar uma política pública de vacinação. Esses dados são posteriormente repassados a uma instituição de pesquisa, com a finalidade específica de subsidiar estudos voltados à saúde coletiva (ANPD, 2023). Neste exemplo, o tratamento posterior dos dados é legítimo, uma vez que está compatível com a finalidade original da coleta.

A adoção desse princípio condiciona o tratamento de dados a uma finalidade determinada, impedindo que sejam tratados como meras mercadorias (Mendes e Doneda, 2018). Doneda e Viola, veem o princípio da finalidade como um reflexo de um entendimento mais profundo, no qual a informação pessoal, sendo uma manifestação direta da identidade do indivíduo, está sempre conectada a ele. Para os autores, é exatamente esse princípio que restringe o uso secundário da informação pessoal sem o consentimento do titular, algo que,

caso fosse permitido, tornaria ineficazes outros mecanismos de proteção e controle sobre os dados pessoais de quem os possui (Doneda e Viola, 2010).

O princípio da adequação, previsto no artigo 6º, inciso II, da Lei Geral de Proteção de Dados Pessoais (LGPD), determina que o tratamento de dados pessoais deve ser compatível com o contexto da coleta e com as legítimas expectativas do titular. Enquanto o princípio da finalidade diz respeito ao motivo que justifica o tratamento, isto é, à razão pela qual os dados são coletados, a adequação refere-se à forma como esse tratamento é realizado, exigindo coerência entre a informação prestada ao titular e o uso efetivo dos dados.

No setor público, esse princípio assume particular relevância, considerando que os dados pessoais são frequentemente utilizados no desenvolvimento de políticas públicas e na implementação de programas sociais. A adequação impõe ao poder público o dever de assegurar que o uso das informações respeite não apenas os objetivos institucionais, mas também o cenário informado ao titular no momento da coleta.

Por exemplo, ao coletar dados para um programa de assistência social, o órgão público deve garantir que essas informações serão utilizadas exclusivamente para a execução e gestão do referido programa, evitando qualquer uso posterior que possa ser prejudicial ou incompatível com os direitos dos titulares. A observância ao princípio da adequação, nesse contexto, reforça o dever de respeito e responsabilidade do poder público, assegurando que os dados pessoais sejam tratados de maneira ética e em conformidade com os parâmetros comunicados no momento da coleta (Wimmer, 2021).

Esse princípio representa, portanto, um compromisso ético e jurídico de proteção ao titular, funcionando como um mecanismo de controle sobre a forma de uso das informações pessoais. Ao exigir coerência, transparência e proporcionalidade no tratamento de dados, a adequação fortalece a confiança dos cidadãos nas instituições públicas e contribui para a consolidação de uma cultura de respeito à privacidade e aos direitos fundamentais.

O princípio da necessidade, conforme o artigo 6º, inciso III, da LGPD, impõe um limite ao tratamento de dados, determinando que sejam coletados apenas os dados estritamente necessários para o cumprimento de um objetivo pretendido. Pode-se dizer que os dados coletados devem ser os mínimos indispensáveis para atender ao propósito informado ao titular. Esse princípio é fulcral para o setor público, onde a coleta de dados é, muitas vezes, uma etapa obrigatória em diversos processos administrativos e pode gerar riscos de exposição desnecessária à privacidade dos indivíduos (ANPD, 2023).

A aplicação prática desse princípio significa que os órgãos públicos devem avaliar cuidadosamente quais informações são realmente necessárias para atingir os objetivos das políticas públicas e dos serviços oferecidos. A Secretaria Municipal de Educação realiza uma licitação para contratar uma empresa responsável pelo fornecimento de merenda escolar. Para formalizar o contrato, são exigidos dados pessoais tanto do representante legal da empresa quanto do servidor público encarregado da assinatura, como nome completo, CPF, RG, profissão, estado civil e endereço. Em cumprimento às exigências legais de transparência, os dados constam no contrato, que é disponibilizado no site oficial da Secretaria, garantindo publicidade ao ato administrativo (ANPD, 2023). Neste exemplo, o tratamento posterior de dados é ilegítimo por violar o princípio da necessidade ao expor dados excessivos e desnecessários com o fim de publicizar.

Esse princípio é essencial para prevenir o uso excessivo de dados no setor público, em que a coleta muitas vezes ocorre em larga escala. O princípio da necessidade exige que apenas os dados essenciais para a realização da finalidade pública sejam coletados e tratados. No caso de um processo seletivo para estágio em órgão público, a solicitação de dados como nome completo, contato, CPF e comprovante de matrícula é necessária para avaliar a inscrição. No entanto, exigir informações como religião, orientação sexual ou filiação partidária não se justifica para essa finalidade e configura excesso. O princípio da necessidade impõe justamente essa limitação: apenas os dados estritamente indispensáveis ao objetivo pretendido devem ser coletados, evitando a coleta desproporcional e protegendo a privacidade do titular (Wimmer, 2021).

Desse modo, o tratamento de dados pessoais pelo Poder Público tem sido historicamente objeto de debate, oscilando entre duas perspectivas fundamentais. De um lado, há a preocupação com os riscos da vigilância estatal e do controle social, que podem comprometer direitos fundamentais, especialmente a privacidade e a autodeterminação informativa. De outro, enfatiza-se a eficiência e a modernização administrativa, destacando a importância do uso de dados para a otimização de políticas públicas e a melhoria da gestão estatal.

Segundo Wimmer (2021), essa dualidade também se manifesta na interpretação dos princípios jurídicos aplicáveis ao tratamento de dados pela Administração Pública. De um lado, os princípios previstos no artigo 6º da LGPD, que têm por objetivo garantir a proteção dos direitos do titular dos dados e assegurar sua autodeterminação informativa, permitindo que o indivíduo mantenha o controle sobre suas informações pessoais. De outro, os princípios gerais

da Administração Pública, previstos na Constituição Federal, na legislação infraconstitucional e na doutrina jurídica, que estabelecem diretrizes como publicidade, eficiência e interesse público, orientando a atuação estatal na gestão de dados.

O desafio central reside na harmonização de dois conjuntos normativos: de um lado, os princípios da LGPD, que visam a proteção dos direitos dos titulares; de outro, os princípios da Administração Pública, como publicidade, eficiência e interesse público. Essa harmonização é fundamental para que o Estado utilize os dados de forma eficiente e em conformidade com o interesse público, sem comprometer os direitos fundamentais dos indivíduos, assegurando transparência e respeito à privacidade.

2.2 LIVRE ACESSO, QUALIDADE DOS DADOS E TRANSPARÊNCIA

A transparência e o direito à informação são fundamentais na relação entre Estado e titulares de dados pessoais. No setor público, os princípios de transparência, livre acesso e qualidade dos dados, conforme os artigos 6º, incisos IV, V e VI, da LGPD, são essenciais para que os titulares compreendam como suas informações pessoais são tratadas e possam exercer controle sobre elas.

A LGPD impõe, a todos os agentes de tratamento — públicos ou privados — o dever de fornecer informações claras, acessíveis e precisas [7] sobre o uso de dados pessoais, fortalecendo o controle social e a *accountability*. O princípio do livre acesso assegura ao titular o direito de consultar, de forma gratuita e facilitada, informações sobre a coleta, o uso e o compartilhamento de seus dados, conforme previsto no artigo 9º da LGPD.

A transparência, [8] além de permitir que os indivíduos compreendam o ciclo de tratamento de seus dados, viabiliza o acompanhamento das práticas da administração pública. No entanto, um dos desafios é garantir que as informações estejam acessíveis em linguagem

[7] Conforme esclarece Dallari (2002), embora o direito à informação esteja incluído entre os direitos individuais, no Brasil ele assumiu predominantemente as características de um direito coletivo, o que influenciou a forma como é protegido juridicamente. Nesse sentido, a Constituição Federal previu expressamente a hipótese de sigilo por razões de segurança, distinção que não foi aplicada às informações que podem ser objeto do habeas data. Dessa forma, fica evidente que o legislador constituinte buscou estabelecer um tratamento diferenciado entre informações de interesse individual ou coletivo que não envolvem dados pessoais e aquelas que dizem respeito a pessoas determinadas.

[8] O habeas data garante o direito fundamental de acesso às informações pessoais armazenadas por entidades públicas ou governamentais, assegurando que o titular possa conhecer e retificar dados que lhe dizem respeito. Esse entendimento foi reforçado ao se reconhecer, conforme Mendes (2018), a existência de um direito material à autodeterminação informativa, que fundamenta essa proteção processual e reforça a transparência no tratamento de dados pessoais (Mendes, 2018).

clara e em plataformas de fácil navegação, especialmente em políticas complexas ou serviços automatizados.

Ao ingressar em um edifício público, uma pessoa fornece seus dados na recepção, como medida de controle de acesso e proteção dos servidores e do patrimônio. Caso participe de uma reunião com alguma autoridade do órgão, seu nome poderá constar na agenda institucional divulgada publicamente, conforme regras de transparência, exceto quando houver previsão legal que justifique a restrição dessa informação (ANPD, 2023).

A qualidade dos dados tem impacto direto na eficiência das políticas públicas. Informações incorretas ou desatualizadas podem prejudicar os titulares de dados pessoais, por exemplo, ao comprometer cadastros sociais e limitar o acesso a serviços essenciais. Assim, cabe à administração pública garantir que os dados sejam exatos e atualizados, prevenindo distorções e injustiças (ANPD, 2023).

Embora esses princípios promovam um ambiente de transparência e confiança, desafios persistem. A acessibilidade das informações e o acesso pleno a dados atualizados continuam sendo obstáculos para a administração pública, especialmente no que diz respeito ao equilíbrio entre o direito à privacidade e a efetividade das políticas públicas. A Lei de Acesso à Informação (LAI), ao assegurar o direito à informação, impõe a necessidade de conciliar esse direito com a proteção de dados pessoais, exigindo soluções que preservem a privacidade dos cidadãos, sem comprometer a efetividade e a transparência nas ações governamentais

2.3 SEGURANÇA, PREVENÇÃO, RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS *(ACCOUNTABILITY)*

A LGPD determina que os agentes de tratamento de dados, incluindo os órgãos públicos, devem adotar medidas rigorosas de segurança, prevenção e responsabilização para proteger as informações dos titulares, segundo o artigo 6º, incisos VII, VIII e X, da LGPD. Esses dispositivos visam garantir um tratamento de dados ético, transparente e seguro, prevenindo incidentes e promovendo a confiança da população nas instituições.

No setor público, que processa um grande volume de dados pessoais, a segurança é prioridade. Para isso, é essencial a implementação de medidas técnicas e administrativas que previnam acessos não autorizados, perdas e destruições de dados. Um dos maiores desafios é a proteção contra-ataques cibernéticos, que possam comprometer informações críticas e afetar a credibilidade do Estado.

Além da segurança, a LGPD impõe ao Estado uma postura proativa na prevenção de danos aos titulares, mediante políticas de governança, avaliações de impacto e monitoramento contínuo de riscos.

A proteção de dados pessoais exige a adoção de medidas de segurança[9] compatíveis com os riscos inerentes ao tratamento dessas informações. Tais riscos envolvem, por exemplo, vazamentos, acessos não autorizados, alterações indevidas, uso discriminatório ou até mesmo a exclusão acidental de dados pessoais, o que pode gerar prejuízos significativos aos titulares, como violação de privacidade, discriminação ou uso abusivo de informações sensíveis.

Para mitigar esses riscos, a legislação impõe aos agentes de tratamento a implementação de soluções técnicas e administrativas preventivas. Nesse sentido, destaca-se o conceito de *privacy by design* (Wimmer, 2021) que determina a incorporação de medidas de segurança desde a concepção até a implementação de produtos e serviços que envolvam dados pessoais (Gonçalves, 2019).

O princípio da responsabilização e prestação de contas, frequentemente associado ao conceito de *accountabili*ty,[10] desempenha um papel central nos debates sobre a proteção de dados pessoais. A consolidação desse princípio sobre Privacidade da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) de 1980, que estabeleceram a obrigação do controlador de dados de adotar medidas eficazes para garantir o cumprimento das normas de proteção de dados (Wimmer, 2021). Apesar da dificuldade em traduzir o termo com exatidão

[9] Cabe destacar a promulgação da Política Nacional de Segurança da Informação (PNSI), instituída pelo Decreto nº 9.637/2018, que estabelece diretrizes para a proteção de informações sensíveis no âmbito governamental. Essa política define as competências do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e do Comitê Gestor de Segurança da Informação (CGSI), órgão colegiado que reúne representantes de 22 entidades da administração pública federal para coordenar estratégias de segurança da informação.

[10] O termo *accountability* deriva do mundo anglo-saxão, onde é amplamente utilizado e compreendido, embora sua definição prática seja complexa. De modo geral, a ênfase está em demonstrar como a responsabilidade é essencial e em tornar essa obrigação verificável. Responsabilidade e *accountability* são dois lados da mesma moeda, ambos constituindo elementos fundamentais para uma boa governança. Apenas quando se pode definir e comprovar a responsabilidade é que a confiança pode se desenvolver. Na maioria dos outros países, especialmente devido a diferenças nos sistemas jurídicos, o termo *accountability* não possui uma tradução direta e, consequentemente, pode ser interpretado de formas distintas, gerando desafios para a harmonização conceitual. Outras expressões que têm sido sugeridas para capturar seu significado incluem *reinforced responsibility*, *assurance*, *reliability*, *trustworthiness* e, em francês, *obligation de rendre compte*. Pode-se, assim, argumentar que *accountability* se refere à implementação de princípios de proteção de dados (Article 29 Data Protection Working Party, 2010).

para outros idiomas, a *accountability*[11] e estratégias de corregulação, além de se conectar à gestão baseada em riscos *(risk-based approach*).[12]

O mencionado princípio confere ao agente regulado a responsabilidade de implementar e comprovar a eficácia de mecanismos técnicos e administrativos que assegurem a conformidade e a mitigação de riscos no tratamento de dados.

A LGPD determina que os agentes de tratamento demonstrem o cumprimento das normas de proteção de dados, permitindo auditorias e verificações independentes. No setor público, essa exigência reforça a transparência e assegura que as instituições adotem boas práticas na gestão das informações pessoais. Embora esses princípios fortaleçam a proteção de dados, desafios persistem, como o combate a ataques cibernéticos e a implementação efetiva de políticas de prevenção. Para enfrentar essas questões, a administração pública precisa investir em tecnologias adequadas e fomentar uma cultura organizacional voltada à segurança e à ética no tratamento de dados.

2.4 NÃO DISCRIMINAÇÃO

O uso de dados pode impactar diretamente a vida dos indivíduos. A não discriminação protege os cidadãos de práticas estigmatizantes, reforçando a igualdade no acesso aos serviços públicos. Assim, o princípio da não discriminação, previsto na LGPD, estabelece que o tratamento de dados pessoais não pode ter finalidade discriminatória ilícita ou abusiva. Essa diretriz busca evitar que informações sensíveis sejam utilizadas para restringir direitos ou gerar desigualdades injustificadas.

A proteção contra discriminação no uso de dados pessoais é uma preocupação global. Normas internacionais, como as Diretrizes de Privacidade da OCDE e o RGPD europeu

[11] A regulação responsiva é uma abordagem que busca promover a conformidade de maneira mais eficaz e justa, incentivando a autorregulação e a participação dos regulados na definição de metas e práticas. Ela se baseia no princípio do diálogo regulatório, no qual há colaboração e aprendizado mútuo entre reguladores e regulados. O modelo é representado pela pirâmide regulatória, onde, inicialmente, há pouca intervenção estatal, priorizando a autorregulação. A intervenção do Estado aumenta conforme a resposta dos regulados. Essa abordagem se alinha ao *risk-based approach*, que foca em identificar e priorizar riscos para direcionar as intervenções, além de se conectar com a *accountability*, pois exige que os agentes públicos sejam responsáveis pela proteção de dados, com transparência e prestação de contas (ANEEL, 2023).

[12] Essa perspectiva parte da premissa de que nem todos os riscos são equivalentes, de modo que os esforços de conformidade devem ser direcionados prioritariamente às situações com maior potencial de impacto negativo. Trata-se, portanto, de uma estratégia que exige diagnóstico contínuo, sensibilidade para mudanças regulatórias e atenção às dinâmicas internas da organização. No setor público, essa lógica implica identificar os fluxos de dados mais sensíveis, analisar os efeitos que determinadas práticas podem gerar sobre os titulares e implementar controles proporcionais, capazes de prevenir danos relevantes (Gallardo Guerra; Rivero Prado, 2021).

(Wimmer, 2021), adotam mecanismos semelhantes para prevenir práticas discriminatórias indevidas. No Brasil, a LGPD reconhece essa preocupação ao classificar certas informações como dedos sensíveis,[13] devido ao potencial impacto sobre os direitos fundamentais dos indivíduos.

O avanço das tecnologias trouxe novos desafios, especialmente no uso de algoritmos e inteligência artificial para a formação de perfis comportamentais. Esses mecanismos podem resultar em discriminação indireta, afetando contratações, concessão de crédito e acesso a serviços. Para mitigar esse risco, a LGPD garante ao titular o direito de solicitar a revisão de decisões automatizadas, especialmente quando envolvem a definição de perfis pessoais, profissionais ou de consumo.

Contudo, o conceito de não discriminação na LGPD não pode ser entendido de forma absoluta, pois a norma não proíbe toda e qualquer diferenciação entre indivíduos, mas apenas aquelas que tenham fins ilícitos ou abusivos.[14]

No setor público, a aplicação da LGPD deve considerar que o tratamento de dados pessoais, especialmente os dados sensíveis, pode ser fundamental para a implementação de políticas públicas voltadas à promoção da equidade. A coleta e o uso de informações relativas à raça, deficiência, identidade de gênero ou orientação sexual, por exemplo, são muitas vezes indispensáveis para a identificação de desigualdades e a formulação de ações afirmativas. O Supremo Tribunal Federal (STF) reconheceu a constitucionalidade das ações afirmativas,[15] reforçando que a igualdade material pode exigir diferenciações legítimas para corrigir desigualdades estruturais. No julgamento da ADPF 186, que analisou a política de cotas raciais da Universidade de Brasília, o STF afirmou que a igualdade formal, prevista no artigo 5º da Constituição, não impede a adoção de medidas voltadas à superação de desigualdades históricas (Lewandowski, 2012). Dessa forma, a LGPD não deve ser interpretada como obstáculo à adoção de políticas públicas inclusivas, mas sim como instrumento que garante que o tratamento de dados ocorra com segurança jurídica, respeito aos direitos dos titulares e compromisso com a justiça social.

---

[13] Informação relacionada a aspectos mais íntimos da pessoa, como convicção religiosa, dados de saúde, origem racial e étnica, liação a sindicato, entre outros (Brasil, 2024).

[14] Certas formas de discriminação são juridicamente admitidas, como nos casos de restrição etária para condução de veículos ou consumo de bebidas alcoólicas. Tais exemplos ajudam a compreender os limites entre tratamento legítimo e discriminação algorítmica no âmbito da LGPD (Mendes; Mattiuzzo; Fujimoto, 2021).

[15] Exemplos dessa abordagem podem ser encontrados em decisões como a MC-ADI 1.276/SP, sob relatoria do Ministro Octávio Gallotti; a ADI 1.276/SP, relatada pela Ministra Ellen Gracie; o RMS 26.071, de relatoria do Ministro Ayres Britto; e a ADI 1.946/DF, assim como sua medida cautelar, ambas sob relatoria do Ministro Sydnei Sanches.

Dessa forma, a interpretação da não discriminação na LGPD deve ser harmônica com outros princípios constitucionais, permitindo que o tratamento de dados viabilize políticas de inclusão e justiça social, sem comprometer a proteção dos direitos fundamentais.

3 ANÁLISE DA APLICAÇÃO DAS BASES LEGAIS DA LGPD NO SETOR PÚBLICO

Este capítulo aborda as principais controvérsias envolvendo as bases legais aplicáveis – ou não – ao tratamento de dados pessoais no setor público, segundo a Lei Geral de Proteção de Dados (LGPD). A análise foca especialmente nas hipóteses legais mais frequentemente utilizadas ou discutidas no contexto da Administração Pública, como o consentimento,[16] o cumprimento de obrigação legal e o legítimo interesse como pressuposto constitucional. Busca-se examinar as especificidades e os desafios que envolvem a escolha de fundamentos jurídicos adequados, a compatibilização com os princípios da LGPD e a necessidade de garantir transparência e respeito aos direitos dos titulares de dados pessoais no setor público.

Conforme o artigo 3º da Lei nº 13.709/2018 (LGPD), a norma se aplica amplamente a toda a Administração Pública, alcançando os entes federativos, União, Estados, Distrito Federal e Municípios, em todas as esferas de poder: Executivo, Legislativo e Judiciário. Ainda que haja discussões sobre a natureza institucional de órgãos como o Ministério Público e as Cortes de Contas, frequentemente reconhecidos como autônomos em relação aos poderes tradicionais, esses também estão submetidos à LGPD (ANPD, 2023), na medida em que realizam tratamento de dados pessoais no exercício de suas funções institucionais. Além disso, as regras da LGPD se aplicam a entidades administrativas como empresas públicas e sociedades de economia mista. Quando atuam sem finalidade econômica, prestando serviço público ou exercendo função típica do Estado, aplicam-se as disposições específicas para o setor público. Já quando atuam em regime de concorrência, como agentes econômicos no mercado, devem observar as normas aplicáveis aos entes privados. Essas disposições visam garantir que o tratamento de dados pessoais no setor público ocorra dentro de um conjunto normativo uniforme e direcionado à proteção dos direitos dos titulares de dados pessoais, permitindo ao Estado desenvolver suas funções com responsabilidade e respeito à privacidade (ANPD, 2023).

[16] Como por exemplo uma universidade pública exige que os calouros informem seus dados pessoais para fins de registro acadêmico. Todo o processo é feito por meio de uma plataforma online, e, para avançar às próximas etapas — como a escolha de disciplinas e horários —, o estudante precisa aceitar os termos apresentados sobre o uso dos dados.

3.1 BASES LEGAIS: CONSENTIMENTO, OBRIGAÇÃO LEGAL E LEGÍTIMO INTERESSE

Para legitimar o tratamento de dados pessoais pelo setor público, os artigos 7º e 11 da Lei Geral de Proteção de Dados (LGPD) estabelecem diversas bases legais. Neste trabalho, optou-se por agrupar e analisar três delas — consentimento,[17] cumprimento de obrigação legal e legítimo interesse — por serem as mais recorrentes na prática administrativa ou por levantarem discussões relevantes na doutrina. Aborda-se, em outro tópico, o interesse público, que, embora não constitua uma base legal autônoma, configura um pressuposto legitimador do tratamento de dados no contexto da administração pública.

A base do consentimento está prevista no artigo 7º, incisos I e V, e no artigo 11, inciso I, da LGPD. No caso do artigo 7º, refere-se ao tratamento de dados pessoais comuns, mediante manifestação livre, informada e inequívoca do titular. Já no artigo 11, aplica-se ao tratamento de dados pessoais sensíveis, exigindo, além disso, que o consentimento seja específico e destacado.

Contudo, no setor público, sua utilização é limitada, pois a assimetria de poder entre o Estado e o cidadão pode comprometer a liberdade da escolha (ANPD, 2023). Assim, o consentimento é reservado a situações específicas em que a vontade do titular possa ser manifestada de forma autêntica. Suponha que um estudante se inscreva para participar de um seminário promovido por uma instituição pública de ensino. Durante o processo de inscrição, ele é solicitado a informar dados básicos, como seu nome e número de matrícula, os quais são necessários para viabilizar benefícios como a isenção de taxa para estudantes. Além disso, é oferecida a opção de fornecer um endereço de e-mail, caso o estudante deseje receber informações sobre futuros eventos organizados pela instituição. A decisão de fornecer o e-mail é inteiramente voluntária e não condiciona a participação no evento. Nessa situação, o uso do consentimento como base legal é legítimo, pois há uma finalidade clara e específica, e o titular tem liberdade real para decidir, sem prejuízo ou restrições (ANPD, 2023).

Já o cumprimento de obrigação legal, previsto nos artigos 7º, incisos II, VI e X, e 11º, inciso II, alíneas "a", "d" e "g", constitui uma das bases mais frequentemente utilizadas pelo Poder Público. Essa base legal abrange o tratamento necessário para atender a determinações legais ou regulamentares, o exercício regular de direitos em processos judiciais, administrativos

[17] Esses termos, no entanto, são vagos e indicam que as informações poderão ser utilizadas para “finalidades educacionais e similares”. Há ainda um aviso informando que, sem essa aceitação, o estudante não poderá concluir a matrícula nem acessar benefícios como programas de assistência estudantil ou o sistema de empréstimo da biblioteca (ANPD, 2023).

ou arbitrais, e a proteção do crédito. Por exemplo, uma Assembleia Legislativa planeja criar um canal de televisão próprio. Para obter a autorização necessária, o órgão regulador exige que sejam fornecidos dados pessoais dos parlamentares e servidores responsáveis pela gestão do canal. Caso esses dados não sejam apresentados, o pedido de autorização poderá ser negado. Nesse cenário, o tratamento dos dados pessoais realizado pela Assembleia é justificado e permitido, pois está fundamentado no artigo 7º, inciso II, da LGPD, que autoriza o processamento para cumprir obrigações legais e regulatórias impostas por entidades competentes, conforme a legislação vigente (ANPD, 2023).

A base do legítimo interesse é tratada apenas no artigo 7º, inciso IX, da LGPD, e permite o tratamento de dados quando necessário para atender aos interesses legítimos do controlador ou de terceiros, desde que não se sobreponham os direitos e liberdades fundamentais do titular. Embora prevista na LGPD, sua aplicação à Administração Pública é controvertida na doutrina, que em geral entende que a atuação estatal deve estar fundada em finalidades públicas expressamente previstas em lei. Apesar disso, não há vedação legal explícita à sua aplicação. Um exemplo seria um órgão público usa dados dos servidores para proteger seus sistemas, como para confirmar quem acessa e evitar ataques. Como não é uma função típica do Estado, pode usar o legítimo interesse, mas precisa respeitar os direitos das pessoas e ser transparente.

Assim, embora a LGPD estabeleça um conjunto amplo de bases legais, a sistematização aqui adotada busca organizar as hipóteses mais comuns ou problemáticas com base na lógica de atuação estatal, facilitando a compreensão e a aplicação prática dos dispositivos legais, sem prejuízo à proteção dos direitos fundamentais dos titulares.

3.2 SUPREMACIA DO INTERESSE PÚBLICO E HARMONIZAÇÃO COM DIREITOS FUNDAMENTAIS

No contexto da proteção de dados pessoais pelo Poder Público, é comum a invocação do princípio da supremacia do interesse público como justificativa para práticas de tratamento de dados. De fato, a formulação e execução de políticas públicas frequentemente depende da coleta, uso e compartilhamento de informações pessoais. No entanto, embora o direito à privacidade já fosse reconhecido como direito fundamental, a Emenda Constitucional nº 115/2022 elevou expressamente a proteção de dados pessoais à condição de direito fundamental autônomo, o que impõe uma reavaliação da tradicional invocação da supremacia

do interesse público, que não pode mais ser afirmada de modo automático diante de direitos individuais.

No Estado Democrático de Direito, a ideia tradicional de que o interesse público se sobrepõe automaticamente ao interesse privado perde força. Como analisa Binenbojm (2019a), o Direito Administrativo clássico foi estruturado sob uma lógica autoritária e coletivista, legitimando a vontade estatal sem maior justificativa. Essa concepção se revela incompatível com o constitucionalismo contemporâneo, que exige a prevalência da deliberação democrática e da proteção dos direitos fundamentais.

O interesse público, como já mencionado é um pressuposto legitimador do tratamento de dados no setor público. Assim, ele incide sobre todo e qualquer tratamento de dados pessoais realizado pelo poder público, independentemente da base legal adotada. Tratando-se de hipóteses frequentemente utilizadas pela Administração Pública, destacam-se as bases previstas nos artigos 7º ou 11 da LGPD, como nos incisos III e IV do artigo 7º e nas alíneas "b", "c", "e" e "f" do inciso II do artigo 11. Essas bases legitimam o tratamento necessário à execução de políticas públicas previstas em leis ou contratos, à realização de estudos por órgãos de pesquisa, à atuação de autoridades sanitárias e à prevenção de fraudes. A Secretaria de Saúde processa dados pessoais de pacientes fumantes atendidos em hospitais públicos, com o objetivo de planejar e implementar uma política pública voltada ao controle do tabagismo e à prevenção e tratamento do câncer pulmonar (ANPD, 2023). Essa política está formalizada em uma norma infralegal que define seus objetivos, atribuições e fontes de financiamento. Os dados são gerenciados pela própria Secretaria e, quando necessário, compartilhados com a autarquia encarregada de conduzir programas de apoio para pessoas que desejam parar de fumar.

Conforme destaca Gonçalves (2019), o artigo 11, II, b, da LGPD dispensa o consentimento para o tratamento compartilhado de dados pelo poder público na execução de políticas públicas, desde que haja ampla publicidade quanto à dispensa e às razões que a justificam. No entanto, essa autorização legal, embora vise dar efetividade à atuação estatal, pode abrir margem para interpretações amplas e inseguras, expondo os titulares de dados a riscos à privacidade diante da falta de regras mais claras.

Como os dados envolvem informações sensíveis, o tratamento é realizado com base no artigo 11, inciso II, alínea b, da LGPD (ANPD, 2023). Além disso, o cruzamento de dados entre órgãos públicos para combater fraudes em programas sociais é amparado pelo interesse público, desde que respeitados os princípios da necessidade, proporcionalidade e finalidade. Nesse tipo

de tratamento, recomenda-se a anonimização dos dados pessoais sempre que possível, como medida adicional de proteção à privacidade.

O artigo 23[18] da Lei Geral de Proteção de Dados estabelece que o tratamento de dados pessoais por entes públicos deve atender a finalidades públicas legítimas, na persecução do interesse público, nos limites de suas competências legais. Esse dispositivo explicita que essa atuação não é ilimitada, devendo observar os princípios da finalidade, transparência e responsabilidade. Nesse sentido, a crítica de Binenbojm à lógica da supremacia automática do interesse público é especialmente pertinente, ao defender uma atuação estatal fundamentada, com delimitação clara de propósitos, conforme exigem os incisos I e III do mesmo artigo.

A evocação genérica da "supremacia do interesse público" torna-se, assim, uma fórmula vazia, incapaz de resolver, por si só, os conflitos entre posições jurídicas individuais e interesses coletivos. Binenbojm propõe em substituição a esse automatismo, uma abordagem mais sofisticada, que leve em conta: (i) a existência de posições jurídicas individuais irredutíveis, como o núcleo essencial dos direitos fundamentais e da dignidade da pessoa humana; (ii) a *primazia prima facie* dos direitos fundamentais, mesmo diante de finalidades públicas relevantes; e (iii) a polissemia do próprio conceito de interesse público, que pode abarcar tanto a proteção de direitos individuais quanto a promoção de fins coletivos (Binenbojm, 2019b).

Nesse novo modelo, Binenbojm (2019a) entende que a relação entre autonomia pública e autonomia privada é de equiprimordialidade:[19] os direitos fundamentais dos indivíduos e os mecanismos democráticos de formação da vontade estatal se condicionam reciprocamente. De um lado, a democracia pressupõe indivíduos previamente emancipados por direitos fundamentais; de outro, os próprios contornos desses direitos são definidos, em alguma medida, por meio da deliberação democrática. Isso significa que os interesses públicos e privados não estão mais em uma relação de hierarquia rígida, mas sim em uma tensão dinâmica. A resolução dessa tensão (Binenbojm, 2019b) exige a adoção de critérios como a ponderação e a proporcionalidade, que reconhecem tanto a existência de posições jurídicas individuais inegociáveis quanto a complexidade e pluralidade do conceito de interesse público

[18] Art. 23, LGPD: "O tratamento de dados pessoais pelas pessoas jurídicas de direito público [...] deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: I – sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas [...]; III – seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais [...]."

[19] Equiprimordialidade se refere à ideia de que os direitos fundamentais dos indivíduos e os interesses públicos possuem a mesma relevância, não prevalecendo um sobre o outro de forma automática, mas influenciando-se mutuamente (Binenbojm, 2019a).

Um exemplo paradigmático dessa lógica pode ser encontrado na disciplina constitucional das desapropriações (Binenbojm, 2019b). Embora o artigo 184 da Constituição Federal autorize a desapropriação de imóveis rurais para fins de reforma agrária, o artigo 185 impõe limites à atuação estatal, como a vedação da desapropriação da pequena e da média propriedade produtiva. Trata-se de uma preponderação constitucional, que evidencia a impossibilidade de se afirmar, de modo absoluto, a prevalência do interesse coletivo sobre os direitos individuais. Aplicado à proteção de dados pessoais, esse entendimento impõe à Administração Pública o dever de justificar, com base em critérios objetivos e proporcionais, a necessidade, adequação e razoabilidade das práticas de tratamento de dados, especialmente quando envolvem dados sensíveis ou afetam significativamente a esfera privada dos indivíduos. A simples invocação do interesse público não é mais suficiente para legitimar tais práticas. É necessário demonstrar, à luz da ponderação de direitos, que o interesse coletivo em questão não anula, mas busca compatibilizar-se com os direitos individuais de forma equilibrada e proporcional.

Assim, no Estado Constitucional, o tratamento de dados pelo Poder Público deve seguir o princípio da proporcionalidade. Isso significa que não basta alegar uma finalidade pública para justificar a coleta ou o uso de dados pessoais. É preciso demonstrar que a medida é necessária, adequada e proporcional, especialmente quando envolve dados sensíveis ou atinge de forma relevante a esfera privada dos indivíduos. A teoria da equiprimordialidade, proposta por Binenbojm, reforça essa exigência ao afirmar que o interesse público e os direitos individuais têm o mesmo peso na ordem constitucional e devem ser equilibrados. No âmbito de proteção de dados, essa lógica se traduz na obrigação de o Estado justificar suas escolhas de forma transparente. A LGPD incorpora esse entendimento ao estabelecer, no artigo 23, as condições para o tratamento de dados pelo setor público e, em outros dispositivos, ao prever mecanismos como a avaliação de impacto à proteção de dados.[20] Além disso, a atuação da ANPD e a exigência de transparência reforçam que o interesse público não pode ser usado como justificativa genérica, devendo sempre ser conciliado com os direitos fundamentais de forma responsável e equilibrada.

[20] O Relatório de Impacto à Proteção de Dados Pessoais (RIPD), previsto no artigo 5º, XVII, e no artigo 38, parágrafo único, da LGPD, é um documento elaborado pelo controlador com o objetivo de avaliar os riscos envolvidos nas operações de tratamento de dados pessoais. Ele descreve os tipos de dados coletados, a metodologia aplicada, as medidas de segurança adotadas e os mecanismos de mitigação de riscos que possam comprometer os direitos fundamentais e as liberdades civis dos titulares.

4 CONFLITO ENTRE TRANSPARÊNCIA E PUBLICIDADE E PROTEÇÃO DE DADOS NO SETOR PÚBLICO

A formulação clássica do direito à privacidade, consagrada por Warren e Brandeis em 1890, assentava-se na ideia do "direito de estar só" (*the right to be let alone*) de Warren e Brandeis (1890) em resposta à crescente intrusão da imprensa na esfera íntima dos indivíduos. Essa concepção fundacional associava a privacidade à reserva, segredo e dignidade, valores que ainda hoje permeiam a proteção de dados pessoais.

Contudo, no contexto da sociedade da informação, caracterizada pela coleta sistemática, tratamento automatizado e circulação massiva de dados, a noção clássica de privacidade como simples direito à intimidade e reserva se mostrou limitada. Diante desses novos desafios, o direito à proteção de dados pessoais passa a ser reconhecido como uma categoria autônoma, embora relacionada à privacidade (Doneda, 2020).

O sigilo permanece vinculado à lógica tradicional da privacidade, permitindo ao titular restringir o acesso de terceiros a seus dados. Já o controle representa um avanço conceitual importante: refere-se à capacidade do indivíduo de participar ativamente das decisões que envolvem o tratamento de suas informações pessoais, da coleta à eliminação, passando pela finalidade, compartilhamento e segurança. Essa perspectiva evidencia ampliação do conceito de privacidade, incorporando a autodeterminação informacional como elemento central do direito à proteção de dados.

Nessa leitura, o direito à proteção de dados exige não apenas a abstenção de interferências indevidas, mas também a criação de mecanismos normativos e institucionais que garantam transparência, participação e responsabilidade dos agentes que tratam dados. A centralidade do controle no exercício desse direito evidencia sua íntima conexão com a dignidade da pessoa humana, especialmente em contextos assimétricos, como os das relações com o poder público e as plataformas digitais. O que antes se resumia ao direito de se manter fora do alcance alheio se transforma, hoje, no direito de governar conscientemente o próprio fluxo informacional.

A particularidade dessa tensão decorre do fato de que, diferentemente do setor privado, o Estado está sujeito aos princípios constitucionais da publicidade e da transparência (artigo 37, caput, da CF). A Administração Pública tem o dever jurídico de prestar contas à sociedade, o que inclui a divulgação de informações sobre sua atuação, seus servidores, gastos, políticas públicas e decisões administrativas. Esses elementos são centrais para o exercício do controle

social e para a promoção da *accountability,* valores democráticos que sustentam o regime republicano.

Ao mesmo tempo, a LGPD estabelece limites claros ao tratamento de dados pessoais, mesmo no exercício de funções públicas. Conforme os artigos 6º, 7º e 23 da LGPD, o tratamento de dados pelo Poder Público deve observar os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, segurança e transparência. Além disso, a proteção de dados pessoais foi alçada a direito fundamental pela Emenda Constitucional nº 115/2022, reforçando a obrigação do Estado de assegurar esse direito aos cidadãos.

Nesse sentido, outro aspecto relevante é a transparência governamental, que, embora essencial para um governo democrático, enfrenta desafios significativos quando se trata da disponibilização de dados pessoais. A forma como essas informações são apresentadas deve levar em consideração o nível de agregação e a sensibilidade das informações envolvidas. Para tanto, são necessários investimentos substanciais em infraestrutura de segurança da informação, incluindo o uso de tecnologias como criptografia e anonimização,[21] bem como a capacitação de equipes especializadas. O fornecimento de dados pelo setor público, portanto, demanda um equilíbrio delicado entre garantir a transparência e proteger a privacidade dos titulares de dados pessoais.

Assim, surgem dilemas práticos relevantes: até que ponto a Administração Pública pode divulgar dados de cidadãos em nome da transparência? Como assegurar que portais de acesso à informação não violem a privacidade individual? De que maneira políticas públicas que se baseiam em dados sensíveis — como saúde, assistência social ou segurança — podem ser executadas sem comprometer os direitos dos titulares?

A resolução dessa tensão exige não apenas normas claras, mas também soluções técnicas e institucionais, como: a adoção de padrões de anonimização; a limitação da publicidade excessiva em portais de transparência; e a atuação efetiva da ANPD na regulação das atividades do setor público.

A ponderação entre os princípios da publicidade e da proteção de dados deve, por fim, ser feita à luz da colisão de direitos fundamentais, conforme a teoria de Robert Alexy, a partir de critérios como a proporcionalidade, a adequação, a necessidade e a busca do menor sacrifício possível. O desafio está justamente em promover políticas públicas eficazes e transparentes

[21] Trata-se de dados que, após passarem por procedimentos técnicos específicos, deixam de permitir a identificação de uma pessoa natural. Esse tipo de tratamento, conhecido como anonimização, tem como objetivo retirar os elementos que possibilitam a associação dos dados a um indivíduo (Brasil, 2024).

sem violar o direito à privacidade dos indivíduos, construindo, assim, uma Administração Pública digital ética, eficiente e comprometida com os direitos fundamentais.

Um caso marcante do conflito entre transparência e proteção de dados no setor público é o julgamento do Tema 483 da Repercussão Geral pelo STF, Recurso nº 2.367, com decisão proferida em 13 de março de 2017.[22] Nessa decisão, a Corte considerou legítima a divulgação de nomes, salários e locais de trabalho de servidores públicos, destacando a relevância dessas informações para o controle social da administração.

O relator, Ministro Joaquim Barbosa, teve sua decisão mantida pelo órgão colegiado do STF, que rejeitou o agravo interno interposto contra a divulgação. O Ministro Luís Roberto Barroso, ao se manifestar no colegiado, argumentou que a exposição desses dados não viola a intimidade ou a vida privada dos servidores, pois se referem ao exercício de função pública, custeada com recursos públicos. O STF, então, reafirmou que, em casos de interesse público claro, a transparência pode prevalecer sobre a proteção de dados.

A União defendeu que a pretensão da associação autora da ação impediria a concretização de uma política pública de publicidade dos gastos públicos, especialmente no Judiciário. A associação, por sua vez, alegava que a divulgação de remunerações violaria o direito à privacidade. No entanto, o STF entendeu que o interesse público na transparência dos gastos se sobrepõe ao direito à privacidade, consolidando a ideia de que a exposição de informações funcionais não configura violação de dados pessoais sensíveis.

> Ementa: DIREITO CONSTITUCIONAL. RESOLUÇÕES N.ºs 151/2012 e 215/2015, DO CONSELHO NACIONAL DE JUSTIÇA. DIVULGAÇÃO DE REMUNERAÇÃO. 1. **Não há violação à intimidade ou à vida privada na divulgação nominal e pormenorizada da remuneração de magistrados, pois os dados são de interesse público e a transparência se impõe.** Precedentes. 2. A jurisprudência do STF entende prevalecer, no caso, **o princípio da publicidade administrativa**, que concretiza a República como forma de governo. 3. Pedido julgado improcedente. (…) 14. No mérito, destaco que a jurisprudência desta Corte firmou-se no sentido de que, sendo o agente remunerado pelo Poder Público, seus vencimentos, acompanhados de nome e de lotação, representam informação de caráter estatal, decorrente da natureza pública do cargo: (…) 15. Portanto, não havendo violação à intimidade e à vida privada, não 33 existe conflito de normas, nem desrespeito

[22] O Tema 483 da Repercussão Geral, que trata da divulgação de dados como nome e remuneração de servidores públicos, exemplifica a priorização do acesso à informação em detrimento da privacidade, uma vez que esses dados podem ser publicados em sítios institucionais. Em relação ao conceito de privacidade, Danilo Doneda destaca que sua definição pode variar conforme o contexto e o ordenamento jurídico. Ele observa que, embora haja um movimento em direção a uma concepção mais uniforme de privacidade, esse conceito ainda se adapta às necessidades de cada sistema jurídico, sendo passível de manipulação para atender a diferentes exigências estruturais do direito. (Doneda, 2006.)

> ao princípio da legalidade. (…)18. Não há dúvidas de que o entendimento reiterado do STF se aplica aos magistrados federais, seja porque são agentes públicos, seja porque as informações são de interesse coletivo e geral, o que atrai a aplicação da regra do art. 5º, XXXIII, da CF, sem que a eles se aplique a exceção prevista na parte final do mesmo dispositivo ("todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado"). 19. Os atos do Conselho Nacional de Justiça não apenas densificam a interpretação constitucional conferida pelo Supremo Tribunal Federal, como promovem a transparência. Como venho afirmando nesta Corte, a transparência se impõe porque decorre (i) do princípio democrático (CF/1988, art. 1º, caput), (ii) do sistema representativo (CF/1988, art. 1º, parágrafo único), (iii) do regime republicano (CF/1988, art. 1º,caput), e (iv) do princípio da publicidade (CF/1988, art 37, caput). Ao especificar o conteúdo desses princípios no exercício de suas competências constitucionais, o ato do CNJ não exorbita do poder regulamentar, mas antes confere efetividade ao disposto na Constituição Federal. 20. Por todo o exposto, julgo improcedente o pedido formulado na inicial, e prejudicado o agravo interno interposto, declarando legítima a determinação do Conselho Nacional de Justiça de que devem ser publicados nos sítios eletrônicos do Poder Judiciário a remuneração e proventos percebidos por todos os membros e servidores ativos, inativos, pensionistas e colaboradores do órgão, incluindo-se as indenizações e outros valores pagos a qualquer título, bem como os descontos legais, com **identificação individualizada e nominal do beneficiário e da unidade na qual efetivamente presta serviços, com detalhamento individual de cada uma das verbas pagas sob as rubricas** 'Remuneração Paradigma', 'Vantagens Pessoais', 'Indenizações', 'Vantagens Eventuais' e 'Gratificações', conforme quadro descrito no anexo da Resolução CNJ n.º 215/2015. 21. Sem custas. Fixo os honorários em R$ 5.000,00 (cinco mil reais), na forma do art. 85, §8º, do CPC. Publique-se. Intimem-se. Brasília, 23 de agosto de 2018. Ao Nº 2.367, Relator: Ministro Luís Roberto Barroso julgamento em 13/03/2017, publicação em 28/08/2018, grifou-se).

Portanto, o problema central está na falta de uma regulamentação clara e específica para o tratamento de dados pessoais pelo setor público, o que gera insegurança jurídica e impede a aplicação eficaz da LGPD. Além disso, é fundamental garantir um equilíbrio entre transparência governamental e a proteção da privacidade, de modo a não comprometer a confiança pública e a segurança jurídica no tratamento de dados pessoais pelo setor público.

5 COMPARTILHAMENTO DE DADOS PELO PODER PÚBLICO E PARÂMETROS CONSTITUCIONAIS: ANÁLISE DA ADI 6649, MP 954/2020 E ADPF 695

O Decreto nº 10.046/2019 estabeleceu normas secundárias para a governança do compartilhamento de dados no âmbito da administração pública federal, instituindo o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Seu objetivo era integrar bases de dados preexistentes, com vistas à eficiência administrativa e à prevenção de fraudes. No

entanto, sua edição provocou intenso debate constitucional, sobretudo em razão dos potenciais impactos à autodeterminação informativa[23] e à proteção de dados pessoais (Gonçalves, 2019).

Entretanto, a recepção normativa do Decreto não se deu sem controvérsias. Apesar das justificativas pautadas na eficiência administrativa, a norma foi objeto de questionamento por seu potencial de permitir práticas de tratamento de dados incompatíveis com o arcabouço constitucional, especialmente diante da Emenda Constitucional nº 115/2022, que introduziu expressamente o direito fundamental à proteção de dados pessoais no texto constitucional.

Nesse contexto, foi ajuizada a Ação Direta de Inconstitucionalidade n.º 6649, pelo Conselho Federal da Ordem dos Advogados do Brasil, com fundamento na violação de princípios constitucionais como a dignidade da pessoa humana (artigo, 1º, inciso, III, da Constituição Federal), a inviolabilidade da intimidade e da privacidade (artigo, 5º, inciso X, da Constituição Federal) e o sigilo de dados (artigo, 5º, inciso XII, da Constituição Federal).

Segundo as informações prestadas pela Presidência da República no julgamento da ADI 6649:

> O Decreto n. 10.046/2019 permite a gestão e o uso de dados já gerados nos sistemas da Administração Pública Federal de forma a garantir qualidade da informação, com o uso da tecnologia para promover eficiência nos processos, bem como **garantir a segurança da informação através de critérios previstos pelo próprio decreto e com base na Lei Geral de Proteção de Dados** (p. 75).

Adicionalmente, ressaltou-se que:

> Tendo em vista a pluralidade de bases de dados já custodiadas pelo Estado, é crucial a interoperabilidade entre elas para fins, dentre outros, de **cruzamento dos dados nela existentes**. Frequentemente, tais dados se referem à mesma pessoa física ou jurídica, mas revelam informações contraditórias. Com isso, é inviabilizado o acesso a serviços públicos a cidadãos que fariam jus a benefícios. **Analogamente, essa inconsistência poderia implicar a concessão de acesso a pessoas que, por sua vez, não estariam legalmente habilitadas** (p. 75).

O Ministro Presidente Luiz Fux enfatizou que:

> Com a emergência da orientação jurisprudencial do STF no sentido de considerar autônomo o direito fundamental à proteção de dados e à autodeterminação informativa e, posteriormente, com a inclusão no rol de direitos e garantias individuais do art. 5º, inciso LXXIX, da Constituição da República, a discussão referente aos supracitados direitos de personalidade merece escopo de análise mais restrito (p. 140).

[23] Segundo a professora Laura Schertel Mendes, é decisivo para a concepção do direito à autodeterminação: o princípio segundo o qual não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado dos danos, de modo que o risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados mesmos (ou no fato que quão sensíveis ou íntimos eles são) (Mendes, 2020).

Em sua fundamentação, destacou a necessidade de um controle rigoroso sobre o compartilhamento de dados entre órgãos da administração pública, enfatizando que tal prática deve observar critérios estritos de legalidade, necessidade e proporcionalidade, conforme disposto na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Além da análise jurídica nacional, o julgamento também trouxe contribuições do direito comparado. A Ministra Rosa Weber, em seu voto (p. 310), mencionou o *only-once principle* (*OOP*), adotado por diversos países europeus e pela OCDE, segundo o qual os cidadãos não devem ser obrigados a fornecer as mesmas informações a diferentes órgãos públicos. Quando aplicado corretamente, esse princípio tem o potencial de transformar profundamente o funcionamento da máquina pública. Sua implementação exige, porém, mecanismos robustos de identidade e interoperabilidade, inserindo-se em uma lógica mais ampla de transformação digital do Estado, por meio do modelo de *Governo como Plataforma* (*GaaP*).[24] Além disso, a aplicação do OOP no Brasil demandaria a integração de diferentes plataformas governamentais, com foco na proteção e segurança dos dados, conforme as diretrizes da Lei Geral de Proteção de Dados Pessoais (LGPD). Essa mudança exigiria um esforço significativo de adaptação das estruturas governamentais, mas teria o potencial de otimizar a gestão pública, tornando-a mais eficiente e menos burocrática, sem comprometer os direitos fundamentais dos cidadãos.

Complementando a análise internacional, o Ministro Fux também trouxe à baila experiências do Reino Unido, destacando que *"os obstáculos são parcialmente jurídicos e parcialmente não jurídicos. Entre os fatores legais, a insegurança é usualmente identificada como o principal obstáculo, impedindo órgãos públicos de compartilharem dados"* (STF, ADI nº 6649, Rel. Min. Gilmar Mendes, voto do Min. Fux, p. 159, 2022). Essas referências revelam que, embora a digitalização possa promover maior eficiência governamental, sua concretização exige a criação de marcos normativos sólidos que garantam a efetiva proteção dos direitos fundamentais (Law commission, 2014, p. 5–7).

[24] Tradução livre de RASHID (2020, p. 2): "Quando bem implementada, a OOP tem o potencial de transformar fundamentalmente as operações governamentais. Isso porque a implementação da OOP exige o desenvolvimento e o uso de seus elementos subjacentes — mecanismos de identidade e de compartilhamento de dados — em múltiplas camadas do governo. Subsequentemente, esses elementos podem ser aproveitados para diversos outros fins. Assim, a OOP não é uma política isolada, mas se encaixa em uma discussão mais ampla sobre a digitalização do governo, particularmente o Governo como Plataforma (GaaP). Na verdade, embora a OOP seja frequentemente apresentada ao público como centrada no usuário, ela também pode ser uma forma de ajudar os governos a fazer a transição para o GaaP. O GaaP é considerado a base para os serviços públicos de próxima geração e vai muito além da simples digitalização. Em vez de apenas alterar o meio principal de interface entre governo e cidadãos, do papel para o digital, o GaaP busca transformar o propósito fundamental do governo de um sistema que entrega resultados em troca de insumos para um 'articulador e facilitador' e um 'instrumento de coordenação da ação coletiva dos cidadãos'."

Importa observar que, à época da edição do Decreto 10.046/2019, a Autoridade Nacional de Proteção de Dados (ANPD) ainda não exercia plenamente suas competências normativas e fiscalizatórias, o que agravou o cenário de incerteza jurídica quanto aos parâmetros de compartilhamento de dados entre órgãos públicos.

A ausência de regulamentação específica permitiu interpretações amplas sobre os limites e finalidades do tratamento, especialmente à luz do artigo 23 da LGPD, cujo §1º estabelece, de maneira genérica, que o tratamento de dados pelo poder público deve atender à sua finalidade pública e à persecução do interesse público.

Diante disso, o STF impõe interpretação conforme à Constituição ao Decreto 10.046/2019, evitando sua nulidade integral, mas condicionando sua aplicação à observância do regime constitucional de proteção de dados. [25] Para tanto, determinou que o compartilhamento de dados entre os órgãos e entidades da Administração Pública deve respeitar os direitos fundamentais à intimidade e à vida privada (artigo 5º, X, da Constituição Federal) e o princípio da dignidade da pessoa humana (artigo 1º, III, da Constituição Federal).

Além disso, a Corte exigiu que a aplicação do Decreto esteja em consonância com os princípios da finalidade, necessidade, proporcionalidade e publicidade, nos termos dos arts. 6º, 7º, 21 e 23 da LGPD. Também foi fixado que a motivação dos atos administrativos envolvendo o tratamento de dados deve ser clara e acessível ao cidadão, assegurando-se a autodeterminação informativa e o controle social.

A ADI 6649 tornou-se marco no debate sobre a interoperabilidade estatal e os direitos à privacidade e autodeterminação informativa, ressaltando a centralidade do princípio da proporcionalidade e segurança informacional. A decisão reforça a centralidade da proporcionalidade como critério de conformação das políticas públicas na era digital.[26]

Esse cenário mudou de forma significativa com o julgamento conjunto das ADI 6387, ADI 6388, ADI 6389, ADI 6390 e ADI 6393 que tem por objeto a Medida Provisória

[25] Segundo a professora Laura Schertel Mendes, a relevância da proteção de dados pessoais "reside menos nos dados em si, mas no processo de coleta, armazenamento, utilização ou transferência, a partir do qual são extraídas informações pessoais a serem utilizadas em um determinado contexto para determinados fins" (Mendes, 2022).
[26] Segundo Danilo Doneda, "sem perder de vista que o controle sobre a informação foi sempre um elemento essencial na definição de poderes dentro de uma sociedade, a tecnologia proporcionou a intensificação dos fluxos de informação e, consequentemente, a multiplicação de suas fontes e de seus destinatários" (Doneda, 2006).

954/2020,[27] em que no contexto da pandemia, determinou o compartilhamento de dados de consumidores de telecomunicações com o IBGE para pesquisas não presenciais.[28]

A medida gerou grande controvérsia e foi contestada pelas mencionadas ADIS que alegaram violação ao sigilo e ao direito à privacidade. A controvérsia sobre o tratamento de dados pessoais pelo poder público ganhou destaque com a edição de um Decreto que autorizava o amplo compartilhamento de bases de dados entre órgãos da administração federal.

Em decisão proferida antes das ADIs sob relatoria do Ministro Gilmar Mendes, o STF declarou a inconstitucionalidade do Decreto, reconhecendo sua incompatibilidade com os direitos fundamentais à privacidade e à proteção de dados. A Corte abordou expressamente a ilicitude da alteração da finalidade para a qual os dados foram inicialmente coletados, apontando que o redirecionamento de uso sem base legal clara ou consentimento viola o princípio da finalidade e compromete a confiança dos cidadãos na atuação estatal.

Trata-se de um julgado paradigmático, por reconhecer a autodeterminação informativa como um direito fundamental autônomo, ainda que implícito na Constituição, afirmando a centralidade dos princípios da necessidade, adequação e proporcionalidade[29] no tratamento de dados pelo Estado.

Posteriormente, no julgamento da ADPF 695, o Supremo voltou a enfrentar a problemática da mudança de finalidade, envolvendo o compartilhamento de dados do Departamento Nacional de Trânsito (Denatran) com a Agência Brasileira de Inteligência (ABIN), em desacordo com a finalidade originalmente consentida. O Ministro Gilmar Mendes destacou a necessidade de mecanismos de controle das finalidades do compartilhamento, reiterando a centralidade dos princípios constitucionais no uso de dados pessoais.

Esses julgados revelam uma crescente sensibilidade do STF quanto à necessidade de um controle rigoroso sobre o tratamento de dados pessoais pelo Estado. Nesse cenário, o

---

[27] A Medida Provisória estabeleceu que os dados seriam usados exclusivamente para a produção de estatísticas oficiais, com a manutenção do sigilo, proibiu seu compartilhamento com terceiros, impôs obrigações de transparência no tratamento dos dados e determinou a exclusão dessas informações das bases do IBGE assim que a emergência de saúde pública fosse resolvida.

[28] Conforme indicado pelo Informativo 976 do STF, o § 1º do artigo 2º da MP 954/2020 estabeleceu que os dados seriam usados exclusivamente pelo IBGE para a produção de estatísticas oficiais, sem definir claramente a finalidade e os parâmetros dessa utilização, o que gerou questionamentos sobre a compatibilidade e a necessidade do tratamento dos dados. O STF destacou a ausência de critérios claros sobre a finalidade do compartilhamento de dados e a falta de uma base legal específica, violando princípios constitucionais relacionados à proteção de dados pessoais (STF, 2020).

[29] Alan Westin, professor da Universidade de Columbia, identificou a relação entre a privacidade e o desenvolvimento da autonomia e do sentido de livre-arbítrio como requisitos necessários para a construção de uma sociedade democrática (Ferreira, 2019).

princípio da finalidade[30] — consagrado na LGPD e na doutrina nacional e internacional — assume papel estruturante, funcionando como parâmetro de legitimidade do uso de dados pessoais no setor público. Ao lado dele, o teste de proporcionalidade[31] surge como ferramenta indispensável para compatibilizar o interesse público com os direitos fundamentais, assegurando que o compartilhamento de dados se dê dentro de balizas claras, transparentes e constitucionalmente adequadas (Wimmer, 2021).

A proteção de dados pessoais no setor público não pode se limitar à mera existência de normas, exigindo, sobretudo, segurança jurídica clara e efetiva para que o compartilhamento de informações não comprometa direitos fundamentais. O STF, ao delimitar balizas constitucionais e reconhecer a autodeterminação informativa, tem pavimentado um caminho indispensável para a governança estatal de dados, mas a efetividade dessa jurisprudência depende da atuação firme da ANPD e da criação de regulamentações específicas que contemplem as peculiaridades do setor público. Sem essas medidas concretas, o risco de violações e insegurança jurídica continuará a frear a inovação administrativa e a desconfiança social, comprometendo a legitimidade democrática.

6 CONCLUSÃO

A proteção de dados pessoais no setor público brasileiro é um tema de grande relevância no contexto atual, marcado por intensos debates sobre o papel do Estado e suas responsabilidades na era digital. Embora a LGPD represente um marco normativo relevante, o trabalho demonstrou que sua aplicação ao setor público ainda se revela deficitária, especialmente diante da ausência de diretrizes específicas e uniformes que orientem o tratamento e o compartilhamento de dados pelos entes estatais.

A análise da legislação, dos princípios fundamentais e da jurisprudência constitucional evidenciou que, mesmo após o reconhecimento do direito à proteção de dados como direito fundamental pela Emenda Constitucional nº 115/2022, persistem lacunas regulatórias que colocam em risco a efetividade dessa garantia. A margem interpretativa excessiva deixada ao

[30] Art. 6º inciso I da LGPD: "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades." (Grifou-se).

[31] O teste da proporcionalidade é um critério metodológico essencial para justificar medidas que impactam direitos fundamentais. A aplicação adequada desse teste permite uma argumentação mais objetiva e racional nas decisões judiciais, promovendo segurança jurídica e proteção equilibrada dos direitos (Gavião Filho; 2022).

poder público, notadamente no artigo 23 da LGPD, e a indefinição sobre os contornos da finalidade pública e do interesse público legítimo, geram insegurança jurídica e dificultam a conformidade institucional.

As decisões proferidas pelo Supremo Tribunal Federal — especialmente a ADI 6649, que inaugurou a compreensão da autodeterminação informativa como direito autônomo implícito na Constituição — e, posteriormente, a ADPF 695 e a análise da constitucionalidade da MP 954/2020, demonstram a sensibilidade do Judiciário à matéria. No entanto, esses julgados também evidenciam a fragilidade da estrutura normativa voltada ao tratamento de dados na Administração Pública. Sem balizas claras e orientações coesas, os órgãos estatais enfrentam dificuldades práticas para compatibilizar eficiência administrativa e proteção de dados, comprometendo tanto a segurança jurídica quanto os direitos dos titulares.

Nesse cenário, torna-se evidente que a Autoridade Nacional de Proteção de Dados (ANPD) deve exercer papel central na construção de uma governança pública[32] de dados pessoais que seja coerente e acessível. A solução não está necessariamente na criação de novas normas, mas na articulação, consolidação e unificação das diretrizes já existentes, com vistas a garantir interpretação uniforme e aplicação segura da LGPD no setor público.

Essa unificação normativa pode assumir a forma de instrumentos orientadores de aplicação coordenada da legislação vigente, como guias técnicos, recomendações vinculantes, pareceres de referência e diretrizes consolidadas, a partir de uma leitura sistemática do artigo 23 da LGPD e dos princípios que a fundamentam. O foco deve estar na delimitação de parâmetros para o compartilhamento de dados, na definição clara de finalidades legítimas e na harmonização entre transparência e proteção de dados.

Além disso, é desejável que esse processo de consolidação seja construído de forma participativa, envolvendo gestores públicos, especialistas e sociedade civil, a fim de garantir legitimidade técnica e funcionalidade prática. A atuação da ANPD, nesse sentido, deve ser pedagógica e coordenadora, promovendo um ambiente institucional de confiança, previsibilidade e respeito aos direitos fundamentais.

[32] A governança pública de dados pessoais envolve a definição clara das funções e responsabilidades dos agentes de tratamento — como o controlador e o operador —, além da adoção de padrões mínimos de transparência, segurança e prestação de contas. No setor público, essa governança deve garantir a conformidade com a LGPD sem comprometer a eficiência administrativa, o que exige atuação articulada entre os órgãos estatais. À ANPD cabe o papel estratégico de orientar essa estrutura, promovendo diretrizes técnicas que assegurem a uniformidade interpretativa e a proteção efetiva dos direitos dos titulares.

REFERÊNCIAS

ALEXY, Robert. Teoria dos Direitos Fundamentais. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2015.

ANEEL. Regulação responsiva. Bibliografia temática, v. 5, n. 3, jun. 2023. Agência Nacional de Energia Elétrica.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Tratamento de dados pessoais pelo Poder Público: guia orientativo*. Versão 2.0. Brasília, DF, jun. 2023. Elaborado por: Cristiane Landerdahl, Isabela Maiolino, Jeferson Dias Barbosa, Lucas Borges de Carvalho. Projeto gráfico e editoração: André Scofano. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_orientativo_tratamento_de_dados_pessoais_pelo_poder_publico. Acesso em: 28 maio 2025.

ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 3/2010 on the principle of accountability. Adotada em 13 de julho de 2010.

ÁVILA, Humberto. Teoria dos Princípios: da definição à aplicação dos princípios jurídicos. São Paulo: Malheiros, 2004.

BARCELLOS, Ana Paula de. Ponderação, racionalidade e atividade jurisdicional. Rio de Janeiro: Renovar, 2005.

BARROSO, Luís Roberto. A dignidade da pessoa humana no direito constitucional contemporâneo: a construção de um conceito jurídico à luz da jurisprudência mundial. Belo Horizonte: Fórum, 2016.

BESSA, Leonardo Roscoe. O consumidor e os limites dos bancos de dados de proteção ao crédito. São Paulo: Revista dos Tribunais, 2003.

BINENBOJM, Gustavo. Ainda a supremacia do interesse público. Revista da EMERJ, v. 21, n. 3, tomo 1, p. 236-240, set./dez. 2019b. Disponível em: https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista_v21_n3/tomo1/revista_v21_n3_tomo1_236.pdf. Acesso em: 6 abr. 2025.

BINENBOJM, Gustavo. Ainda a supremacia do interesse público. Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro - PGE-RJ, v. 2, n. 2, p. 11-20.

BINENBOJM, Gustavo. Da supremacia do interesse público ao dever de proporcionalidade: um novo paradigma para o direito administrativo. In: SARMENTO, Daniel; BINENBOJM, Gustavo (org.). Direitos fundamentais, democracia e administração pública. Rio de Janeiro: Lumen Juris, 2019a.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BOURDIEU, Pierre. A produção da crença: contribuição para uma economia dos bens simbólicos. São Paulo: Zouk, 2. ed., 2004.

BRASIL. COMISSÃO EUROPEIA. Adequacy of the protection of personal data in non-EU countries. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en. Acesso em: 6 nov. 2024.

BRASIL. Supremo Tribunal Federal. ADI 6649/DF. Relator: Min. Gilmar Mendes. Julgamento em 15 set. 2022. Publicação em 19 jun. 2023. Tribunal Pleno. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false. Acesso em: 15 maio 2025.

BRASIL. Supremo Tribunal Federal. Guia rápido: Semana de Proteção de Dados. Brasília: STF, Secretaria de Relações com a Sociedade; Encarregado de Proteção de Dados, 2024.

BRASIL. Supremo Tribunal Federal. *Nome do processo* (ADPF 186). Relator: Min. Ricardo Lewandowski. Julgado em 26 abr. 2012. Disponível em: https://www.stf.jus.br. Acesso em: 18 maio 2025.

LANDERDAHL, Cristiane; MAIOLINO, Isabela; BARBOSA, Jeferson Dias; CARVALHO, Lucas Borges de. Brasília, DF: 2023.

CANOTILHO, J. J. Gomes; MACHADO, Jónatas E. M. "Reality Shows" e liberdade de programação. Coimbra: Coimbra Editora, 2003.

CARVALHO, Laura B. A LGPD e o acesso à informação pública: dado pessoal e dado sigiloso? Portal Jota, 16 dez. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-informacao-publica-16122020. Acesso em: mar. 2025.

COUTINHO, Diogo R. O direito nas políticas públicas. Disponível em: http://www.fd.unb.br/images/PosGraduacao/Processo_Seletivo/Processo_Seletivo_2016/Prova_de_Conteudo/14_05_12_15O_direito_nas_politicas_publicas_FINAL.pdf. Acesso em: 6 abr. 2025.

DALLARI, Dalmo de Abreu. O Habeas Data no sistema jurídico brasileiro. Seminário sobre Acción de Amparo y Habeas Data, Universidad de Talca, Chile, abr. 1997. Atualizado em jul. 2002.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. Da privacidade e a proteção dos dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo. From privacy to the protection of personal data. Rio de Janeiro: Renovar, 2019.

DONEDA, Danilo; VIOLA, Marcelo. Risco e informação pessoal: o princípio da finalidade e a proteção de dados no ordenamento brasileiro. Revista Brasileira de Risco e Seguro, v. 5, n. 10, p. 85-102, out. 2009/mar. 2010.

DWORKIN, Ronald. Taking Rights Seriously. Cambridge, Massachusetts: Harvard University Press, 1978.

FERREIRA, Lucia Maria Teixeira. Novas tecnologias, cidadania e o cuidado: premissas para a regulação jurídica da inteligência artificial. In: PEREIRA, Tania da Silva; OLIVEIRA, Guilherme de; COLTRO, Antônio Carlos Mathias (orgs.). Cuidado e cidadania: desafios e possibilidades. Rio de Janeiro: Editora GZ, 2019. p. 341-365.

FREITAS, Christiana Soares de. Mecanismos de dominação simbólica nas redes de participação política digital. In: SILVA, Sivaldo Pereira da; BRAGATTO, Rachel Callai; SAMPAIO, Rafael Cardoso (orgs.). Democracia digital, comunicação política e redes: teoria e prática. Rio de Janeiro: Folio Digital: Letra e Imagem, 2016. p. 110-135.

GALLARDO GUERRA, Miguel; RIVERO PRADO, Samuel Uziel. What is a risk-based approach? Bello, Gallardo, Bonequi y García (BGBG), 7 out. 2021. Disponível em: https://www.ibanet.org/Oct-21-risk-based-approach. Acesso em: 18 abr. 2025.

GONÇALVES, Tânia Carolina Nunes Machado. Gestão de dados pessoais e sensíveis pela administração pública federal: desafios, modelos e principais impactos com a nova lei. Brasília, 2019. Monografia (Graduação em Direito) — Universidade de Brasília.

LAW COMMISSION (Reino Unido). Data sharing between public bodies: a consultation paper. Consultation Paper nº 214, p. 5-7.

MARANHÃO, Juliana; CAMPOS, Renato. A divisão informacional de poderes e o Cadastro Base do Cidadão. Portal Jota, 18 out. 2019.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. Direitos Fundamentais & Justiça, v. 12, n. 39, p. 185-216, jul./dez. 2018. Disponível em: https://doi.org/10.30899/dfj.v12i39.655. Acesso em: abr. 2025.

MENDES, Laura Schertel. Privacidade, proteção de dados pessoais e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. Portal Jota, 10 maio 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecaode-dados-pessoais-10052020. Acesso em: fev. 2025.

MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito (no prelo).

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, v. 120, ano 27, p. 469-483.

MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (orgs.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021.

MENDES, Laura Schertel; MATTIUZZO, Mariana; FUJIMOTO, Mônica. In: MENDES, L. S.;

DONEDA, D.; SARLET, L. W.; RODRIGUES JR., O. L. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 428

NISSENBAUM, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press, 2010.

RASHID, Naeha. Deploying the Once-Only Policy: a privacy-enhancing guide for policymakers and civil society actors. Policy Briefs Series. Ash Center for Democratic Governance and Innovation, Harvard Kennedy School, nov. 2020. Disponível em: https://ash.harvard.edu/files/ash/files/deploying-once-only-policy.pdf. Acesso em: 6 abr. 2025.

SCHREIBER, Anderson. Direitos da personalidade. Rio de Janeiro: Atlas, 2011.

SIMITIS, Spiros. Reviewing Privacy in an Information Society. University of Pennsylvania Law Review, v. 135, mar. 1987.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. Harvard Law Review, v. 4, n. 5, p. 193–220, 15 dez. 1890. Disponível em: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em: 4 abr. 2025.

WIMMER, Miriam. A LGPD e o balé dos princípios: tensões e convergências na aplicação dos princípios de proteção de dados pessoais ao setor público. In: FRANCOSKI, Denise de Souza Luiz;
TASSO, Fernando Antonio (orgs.). A Lei Geral de Proteção de Dados Pessoais: aspectos práticos e teóricos relevantes no setor público e privado. São Paulo: Thomson Reuters Revista dos Tribunais, 2021. v. 1, p. 1-20, 178-182

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.