



Revista Eurolatinoamericana de Derecho Administrativo
ISSN: 2362-583X
editorial@unl.edu.ar
Universidad Nacional del Litoral
Argentina

FÁCIO, RAFAELLA NÁTALY
A transparência e o direito de acesso no tratamento de dados pessoais: considerações sobre intersecções entre Lei Geral de Proteção de Dados e Lei de Acesso à Informação no Brasil

Revista Eurolatinoamericana de Derecho Administrativo,
vol. 10, núm. 2, 13413, 2023, Julio-Diciembre
Universidad Nacional del Litoral
Santa Fe, Argentina

DOI: <https://doi.org/10.14409/redoeda.v10i2.13413>

Disponible en: <https://www.redalyc.org/articulo.oa?id=655978330007>

- Cómo citar el artículo
- Número completo
- Más información del artículo
- Página de la revista en redalyc.org

redalyc.org

Sistema de Información Científica Redalyc
Red de revistas científicas de Acceso Abierto diamante
Infraestructura abierta no comercial propiedad de la academia

REVISTA EUROLATINOAMERICANA DE DERECHO ADMINISTRATIVO

VOL. 10 | N.2 | JULIO/DICIEMBRE 2023 | ISSN 2362-583X



RED DOCENTE
EUROLATINOAMERICANA
DE DERECHO ADMINISTRATIVO



A transparência e o direito de acesso no tratamento de dados pessoais: considerações sobre intersecções entre Lei Geral de Proteção de Dados e Lei de Acesso à Informação no Brasil

Transparency and the Right of Access in Personal Data Processing: Considerations on Intersections between the Brazilian General Data Protection Law and the Access to Information Law

RAFAELLA NÁTALY FÁCIO ^{1, *}

¹ Universidade Federal do Paraná (Curitiba, Brasil)

rafaellafacio@gmail.com

<https://orcid.org/0000-0001-8580-1488>

Recibido el/Received: 27.08.2023 / 27 August 2023

Aprobado el/Approved: 19.11.2023 / 19 November 2023

RESUMO

O objetivo do presente trabalho é analisar a transparência e o direito de acesso no tratamento de dados pessoais a partir de considerações sobre as intersecções entre Lei Geral de Proteção de Dados (LGPD) e Lei de Acesso à Informação (LAI). O procedimento metodológico utilizado combinou as seguintes técnicas: raciocínio dedutivo, pesquisa qualitativa e revisão bibliográfica. As conclusões foram as seguintes: (1) Transparência, acesso e accountability no tratamento de dados pessoais têm elevada importância, seja porque não é possível interromper o fluxo informacional, mas apenas adequá-lo tornando-o transparente, seja porque esses são os antídotos aos diversos riscos inerentes à atividade de tratamento desenvolvida pelo Estado. (2) Para a efetivação do direito de acesso aos dados tratados pelo Estado, foram feitas proposições a respeito da abrangência do escopo

ABSTRACT

The objective of this paper is to analyze transparency and the right of access in the processing of personal data through considerations about the intersections between the General Data Protection Law (LGPD) and the Access to Information Law (LAI). The methodological approach employed combined the following techniques: deductive reasoning, qualitative research, and literature review. The conclusions drawn are as follows: (1) Transparency, access, and accountability in the processing of personal data hold significant importance, either because it is not possible to interrupt the flow of information but only adapt it to make it transparent, or because these are the antidotes to the various risks inherent in the data processing activities carried out by the State. (2) In order to effectively realize the right of access to data processed by the State, propositions were made regarding the scope of the right of access, as well as

Como citar este artículo | *How to cite this article:* FÁCIO, Rafaella Nátaly. A transparência e o direito de acesso no tratamento de dados pessoais: considerações sobre intersecções entre Lei Geral de Proteção de Dados e Lei de Acesso à Informação no Brasil. **Revista Eurolatinoamericana de Derecho Administrativo**, Santa Fe, vol. 10, n. 2, e247, jul./dic. 2023. DOI 10.14409/redoeda.v10i2.13413

* Mestra e Bacharela em Direito do Estado pela Universidade Federal do Paraná – UFPR (Curitiba, Brasil). Especialista em Direito Administrativo pelo Instituto de Direito Romeu Felipe Bacellar – IDRFB (Curitiba, Brasil). Membro do Instituto Paranaense de Direito Administrativo – IPDA. Advogada.



do direito de acesso, bem como sobre possíveis modulações do direito, de modo a manter a sua efetividade mesmo em casos de restrição. (3) Para que a LGPD não seja inadequadamente invocada como forma de restrição ao acesso às informações públicas determinado pela LAI, defendeu-se a necessidade de interpretação de ambas as legislações de acordo com seu ponto de convergência, bem como a utilização de critério adequado para selecionar e equilibrar os interesses em conflito.

Palavras-chave: tratamento de dados pessoais pelo Estado; proteção de dados pessoais; direito de acesso; transparência; *accountability*.

possible modulations of the right, to maintain its effectiveness even in cases of restriction. (3) To ensure that the LGPD is not improperly invoked as a means of restricting access to public information mandated by the LAI, it was argued for the need to interpret both legislations in accordance with their points of convergence, as well as the use of an appropriate criterion to select and balance conflicting interests.

Keywords: State processing of personal data; personal data protection; right of access; transparency; *accountability*.

SUMÁRIO

1. Introdução; 2. Transparência, acesso e *accountability* no tratamento de dados pessoais: conteúdo e contornos; 3. O direito de acesso pelo titular dos dados: proposições e modulação a partir da LGPD e da LAI; 4. LAI e LGPD: convergências e conflitos quanto à transparência de dados pessoais; 5. Conclusões; 6. Referências.

1. INTRODUÇÃO

Os desafios que se apresentam diante do aumento de tratamento de dados feito pelo Estado e as potenciais práticas de vigilância¹ dele decorrente causam dúvidas sobre a abordagem adequada de pesquisas que endereçam o tema. O foco de investigações poderia se voltar, por exemplo, para a limitação de quais dados podem ser coletados pelo Estado, de modo que todos os problemas subsequentes do tratamento seriam evitados. Essa não é, entretanto, a abordagem do presente trabalho, que parte da premissa de que é utópico pensar em extirpar a infraestrutura informativa das organizações sociais.² Conforme assinala Stefano Rodotà, o “empobrecimento dos fluxos de informação” ou um “corte na comunicação social” são medidas pouco efetivas.³

¹ Vigilância, no presente trabalho, é compreendida como a observação, o registro e a categorização de informação sobre pessoas, processos e instituições, o que envolve a coleta de informação, o seu armazenamento, análise e transmissão. (BALL, Kirstie; WEBSTER, Frank. *The Intensification of Surveillance*. In: BALL, Kirstie; WEBSTER, Frank (Eds.). **The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age**. London: Pluto Press, 2003, pp. 1-15. p. 1) É um conceito simples, mas empiricamente complexo porque envolve dinâmicas de poder. (WOOD, David; KONVITZ, Eli; BALL, Kirstie. *The Constant State of Emergency?: Surveillance after 9/11*. In: BALL, Kirstie; WEBSTER, Frank (Eds.). **The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age**. London: Pluto Press, 2003, pp. 137-150. p. 150)

² RODOTÀ, Stefano. **A vida na sociedade da vigilância: A privacidade hoje**. Renovar: Rio de Janeiro, 2008. p. 39. Chama-se a atenção para o fato de que afirmar ser impossível extirpar a infraestrutura da informação não equivale a entender que o avanço de determinadas tecnologias é inevitável, e que ele significa progresso. Nenhuma tecnologia é inevitável porque não é como um fenômeno natural irresistível, e mudança nem sempre é direcionada para progresso – o que quer se compreenda por isso. (VÉLIZ, Carissa. **Privacy is Power: why and how you should take back control of your data**. London: Bantam Press, 2020. p. 31-32)

³ RODOTÀ, Stefano. **A vida na sociedade da vigilância: A privacidade hoje**. Renovar: Rio de Janeiro, 2008. p. 58.



A utilização de dados (inclusive os pessoais) pelo Poder Público não é, em si mesma, um problema. É ela, inclusive, que torna possível o planejamento administrativo,⁴ pois é indispensável a reunião de elementos para preparação e gestão de programas de intervenção,⁵ e pode criar oportunidades para setores tradicionais da atividade econômica e social, tais como transporte, saúde, educação, agroindústria e segurança.⁶ Por isso, a presente pesquisa parte do pressuposto de que para a proteção de dados pessoais não é necessária a interrupção do fluxo de dados, mas, sim, a sua adequação.

A adequação do fluxo de dados está diretamente relacionada à transparência no seu tratamento. São diversos os riscos decorrentes da vigilância estatal: controle da conformidade dos cidadãos à gestão política dominante;⁷ a “classificação social” (“*social sorting*”) para promover discriminação ou reproduzir e reforçar divisões sociais, econômicas e culturais;⁸ proporciona o acúmulo assimétrico de conhecimento, o que leva ao exercício desproporcional de poder;⁹ ainda, do ponto de vista da psicologia social sobre vigilância e suas implicações na identidade e no “eu”, o controle exercido por meio da gestão de dados pessoais pode assentar obstáculos reais ao livre desenvolvimento da personalidade individual.¹⁰

O antídoto contra todos esses riscos é o aumento da transparência para fins de propiciar um espaço de confiança, mutualidade e controle.¹¹ Danilo Doneda destaca os benefícios da gestão de dados pelo Estado, mas ressalva que tal atividade deve ser

⁴ DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2020. p. 26.

⁵ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: A privacidade hoje. Renovar: Rio de Janeiro, 2008. p. 28.

⁶ BELLOCHIO, Lucía. Big Data in the Public Sector. **A&C – Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 18, n. 72, pp. 13-29, abr./jun. 2018. p. 16. A importância da informação para a formulação das políticas públicas de modo eficiente é sintetizada por Maria Paula Dallari Bucci: “A gestão pública mais moderna no mundo desenvolvido há muito tempo deixou de privilegiar os ritos e as regras administrativas, em favor do resultado da ação, por meio dos chamados indicadores de desempenho, elementos quantitativos, fixados, evidentemente, com base em parâmetros qualitativos. Quantos beneficiários, com que perfil social, a que custo e em que prazo são informações absolutamente relevantes para qualificar a ação administrativa. Essas informações também são importantes para valorar a conduta do gestor público no que diz respeito ao significado político e social de suas ações e para informar o estabelecimento de prioridades.” (BUCCI, Maria Paula Dallari. **Fundamentos para uma teoria jurídica das políticas públicas**. São Paulo: Saraiva, 2013. p. 180)

⁷ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: A privacidade hoje. Renovar: Rio de Janeiro, 2008. p. 28.

⁸ LYON, David. Surveillance after September 11, 2001. In: BALL, Kirstie; WEBSTER, Frank (Eds.). **The Intensification of Surveillance**: Crime, Terrorism and Warfare in the Information Age. London: Pluto Press, 2003, pp. 16-25. p. 22.

⁹ VÉLIZ, Carissa. **Privacy is Power**: why and how you should take back control of your data. London: Bantam Press, 2020. p. 31.

¹⁰ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: A privacidade hoje. Renovar: Rio de Janeiro, 2008. p. 83; BALL, Kirstie; WEBSTER, Frank. The Intensification of Surveillance. In: BALL, Kirstie; WEBSTER, Frank (Eds.). **The Intensification of Surveillance**: Crime, Terrorism and Warfare in the Information Age. London: Pluto Press, 2003, pp. 1-15. p. 14.

¹¹ GUEDES, Luciana Kellen Santos Pereira; FARIA, Edimir Ferreira de. O aparente controle social no âmbito da Administração Pública brasileira. **A&C – Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 21, n. 86, p. 249-274, out./dez. 2021. DOI: 10.21056/aec.v21i83.1353.



fiscalizada por instrumentos regulatórios que possibilitem aos cidadãos efetivo controle em relação aos seus dados pessoais, garantindo-lhes o acesso, a veracidade, a segurança, o conhecimento da finalidade para a qual seus dados serão utilizados, entre outras garantias.¹² David Lyon, no mesmo sentido, defende que atualmente se reclama mais que nunca *accountability*, escrutínio democrático e ético dos sistemas de vigilância.¹³

Ademais, segundo a adequada noção de proteção de dados pessoais, ela envolve não apenas o direito de cada sujeito controlar os seus próprios dados, senão a suscetibilidade do tratamento ao controle de forma ampla,¹⁴ de modo a equilibrar poderes, reduzir a assimetria de informações, bem como promover a transparência e *accountability*.¹⁵ Para Rodotà, é de fulcral importância partir da consideração de que a nossa sociedade é cada vez mais baseada na acumulação e circulação de informações, o que culmina no estabelecimento de novas situações de poder. Surge, então, o problema da legitimação desse poder fundado na informação. E, segundo o autor, para legitimar esse tipo de poder não basta identificar o núcleo duro da privacidade e assegurar a sua proteção, mas são necessárias diversas medidas relacionadas à publicidade e circulação, no sentido de que a atenção deve ser deslocada do sigilo para o controle e equilíbrio de poderes.¹⁶ Segundo Helen Nissenbaum, a proteção de dados pessoais não é um direito ao segredo e nem ao controle de suas informações, senão direito a um apropriado fluxo de dados pessoais.¹⁷ E para Eneida Desiree Salgado e Vitoria Hiromi Saito, privacidade não significa defender o fim da coleta de dados pessoais, mas, sim, exigir maiores níveis de *accountability* dos agentes de tratamentos de dados.¹⁸

A inevitabilidade do fluxo informacional, o antídoto aos riscos inerentes ao tratamento de dados e a adequada concepção do que é a proteção de dados pessoais

¹² DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2020. p. 26.

¹³ LYON, David. Surveillance after September 11, 2001. In: BALL, Kirstie; WEBSTER, Frank (Eds.). **The Intensification of Surveillance**: Crime, Terrorism and Warfare in the Information Age. London: Pluto Press, 2003, pp. 16-25. p. 22 e 24.

¹⁴ DOMÍNGUEZ ÁLVAREZ, José Luis. Public administration's challenges in order to guarantee the fundamental right of personal data protection in the post-COVID-19 era. **Revista Eurolatinoamericana de Derecho Administrativo**, Santa Fe, vol. 7, n. 1, p. 167-191, ene./jun. 2020. DOI 10.14409/redeoda.v7i2.9551.

¹⁵ VALENCIA-TELLO, Diana Carolina. El control externo de la administración pública: análisis del caso brasileiro. **Revista de Direito Econômico e Socioambiental**, Curitiba, v. 13, n. 2, p. 276-301, maio/ago.2022. doi: 10.7213/revdireconsoc.v13i2.29872.

¹⁶ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: A privacidade hoje. Renovar: Rio de Janeiro, 2008. p. 36, 68 e 72.

¹⁷ NISSENBAUM, Helen. **Privacy in Context**: technology, policy, and the integrity of social life. Stanford: Stanford Law Books, 2009. p. 127.

¹⁸ SALGADO, Eneida Desiree; SAITO, Vitoria Hiromi. Privacidade e proteção de dados: por uma compreensão ampla do direito fundamental em face da sua multifuncionalidade. **International Journal of Digital Law**, Belo Horizonte, ano 1, n. 3. pp. 117-137, set./dez. 2020. p. 134.



apontam para a mesma conclusão: a transparência e *accountability* devem ser incrementados para que os poderes sejam equilibrados, e para que a assimetria de informações seja diminuída. Por essas razões, a presente pesquisa volta-se à incidência do princípio da transparência e do princípio do acesso pelo titular no tratamento de dados realizado pelo Estado.

2. TRANSPARÊNCIA, ACESSO E ACCOUNTABILITY NO TRATAMENTO DE DADOS PESSOAIS: CONTEÚDO E CONTORNOS

O princípio da transparência está previsto no artigo 6º, inciso VI da Lei Geral de Proteção de Dados (LGPD), que assim dispõe: “transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”. Ele revela que o direito à proteção de dados pessoais é mais amplo que a mera defesa contra a coleta ou tratamento indevidos, ou resguardo dos dados pessoais contra a sua divulgação.¹⁹ O direito à proteção de dados pessoais reclama que o seu tratamento seja feito de forma transparente.²⁰ Nesse aspecto se evidencia, mais uma vez, a diferença funcional entre os valores que estão implicados na concepção contemporânea de proteção de dados e aqueles tradicionalmente relacionados à proteção da privacidade: a prioridade não é retirar determinadas informações da esfera pública, senão promover o seu tratamento de forma adequada – ou seja, entre outros aspectos, transparente.²¹

O princípio da transparência está associado ao direito de livre acesso pelo titular, mas não se limita a ele. O livre acesso pelo titular consiste na “garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais” (artigo 6º, inciso IV da LGPD). O artigo 9º detalha quais são as informações às quais o titular tem acesso: finalidade específica do tratamento, forma e duração do tratamento, identificação e informações de contato do controlador, informações acerca do uso compartilhado de dados pelo controlador e a

¹⁹ PHILIPPI, Juliana Horn Machado. Transformação digital e urgência da cultura de dados na Administração Pública brasileira. **Revista Eurolatinoamericana de Derecho Administrativo**, Santa Fe, vol. 10, n. 1, e232, ene./jun. 2023. DOI: 10.14409/redoeda.v10i1.12401.

²⁰ MARTINS, Ricardo Marcondes. Proteção de dados, competências dos entes federativos e a Emenda Constitucional n. 115/22. **Revista de Investigações Constitucionais**, Curitiba, vol. 9, n. 3, p. 645-658, set./dez. 2022. DOI: 10.5380/rinc.v9i3.87107.

²¹ A LGPD já contém algumas disposições que contemplam esse dever de garantir o tratamento de modo transparente. A criação de uma autoridade nacional e independente, por exemplo, é uma delas. Para fins do objeto que é delimitado no presente trabalho, outras se destacam: o dever de informação, pelo Poder Público, sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas no tratamento de dados que é feito para o exercício de suas competências, preferencialmente em seus sítios eletrônicos (artigo 23, inciso I da LGPD); o dever de registro, pelo controlador e operador, das operações de tratamento de dados pessoais (artigo 37 da LGPD); dever de elaboração de relatório de impacto à proteção de dados pessoais (artigo 32 da LGPD); possibilidade de implementação, pelos controladores e operadores, de regras de boas práticas e de governança (artigo 50 da LGPD), entre diversas leituras que possam ser extraídas da referida legislação.



finalidade, responsabilidades dos agentes que realizarão o tratamento e os direitos do titular. O artigo 18, inciso II, dispõe que o acesso aos dados é um direito do titular.²² O artigo 19 prevê que o acesso será concedido mediante requisição.²³

O princípio de acesso é representativo de uma técnica jurídica que supera uma enunciação negativa e passiva da proteção de dados e passa a ser positiva e dinâmica. Ao invés de atribuir ao sujeito privado um direito acionável apenas depois de uma violação, a ele é concedido um poder de controle direto e contínuo sobre os coletores de informações. Assim, a técnica de proteção da privacidade se desloca para o bom funcionamento das regras sobre a circulação das informações.²⁴

O referido princípio é apontado como a principal garantia assegurada aos titulares de dados pessoais.²⁵ Ele é indispensável para que o titular dos dados: (i) acompanhe a utilização de suas informações; (ii) controle o fluxo informacional que lhe diga respeito; (iii) avalie eventuais inexistências ou uso indevido; (iv) realize o requerimento de encerramento do tratamento, se for o caso.²⁶ O controlador deve ser capaz de informar ao titular os tipos de dados que trata, com quem compartilha, suas respectivas identidades e para quais finalidades. Esse é o conjunto de informações que viabilizará ao titular a avaliação do processamento, se em conformidade ou não, o que significa que o titular de dados é parte relevante no processo de *accountability*. Nesse sentido, o direito de acesso integra a autodeterminação informativa, pois ele é o instrumento capaz de empoderar os titulares dos dados pessoais de modo a viabilizar a equalização das relações de poder e ampliar as possibilidades de controle.²⁷

Segundo Clèmerson Clève e Júlia Franzoni, *accountability* é um conceito relacional que tem dois lados: (i) a disponibilização de meios, dados e informações por parte do Poder Público, bem como a criação de procedimentos que permitam a participação dos

²² **Art. 18.** O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...) II - acesso aos dados;”

²³ **Art. 19.** A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:”

²⁴ RODOTÀ, Stefano. **A vida na sociedade da vigilância: A privacidade hoje.** Renovar: Rio de Janeiro, 2008. p. 60.

²⁵ SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais: pluralismo jurídico e transparência em perspectiva.** São Paulo: Revista dos Tribunais, 2020. Versão e-book, sem paginação, capítulo 6.

²⁶ VAINZOF, Rony. Comentários ao artigo 6º. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). **LGPD: Lei Geral de Proteção de Dados comentada.** São Paulo: Revista dos Tribunais, pp. 126-200. p. 137-138. O direito de acesso desponta como base para o desdobramento de outros direitos, tais como o direito de retificação, o direito de exclusão, o direito de revisão de decisões automatizadas e o direito à portabilidade. (SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais: pluralismo jurídico e transparência em perspectiva.** São Paulo: Revista dos Tribunais, 2020. Versão ebook sem paginação, capítulo 6)

²⁷ SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais: pluralismo jurídico e transparência em perspectiva.** São Paulo: Revista dos Tribunais, 2020. Versão ebook sem paginação, capítulo 6.



cidadãos na ação política e no controle de seus resultados; e (ii) estímulos para a transformação da postura passiva do cidadão em ativa. A *accountability*, portanto, “exige a operacionalização da razão prática supondo a transparência da Administração Pública e a vontade de inserção e envolvimento da sociedade.”²⁸

Considerando os múltiplos entendimentos e funções que podem ser atribuídos à *accountability*,²⁹ para a sua adequada apreensão no âmbito de tratamento de dados é útil a abordagem denominada *Privacy By Design (PbD)*. Segundo essa abordagem, a privacidade deve ser incorporada de forma integral nas prioridades das organizações, seus objetivos, desenhos de seus processos e projetos.³⁰ De acordo com uma concepção mais restrita da *PbD*, ela consiste em métodos para a incorporação de ferramentas tecnológicas de proteção de dados em sistema de tecnologia de informação.³¹ Considerando o escopo do presente trabalho, as menções à *PbD* são feitas considerando o seu sentido na concepção mais ampla.

Os princípios da *PbD* são um conjunto universal de estrutura ou conjunto de conceitos, práticas e ferramentas (“*framework*”), para uma proteção mais forte de privacidade,³² e são os seguintes: (i) proatividade e não reatividade, preventiva e não remediadora; (ii) privacidade como uma configuração padrão; (iii) a privacidade é incorporada ao desenho; (iv) promoção de funcionalidade completa, ou soma positiva ao invés de soma zero. (v) segurança de ponta a ponta, ou proteção do ciclo de vida completo; (vi) visibilidade, transparência e abertura; (vii) respeito pela privacidade do usuário, ou manter o usuário no centro.³³

Os autores Heike Felzmann, Eduard Fosch-Villaronga, Christoph Lutz e Aurelia Tamò-Larriex partem da mesma abordagem da *PbD* para propor a *Transparency by Design (TbD)*. Afinal de contas, a transparência é um elemento da proteção de dados

²⁸ CLÈVE, Clèmerson Merlin; FRANZONI, Júlia Ávila. Administração Pública e a nova Lei de Acesso à Informação. **Interesse Público - IP**, Belo Horizonte, ano 15, n. 79, pp. 1-23, mai./jun. 2013. p. 6.

²⁹ CRISTÓVAM, José Sérgio da Silva; BERGAMINI, José Carlos Loitey. A centralidade da noção de *accountability* como instrumento de concretização do modelo de Administração Pública sustentável. **A&C – Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 21, n. 84, p. 87-108, abr./jun. 2021. DOI: 10.21056/aec.v21i84.1372

³⁰ CAVOUKIAN, Ann. **Privacy by Design - The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices**. p. 2. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf>. Acesso em: 1 mar. 2023.

³¹ SCHAAR, Peter. *Privacy by Design. Identity in the Information Society*, [s.l.], vol. 3, pp. 267-274, 2010. p. 267. Segundo o autor, esse tipo de abordagem endereça especificamente os perigos escondidos em novos sistemas tecnológicos, e que são difíceis de serem superados depois que o *design* básico do sistema já foi estabelecido.

³² CAVOUKIAN, Ann. **Privacy by Design - The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices**. p. 2. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf>. Acesso em: 1 mar. 2023.

³³ CAVOUKIAN, Ann. **Privacy by Design - The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices**. p. 5. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf>. Acesso em: 1 mar. 2023.



ou da privacidade, como se viu. Eles partem de três conclusões principais da discussão sobre *PbD*: (i) as soluções práticas decorrentes de seus princípios resultaram em sua apreensão por algumas legislações, e se espera o mesmo das propostas da *TbD*; ³⁴ (ii) o objetivo da *TbD* também é o de enfrentar desafios para a efetiva governança que exsurtem da complexidade técnica e social da transparência em novas tecnologias;³⁵ (iii) assim como a *PbD*, é inerente à *TbD* a noção de equilíbrio ou soma positiva, no sentido de que a privacidade e transparência não são fatores limitadores, mas, sim, valores agregados.³⁶

A transparência, no âmbito do tratamento de dados, é um construto complexo: pode se referir à capacidade de explicação (“explicabilidade”), capacidade de interpretação, abertura, acessibilidade e visibilidade, entre outros aspectos. Ela não se resume à mera transferência de informações de um agente ao outro (perspectiva puramente informacional), não sem a atenção aos significados, valores e funções sociais associados a essa transferência. Além de a transparência ser uma virtude (ter a qualidade daquilo que é aberto etc.), ela também é relacional, no sentido de que não é uma característica individual, senão uma relação entre o agente e o destinatário, e também é sistêmica, no sentido de que leva em conta o contexto institucional no qual se insere.³⁷

Os desafios da transparência no âmbito de tratamento de dados são: (i) para que a divulgação de informação se transforme em transparência, é necessário adaptá-la às necessidades da audiência; (ii) o foco não deve ser apenas na disponibilização da informação, mas também na natureza e no contexto desta informação e o processo

³⁴ Um exemplo de incorporação, pela legislação do *PbD* é o artigo 25 do Regulamento Geral de Proteção de Dados da União Europeia (RGPD): “**Art. 25.** Data protection by design and by default. **1.** Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. **2.** The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. **3.** In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. **3.** An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.”

³⁵ Os autores abordam especificamente os desafios decorrentes da inteligência artificial.

³⁶ FELZMANN, Heike; FOSCH-VILLARONGA, Eduard; LUTZ, Christoph; TAMÒ-LARRIEUX, Aurelia. Towards Transparency by Design for Artificial Intelligence. *Sci Eng Ethics*, [s.l.], vol. 26, n. 6, pp. 3333-3361, dec. 2020. p. 3344.

³⁷ FELZMANN, Heike; FOSCH-VILLARONGA, Eduard; LUTZ, Christoph; TAMÒ-LARRIEUX, Aurelia. Towards Transparency by Design for Artificial Intelligence. *Sci Eng Ethics*, [s.l.], vol. 26, n. 6, pp. 3333-3361, dec. 2020. p. 3335- 3336.



de como a informação é obtida e disponibilizada.³⁸ A transformação de transparência em *accountability* depende do contexto institucional, estruturas de poder, demanda e pressão por *accountability*, entre outros fatores. Em síntese, se o público destinatário não puder tirar proveito das informações porque elas permanecem de difícil acesso, ou porque são apresentadas de maneira complexa e obscura, não há aumento de autonomia e controle. O desafio que se coloca, então, é a construção de novos modos de entrega de informações que são necessários para facilitar o aumento pretendido de autonomia e controle por meio da transparência.³⁹ A pergunta que a presente pesquisa pretende responder é: como efetivar a transparência e o direito de acesso no tratamento de dados, inclusive em atividades estatais que, por vezes, impõem medidas de sigilo? O questionamento será respondido à luz não apenas do que dispõe a LGPD, mas também à luz do arcabouço normativo que por excelência disciplina a transparência das atividades estatais: a Lei de Acesso à Informação (LAI).

3. O DIREITO DE ACESSO PELO TITULAR DOS DADOS: PROPOSIÇÕES E MODULAÇÃO A PARTIR DA LGPD E DA LAI

O direito de acesso consiste na “garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais” (artigo 6º, inciso IV da LGPD). Os elementos mínimos que integram o seu escopo estão elencados no artigo 9º da LGPD: finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e a finalidade; responsabilidades dos agentes que realizarão o tratamento; e direitos do titular.

O valor do direito de acesso consiste no fato de que ele renegou a impenetrabilidade das coletâneas de informações, tanto em mãos públicas quanto privadas, e também porque foi adotado um critério de controle difuso, exercido diretamente pelos interessados, e não confiado apenas a órgãos. Ele é visto com ceticismo, porém, por aqueles que apontam sua escassa funcionalidade, uma vez que os interessados fazem pouco uso do instrumento, e afirmam que ele se resumiria ao “direito de saber ter sido fichado”. Assim, há quem argumente que o direito de acesso não daria nenhum real poder de controle sobre as coletâneas de informações, cuja existência, aliás, ele acabaria por legitimar.⁴⁰

³⁸ FELZMANN, Heike; FOSCH-VILLARONGA, Eduard; LUTZ, Christoph; TAMÒ-LARRIEUX, Aurelia. Towards Transparency by Design for Artificial Intelligence. *Sci Eng Ethics*, [s.l.], vol. 26, n. 6, pp. 3333-3361, dec. 2020. p. 3339.

³⁹ FELZMANN, Heike; FOSCH-VILLARONGA, Eduard; LUTZ, Christoph; TAMÒ-LARRIEUX, Aurelia. Towards Transparency by Design for Artificial Intelligence. *Sci Eng Ethics*, [s.l.], vol. 26, n. 6, pp. 3333-3361, dec. 2020. p. 3341.

⁴⁰ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: A privacidade hoje. Renovar: Rio de Janeiro, 2008. p. 66-67.



O pouco uso do direito de acesso, entretanto, não pode ser considerado definitivo ou irrelevante. Em primeiro lugar, a forte reação de algumas organizações a esse direito, ainda que ele seja exercido de forma limitada, demonstra que elas não são indiferentes a esse instrumento. Independentemente do nível do seu exercício no caso concreto, é possível inferir que o seu reconhecimento formal induz o coletor de informação a se adequar espontaneamente às novas prescrições legislativas.⁴¹ Ademais, o direito do acesso é instrumental para garantir a efetividade de outros princípios (correção, exatidão ou finalidade),⁴² pois com o conhecimento a respeito dos dados que estão sendo tratados, o titular pode formular requerimentos e tomar providências.

Esse pouco uso do direito de acesso é atribuído aos seguintes fatores: pouca informação, custos do acesso (custo de tempo, dinheiro, entre outros), aderência de alfabetização, desnível de poder entre indivíduos e grandes burocracias públicas e privadas que detêm as informações, excesso de proibições de acesso a determinadas categorias de informações; e escassa relevância das informações fornecidas quando se ignora o funcionamento geral do sistema no qual estão inseridas. A efetividade do direito de acesso depende da possibilidade de superar esse conjunto de obstáculos,⁴³ bem como decorre da disponibilidade de um número mais amplo de informações sobre quem coleta os dados, e, principalmente, o direito de acesso confirma a sua tendência de ser um instrumento que torna a atividade de organismos públicos o mais transparente possível, de modo a efetivar institucionalmente as condições para um controle social difuso.⁴⁴ Considerando os obstáculos acima, algumas proposições serão feitas com o intuito de contribuir para a efetivação do direito de acesso.

Em primeiro lugar, quanto maior o nível de informações sobre o tratamento de dados, e quanto maior a sua complexidade, mais amplo e mais detalhado será o escopo do direito de acesso (primeira proposição). O art. 9º da LGPD elenca elementos mínimos e genéricos que integram o direito de acesso, como, por exemplo, “forma e duração do tratamento”. Se o tratamento envolve inúmeros agentes, órgãos, em múltiplas

⁴¹ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: A privacidade hoje. Renovar: Rio de Janeiro, 2008. p. 68.

⁴² RODOTÀ, Stefano. **A vida na sociedade da vigilância**: A privacidade hoje. Renovar: Rio de Janeiro, 2008. p. 60.

⁴³ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: A privacidade hoje. Renovar: Rio de Janeiro, 2008. p. 68. Stefano Rodotà propõe as possíveis linhas de intervenção, que, segundo o autor, podem ser sintetizadas como medidas de reforço da posição dos indivíduos, seja para tornar mais eficaz o acesso, seja para diminuir a assimetria de poder entre os indivíduos e detentores das informações. Para realizar esse objetivo, ele argumenta, é indispensável: (i) permitir um acesso “assistido” por especialistas, de modo a viabilizar não somente o conhecimento das informações pessoais referentes ao interessado, mas também os critérios utilizados para os tratamentos automáticos; (ii) reconhecer um direito de acesso individual “integrado” pela presença de um sujeito coletivo (sindicato, associação de direitos civis, entre outros). (iii) Esses sujeitos coletivos devem dispor, inclusive, de legitimação autônoma de acesso, ainda que essa dependa de consentimento do interessado, porque eles podem assumir, entre suas funções institucionais no exercício sistemático do direito de acesso, realizando, assim, um controle efetivo sobre os coletores de informações. (p. 68) Não serão essas, entretanto, as sugestões feitas no presente trabalho.

⁴⁴ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: A privacidade hoje. Renovar: Rio de Janeiro, 2008. p. 72.



operações, é necessário fornecer todas as informações disponíveis sobre ele. Informações genéricas ou que omitam outros eventuais elementos além daqueles arrolados no artigo 9º da LGPD descumprem os preceitos de *accountability* e *Transparency by Design* abordados no tópico anterior.

Em segundo lugar, nos casos nos quais não se aplica a LGPD em sua totalidade, como ocorre no tratamento de dados pessoais para fins de segurança pública, eventual sigilo não necessariamente implicará negativa completa do acesso. Caso não possa ser plenamente atendido, isto é, mediante fornecimento imediato de todas as informações, ele deverá ser respondido: (i) com a quantidade máxima de informações disponíveis; (ii) e assim que possível, ou seja, se não imediatamente, no futuro quando não mais recair sigilo sobre a informação. Desse modo, o direito de acesso deve ser respeitado mediante a disponibilização parcial dessas informações, e/ou adiamento do acesso às informações não divulgadas.⁴⁵ O franqueamento de acesso modulado, quando não seja possível disponibilizá-lo de forma completa, atende a outro princípio de proteção de dados: de necessidade, na medida em que a restrição só ocorrerá quando necessária para a realização de finalidade de segurança pública.

Para definir se a disponibilização parcial e/ou o adiamento do acesso deverá se dar na forma prevista pela Lei de Acesso à Informação (LAI) (hipóteses de sigilo, prazos e processo de classificação), é necessário esclarecer o seguinte questionamento: o “direito de acesso à informação” (artigo 5º, inciso XXXIII da Constituição) equivale ao “direito de acesso pelo titular” (decorrente do direito fundamental à proteção de dados, previsto no artigo 5º, inciso LXXIX)?

A pergunta pode começar a ser respondida a partir das considerações feitas pela doutrina especializada acerca do direito de acesso à informação (inciso XXXIII) e o direito de se informar (inciso XIV).⁴⁶ Segundo Ricardo Marcondes Martins, eles não se confundem. O autor sustenta que o último decorre do direito geral de liberdade como direito de defesa, que tem significado próximo à liberdade de informação jornalística, e compreende o direito de se inteirar de fatos em três desdobramentos: direito de informar, o direito de se informar e o direito de ser informado. Já o primeiro consiste no direito ao acesso à informação, direito à ação estatal positiva, de efetivo fornecimento dos dados.⁴⁷ Eneida Desiree Salgado, por outro lado, parte das noções de transparência ativa e da exigência de divulgação de dados a serem produzidos pelos agentes

⁴⁵ Essa abordagem está contemplada no Projeto de Lei n. 1515/2022: “**Art. 26.** A prestação de informações e a concessão e acesso a dados pode ser adiada, limitada ou recusada se e enquanto tal for necessário e proporcional para: (...)”. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2326300>. Acesso em: 3 mar. 2023.

⁴⁶ **Artigo 5º, “XIV** - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;”.

⁴⁷ MARTINS, Ricardo Marcondes. Direito fundamental de acesso à informação. **A&C – R. de Dir. Administrativo & Constitucional**, Belo Horizonte, ano 14, n. 56, pp. 127-146, abr./jun. 2014. p. 134.



públicos para sustentar a convergência entre ambos os direitos.⁴⁸ De todo modo, todos os direitos fundamentais têm tanto uma função de defesa quanto de prestação, portanto, esse não é o critério adotado no presente trabalho para fins de delimitar o âmbito de proteção de cada um deles. Concorde-se com a autora citada acima quanto à afinidade entre ambos os direitos, e que, por exemplo, apenas o direito de se informar (inciso XIV) já seria *substrato* suficiente para impor ao Poder Público deveres de transparência ativa e passiva, tanto na dimensão de defesa quanto na dimensão de prestação.

O direito de acesso, por sua vez, consiste na garantia do titular à “consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais”. Partindo das mesmas premissas de Eneida Desiree Salgado, trata-se de um direito com pontos de convergência com o direito de se informar (inciso XIV) na medida em que dispõe sobre a garantia de obter conhecimento sobre algo. Mas é possível afirmar que há uma identidade entre o direito de acesso à informação e o direito de acesso sobre tratamento de dados feito pelo Estado, para, então, concluir-se pela aplicação de disposições da LAI nesse último caso?

Segundo Bruno Bioni, Paula da Silva e Pedro Martins, o direito de acesso à informação previsto no artigo 5º, inciso XXXIII da Constituição se diferencia do direito do titular de acesso aos dados em vários aspectos: quanto aos fundamentos, quanto aos objetivos e quanto ao escopo. Em relação aos fundamentos, os do primeiro são o princípio da transparência e da privacidade, e o do segundo o direito à proteção de dados; em relação aos objetivos, o do primeiro é proporcionar a governança social e a fiscalização do Poder Público, e o do segundo é assegurar a autodeterminação informativa; por fim, em relação ao escopo, o do primeiro compreende as informações de caráter e interesse público, e o do segundo o acesso a dados pessoais do titular requerente.⁴⁹

Discorda-se dos autores em relação às diferenças delimitadas sobre os fundamentos, objetivos e escopos dos dois direitos de acesso. Em relação aos primeiros, os princípios da publicidade e da transparência também são fundamentos do direito de acesso pelo titular às informações sobre o tratamento feito pelo Poder Público. Em relação aos objetivos, o acesso aos dados também tem a finalidade de proporcionar a governança social e a fiscalização do Poder Público quando o tratamento é feito por ele; conforme exposto anteriormente, as atividades de tratamento de dados criam dinâmicas de poder, e este, por sua vez, deve ser controlado. Por fim, em relação ao escopo, o direito de acesso aos dados não recai apenas sobre dados pessoais sem qualquer caráter público, pois dados pessoais e seu tratamento não têm uma dimensão apenas privada,

⁴⁸ SALGADO, Eneida Desiree. **Lei de Acesso à Informação**: Lei 12.527/2011. São Paulo: Revista dos Tribunais, 2020. p. 27.

⁴⁹ BIONI, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. **Cadernos Técnicos da CGU**, Brasília, v. 1, pp. 8-19, 2022. p. 12 e 16.



mas também coletiva. Portanto, assim como há certa sobreposição entre o direito de se informar (inciso XIV) e o acesso à informação (inciso XXXIII), também há sobreposição entre o último e o direito de acesso que decorre do direito à proteção de dados pessoais (inciso LXXIX).⁵⁰

Há uma sobreposição, mas ela não é completa. É possível, portanto, que o acesso a uma informação seja restringido para o público no geral e que, ao mesmo tempo, ela se mantenha completamente acessível pelo seu titular. A lógica pode ser ilustrada com o seguinte exemplo: a divulgação de uma informação relacionada à segurança pública pode ser prejudicial se feita na ampla escala da LAI (que permite o acesso a ela por qualquer interessado, bem como a sua disponibilização em portais de transparência), mas o mesmo risco pode não se configurar se o acesso for franqueado apenas ao titular dos dados.

De todo modo, a sobreposição entre os dois tipos de acesso justifica a incidência das hipóteses de sigilo, prazos e processo de classificação previstas na LAI para fins de restrição ao direito de acesso à informações sobre tratamento de dados em hipóteses de sigilo. A Constituição brasileira contém uma expressa restrição ao acesso à informação nos casos em que o sigilo seja imprescindível para a segurança da sociedade e do Estado (artigo 5º, inciso XXXIII da Constituição), por exemplo.⁵¹ Isso significa que o próprio constituinte deixou consignado no sistema o resultado de sua ponderação no plano abstrato.⁵² A referida norma constitucional foi regulamentada pelo artigo 23

⁵⁰ ROBLES OSOLLO, Ana Gloria. El derecho a la privacidad y la protección de datos personales transfronterizos. **Revista Eurolatinoamericana de Derecho Administrativo**, Santa Fe, vol. 8, n. 1, p. 35-60, ene./jun. 2021. DOI 10.14409/reoedea.v8i1.9543.

⁵¹ **Artigo 5º, "XXXIII** - 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;". No mesmo sentido preveem o art. 19.3.b do Pacto Internacional sobre Direitos Civis e Políticos e artigo 13.2.b da Convenção Americana sobre Direitos Humanos:

"Artigo 19. 1. Ninguém poderá ser molestado por suas opiniões. **2.** Toda pessoa terá direito à liberdade de expressão; esse direito incluirá a liberdade de procurar, receber e difundir informações e idéias de qualquer natureza, independentemente de considerações de fronteiras, verbalmente ou por escrito, em forma impressa ou artística, ou por qualquer outro meio de sua escolha. **3.** O exercício do direito previsto no parágrafo 2 do presente artigo implicará deveres e responsabilidades especiais. Consequentemente, poderá estar sujeito a certas restrições, que devem, entretanto, ser expressamente previstas em lei e que se façam necessárias para: **a)** assegurar o respeito dos direitos e da reputação das demais pessoas; **b)** proteger a segurança nacional, a ordem, a saúde ou a moral públicas."

"Artigo 13. Liberdade de pensamento e de expressão. **1.** Toda pessoa tem direito à liberdade de pensamento e de expressão. Esse direito compreende a liberdade de buscar, receber e difundir informações e idéias de toda natureza, sem consideração de fronteiras, verbalmente ou por escrito, ou em forma impressa ou artística, ou por qualquer outro processo de sua escolha. **2.** O exercício do direito previsto no inciso precedente não pode estar sujeito a censura prévia, mas a responsabilidades ulteriores, que devem ser expressamente fixadas pela lei e ser necessárias para assegurar: **a.** o respeito aos direitos ou à reputação das demais pessoas; ou **b.** a proteção da segurança nacional, da ordem pública, ou da saúde ou da moral públicas.

⁵² MARTINS, Ricardo Marcondes. Direito fundamental de acesso à informação. **A&C – R. de Dir. Administrativo & Constitucional**, Belo Horizonte, ano 14, n. 56, pp. 127-146, abr./jun. 2014. p. 131.



da Lei de Acesso à Informação, que dispõe sobre as informações que são “consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação”.⁵³

Enfim, a proposta de segunda forma de efetivação do direito de acesso aos dados tratados pelo Estado: caso o pedido de acesso não possa ser plenamente atendido, isto é, mediante fornecimento imediato de todas as informações, ele deverá ser respondido com a quantidade máxima de informações disponíveis e assim que possível, bem como a restrição às informações só poderá ser da forma prescrita pela Lei de Acesso à Informação.

A terceira e quarta proposições para a efetivação do direito de acesso aos dados tratados para fins de segurança pública são as seguintes. Além de o titular poder formular pedido de acesso em relação aos seus próprios dados, terceiros podem formular pedidos de acesso à informação sobre atividades de tratamento, mesmo que não tenham seus dados envolvidos na operação. Ou seja, deve-se viabilizar o pedido de acesso a informações relacionadas às atividades de tratamento, sem, necessariamente, revelar os dados pessoais que estão sob ele (terceira proposição). E esse direito de acesso às informações sobre tratamento de dados que não dizem respeito aos do próprio solicitante se aplica também aos dados anônimos. Ambas serão justificadas conjuntamente a seguir (quarta proposição).

O direito de acesso até o presente momento foi abordado como a garantia do titular em requerer informações sobre o tratamento que é feito sobre os seus próprios dados, ou seja, por meio do acesso o requerente sabe quais dados estão sendo tratados e de que forma. Caso ele permaneça limitado a essa faculdade, o instrumento, fatalmente, estará condenado às mesmas limitações que acometem outros instrumentos de controle individualizados, tais como o consentimento. Há diversos fatores que influenciam o não exercício do direito de acesso pelo titular, como visto acima, então é necessário

⁵³ “**Art. 23.** São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam: **I** - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional; **II** - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais; **III** - pôr em risco a vida, a segurança ou a saúde da população; **IV** - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País; **V** - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas; **VI** - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional; **VII** - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou **VIII** - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.” A possibilidade de restrição de acesso à informação consta também na Política Nacional de Arquivos Públicos e Privados (Lei n. 8.159/1991): “**Art. 4º** - Todos têm direito a receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral, contidas em documentos de arquivos, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujos sigilo seja imprescindível à segurança da sociedade e do Estado, bem como à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.”



garantir que terceiros possam pedir informações sobre o tratamento de determinados dados, ainda que não sejam os seus próprios.

A proposta, entretanto, não é a de que terceiros possam acessar qualquer dado pessoal que esteja sendo tratado pelo Estado, afinal de contas, “não há razão de se divulgar dados relativos à vida privada e que não se apresentam como de interesse público”.⁵⁴ Será, então, um direito de acesso cujo escopo abrange informações mais genéricas, sobre a forma e duração do tratamento de determinado tipo de dado, e não sobre a integralidade dos dados tratados em si. Isso permitirá que uma quantidade maior de pessoas tenha acesso a informações relevantes e que promoverão a transparência do tratamento de dados no contexto geral no qual ele ocorre.

Em relação aos dados anonimizados, sabe-se que eles são considerados como dados pessoais caso sejam utilizados para a formação de perfis comportamentais (artigo 12, § 2º da LGPD).⁵⁵ Nesse caso persiste, então, o direito de o titular ter acesso às informações completas sobre o tratamento que é feito sobre seus dados, ainda que já anonimizados (quarta proposição).

Em relação aos dados anônimos, ainda que não sejam utilizados para a formação de perfis comportamentais, persiste o direito ao acesso de modo genérico, na forma delimitada pela terceira proposição feita acima. A legitimação para pedir informações não pessoais, tais como aquelas relacionadas ao tratamento automático de dados, pode ser atribuída a sujeitos interessados diferentes dos interessados diretos (isto é, aqueles que tiveram as suas informações coletadas), e sem a necessidade de autorização destes. O direito de acesso franqueado a esses sujeitos torna-se uma face dinâmica do direito à informação, que pode se concretizar por meio de iniciativa direta do indivíduo ou por meio de grupos, operando-se, então, uma forma de redistribuição de poder.⁵⁶

4. LAI E LGPD: CONVERGÊNCIAS E CONFLITOS QUANTO À TRANSPARÊNCIA DE DADOS PESSOAIS

A Lei de Acesso à Informação regula o “direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral” (artigo 5º, inciso XXXIII da Constituição). Trata-se de uma legislação bastante esperada e celebrada no contexto brasileiro de democratização. Segundo Clèmerson Clève e Júlia Franzoni, um

⁵⁴ BIONI, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. *Cadernos Técnicos da CGU*, Brasília, v. 1, pp. 8-19, 2022. p. 12.

⁵⁵ “**Art. 12.** Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. (...) § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.”

⁵⁶ RODOTÁ, Stefano. *A vida na sociedade da vigilância*: A privacidade hoje. Renovar: Rio de Janeiro, 2008. p. 72-73.



contexto de requalificação da legitimidade institucional, no qual “as premissas democráticas incorporadas na Constituição se arranjam com os direitos fundamentais e permitem uma construção normativa que alça a transparência”, o que viabiliza um “Estado plural, republicano e aberto às exigências de controle racional das decisões.”⁵⁷

A sua efetivação, entretanto, é desafiadora. Segundo Caroline Bitencourt e Janriê Reck, atualmente o controle social na contemporaneidade do Brasil está comprometido em razão das relações entre neoliberalismo e Estado de Exceção. Os autores listam uma série de características dessa conjuntura, sendo uma delas a utilização do “discurso dos direitos fundamentais contra os direitos fundamentais, como se houvesse direitos capazes de sobrepor-se aos outros, como se fosse necessário sacrificar alguns direitos em nome de um bem maior (...)”⁵⁸ O exemplo dado pelos autores de decadência democrática no âmbito do acesso à informação foi a edição do Decreto n. 9.690/2019 da Medida Provisória n. 928/2020, que restringiram o acesso à informação.⁵⁹

Outro exemplo que pode ser dado de ameaça à efetivação do direito ao acesso à informação é a aplicação indevida da LGPD. O aparente conflito entre Lei de Acesso à Informação e Lei Geral de Proteção de Dados pessoais é vislumbrado nos seguintes termos: o direito à informação segue a premissa de máxima divulgação e acesso facilitado, de publicidade como regra e sigilo como exceção; já o direito à proteção de dados pessoais teria como objetivo a proteção da privacidade, o que impediria a divulgação de informações e documentos que contenham esse tipo de informação. Nesse sentido, foram numerosas as notícias de pedidos de acesso à informação sendo denegados com fundamento na LGPD (e no artigo 31 da LAI). Um exemplo é o indeferimento de recurso em pedido de acesso aos resultados de exames para *Covid-19* feitos pelo então Presidente da República.⁶⁰

⁵⁷ CLÊVE, Clèmerson Merlin; FRANZONI, Júlia Ávila. Administração Pública e a nova Lei de Acesso à Informação. **Interesse Público - IP**, Belo Horizonte, ano 15, n. 79, pp. 1-23, mai./jun. 2013. p. 2.

⁵⁸ BITENCOURT, Caroline Müller; RECK, Janriê Rodrigues. Os Desafios do Acesso à Informação e o Controle Social no Estado Pós-Democrático: normalidade ou exceção? **Seqüência**, Florianópolis, n. 84, pp. 183-208, abr. 2020. p. 192.

⁵⁹ O Decreto previu a possibilidade de delegação da competência para o estabelecimento da classificação das informações, e a Medida Provisória alterou uma lei específica para políticas de enfrentamento à pandemia causada pelo vírus *Covid-19*, com a inserção de normas que restringiam os pedidos de acesso à informação, especula-se, com o objetivo de esconder exames médicos do então Presidente da República.

⁶⁰ Trecho da decisão da Comissão: “Conforme os autos, o Cidadão recorre a esta Comissão para obter acesso aos resultados dos exames diagnósticos para COVID-19 feitos pelo Presidente da República nos anos de 2020 e 2021. Verifica-se que o Órgão recorrido negou provimento ao pedido com base no art. 31 da Lei nº 12.527, de 2011, por entender que as informações requeridas são pessoais. Sobre o tema, cumpre pontuar que, de acordo com o referido dispositivo legal, o tratamento das informações pessoais de posse da Administração deve ser feito com respeito à intimidade, à vida privada, à honra e à imagem das pessoas, bem como às liberdades e garantias individuais, de modo a preservar informações que revelem características íntimas e particulares de um indivíduo, podendo tais informações ser divulgadas ou ter acesso por terceiro mediante previsão legal ou, então, por expresse consentimento da pessoa a que se referirem. Nessa mesma ótica, verifica-se que, conforme o art. 5º, inciso II, Lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), os dados pessoais relativos à saúde são dados pessoais sensíveis.” (BRASIL. Comissão Mista de Reavaliação de Informações.



A proteção de dados pessoais, entretanto, não está vinculada apenas à privacidade, no sentido de recolhimento ou resguardo de uma informação. Enquanto a privacidade se restringe à dicotomia entre público e privado, “a proteção de dados é, na verdade, uma ferramenta de transparência, e não de opacidade”, e a lógica da LGPD “não é de restringir a circulação da informação, mas, muito pelo contrário, de estimulá-la”, de “garantir um fluxo informacional adequado”.⁶¹ A LGPD, aliás, confere ainda mais segurança jurídica na disponibilização de informações pessoais para cumprimento do disposto na Lei de Acesso à Informação, pois trata-se de uma obrigação legal do Poder Público,⁶² e ele pode realizar tratamento de dados para o cumprimento de obrigações e competências legais.⁶³ Além disso, a LGPD prevê uma equalização da assimetria informacional quando o Estado atua como agente de tratamento de dados,⁶⁴ o que se evidencia no Capítulo IV da LGPD, específico para o tratamento de dados pessoais pelo Poder Público, e que contém regras expressas de reforço do princípio da transparência ativa e passiva.⁶⁵

A transparência é uma premissa para uma presença efetiva dos cidadãos no interior das organizações sociais e políticas. E a democracia, que se pretende ser um “governo do povo”, só pode se concretizar como um “governo em público” ou um “governo do poder visível”. Há, nesse sentido, uma união entre esfera pessoal e esfera pública: o grau

Processo n. 00137.017441/2021-38. Decisão n. 7/2022. Julgado em 08/02/2022. Disponível em: <https://bit.ly/42NNVTG>. Acesso em: 18 mar. 2023.

⁶¹ BIONI, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo. Interseções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. **Cadernos Técnicos da CGU**, Brasília, v. 1, pp. 8-19, 2022. p. 9-10. Também opinam pela convergência entre as legislações: FORTINI, Cristiana; AMARAL, Greycielle; CAVALCANTI, Caio Mário Lana. LGPD X LAI: sintonia ou antagonismo? In: PIRONTI, Rodrigo (Coord.). **Lei Geral de Proteção de Dados no Setor Público**. Belo Horizonte: Fórum, 2021. Versão ebook sem paginação, capítulo 6.

⁶² BIONI, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo. Interseções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. **Cadernos Técnicos da CGU**, Brasília, v. 1, pp. 8-19, 2022. p. 10.

⁶³ Fundamentos da LGPD: “**Art. 7º** O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) **II** - para o cumprimento de obrigação legal ou regulatória pelo controlador;”; “**Art. 11.** O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: (...) **II** - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: **a)** cumprimento de obrigação legal ou regulatória pelo controlador;”; “**Art. 23.** O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), 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: (...)”.

⁶⁴ ARAÚJO, Valter Shuenquener de; PERIM, Maria Clara Mendonça; RIBEIRO, Koryander Figueirêdo. As assimetrias da regulação estatal para a proteção de dados pessoais e a afirmação dos direitos fundamentais de primeira dimensão. **A&C – Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 22, n. 87, p. 267-296, jan./mar. 2022. DOI: 10.21056/aec.v22i87.1453.

⁶⁵ BIONI, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo. Interseções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. **Cadernos Técnicos da CGU**, Brasília, v. 1, pp. 8-19, 2022. p. 11.



de proteção que o indivíduo tem para a sua esfera privada decorre das condições gerais de funcionamento do sistema político, e das regras de circulação das informações que estão destinadas a incidir sobre a distribuição de poder na sociedade. É um aparente paradoxo. São os sistemas de governo “em público” que privilegiam o valor da transparência ao aumentar as possibilidades de tutela efetiva da esfera privada dos cidadãos. O contrário ocorre em sistemas com lógicas e práticas autoritárias: a opacidade e segredo são regras fundamentais que propiciam o seu funcionamento desse modo.⁶⁶

O tema da privacidade faz emergir de forma indissociada, portanto, o tema da transparência. O acesso aos bancos de dados públicos pode viabilizar que o controlado se torne controlador e, dessa forma, sejam mais transparentes os comportamentos de quem colhe a informação: “Não se pode, portanto, traçar um limite, como se o mundo da defesa da privacidade e o da ação pública fossem hostis ou não comunicantes. Não existe uma separação, mas um *continuum*.” Não se trata de uma escolha entre valores diametralmente contrapostos, senão de um balanceamento complexo entre diferentes interesses em jogo, para a um só tempo garantir direitos sociais e a progressiva abertura da sociedade.⁶⁷

Assentada a convergência de valores entre a transparência e a proteção de dados, é inegável que desdobramentos das duas disciplinas podem produzir conflitos e condições nem sempre fáceis de serem resolvidos, e as relações entre leis sobre proteção de dados e leis sobre a liberdade de informação é um assunto delicado e urgente.⁶⁸

Danilo Doneda, ainda antes da edição da Lei Geral de Proteção de Dados, abordou o assunto. O autor desde então reconheceu um autônomo direito à proteção de dados pessoais no ordenamento jurídico. Ainda assim, concluiu que a restrição ao fornecimento de informações com fundamento no artigo 31 da Lei de Acesso à Informação só é cabível nos casos em que fosse necessária a proteção da intimidade, vida privada, honra e imagem.⁶⁹ É dizer, os dados pessoais, aqueles compreendidos como relacionados à pessoa identificada ou identificável, não justificam por si mesmos a restrição do acesso à informação. Desse modo, é seguro afirmar que a LGPD não criou outras hipóteses de restrição ao acesso à informação além daquela prevista no artigo 31 da LAI.

O desafio, então, é saber em quais casos a divulgação de dados pessoais implicará ofensa à intimidade, vida privada, honra e imagem. Mas, especialmente no contexto

⁶⁶ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: A privacidade hoje. Renovar: Rio de Janeiro, 2008. p. 45.

⁶⁷ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: A privacidade hoje. Renovar: Rio de Janeiro, 2008. P. 47-48.

⁶⁸ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: A privacidade hoje. Renovar: Rio de Janeiro, 2008. p. 69-70.

⁶⁹ DONEDA, Danilo Cesar Maganhoto; VIOLA, Mario. Proteção de dados pessoais como limite ao acesso à informação e seu tratamento posterior. In: SARLET, Ingo Wolfgang; MARTOS, José Antonio Montilla Martos; RUARO, Regina Linden (Coords.). **Acesso à informação como direito fundamental e dever estatal**. Porto Alegre: Livraria do Advogado, 2016, pp. 117-131. p. 124.



de processamento automatizado de dados pessoais, é impossível determinar quais as consequências que decorrem do acesso a determinados dados pessoais. Isso inviabiliza uma associação apriorística do tratamento de um dado pessoal a um determinado efeito (violação ou não da honra, por exemplo).⁷⁰ No mesmo sentido, Stefano Rodotà afirma que nenhuma informação representa um valor em si mesma, mas em virtude do contexto no qual está inserida, ou pelas finalidades para as quais é utilizada, ou ainda pelas outras informações às quais tem sido associada. Portanto, é falha a tentativa de conceber uma regra definitiva a respeito de qual regime jurídico deve incidir sobre cada tipo de dado. As regras sobre circulação de dados tendem, então, à orientação para a consideração de contextos, funções e associações.⁷¹ Sendo assim, a divulgação ou não de um dado pessoal dependerá da análise de seus impactos na esfera do titular, bem como de ponderação com o interesse público presente no caso (artigo 31, §3º, inciso V da LAI).⁷²

Considerando a indefinição do quadro acima, o autor faz a ponderação de que “Adentrando este campo mais, digamos, objetivo, verifica-se que algumas espécies de dados pessoais, como os dados sensíveis, (...) seriam de antemão dados pessoais que mereceriam um grau maior de proteção”.⁷³ Ainda que a categoria dados sensíveis possa em certa medida objetivar a resolução de casos concretos, trata-se de um preceito não absoluto. O Poder Público pode tratar dados pessoais sensíveis para fins de cumprir a obrigação legal de disponibilizar informações, e é o que ocorre quando, por exemplo, num certame de concurso público é divulgada a raça de determinados candidatos.

Não é possível detalhar todas as áreas de interferência entre liberdade de informação e proteção de dados e as respectivas soluções, mas pode-se, por meio da combinação de princípios, definir critérios capazes de selecionar e equilibrar os interesses

⁷⁰ DONEDA, Danilo Cesar Maganhoto; VIOLA, Mario. Proteção de dados pessoais como limite ao acesso à informação e seu tratamento posterior. In: SARLET, Ingo Wolfgang; MARTOS, José Antonio Montilla Martos; RUARO, Regina Linden (Coords.). **Acesso à informação como direito fundamental e dever estatal**. Porto Alegre: Livraria do Advogado, 2016, pp. 117-131. p. 125-126.

⁷¹ RODOTÀ, Stefano. **A vida na sociedade da vigilância: A privacidade hoje**. Renovar: Rio de Janeiro, 2008. p. 77.

⁷² “**Art. 31.** O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. **§ 1º** As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: **I** - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e **II** - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. (...) **§ 3º** O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: (...) **V** - à proteção do interesse público e geral preponderante.”

⁷³ DONEDA, Danilo Cesar Maganhoto; VIOLA, Mario. Proteção de dados pessoais como limite ao acesso à informação e seu tratamento posterior. In: SARLET, Ingo Wolfgang; MARTOS, José Antonio Montilla Martos; RUARO, Regina Linden (Coords.). **Acesso à informação como direito fundamental e dever estatal**. Porto Alegre: Livraria do Advogado, 2016, pp. 117-131. p. 126.



em conflito. Os procedimentos de tutela de privacidade variam, e se fundam não sobre um, mas sobre diversos critérios de seleção dos interesses que prevalecerão no caso concreto. Isso não é novidade, já que desde sempre as informações pessoais foram submetidas a regimes jurídicos distintos segundo um espectro que vai do máximo de opacidade ao máximo de transparência, com nuances intermediárias, segundo se considere prevalecente o interesse privado à intimidade ou o interesse coletivo à publicidade.⁷⁴

O critério adotado por Danilo Doneda é o princípio da finalidade como limite à utilização de informações pessoais para fins de aplicação da LAI. O autor argumenta que ainda que as informações sejam divulgadas pela Administração Pública para fins de garantir a transparência e o controle democrático, “elas têm a finalidade de seu tratamento restritivamente definida, o que importa que sua utilização para finalidades distintas estaria vedada, sendo a finalidade nesse caso outro obstáculo ao acesso e utilização posterior dessas informações com base na LAI”. Segundo o autor, antes de ser “meramente abstrata e sujeita à livre disposição, esta informação, à medida que identifica uma pessoa, está sempre vinculada a ela”.⁷⁵

O princípio da finalidade impõe que o tratamento principal de dados seja feito de acordo com as finalidades legítimas e informadas, e que o tratamento secundário ou posterior, para propósitos não inicialmente especificados, tenham afinidade com o motivo que gerou a coleta. Assim considerado, a aplicação do princípio da finalidade como critério para fins de disponibilizar informações ao público pelo Poder Público restringiria indevidamente a transparência. Dados pessoais são coletados pelo Estado pelos mais diversos motivos, de modo que a sua divulgação para o atendimento de deveres de transparência raramente é a sua finalidade principal, senão uma consequência.

Um critério mais adequado é o princípio da necessidade, que impõe que o tratamento se restrinja ao mínimo indispensável para atender à finalidade pretendida, de forma proporcional e não excessiva. Desse modo, “a administração pública deve realizar um juízo de necessidade acerca de quais dados pessoais deverão ser disponibilizados para o atendimento de um pedido de acesso à informação”, o que não significa que não se possa disponibilizar qualquer dado pessoal.⁷⁶

⁷⁴ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: A privacidade hoje. Renovar: Rio de Janeiro, 2008. p. 71 e 77.

⁷⁵ DONEDA, Danilo Cesar Maganhoto; VIOLA, Mario. Proteção de dados pessoais como limite ao acesso à informação e seu tratamento posterior. In: SARLET, Ingo Wolfgang; MARTOS, José Antonio Montilla Martos; RUARO, Regina Linden (Coords.). **Acesso à informação como direito fundamental e dever estatal**. Porto Alegre: Livraria do Advogado, 2016, pp. 117-131. p. 130.

⁷⁶ BIONI, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. **Cadernos Técnicos da CGU**, Brasília, v. 1, pp. 8-19, 2022. p. 16.



5. CONCLUSÕES

As conclusões da presente pesquisa são as seguintes:

Para proteger os dados pessoais não é possível interromper o seu fluxo, dado o informacionismo que permeia a sociedade, então, é necessário adequá-lo. E essa adequação envolve mecanismos de transparência, controle e *accountability* democrático e ético, pois eles têm um papel central na proteção de dados pessoais.

A vigilância, compreendida como observação, o registro e a categorização de informação sobre pessoas, processos e instituições, e o tratamento de dados pessoais não são, em si, um problema. Mas ambos, a depender das dinâmicas de poder, podem assumir uma conotação negativa e têm riscos negativos.⁷⁷ São alguns deles: práticas totalitárias levadas a cabo pela gestão pública dominante, exclusão e classificação social, óbice ao livre desenvolvimento por meio da imobilização de pessoas ou grupos em perfis historicamente determinados e perdas de independência, autonomia, espontaneidade e criatividade. Para combatê-los, são necessários mecanismos de transparência, controle e *accountability* democrático e ético. Daí, então, o foco temático do trabalho.

Foram feitas as seguintes proposições para a efetivação do direito de acesso aos dados tratados pelo Estado: (1) quanto maior o nível de informações sobre o tratamento de dados, e quanto maior a sua complexidade, mais amplo e mais detalhado será o escopo do direito de acesso; (2) em casos nos quais não se aplica a LGPD em sua totalidade, como ocorre no tratamento de dados pessoais para fins de segurança pública, o eventual sigilo não necessariamente deve implicar negativa completa do acesso, mas, prioritariamente, ser modulado quanto à extensão do conteúdo e quanto ao momento do acesso, feita de acordo com as normas sobre classificação previstas na Lei de Acesso à Informação; (3) além de o titular poder formular pedido de acesso em relação aos seus próprios dados, terceiros podem formular pedidos de acesso à informação sobre atividades de tratamento, mesmo que não tenha dados próprios envolvidos; (4) esse direito de acesso às informações sobre tratamento de dados que não diz respeito aos do próprio solicitante se aplica também aos dados anônimos, sejam eles utilizados para a formação de perfis comportamentais ou não.

Não há conflito de valores entre Lei de Acesso à Informação e Lei Geral de Proteção de Dados. O amplo conhecimento de informações de interesse público e a proteção de dados pessoais convergem para o mesmo denominador em comum: o imperativo de transparência. A LGPD não criou novas hipóteses de sigilo, ao contrário, apenas reforçou a segurança jurídica em relação aos tratamentos necessários para a publicização de informações. Portanto, a presença de um dado pessoal não torna uma informação

⁷⁷ RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. Personal data protection and State surveillance: the risks of digital discrimination and the Federal Supreme Court's vision. **A&C – Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 22, n. 90, p. 63-85, out./dez. 2022. DOI: 10.21056/aec.v22i90.1658.



ou documento sigilosos, mas, sim, a potencial ofensa à intimidade, vida privada, honra e imagem, o que sempre dependerá do contexto e do caso concreto. Um critério adequado para selecionar e equilibrar os interesses em conflito é a aplicação do princípio da necessidade, segundo o qual devem ser divulgados dados pessoais na medida do mínimo indispensável para atender à finalidade de publicização.

6. REFERÊNCIAS

ARAÚJO, Valter Shuenquener de; PERIM, Maria Clara Mendonça; RIBEIRO, Koryander Figueirêdo. As assimetrias da regulação estatal para a proteção de dados pessoais e a afirmação dos direitos fundamentais de primeira dimensão. **A&C – Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 22, n. 87, p. 267-296, jan./mar. 2022. DOI: 10.21056/aec.v22i87.1453.

BALL, Kirstie; WEBSTER, Frank. The Intensification of Surveillance. In: BALL, Kirstie; WEBSTER, Frank (Eds.). **The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age**. London: Pluto Press, 2003, p. 1-15.

BELLOCHIO, Lucía. Big Data in the Public Sector. **A&C – Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 18, n. 72, pp. 13-29, abr./jun. 2018.

BIONI, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo. Interseções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. **Cadernos Técnicos da CGU**, Brasília, v. 1, pp. 8-19, 2022.

BITENCOURT, Caroline Müller; RECK, Janriê Rodrigues. Os Desafios do Acesso à Informação e o Controle Social no Estado Pós-Democrático: normalidade ou exceção? **Seqüência**, Florianópolis, n. 84, pp. 183-208, abr. 2020.

BRASIL. Comissão Mista de Reavaliação de Informações. **Processo n. 00137.017441/2021-38**. Decisão n. 7/2022. Julgado em 08/02/2022. Disponível em: <https://bit.ly/42NNVTG>. Acesso em: 18 mar. 2023.

BUCCI, Maria Paula Dallari. **Fundamentos para uma teoria jurídica das políticas públicas**. São Paulo: Saraiva, 2013.

CAVOUKIAN, Ann. **Privacy by Design - The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices**. p. 2. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf>. Acesso em: 1 mar. 2023.

CLÈVE, Clèmerson Merlin; FRANZONI, Júlia Ávila. Administração Pública e a nova Lei de Acesso à Informação. **Interesse Público - IP**, Belo Horizonte, ano 15, n. 79, pp. 1-23, mai./jun. 2013.

CRISTÓVAM, José Sérgio da Silva; BERGAMINI, José Carlos Loitey. A centralidade da noção de accountability como instrumento de concretização do modelo de Administração Pública sustentável. **A&C – Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 21, n. 84, p. 87-108, abr./jun. 2021. DOI: 10.21056/aec.v21i84.1372.



DOMÍNGUEZ ÁLVAREZ, José Luis. Public administration's challenges in order to guarantee the fundamental right of personal data protection in the post-COVID-19 era. **Revista Eurolatinoamericana de Derecho Administrativo**, Santa Fe, vol. 7, n. 1, p. 167-191, ene./jun. 2020. DOI 10.14409/redoeda.v7i2.9551

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2020.

DONEDA, Danilo Cesar Maganhoto; VIOLA, Mario. Proteção de dados pessoais como limite ao acesso à informação e seu tratamento posterior. In: SARLET, Ingo Wolfgang; MARTOS, José Antonio Montilla Martos; RUARO, Regina Linden (Coords.). **Acesso à informação como direito fundamental e dever estatal**. Porto Alegre: Livraria do Advogado, 2016, pp. 117-131.

FELZMANN, Heike; FOSCH-VILLARONGA, Eduard; LUTZ, Christoph; TAMÒ-LARRIEUX, Aurelia. Towards Transparency by Design for Artificial Intelligence. **Sci Eng Ethics**, [s.l.], vol. 26, n. 6, pp. 3333-3361, dec. 2020.

FORTINI, Cristiana; AMARAL, Greycielle; CAVALCANTI, Caio Mário Lana. LGPD X LAI: sintonia ou antagonismo? In: PIRONTI, Rodrigo (Coord.). **Lei Geral de Proteção de Dados no Setor Público**. Belo Horizonte: Fórum, 2021. Versão ebook sem paginação, capítulo 6.

GUEDES, Luciana Kellen Santos Pereira; FARIA, Edimur Ferreira de. O aparente controle social no âmbito da Administração Pública brasileira. **A&C – Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 21, n. 86, p. 249-274, out./dez. 2021. DOI: 10.21056/aec.v21i83.1353.

LYON, David. Surveillance after September 11, 2001. In: BALL, Kirstie; WEBSTER, Frank (Eds.). **The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age**. London: Pluto Press, 2003, pp. 16-25.

MARTINS, Ricardo Marcondes. Direito fundamental de acesso à informação. **A&C – R. de Dir. Administrativo & Constitucional**, Belo Horizonte, ano 14, n. 56, pp. 127-146, abr./jun. 2014.

MARTINS, Ricardo Marcondes. Proteção de dados, competências dos entes federativos e a Emenda Constitucional n. 115/22. **Revista de Investigações Constitucionais**, Curitiba, vol. 9, n. 3, p. 645-658, set./dez. 2022. DOI: 10.5380/rinc.v9i3.87107.

NISSENBAUM, Helen. **Privacy in Context**: technology, policy, and the integrity of social life. Stanford: Stanford Law Books, 2009.

PHILIPPI, Juliana Horn Machado. Transformação digital e urgência da cultura de dados na Administração Pública brasileira. **Revista Eurolatinoamericana de Derecho Administrativo**, Santa Fe, vol. 10, n. 1, e232, ene./jun. 2023. DOI: 10.14409/redoeda.v10i1.12401.

ROBLES OSOLLO, Ana Gloria. El derecho a la privacidad y la protección de datos personales transfronterizos. **Revista Eurolatinoamericana de Derecho Administrativo**, Santa Fe, vol. 8, n. 1, p. 35-60, ene./jun. 2021. DOI 10.14409/redoeda.v8i1.9543.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: A privacidade hoje. Renovar: Rio de Janeiro, 2008.



RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. Personal data protection and State surveillance: the risks of digital discrimination and the Federal Supreme Court's vision. **A&C – Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 22, n. 90, p. 63-85, out./dez. 2022. DOI: 10.21056/aec.v22i90.1658.

SALGADO, Eneida Desiree. **Lei de Acesso à Informação**: Lei 12.527/2011. São Paulo: Revista dos Tribunais, 2020.

SALGADO, Eneida Desiree; SAITO, Vitoria Hiromi. Privacidade e proteção de dados: por uma compreensão ampla do direito fundamental em face da sua multifuncionalidade. **International Journal of Digital Law**, Belo Horizonte, ano 1, n. 3. pp. 117-137, set./dez. 2020.

SCHAAR, Peter. Privacy by Design. **Identity in the Information Society**, [s.l.], vol. 3, pp. 267-274, 2010.

SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**: pluralismo jurídico e transparência em perspectiva. São Paulo: Revista dos Tribunais, 2020. Versão *e-book*.

VAINZOF, Rony. Comentários ao artigo 6º. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). **LGPD**: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, pp. 126-200.

VALENCIA-TELLO, Diana Carolina. El control externo de la administración pública: análisis del caso brasileiro. **Revista de Direito Econômico e Socioambiental**, Curitiba, v. 13, n. 2, p. 276-301, maio/ago. 2022. doi: 10.7213/revdireconsoc.v13i2.29872.

VÉLIZ, Carissa. **Privacy is Power**: why and how you should take back control of your data. London: Bantam Press, 2020.

WOOD, David; KONVITZ, Eli; BALL, Kirstie. The Constant State of Emergency?: Surveillance after 9/11. *In*: BALL, Kirstie; WEBSTER, Frank (Eds.). **The Intensification of Surveillance**: Crime, Terrorism and Warfare in the Information Age. London: Pluto Press, 2003, p. 137-150.