UNICENTRO PARANÁ
REOC
REVISTA DE ESTUDOS EM ORGANIZAÇÕES E CONTROLADORIA ISSN 2763-9673

O USO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS POR GESTORES PÚBLICOS: ORIGENS E FUNÇÕES PROCEDIMENTAIS EM POLÍTICAS PÚBLICAS NO BRASIL[1]

THE USE OF THE GENERAL PERSONAL DATA PROTECTION LAW BY PUBLIC MANAGERS: ORIGINS AND PROCEDURAL FUNCTIONS IN PUBLIC POLICIES IN BRAZIL

RAFAEL AUGUSTO FERREIRA ZANATTA
Universidade de São Paulo (USP)
E-mail: rafa.zanatta@gmail.com

Resumo
A implementação eficaz da Lei Geral de Proteção de Dados Pessoais (LGPD) é um desafio complexo para os gestores públicos, dada sua necessidade de conciliar a proteção de direitos fundamentais com a promoção de usos inovadores e o fluxo amplo de dados. Este artigo argumenta que a aplicação correta da LGPD enfrenta desafios no Brasil, incluindo a confusão entre proteção de dados e sigilo da informação, a percepção de que a LGPD dificulta o uso secundário de dados em políticas públicas e interpretações equivocadas da lei em casos envolvendo conflitos com o direito de acesso à informação. Por meio de uma revisão bibliográfica embasada na teoria do direito e políticas públicas, este estudo adota um método hipotético-dedutivo para explorar como uma abordagem procedimental da proteção de dados, distinta da privacidade e sigilo, pode esclarecer o papel da LGPD na formulação e execução de políticas públicas.

Palavras-Chave: Proteção de dados pessoais, políticas públicas, gestores públicos.

ABSTRACT
The effective implementation of the General Personal Data Protection Law (LGPD) is a complex challenge for policymakers, given their need to reconcile the protection of fundamental rights with the promotion of innovative uses and the broad flow of data. This article argues that the correct application of the LGPD faces challenges in Brazil, including the confusion between data protection and information confidentiality, the perception that the LGPD hinders the secondary use of data in public policies, and misinterpretations of the law in cases involving conflicts with the right of access to information. Through a bibliographical review based on the theory of law and public policies, this study adopts a hypothetical-deductive method to explore how a procedural approach to data protection, distinct from privacy and secrecy, can clarify the role of the data protection law in the formulation and execution of public policies.

Key-words: Protection of personal data, public policies, public managers.

1 DOI: https://doi.org/10.5935/2763-9673.20230014

1. INTRODUÇÃO

A aprovação da Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018 – "LGPD") trouxe um conjunto de novas preocupações para gestores públicos no Brasil, considerando que a legislação exige que, para cada tratamento de dados pessoais, exista um fundamento jurídico que o autorize. Em vigência desde 2020, a legislação tem sido adotada gradativamente pelo poder público. Como demonstrado empiricamente pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic) em 2022, sua adoção pela administração pública não é plena.

Apesar de uma série de recomendações feitas pelo Ministério da Economia, pelo Conselho Nacional da Justiça e pelo Tribunal de Contas da União, 56% dos órgãos do Executivo "mencionaram a presença de pessoa ou área responsável pela implementação da legislação" (CETIC, 2022, p. 97). É muito recente o processo de adaptação à LGPD nas Prefeituras, governos de Estado, autarquias, universidades e entre formuladores de políticas públicas. A pesquisa do Cetic mostra que este percurso está apenas começando, em um processo um pouco conturbado e lento.

A LGPD é uma lei inescapável aos gestores públicos. Ela se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado. Seu escopo também é abrangente. Em termos jurídicos, o tratamento de dados pessoais é definido amplamente como toda operação realizada com dados pessoais, como as que se referem a "coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração"[2], conforme art. 5º, inciso X, LGPD.

Os dados pessoais possuem um conceito amplo. Trata-se de informações relacionadas a uma pessoa natural identificada ou identificável. Portanto, os dados pessoais não se resumem apenas aos identificadores tradicionais como nome completo, filiação e registros como matrícula de nascimento, RG e CPF. Por dados pessoais, também devemos entender os dados de geolocalização, o

2 Para facilitar a fluidez da leitura, a Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018) será sempre mencionada como LGPD neste texto.

protocolo IP, os registros de dispositivos (*devices Ids*) e identificadores produzidos por rastreadores, desde que seja possível a identificação pessoal com baixo esforço e custo. Como afirmado pela Autoridade Nacional de Proteção de Dados Pessoais,[3] "são também considerados dados pessoais outros dados que estejam relacionados com uma pessoa natural, tais como seus hábitos de consumo, sua aparência e aspectos de sua personalidade" (ANPD, 2023).

Considerando que a LGPD é "um dos principais desafios para a administração pública" (CETIC, 2022, p. 96) e que ela busca o "equilíbrio entre o tratamento de dados pessoais para melhorar a atuação do setor público e minimizar potenciais riscos aos cidadãos" (CETIC, 2022, p. 96), propõe-se apresentar delineamentos iniciais sobre a LGPD, em especial sua origem e sua natureza multidimensional, e explicar como ela se relaciona com a elaboração de políticas públicas, considerando as demandas de gestores públicos.[4] Gestores públicos estão na linha frente das políticas públicas e precisam tomar decisões estratégicas com relação ao uso de dados pessoais. Uma das justificativas para o presente recorte é a evidente relação que existe entre a formulação de políticas públicas no século XXI, que são intensivas em dados pessoais em razão do estado atual de ubiquidade dos computadores e do barateamento do processamento e armazenamento de informações (BOULET; LAJAUNIE; MAZZEGA, 2019; TREIN; VARONE, 2023), com o regime jurídico da proteção de dados pessoais, que é assegurado por uma lei federal e pela compreensão do Supremo Tribunal Federal de que este é um "direito fundamental autônomo", que gera obrigações, por parte do Estado e dos gestores públicos, para seu devido gozo pelos cidadãos.

Ao focalizar no gestor público que está tendo um primeiro contato com a discussão sobre LGPD, parte-se do pressuposto que ele não possui contato com a literatura técnica que explica as razões da diferenciação entre privacidade e proteção de dados pessoais (DONEDA, 2006; SCHERTEL MENDES, 2014) e a importância dos princípios de tratamento de dados pessoais, que possui uma

3 A ANPD é uma autarquia de natureza especial, vinculada ao Ministério da Justiça e Segurança Pública, responsável por zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil.

4 Para uma definição simplificada de "gestor público", utiliza-se o conceito dado pelo Governo do Estado do Paraná, em documento chamado Gestão em Foco, que conceitualiza o gestor público como o "profissional que administra, atua e tem responsabilidade direta com o patrimônio público pelo qual se deve zelar e prestar contas à sociedade" (GOVERNO DO PARANÁ, 2018, p. 9).

longa origem histórica (DONEDA; ZANATTA, 2022; ZANATTA; BIONI, 2021; ZANATTA, 2023). Por isso, há uma apresentação sobre os principais contornos do surgimento da proteção de dados pessoais, com base na literatura jurídica especializada.

O presente artigo tem como objetivo apresentar três concepções problemáticas sobre a LGPD, removendo essas preconcepções negativas com relação à compatibilização da proteção de dados pessoais com políticas públicas. A pergunta de fundo é: de que modo uma concepção procedimental da proteção de dados pessoais, distinta da ideia de privacidade e sigilo, permite compreender as funções da LGPD em políticas públicas?

Ao aprofundar a análise de tais concepções problemáticas, são explicitadas as relações da LGPD com políticas públicas, o modo como a LGPD trabalha explicitamente com uma autorização jurídica para tratamento de dados pessoais no desenho de políticas públicas, sendo compatível, também, com uma cultura de dados abertos no Brasil. Partindo de uma revisão bibliográfica de matriz teórica no campo do direito e das políticas públicas – em especial artigos e livros especializados na temática –, o artigo vale-se de método hipotético-dedutivo para responder a problemática central da pesquisa (MEZZAROBA, 2014). Nesse sentido, busca-se testar o argumento de que a LGPD é um ferramental importante para políticas públicas no Brasil e possui uma natureza procedimental, habilitando os fluxos adequados de dados pessoais em uma sociedade datificada (BIONI; ZANATTA, 2021).

2. PROTEÇÃO DE DADOS É EQUIVALENTE A SIGILO? A INCOMPREENSÃO SOBRE AS ORIGENS DAS NORMAS SOBRE PROTEÇÃO DE DADOS PESSOAIS

Um dos grandes desafios de se pensar a proteção de dados pessoais é pensar para além das categorias de *sigilo* e *confidencialidade das informações*. Se você digitar “proteção de dados pessoais” no Google, Bing ou DuckDuckGo, certamente aparecerão imagens de cadeados ou objetos imagéticos que remetem à sigilo e não intrusão. O cadeado serve como metáfora de impossibilitar o acesso. Trata-se de uma imagem pouco adequada para compreender o

significado da LGPD. Para desfazer a concepção problemática de que a LGPD transforma tudo em sigilo – o que serve apenas para limitar o acesso a terceiros –, é fundamental uma recapitulação histórica sobre o direito à privacidade e o modo como uma concepção de não intrusão foi central em grande parte do século passado, o que prejudica a compreensão da proteção de dados pessoais como direito fundamental distinto do direito à privacidade.

A inviolabilidade dos dados é um direito constitucional previsto no art. 5º, XII. O direito à privacidade está previsto no art. 5º, X, ao afirmar que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas". Em 2022, modificou-se a Constituição para afirmar que "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais" (art. 5º, LXXIX). Mesmo sendo um direito fundamental autônomo, há uma confusão com sigilo e privacidade.

2.1. As Origens do Direito à Privacidade nos EUA

Como explicado por Danilo Doneda em sua obra *Da Privacidade à Proteção de Dados Pessoais*, a proteção de dados pessoais é originária do direito à privacidade, mas não se confunde com ele (DONEDA, 2006). As origens do direito à privacidade remetem a um artigo clássico escrito em 1890 por Samuel Warren e Louis Brandeis e publicado na *Harvard Law Review*. A partir do problema do surgimento das máquinas fotográficas e de novos dispositivos capazes de registrar imagens e disseminá-los em meios de comunicação na região de Cambridge (EUA), o artigo argumentou que o direito civil estadunidense precisaria de uma nova categoria jurídica para lidar com casos de responsabilidade civil diante das expansões de tecnologias de registro de imagens. O fundamento da argumentação dos autores era o surgimento de um novo tipo de ilícito, capaz de produzir um direito à reparação (o que eles chamam de *tort law*), em razão de violações aos direitos da personalidade. O bem jurídico tutelado seria a própria dignidade das pessoas em razão da utilização comercial de suas próprias imagens. Nesses termos, o *right to privacy* seria um direito de reivindicação contra um ilícito em razão dessa violação da esfera íntima e dos direitos da personalidade.

Já no início do século XX, surgiram os primeiros casos que levaram o chamado "direito à privacidade" para outros patamares, servindo como barreira para uso coercitivo da força pelo Estado. Casos famosos da Suprema Corte dos EUA, como *Olmstead v. United States* (1928), *Nardone v. United States* (1937), *Goldman v. Unites States* (1942), interpretaram a aplicação ou não da Quarta Emenda em casos de grampo telefônico. No famoso caso *Olmstead*, de 1928, a Suprema Corte teve que decidir se agentes federais poderiam incluir grampos telefônicos sem um mandado. O caso foi decidido por 5 votos a 4, tendo como decisão final que a utilização do grampo telefônico não constituía uma violação das cláusulas de devido processo da Quarta Emenda da Constituição dos EUA. O caso gerou uma enorme polêmica pois a tese do ministro William Howard Taft, juiz responsável pelo caso, era de que não havia uma busca (*searching*) e nenhum tipo de apreensão (*seizure*), pois o grampo telefônico seria distinto de apreender papéis e cartas.[5]

O caso *Olmstead* é especialmente famoso pois o ministro que escreveu o voto contrário (o que chamamos de *dissenting opinion*) foi Louis Brandeis, um dos autores do mencionado texto *The Right to Privacy* de 1890. Neste voto, Brandeis argumentou que os avanços tecnológicos da eletrônica e das telecomunicações teriam criado capacidades para "invasão da privacidade" de formas mais sutis. Para Brandeis, não deveria existir diferença alguma entre o sigilo das comunicações por carta e o sigilo das comunicações feitas por telefone. Aliás, para Brandeis, o "incidente diabólico" da invasão da privacidade do telefone seria maior que aqueles envolvidos com a violação das comunicações por carta.

A opinião de Brandeis só se mostrou consagrada em 1967, com a votação do caso *Katz v. United States*, que expandiu as proteções da Quarta Emenda da Constituição para além das pessoas, cases e papéis. A interpretação dada pela Suprema Corte foi de expandir as proteções jurídicas para áreas onde há "expectativas razoáveis de privacidade". Para os ministros da Corte, a regra da Quarta Emenda protege pessoas e não áreas. O caso *Katz* envolvia uma

5 Para o ministro Taft, a Constituição dos EUA proibiria a invasão do domicílio de uma pessoa e proibiria a apreensão ilegal de um bem físico. Para ele, no entanto, os grampos eletrônicos seriam dispositivos que permitiriam escutar a conversa de alguém, o que não seria um problema, especialmente por ser uma cabine telefônica pública, que alguém poderia usar voluntariamente. Partindo de uma posição conservadora sobre o papel do Poder Judiciário, o ministro da Suprema Corte argumentou que o Congresso poderia aprovar leis específicas sobre intercepções telefônicas, mas a Suprema Corte não poderia alargar a interpretação da Quarta Emenda.

investigação do FBI contra um agente ilegal de apostas que utilizava cabines telefônicas para se comunicar. O caso é paradigmático pois reconheceu o direito à privacidade nas comunicações privadas, mesmo que feitas em telefones públicos.

Outro fator de complicação é que o "direito à privacidade" ganhou outros contornos nos EUA na década de 1960. No famoso caso *Griswold* de 1965, o conceito de *privacy* foi utilizado para decidir um caso complexo no qual uma família desejava fazer uso de pílulas anticoncepcionais sem ter a informação registrada por uma clínica médica e transmitida para um órgão governamental. No caso *Griswold*, o direito à privacidade estruturou uma ideia de "privacidade sexual" – muito importante nos debates de teoria de direito (ALLEN, 1988; CITRON, 2018) –, no sentido de que decisões sobre usos de pílulas anticoncepcionais dizem respeito a uma esfera íntima da relação entre casais, não devendo existir pretensão estatal de analisar essas informações. Esses casos estruturam uma clara concepção de privacidade como liberdade negativa e como restrição do acesso.[6]

2.2. O Domínio da Ideia de Sigilo das Comunicações e Liberdades Negativas

Talvez uma das origens da confusão entre privacidade e sigilo, que afeta até hoje a LGPD, esteja na força dos casos *Olmstead* e *Katz* e do problema que eles lidam. O caso *Olmstead* é um caso clássico de "não intrusão" e de liberdades individuais dos cidadãos que devem se sobrepor a qualquer tentativa governamental de obtenção de informação e de poder. Ou seja, trata-se mesmo de uma dimensão liberal clássica dos direitos fundamentais. A liberdade negativa é, por excelência, uma capacidade do cidadão de limitar a atuação de seu governo e do Estado (SCHAEFFER, 1941). Como explicado pelo historiador James Whitman, essa concepção de privacidade como liberdade é uma marca cultural do povo estadunidense, que se explica desde sua fundação contra o

6 Anita Allen e Erin Mack assim define a privacidade: "A privacidade pessoal existe sempre que um certo grau de inacessibilidade protege pessoas ou informações sobre elas de outras pessoas. Reclusão, solidão, anonimato, sigilo, confidencialidade e reserva são formas discretas de privacidade. Embora a privacidade seja um fenômeno em todas as sociedades humanas, a sua disponibilidade e valor percebido variam de acordo com a cultura, a economia, *status*, a idade e o género. O gênero é uma variável social fundamental na disponibilidade de certas formas de privacidade individual e de grupo" (ALLEN; MACK, 1991, p. 444).

império inglês (WHITMAN, 2004) – e que talvez não encontre paralelo nem na Europa nem na América Latina.

No Brasil, as discussões sobre direito à privacidade foram praticamente inexistentes na primeira metade do século XX. O direito civil trabalhava com categorias de intimidade, honra e imagem, mas não com a noção de direito à privacidade. Na década de 1930, a Constituição Federal de 1934, promulgada durante o governo ditatorial de Getúlio Vargas, garantiu uma série de direitos e garantias individuais, como igualdade perante a lei, não privação de direitos por convicções filosófica, políticas ou religiosas, livre manifestação de pensamento, "respondendo cada um pelos abusos que cometer". Também foram assegurados direitos de liberdade de associação para fins lícitos, liberdade de exercício de profissão, liberdade de reunião sem armas, entre outros. Nos termos do art. 113, o que poderíamos entender como direito à privacidade estava afirmado como um direito de sigilo da correspondência e um direito de não intrusão de sua casa e não desapropriação de sua propriedade.[7]

Como observou René Ariel Dotti em estudos pioneiros sobre direito à privacidade feitos no final da década de 1970, a sociedade brasileira sempre lidou mal com os direitos da personalidade e novos direitos constitucionais relacionados às liberdades civis, talvez por uma profunda limitação de exercício de direitos civis que remonta à nossa história e nossa concepção de cidadania (ZANATTA, 2023, pp. 70-75). A tradição brasileira sempre foi muito mais penalista, focada em punir condutas, ao invés de assegurar direitos civis. Tendia a resumir a tutela da intimidade em uma questão de direito penal. O art. 153 do Código Penal, na década de 1940, já dizia que era crime "divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, a cuja divulgação possa produzir

7 Estabeleciam os incisos do artigo 113 da Constituição de 1934: "8) É inviolável o sigilo da correspondência (...) 16) A casa é o asilo inviolável do indivíduo. Nela ninguém poderá penetrar, de noite, sem consentimento do morador, senão para acudir a vítimas de crimes ou desastres, nem de dia, senão nos casos e pela forma prescritos na lei. (...) 17) É garantido o direito de propriedade, que não poderá ser exercido contra o interesse social ou coletivo, na forma que a lei determinar. A desapropriação por necessidade ou utilidade pública far-se-á nos termos da lei, mediante prévia e justa indenização. Em caso de perigo iminente, como guerra ou comoção intestina, poderão as autoridades competentes usar da propriedade particular até onde o bem público o exija, ressalvado o direito à indenização ulterior" (BRASIL, 1934).

dano a outrem". Grande parte da produção jurídica desta época se dedicou a aspectos de direito penal com relação a este tipo penal (GARCIA, 1949).

No Brasil, essa confusão sobre o direito ao sigilo das comunicações e o direito à privacidade foi incrementada por uma série de casos fiscais das décadas de 1980 e 1990. Neles, discutia-se o poder do fisco de obtenção de informações bancárias e os regimes jurídicos de sigilo de informações bancárias, aplicáveis às instituições financeiras. A Constituição Federal de 1988 introduziu, no artigo 5º, inciso XII, a inviolabilidade do sigilo de dados como direito fundamental. Na década de 1980, diversos autores, como René Ariel Dotti e José Afonso da Silva também propuseram novos remédios constitucionais para contenção de abusos informáticos (DONEDA; 2006; ZANATTA, 2023). Essas ideais deram origem ao *habeas data*, um instrumento para "assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público" (art. 5º, LXXII, a. Constituição Federal).

Na década de 1990, o Supremo Tribunal Federal julgou casos importantes sobre sigilo bancário. Um argumento influente foi o feito por Tércio Sampaio Ferraz Junior, professor da Universidade de São Paulo, que elaborou um parecer sobre o conteúdo da previsão constitucional sobre inviolabilidade do sigilo dos dados e os limites do exercício da fiscalização estatal (QUEIROZ; PONCE, 2021). Para Tércio, não existiria um direito fundamental ao sigilo, mas sim "circunstâncias nas quais o sigilo é instrumental à proteção de um direito fundamental" (QUEIROZ; PONCE, 2021, p. 69). O argumento de Tércio prosseguiu para diferenciar o sigilo da "comunicação dos dados" e "dos dados em si". A privacidade seria uma liberdade de negação, uma "imunidade contra o pretendido poder de devassa ou intromissão investigativa em certas esferas das vidas privadas de cidadãos" (QUEIROZ; PONCE, 2021, p. 69). Para Tércio, o texto da Constituição de 1988 focalizou nas limitações para interceptações telefônicas, que envolveriam a comunicação de dados. Em casos de interceptação, deve existir ordem judicial que a autorize.

O argumento lógico construído por Tércio o levou à conclusão de que, quando o Estado pretende obter dados fiscais que estão sob tutela das instituições financeiras, não há uma intercepção de "um ato comunicativo entre

banco e correntistas", mas sim "acesso a dados armazenados nos bancos de dados da instituição financeira" (QUEIROZ; PONCE, 2021, p. 70). Para Tércio, esses dados estariam protegidos pela regra geral da privacidade, mas não pelo sigilo dos dados previstos na Constituição (art. 5º, XII). No entanto, o Supremo Tribunal Federal adotou uma interpretação seletiva da tese de Tércio Sampaio em dois casos importantes (Mandado de Segurança n. 21.729/DF e Recurso Extraordinário 418.416/SC), decidindo que não haveria proteção de sigilo das comunicações em casos de atuação do fisco para identificação de crimes tributários.

O fato de os ministros do STF terem dado muita atenção à discussão sobre sigilo dos dados, e muita pouca atenção ao conteúdo do direito à privacidade e do direito à vida íntima, revela um problema de fundo mais crônico: ainda está em construção, no Brasil, uma visão centrada na dignidade da pessoa humana e na diferenciação entre direito à privacidade e direito à proteção de dados pessoais. Como reconhecido pelo professor Virgílio Afonso da Silva, ainda é muito recente o reconhecimento de que o direito à privacidade não se confunde com o direito à proteção de dados pessoais (SILVA, 2021). Este último está ligado a uma ideia de que existem direitos individuais e coletivos com relação ao uso legítimo de dados – para finalidades específicas, transparentes, leais, seguras e com regras de responsabilização –, e existem direitos de "dimensão objetiva", que implicam em uma obrigação positiva do Estado para agir e garantir que esses direitos são efetivamente garantidos, tal como é o direito fundamental à defesa do consumidor.

2.3. A Guinada para as Liberdades Positivas e o Problema dos Princípios para uso Justo dos Dados pelo Poder Público

Na década de 1950, o Brasil passou a ser influenciado pelos processos constitucionais pós-Guerra, especialmente dos países europeus, que elaboraram Constituições centradas na dignidade da pessoa humana e direitos fundamentais de liberdade. Foi o caso da Constituição da Alemanha e da Itália. A centralidade da dignidade trouxe à tona um debate sobre desenvolvimento da personalidade e uma nova concepção democrática de Estado. Stefano Rodotà chamou esse processo de "revolução do *homo dignus*" (RODOTÀ, 2011), pois houve uma

focalização inédita na ideia da *pessoa humana*. Essa "revolução da dignidade" (RODOTÀ, 2011) foi responsável por colocar no centro das discussões a autodeterminação da pessoa, a construção livre de sua identidade individual e coletiva e as responsabilidades individuais e coletivas. Pelo trauma do nazismo e do holocausto – que levou à morte de milhões de judeus –, retomou-se o espírito da Declaração dos Direitos do Homem e do Cidadão de 1789 que diz que os homens nascem e são livres e iguais em direitos.

A Constituição Italiana, promulgada em 1948, fala no art. 2º em garantia dos direitos invioláveis dos homens, "seja individualmente, seja nas suas formações sociais onde se desenvolve sua personalidade". Há uma grande ênfase na solidariedade. Introduz-se também não somente um princípio de igualdade perante a lei, mas um direito de "dignidade social" (art. 3º). Como explicado por Rodotà (2011), a ênfase na dignidade da pessoa, e não somente na liberdade dos homens, foi o início de uma grande transformação que culminou na Carta de Direitos Fundamentais da União Europeia de 2000.

A Lei Fundamental da República Federal da Alemanha, aprovada em 1949, por exemplo, inicia-se com um capítulo sobre direitos fundamentais. O primeiro artigo trata explicitamente da dignidade da pessoa humana. Diz que "a dignidade da pessoa humana é intangível" e que "respeitá-la e protegê-la é obrigação de todo o poder público" (art. 1, 1). O fundamento da comunidade política é o reconhecimento de "direitos invioláveis e inalienáveis" (art. 1, 2). O segundo artigo, que trata dos direitos de liberdade, afirma que "todos têm direito ao livre desenvolvimento de sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral" (art. 2, 1). No Brasil, autores como Orlando Gomes e San Tiago Dantas também introduziram teorias sobre direitos da personalidade (DONEDA; ZANATTA, 2022), que são ponto de partida para a proteção de dados pessoais no Brasil. O reconhecimento explícito da dignidade só aconteceu no Brasil com a redemocratização e a Constituição de 1988, que estabelece que a República Federativa do Brasil se constitui em Estado Democrático de Direito e tem como fundamento a "dignidade da pessoa humana" (art. 1º, III). Gustavo Tepedino, por exemplo, fala em "tutela dos valores existenciais" no Código de Defesa do Consumidor e no Código Civil. O próprio reconhecimento da boa-fé nessas duas leis, como norma de

comportamento (colaboração, informação, lealdade e sigilo), seria uma funcionalização da proteção de pessoa e de sua dignidade, que são objetivos constitucionais (TEPEDINO, 2006).

Antes das transformações que levaram à Constituição Federal de 1988, o remédio constitucional do *habeas data*, o Código de Defesa do Consumidor e o capítulo sobre direitos da personalidade no Código Civil – os principais elementos jurídicos que se relacionam com privacidade e proteção de dados pessoais antes da elaboração da LGPD –, houve uma transformação significativa do próprio conceito de *privacy* e o surgimento de um campo específico chamado de *informational privacy* ou *data privacy* nos EUA (COHEN, 2017).

Como explicado por Danilo Doneda (2006), a principal modificação do que seria o "direito à privacidade" ocorreu em razão de uma série de transformações no debate público na década de 1960, com a expansão dos movimentos de direitos civis[8] e a expansão dos chamados "direitos da personalidade" no pensamento jurídico europeu. Com a expansão dos computadores e os debates sobre o *National Data Bank* nos EUA em 1965 (um sistema de centralização de bases de dados de políticas públicas de saúde, educação, bem-estar juntamente com informações de natureza fiscal), explodiram as discussões sobre o que seriam usos justos de dados pessoais em sistemas automatizados. Surgiu, nesse período, um amplo debate sobre o que seria a *informational privacy*. Já no final da década de 1960, diversos intelectuais passaram a defender legislações federais específicas que pudessem garantir um uso legítimo de dados pessoais em sistemas automatizados de tratamento e uma autoridade independente, que pudesse funcionar como órgão de fiscalização e controle.

Em *Privacy and Freedom*, de 1967, Alan Westin defendeu uma legislação federal nos EUA que tivesse diversos critérios técnicos sobre responsabilidade dos agentes de tratamento de dados, normas organizacionais que promovam a segurança da informação e medidas técnicas que permitam identificar quais autoridades públicas tiveram acesso às bases de dados, quais decisões foram tomadas e se os usos de dados pessoais foram legítimos para políticas públicas.

8 Casos emblemáticos de direitos civis, como *NAAPC v. Alabama*, afirmaram direitos específicos com relação à não exposição de dados organizacionais que pudessem impactar a liberdade associativa de ativistas negros. Alan Westin, um dos principais intelectuais do campo do direito à privacidade, afirma que as discussões do movimento negro sobre limites da vigilância estatal foram centrais para ampliar o significado do *right to privacy*.

Apesar de nunca terem aprovado uma “lei geral de proteção de dados”, os EUA seguiram um caminho distinto, com a aprovação do *Privacy Act* e uma abordagem que atribui aos indivíduos a responsabilidade pela promoção de seus direitos de privacidade, especialmente quando existir dano. Regulações específicas surgiram na área de proteção ao crédito e na saúde, com regras específicas para empresas que atuam neste setor, mas sem a criação de uma Autoridade Nacional de Proteção de Dados Pessoais (WESTIN, 1979; WESTIN, 1985).

Em 1972, o Secretário de Educação, Saúde e Bem-Estar dos EUA, Elliot L. Richardson, criou um Comitê de Assessoria em *Automated Personal Data Systems*, formulado em resposta às crescentes preocupações sobre consequências danosas que podem resultar do uso descontrolado de aplicações de computadores e tecnologias de telecomunicações na coleta, armazenamento e uso de dados sobre cidadãos individuais. O Comitê tinha como missão produzir recomendações sobre quatro elementos/problemas: consequências prejudiciais que podem resultar do uso de sistemas automatizados de dados pessoais; salvaguardas que podem proteger contra consequências potencialmente prejudiciais; medidas que podem compensar quaisquer consequências prejudiciais; e políticas e práticas relacionadas à emissão e uso de números da Previdência Social (DEPARTMENT OF HEALTH, 1973).

Após meses de trabalho, a principal conclusão chegada pelo Comitê foi que a privacidade dos estadunidenses era precariamente protegida contra práticas arbitrárias ou abusivas de manutenção de registros de informações pessoais. A saída seria a criação um *Federal Code of Fair Information Practice* para todos os sistemas automatizados de tratamento de dados pessoais. A espinha dorsal do Código seria formada por cinco princípios básicos de direito. Primeiro, a proibição de sistemas secretos. Segundo o direito de saber que informação pessoal é usada e para qual fim. Terceiro, o direito de impedir que informações sejam obtidas para uma finalidade e utilizadas para outra, sem seu consentimento. Quarto, o direito de corrigir ou modificar informações erradas. Quinto, um dever geral de precaução e prevenção de usos abusivos de dados. Esses cinco pilares formaram o eixo central dos *Fair Information Practices Principles* (FIPPs), que se tornaram a principal moldura jurídica para direito à privacidade informacional nos EUA.

O relatório defendeu um princípio de "ausência de danos" para uso de dados para fins de pesquisa e estatística. Nele, parece ter surgido a expressão *rights of individual data subjects*, que se tornou linguagem dominante nas leis de proteção de dados pessoais na Europa, especialmente em razão da influência exercida pelo Código na formulação das *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* pelo Comitê de Ministros da OCDE em 1980 e, posteriormente, no desenho do rascunho do *Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, no período constitutivo da integração de mercados na União Europeia. Esse conjunto de medidas, sugerido pelo relatório de 1973, "passou a ser encontrado em várias normativas sobre proteção de dados pessoais", tornando-se uma "espécie de núcleo comum entre diversas normativas sobre proteção de dados" (DONEDA, 2017, p. 144).

As primeiras normas de proteção de dados pessoais surgiram após a elaboração dessas recomendações sobre "usos justos de dados pessoais" e princípios para livre fluxo de dados. Na década de 1970, surgiram legislações que afirmaram esses princípios (como a Lei da Suécia em 1973, o *Privacy Act* de 1974, a Lei Federal da Alemanha em 1977 e a Lei de Liberdades Informáticas da França em 1978). Em 1980, já estavam formulados, pela OCDE, os seguintes princípios: (i) princípio da minimização (*collection limitation*), (ii) princípio da qualidade dos dados (*data quality*), (iii) princípio da especificação da finalidade (*purpose specification*), (iv) princípio da limitação de uso (*use limitation*), (v) princípio das salvaguardas de segurança (*security safeguards*), (vi) princípio da abertura (*openness*), (vii) princípio da participação individual (*individual participation*) e (viii) princípio da responsabilização (*accountability*).[9]

Como explica o cientista político Colin Bennett, esses princípios, que foram inicialmente pensados para problemas primariamente gerados por grandes bases de dados do poder público, se consolidaram, também, como referencial para regulação das atividades do setor privado (BENNETT, 1992). Os regimes jurídicos de proteção de dados pessoais, no entanto, sempre buscaram compatibilizar o livre fluxo de dados, o desenvolvimento das economias de dados e os direitos básicos dos cidadãos com relação à transparência, autodeterminação informativa

9 Para uma rica análise sobre as variações do conceito de *accountability* dentro das discussões técnicas da OCDE, ver o trabalho de Bruno Bioni (2022).

e exercício de direitos com relação aos próprios dados, com direitos de acesso, de retificação, de oposição e de eliminação desses dados.

2.4. A LGPD cria regras para fluxo justo e lícito de dados e não regras para sigilo

A lógica da LGPD não difere muito das normas criadas na década de 1970 e das recomendações feitas pela OCDE na década de 1980, que se tornaram Diretiva da União Europeia em 1995, tornando-se muito influentes na América Latina. Como dizia Danilo Doneda, a LGPD não possuía um espírito profundamente radical – como se fosse uma construção jurídica profundamente inovadora e que causasse estranheza –, mas seguiu uma tendência já consolidada nos últimos 50 anos nas principais democracias do mundo (DONEDA, 2011). O enfoque reside em quatro elementos fundamentais. Primeiro, a definição clara de conceitos tidos como técnicos (tratamento, anonimização, pseudonimização etc.). Segundo a definição de princípios que devem servir como guia para todos os agentes de tratamento. Terceiro, obrigações e direitos para os diferentes agentes, incluindo a obrigação de identificar corretamente a "base legal para tratamento dos dados", o que é chamado de *legal grounds,* ou fundamento jurídico. Quarto, regras de responsabilização caso haja danos ou ilícitos cometidos.

As grandes novidades da LGPD, por influência da *General Data Protection Regulation* (GDPR), ocorreram muito mais em razão dos novos direitos de portabilidade de dados pessoais, de contestação de decisão automatizada e de revisão humana e ampliação da tutela jurídica para fins de *profiling*, que ocorre quando um perfil sobre uma pessoa é criado, por meio de correlações estatísticas em bancos de dados não estruturados (ZANATTA, 2023). Em linhas gerais, no entanto, a LGPD possui uma conexão com os princípios de fluxos de dados elaborados pela OCDE e pelo Conselho da Europa desde a década de 1980. A Convenção 108, de 1981, trouxe o entendimento de que os dados pessoais sujeitos a tratamento devem ser tratados de "forma justa e transparente", devem ser "recolhidos para finalidades explícitas, específicas e legítimas", devem ser "adequados, pertinentes e não excessivos relativamente às finalidades para as

quais são tratados" e devem ser "rigorosos e, se necessário, atualizados" (Convenção 108, art. 5, 4, alíneas a, b, c e d).

Essa mesma lógica é a que estrutura a LGPD. Para que os dados possam adquirir uma dimensão transfronteiriça e possam circular de forma justa, eles devem estar associados a uma finalidade específica, devem ser necessários e adequados ao tratamento pretendido, devem colocar em marcha um conjunto de procedimentos de segurança da informação e precaução a incidentes, e devem ser concebidos como potenciais usos que devem estar sempre associados a direitos subjetivos, considerando que "toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade" (art. 17, LGPD).

Em maio de 2018, o Conselho da Europa decidiu abrir o protocolo à assinatura da Convenção 108, de 1981, para diversos Estados, para além dos Estados membros, em uma clara sinalização de disseminação dos valores europeus. A Convenção reconhece que "é necessário promover, a nível mundial, os valores fundamentais do respeito pela primazia e pela proteção de dados pessoais, comprometendo-se assim à livre circulação de informação entre as pessoas" (CONSELHO DA EUROPA, 2018).

Na sua essência, a LGPD cria regras procedimentais para um dado pessoal seja tratado de forma lícita. Por isso, cria as figuras jurídicas do "controlador"[10], do "operador"[11], do "encarregado"[12] e do "titular"[13]. O controlador é a pessoa física ou jurídica que detém o poder de influência e definição de *para quê um dado é tratado* e *como um dado é tratado*. O operador é a pessoa física ou jurídica que trata um dado pessoal em razão de um comando, uma ordem, do controlador. Por exemplo, os serviços da Amazon Web Services prestados a universidades públicas para armazenamento de informações por serviços de computação em nuvem (*cloud computing*), enquadram a Amazon como *mera operadora*. Se uma universidade utiliza um sistema de armazenamento em nuvem

10 O controlador é "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (art. 5, VI, LGPD).
11 O operador é "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (art. 5, VII, LGPD).
12 O encarregado é "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)".
13 O titular é "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (art. 5, V).

para os dados pessoais de seus milhões de alunos, não cabe à Amazon definir *como e por que* esses dados serão tratados, mas sim à universidade. A responsabilidade pela licitude do tratamento é da universidade, que é controladora dos dados pessoais.

A LGPD proíbe que os dados sejam coletados dos alunos e transferidos para a Amazon para que sejam armazenados fora do país? Evidentemente que não. A LGPD não é uma norma de proibição para tratamento transfronteiriço de dados. Pelo contrário. Como dito, seguindo as recomendações da OCDE, ela é uma norma de habilitação para o fluxo internacional de dados, criando deveres e obrigações para os agentes de tratamento de dados. Neste exemplo, é claro que a Amazon se compromete com uma série de obrigações jurídicas, mesmo sendo uma operadora. Afinal, o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, "causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo" (art. 42, LGPD). De acordo com a lei, o operador "responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador", hipótese em que o operador se equipara ao controlador (art. 42, § 1º, I, LGPD).

Portanto, um gestor público poderia decidir utilizar um serviço de computação em nuvem, da Amazon, que implique em transferência internacional de dados pessoais. Isso em si não seria um ilícito. No entanto, haveria uma obrigação de reparação caso ocorresse um descumprimento dos princípios de segurança da informação pela Amazon, no sentido de não adotar "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (art. 46, LGPD). O parágrafo único do art. 44 é muito explícito ao afirmar que responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Mesmo em uma situação em que o dano não estivesse explícito, mas fosse apenas potencial, haveria uma obrigação de agir e de prevenir o dano. O princípio

da prevenção diz que é necessária a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" (art. 6º, VIII, LGPD). Considerando que os dados pessoais são intrinsicamente ligados aos direitos da personalidade e que o regime jurídico focaliza a *proteção das pessoas*, é possível, também, uma atuação preventiva para remover um ato ilícito, contrário ao direito. Os direitos da personalidade são intransmissíveis e irrenunciáveis. O Código Civil prevê, em seu artigo 12, que "pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade". Nesse sentido, é plenamente possível que a própria universidade – ou mesmo uma associação civil de servidores de uma universidade – ingresse com uma ação judicial para fazer cessar a ameaça a direitos da personalidade, uma vez identificando uma situação fática que implica em riscos significativos no tratamento de dados pessoais.

O que o gestor público deve ter em mente é que a LGPD é um instrumento para fluxos adequados de dados pessoais e não o seu imobilismo. A LGPD não significa que os dados pessoais devem estar resguardados como um "ativo não acessível" a outros, como se estivessem em condição de sigilo. Como será visto, tendo a correta identificação da base legal de execução de políticas públicas, abre-se o caminho para inovações significativas na administração pública.

3. A PROTEÇÃO DE DADOS PESSOAIS ATRAPALHA POLÍTICAS PÚBLICAS?

O percurso de aprovação da LGPD, durante os anos de 2012 a 2018, não foi simples e envolveu um processo de convencimento do próprio governo federal com relação ao valor da legislação. Inicialmente, quando o Anteprojeto de Lei de Proteção de Dados Pessoais foi proposto pelo Ministério da Justiça em 2010, surgiram preocupações por parte de gestores públicos, que consideravam que a lei federal poderia atrapalhar a elaboração de políticas públicas (ZANATTA, 2023). No início das negociações com os Ministérios do governo Dilma, havia a preocupação de que uma lei federal de proteção de dados pessoais poderia atrapalhar políticas públicas que demandassem uma vasta quantidade de dados dos cidadãos.[14]

14 Não se trata de algo excepcional ao Brasil. Como explicado por Alan Westin (1979), gestores públicos nos EUA também tiveram diversos conflitos com normas procedimentais de privacidade e proteção de dados pessoais. O debate sobre o *National Databank* na década de 1960 envolveu

Por exemplo, uma das principais bandeiras do governo Lula foi a implementação do Bolsa Família e a agregação de informações por meio do Cadastramento Único (Cad Único), que já tinha sido estruturado pelo Decreto n. 3.877/2001, durante o governo Fernando Henrique Cardoso. O decreto instituiu o Cadastramento Único "para ser utilizado por todos os órgãos públicos federais para a concessão de programas focalizados do governo federal de caráter permanente, exceto aqueles administrados pelo Instituto Nacional do Seguro Social - INSS e pela Empresa de Processamento de Dados da Previdência Social – Dataprev" (art. 1º). De acordo com o desenho do CadÚnico em 2001, a responsabilidade pelo tratamento dos dados pessoais era da Caixa Econômica Federal.[15]

Em outubro de 2003, Lula reorganizou o CadÚnico de forma integrada com o Bolsa Família, por meio da Medida Provisória n. 132/2003, lançando um grande programa de combate à miséria extrema no Brasil.[16] Foram definidas novas condicionantes e critérios. O arranjo também assumiu um caráter bastante experimental, pois a execução do Programa Bolsa Família foi pensada de "forma descentralizada, por meio da conjugação de esforços entre os entes federados, observada a intersetorialidade, a participação comunitária e o controle social" (art. 3º). O CadÚnico também ficou sob responsabilidade do Conselho Gestor Interministerial do Programa Bolsa Família.

Conforme estudo intitulado "Proteção de dados em políticas de proteção social: contribuições a partir do Programa Bolsa Família", a essência do Bolsa Família é a focalização, que serve do cruzamento de várias bases de dados para encontrar os cidadãos que mais necessitam do benefício e para identificar

---

um grande debate sobre interoperabilidade de dados pessoais de bases de dados de unidades governamentais distintas.

15 Estabelecia o Decreto: "Os dados e as informações coletados serão processados pela Caixa Econômica Federal, que procederá à identificação dos beneficiários e atribuirá o respectivo número de identificação social, de forma a garantir a unicidade e a integração do cadastro, no âmbito de todos os programas de transferência de renda, e a racionalização do processo de cadastramento pelos diversos órgãos públicos".

16 O programa tinha como finalidade a unificação dos procedimentos de gestão e execução das ações de transferência de renda do Governo Federal, especialmente as do Programa Nacional de Renda Mínima vinculado à Educação - "Bolsa Escola", instituído pela Lei no 10.219, de 11 de abril de 2001, do Programa Nacional de Acesso à Alimentação - PNAA, criado pela Lei no 10.689, de 13 de junho de 2003, do Programa Nacional de Renda Mínima vinculada à saúde - "Bolsa Alimentação", instituído pela Medida Provisória no 2.206-1, de 6 de setembro de 2001, do Programa Auxílio-Gás, instituído pelo Decreto no 4.102, de 24 de janeiro de 2002, e do Cadastramento Único do Governo Federal, instituído pelo Decreto no 3.877, de 24 de julho de 2001.

inconsistências que podem levar à exclusão do programa. Entre 2003 e 2020, o Bolsa Família cadastrou 73 milhões de brasileiros (FRAGOSO *et al.*, 2021, p. 9). Ele consolidou, em uma base de dados, "dados de identificação e caracterização de famílias e pessoas em situação de vulnerabilidade econômica (renda mensal de até meio salário-mínimo por pessoa ou total família de até 3 salários-mínimos)" (FRAGOSO *et al.*, 2021, p. 9).

O percurso dos dados pessoais é bastante complexo. Inicialmente, o cidadão se cadastra em um Centro de Referência de Assistência Social (CRAS). Não é necessário que todos os membros da família compareçam, pois uma pessoa pode ser nomeada "Responsável pela Unidade Familiar", preferencialmente a mulher (VALENTE *et al*., 2021). Nesse cadastro, apresentam-se os dados de certidão de nascimento, certidão de casamento, CPF, RG, carteira de trabalho ou título de eleitor. Pode-se exigir também declaração escolar das crianças e autodeclaração de renda. O questionário também focaliza informações como número de pessoas no mesmo domicílio, escolaridade, condições de moradia, condições de acesso, presença de deficiências que possam afetar membros da família, pertencimento a grupos tradicionais e específicos.

Além do percurso interno para aprovação e seleção dos beneficiários, os dados do Cad Único também são compartilhados com entidades estatais e não estatais. De acordo com Fragoso *et al.* (2021), isso pode ocorrer por meio de sistemas da informação integrados, extração da base completa a partir de solicitação, e consulta no Sistema de Consulta, Seleção e Extração de Informações do CadÚnico. O acesso à base também se dá pelo Sistema de Benefícios ao Cidadão da Caixa Econômica Federal.

Em 2010, a ideia da LGPD gerou estranhamento dentro do governo federal. Seria necessário obter o consentimento livre, informado e específico de todos os beneficiários para todas as hipóteses de tratamento de dados pessoais? Seria lícito tratar dados pessoais que revelassem condições de saúde (pessoas com deficiência) e informações étnicas?

É claro que a LGPD traça uma diferença entre o *dado pessoal* e o *dado pessoal sensível*. Este último é qualificado como "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou

à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Tais dados possuem sim um grau elevado de proteção, pois podem acentuar discriminações e afetam os direitos da personalidade das pessoas (MULHOLLAND, 2018).

No entanto, não há proibição de tratamento desses dados para políticas públicas. A LGPD traça uma diferença fundamental entre dois tipos de exigências legais para tratamento de dados pessoais. Se o tratamento de dados pessoais não envolve dados pessoais sensíveis, os fundamentos jurídicos estão no art. 7º da legislação. Eles permitem dez diferentes situações jurídicas para tratamento de dados pessoais. Se o tratamento envolve dados pessoais sensíveis, os critérios são mais reduzidos, não sendo permitido o "legítimo interesse do controlador"[17].

No caso do Programa Bolsa Família, o consentimento, "de forma específica e destacada, para finalidades específicas" (art. 11, I) é dispensável para os principais elementos da política pública, pois a base legal é o "tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos" (art. 11, II, b). O consentimento só é obtido pela Caixa Econômica Federal para o envio de e-mails e mensagens por celular, sendo uma base legal para um tratamento específico, que é a comunicação em meio mais invasivo, por assim dizer, por dispositivo pessoal.

Conforme diz a LGPD, se uma política pública está estruturada em legislação, os tratamentos de dados pessoais para execução da política pública possuem uma base legal específica (art. 11, II, b). É o caso do Bolsa Família, que foi reestruturado pela Lei n. 14.601/2023. A lei define que o Programa Bolsa Família constitui etapa do processo gradual e progressivo de implementação da renda básica de cidadania, de acordo com parágrafo único do art. 6º da Constituição Federal. O tratamento de dados pessoais é legitimado para operacionalizar os três objetivos do Programa, estabelecidos por lei: (i) combater a fome, por meio da transferência direta de renda às famílias beneficiárias, (ii)

17 Estabelece a LGPD neste ponto: "Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei".

contribuir para a interrupção do ciclo de reprodução da pobreza entre as gerações, (iii) promover o desenvolvimento e a proteção social das famílias, especialmente as crianças, dos adolescentes e dos jovens em situação de pobreza (art. 3º, Lei n.º 14.601/2023).

A utilização dos dados pessoais sensíveis está legitimada pela estruturação das condicionantes da política pública, tal como no art. 10 da Lei n.º 14.601/2023. Portanto, a utilização dos dados pessoais de saúde serve especificamente à análise de realização de exame pré-natal, cumprimento do calendário nacional de vacinação e acompanhamento nutricional de crianças de até sete anos de idade. Todas essas utilizações legítimas estão previstas em lei federal, o que dá amparo para que o tratamento ocorra para essas finalidades.

A legislação também é específica em definir que o controlador de dados pessoais é o Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome. A Caixa Econômica Federal é definida como “agente operador e pagador do Programa Bolsa Família”, mediante condições pactuadas com o governo federal. A lei federal também prevê que podem ser contratadas instituições públicas e privadas para apoiar a operacionalização e pagamento dos benefícios do Programa Bolsa Família.

O Programa Bolsa Família não é isento de críticas, do ponto de vista da privacidade e proteção de dados pessoais. Valente *et al.* (2021) apontam riscos, como as autorizações concedidas às distribuidoras de energia para acessar integralmente a base de dados do CadÚnico e riscos de utilização dessas informações para campanhas eleitorais. As autoras apontam para uma coleta pouco orientada por imperativos de minimização (princípio da necessidade) e poucas políticas de acesso e segurança da informação (VALENTE *et al*., 2021). É evidente, portanto, que a LGPD não visa *atrapalhar as políticas públicas*, mas sim melhorá-las e torná-las mais justas.

Como defendem Gasiola *et al*. (2021), dados e informações são imprescindíveis na organização interna dos órgãos e entes públicos. Uma boa gestão da informação, em conformidade com a LGPD, significa também o cumprimento do princípio da eficiência previsto na Constituição Federal. A LGPD possui um capítulo específico sobre “tratamento de dados pessoais pelo poder público”, do art. 23 ao art. 30. Esses artigos definem algumas balizas normativas

cruciais, como a "persecução do interesse público" e o tratamento para "atendimento de sua finalidade pública" (art. 23, LGPD). Há duas condicionantes especiais: a transparência ativa no provimento de informações sobre finalidade do tratamento de dados, procedimentos e práticas utilizadas para execução das atividades; e indicação de um encarregado quando realizem operações de tratamento de dados.

Em 2023, a encarregada pela proteção de dados pessoais do Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome é Eliana Pinto, nomeada pela Portaria MC n.º 538/2021.[18] Qualquer requisição de acesso aos dados pessoais pode ser feita pela plataforma Fala.Br, a partir da integração com dados do Gov.br, que permite o rápido peticionamento pelo sistema de Ouvidoria e Acesso à Informação.

4. A COMPATIBILIZAÇÃO DA LGPD COM UMA CULTURA DE DADOS ABERTOS

A LGPD possui uma conexão intrínseca com dados abertos. O capítulo sobre tratamento de dados pessoais pelo poder público possui uma regra importante, que determina que os dados pela administração pública deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral (art. 25, LGPD). O "uso compartilhado de dados pessoais pelo Poder Público", no entanto, deve "atender a finalidades específicas de execução de políticas públicas" (art. 26, LGPD).

Há um grande debate sobre a compatibilização da LGPD com a Lei de Acesso à Informação. Gasiola *et al.* (2021) chegam a afirmar que "a interação entre o direito de acesso às informações administrativas e a proteção de dados pessoais constitui a principal questão que o direito administrativo da proteção de dados precisa resolver" (GASIOLA *et al*., 2021, p. 184).

Enquanto a LAI preocupa-se com "o acesso a informações" assegurado na Constituição Federal, a LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o "objetivo de proteger os direitos fundamentais

18 Ver https://www.gov.br/mds/pt-br/acesso-a-informacao/lgpd/encarregado-da-lgpd

de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"[19]. Retomando uma antiga expressão de Vittorio Frosini, tanto os direitos de acesso à informação como o direito de proteção contra abusos nos usos de dados pessoais são "as duas faces de Janus" (FROSINI, 1995) dos novos direitos informáticos surgidos no século XX. Além do direito à informação no sentido de poder informar (buscar e produzir informações) e de acessar informações de interesse público, as democracias precisam instituir um "direito reflexivo" (FROSINI, 1995), no sentido de um "direito do cidadão de acessar informações sobre si mesmo, ou seja, checar, corrigir e refutar a propagação de seus dados armazenados em bancos de dados" (FROSINI, 1995, p. 13).

Não deve existir incompatibilidade entre acesso à informação e proteção de dados pessoais, pois seus fundamentos residem nessa concepção democrática dos direitos informáticos (ARCOVERDE; RAMOS; ZANATTA, 2021). O que tem ocorrido – e até mesmo assustado gestores públicos (RAMOS *et al.*, 2022) – é um desvirtuamento do fundamento de "liberdade de expressão, de informação, de comunicação e de opinião" (art. 2º, III, LGPD) em razão de solicitações de não divulgação de informações pessoais por serem, supostamente, uma violação à imagem e honra, como ocorreu em decisões da Controladoria Geral da União em casos envolvendo solicitação de acesso a dados de proprietários rurais constantes do Cadastro Ambiental Rural (VERGILI; SALIBA, 2023).

O que ocorreu no Brasil, entre 2020 e 2022, foi um desvirtuamento da lógica de interpretação da LAI e da LGPD. Infelizmente, partes interessadas na ocultação de informações de interesse público mobilizaram o art. 31 da LAI ("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") para fazer solicitações administrativas de "acesso restrito", chegando ao cúmulo de pedidos de restrição de acesso de até cem anos. A própria LAI, no entanto, estipula que esse controle individual, por meio do consentimento, é dispensável nos casos de informações de proteção do interesse público e geral preponderante.

Como demonstrado por vários autores (ARCOVERDE; RAMOS; ZANATTA, 2021; GASIOLA *et al.*, 2021; VERGILI; SALIBA, 2023), não há uma questão de

19 LGPD, art. 1º.

antinomia da LGPD com a LAI ou de supremacia dos argumentos de intimidade e vida privada. O problema fundamental foi de exercício interpretativo pelas autoridades, em casos concretos. Isso gerou uma altíssima demanda de reversibilidade de decisões administrativas que foram iniciadas pela Controladoria Geral da União em 2023, em uma perspectiva de rever milhares de decisões de má interpretação entre as colisões entre privacidade e dados abertos.

O problema atual é de conhecimento dos gestores públicos com relação às dinâmicas de funcionamento da LGPD, evitando essas equiparações com a ideia de sigilo e ocultação da informação. A tensão provocada pela proteção de dados pessoais é de outra ordem. Como reconhecido por Gasiola *et al.* (2021), enquanto a administração pública é obrigada a dar publicidade de seus atos e fornecer acesso às informações administrativas, exige-se a proteção dos dados pessoais contra qualquer operação de tratamento de dados ilegítima. O conflite exige, portanto, "ponderação, na forma de uma restrição recíproca aos direitos fundamentais" (GASIOLA *et al*., 2021). Há um mandamento de transparência ativa reconhecido no direito brasileiro, o que exige que a administração pública amplie o acesso à informação de forma controlada e apurada.

Parte deste conflito está sendo solucionado pela contundente atuação da Controladoria Geral da União. Já em 2022, o ministro Wagner Rosário (CGU) editou o Enunciado n. 4/2022, que definiu que a LAI, a Lei nº 14.129/2021 (Lei de Governo Digital) e a LGPD são sistematicamente compatíveis entre si e harmonizam os direitos fundamentais do acesso à informação, da intimidade e da proteção aos dados pessoais, não havendo antinomia entre seus dispositivos. O Enunciado também deu primazia à lógica de abertura de dados ao afirmar que a LAI, por ser mais específica, é a norma de regência processual e material a ser aplicada no processamento desta espécie de processo administrativo. Em 2022, a CGU firmou Acordo de Cooperação Técnica com a ANPD para garantir a interpretação sistemática da LAI com LGPD, evitando a utilização dos argumentos de proteção de dados pessoais para fechamento de informações de interesse público. A parceria deu origem a um trabalho interpretativo, direcionado a gestores públicos.

Em 2023, já no governo Lula, o ministro Vinicius Marques de Carvalho editou a Portaria Normativa CGU n.º 71/2023, com doze enunciados à aplicação

da LAI. A Portaria diz, por exemplo, que informações sobre “entradas e saídas de pessoas em órgãos públicos” são passíveis de acesso público, bem como informações sobre registros de entradas e saídas em residências oficiais, informações sobre licitações e contratos por órgãos de polícia e inteligência, informações sobre currículos de agentes públicos, e informações referentes a valores de benefícios pagos e identificação de beneficiários em programas sociais, “desde que respeitado a privacidade dos dados pessoais e dos dados sensíveis”. Mais importante, é o Enunciado 12/2023, que diz o seguinte:

> O fundamento “informações pessoais” não pode ser utilizado de forma geral e abstrata para se negar pedidos de acesso a documentos ou processos que contenham dados pessoais, uma vez que esses podem ser tratados (tarjados, excluídos, omitidos, descaracterizados etc.) para que, devidamente protegidos, o restante dos documentos ou processos solicitados sejam fornecidos, conforme preceitua o § 2º do art. 7º da Lei nº 12.527, de 18 de novembro de 2011, assegurando-se o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo. Além disso, a proteção de dados pessoais deve ser compatibilizada com a garantia do direito de acesso à informação, podendo aquela ser flexibilizada quando, no caso concreto, a proteção do interesse público geral e preponderante se impuser, nos termos do art. 31, § 3º, inciso V da Lei n. 12.527, de 2011, e dos arts. 7º, § 3º, e 23, caput, da Lei nº 13.709, de 14 de agosto de 2018 (CGU, 2023).

Com essas movimentações da CGU, juntamente com a sistemática pressão da sociedade civil organizada pelo Fórum de Acesso às Informações de Interesse Público e o posicionamento em favor da abertura de dados de membros da Autoridade Nacional de Proteção de Dados Pessoais (WIMMER, 2021), vai se criando uma imagem mais clara da compatibilização da LGPD com a cultura de dados abertos no Brasil.

Exercícios de ponderação sobre potenciais violações aos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade não significam que a LGPD promove o fechamento das informações. Exemplo claro disso é a iniciativa do Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio) de divulgar, a partir de agosto de 2023, os dados completos de nome, CPF e CNPJ de autuados por infrações ambientais e de quem teve áreas embargadas pela autarquia. A abertura de dados não fere a LGPD pois trata-se de medida justa para execução de políticas públicas de defesa do meio ambiente que são comandadas pelo ICMBio.

A disponibilização dos dados na Plataforma Dados Abertos ICMBio, disponibilizadas pela Divisão de Informações Geoespaciais e Monitoramento (DGEO), é um exemplo claro de correta interpretação da LGPD no caso de execução de políticas públicas e proteção ambiental. Esse é o mesmo entendimento de Vergili e Saliba (2023), em estudo promovido sobre abertura e disponibilização de informações de pessoas que cometeram ilícitos ambientais e que estão registradas no Cadastro Ambiental Rural. A LGPD, neste caso específico, é instrumental para criar condições procedimentais de uma política pública que objetiva dar mais visibilidade e transparência aos ilícitos ambientais, como casos de criação de gados em territórios indígenas ou áreas de preservação ambiental. Não há ilícito na divulgação de informações pessoais de produtores rurais em condição de violação das normas ambientais, pois tal divulgação relaciona-se com uma política pública da República. Nesse sentido, há uma preponderância do interesse público relacionado à coibição de novos ilícitos ambientais e a ampliação do acesso à informação – para cidadãos, jornalistas e esfera pública – com relação a quem comete tais ilícitos.

Os dispositivos previstos na LGPD permitem plena compatibilização com o espírito democrático da legislação de dados abertos no Brasil. O que a LGPD irá exigir é uma diligência com a natureza dos dados tratados, suas finalidades, a localização do interesse público em sua disponibilização e a correta identificação da base legal para tratamento dos dados.

5. CONCLUSÃO

A proteção de dados pessoais representa um avanço significado no sistema normativo brasileiro, criando condições de tratamento lícito de dados pessoais e formulação de políticas públicas, juntamente com a afirmação de direitos fundamentais fundados na ideia constitucional da dignidade, que são centrais em uma sociedade datificada e mediada por fluxos de informação do ponto de vista da cidadania (RODOTÁ, 2011). Além da efetividade da LGPD desde 2020, o julgamento de importantes casos no Supremo Tribunal Federal – como o caso IBGE (ADI 6387) e o caso do Cadastro Base do Cidadão (ADPF 6649) – permitiram que o Judiciário reconhecesse o caráter autônomo do direito à

proteção de dados pessoais, que não é mais visto com equivalente ao sigilo ou ao direito à privacidade.

Conforme argumentado por diversos autores no Brasil (DoNEDA, 2017; DONEDA, 2021; FRAZÃO; OLIVA; TEPEDINO, 2019; MULHOLLAND, 2018; BIONI; ZANATTA, 2021), a existência de uma normativa geral de proteção de dados pessoais produz segurança jurídica, cria condições de tratamento lícito de dados pessoais, prevê mecanismos claros de responsabilização e habilita a formulação de políticas públicas que estejam alinhadas aos princípios gerais de tratamento de dados pessoais, como a identificação de uma finalidade legítima, a escolha dos meios corretos de tratamento de dados pessoais, a responsabilidade preventiva com relação a danos e um compromisso com a dignidade da pessoa humana, considerando que, mesmo em uma situação de execução de políticas públicas pelo Estado, o cidadão estará no centro das atenções como titular de dados pessoais.

Conforme argumentado neste artigo, a criação de uma adequada cultura de experimentação em políticas públicas e abertura de dados exige um estudo aprofundado das origens da LGPD e de seu conteúdo. Gestores públicos podem se beneficiar enormemente de uma correta compreensão da LGPD. A legislação não se confunde com normas sobre sigilo e não impõe confidencialidade sobre informações da administração pública. Pelo contrário, a LGPD facilita e induz o fluxo de informações na sociedade, desde que o tratamento de dados seja leal, lícito e justo. A LGPD é uma norma flexível, arrojada, formulada para as necessidades de uma sociedade da informação no século XXI. É preciso, portanto, eliminar algumas concepções problemáticas que ainda persistem no imaginário público e que prejudicam a internalização dos valores da LGPD, como a ideia de que a lei impõe sigilo automático às informações pessoais – ou a ideia de que a lei cria um obstáculo elevado para inovação e para usos secundários de dados pessoais na redefinição de políticas públicas.

No entanto, como argumentado, a LGPD não se confunde com sigilo e direito à privacidade. A LGPD não atrapalha políticas públicas, mas sim fomenta políticas públicas intensivas em dados de forma justa. A LGPD não colide com uma cultura de dados abertos. Ela incentiva uma disponibilização lícita de dados, uma vez que seja identificado seu interesse público em ambiente democrático.

Ao aprofundar os exemplos do Bolsa Família e do Cadastro Ambiental Rural neste artigo, buscou-se exemplificar como que políticas públicas ligadas a temas centrais da agenda brasileira, como combate à fome e proteção ambiental (temas considerados como estratégicos pelo Brasil em 2024 na Presidência do G20), estão intimamente ligadas à correta utilização dos dados pessoais e a conformação da LGPD com as políticas públicas. Nesse sentido, defende-se que a LGPD possa ser enxergada, por gestores públicos, a partir do prisma de suas funções procedimentais em políticas públicas, sendo compatível com normas pré-existentes sobre acesso a informação, como a Lei de Acesso à Informação. A proteção de dados pessoais deve ser compatibilizada com a garantia do direito de acesso à informação, do mesmo modo que deve servir de fundamento para a concepção de políticas públicas.

REFERÊNCIAS

ALLEN, A. L.; MACK, E. How privacy got its gender. **Northwestern Illinois University Law Review**, v. 10, p. 441-478, 1989.

ALLEN, A. L. **Uneasy access**: Privacy for women in a free societ**y**. Rowman & Littlefield, 1988.

ARCOVERDE, L.; RAMOS, M. V.; ZANATTA, R. Transparência sob ataque. **Folha de São Paulo**. 4 nov. 2021.

BENNETT, C. J. **Regulating privacy**: Data protection and public policy in Europe and the United States. Itaca: Cornell University Press, 1992.

BEZERRA, M. R. B. Autoridade nacional de proteção de dados pessoais: a importância do modelo institucional independente para a efetividade da lei. **Caderno Virtual**, v. 2, n. 44, 2019.

BIONI, B. R. **Regulação e proteção de dados pessoais**: o princípio da accountability. Rio de Janeiro: Forense, 2022.

BIONI, B.; ZANATTA, R. A infraestrutura jurídica da economia dos dados: dos princípios de justiça às leis de dados pessoais, in: DE SOUZA, A. R. *et al.* **Direito Digital**: direito privado e internet. Indaiatuba: Editora Foco, 2021.

BOBBIO, N. Da Norma Jurídica – Tradução em português. **Novissimo Digesto italiano. Turim: Torinese**, 1958.

BRASIL. **Constituição Federal de 1934**. Brasília: Governo Federal, 1934.

BOULET, R.; LAJAUNIE, C.; MAZZEGA, P. (Ed.). **Law, public policies and complex systems: networks in action**. Cham: Springer, 2019.

CETIC. **Privacidade e Proteção de Dados Pessoais 2021**: perspectivas de indivíduos, empresas e organizações públicas no Brasil. São Paulo: Comitê Gestor da Internet, 2022.

CITRON, D. K. Sexual privacy. **Yale Law Journal**, v. 128, p. 1870, 2018.

CGU. **Portaria Normativa CGU n. 71, de 10 de abril de 2023**. Brasília: Controladoria-Geral da União, 2023.

COHEN, J. E. Examined lives: Informational privacy and the subject as object. In: **Law and Society Approaches to Cyberspace**. Routledge, p. 473-538, 2017.

CONSELHO DA EUROPA. **Convenção 108+: convenção para a proteção das pessoas relativamente ao tratamento de dados de caráter pessoal**. Decisão do Comitê de Ministros (128ª sessão dos comitês de ministros), Elsinore, 18 de maio de 2018.

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

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, v. 12, n. 2, p. 91-108, 2011.

DONEDA, D. A proteção da privacidade e de dados pessoais no Brasil, **Itaú Cultural**, v. 16, pp. 136-146, 2017.

DONEDA, D. Registro da sustentação oral no julgamento da ADI 6389, sobre a inconstitucionalidade do art. 2º, caput e §§1º e 3º da MP 954/2020. **Civilistica.com**. Rio de Janeiro, a. 9, n. 1, 2020.

DONEDA, D.; ZANATTA, R. A. F. Personality rights in Brazilian data protection law: a historical perspective. In**:** ALBERS, Marion; SARLET, Ingo. **Personality and Data Protection Rights on the Internet: Brazilian and German Approaches**. Cham: Springer International Publishing, 2022. p. 35-53.

FRAZÃO, A.; OLIVA, M. D.; TEPEDINO, G. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

FROSINI, V. Towards Information Law. **Informatica e diritto**, v. 4, n. 2, p. 7-16, 1995.

GARCIA, B. Violação de segredo. **Revista da Faculdade de Direito, Universidade de São Paulo**, v. 44, p. 51-67, 1949.

GASIOLA, G.; MACHADO, D.; SCHERTEL MENDES, L. A administração pública entre transparência e proteção de dados, **Revista de Direito do Consumidor**, v. 135, p. 179-201, 2021.

GOVERNO DO PARANÁ. **Introdução à Gestão Pública: o perfil do gestor público**. Curitiba: Secretaria de Educação do Paraná, 2018. Disponível em: http://www.gestaoescolar.diaadia.pr.gov.br/arquivos/File/gestao_em_foco/gestao_publica_unidade2.pdf

MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, L. S.; DONEDA, D. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, v. 120, p. 555, 2018.

MEZZAROBA, O. **Manual de metodologia da pesquisa no direito**. 6 ed. São Paulo: Saraiva, 2014.

MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 159-180, 2018.

QUEIROZ, R. M. R.; PONCE, P. P. Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**, São Paulo, n. 1, p. 64-90, 2020.

RAMOS, M. F. *et al.* **Um país sob censura: sigilos, distorção da lei de proteção de dados e ataque a servidores são as marcas da gestão Bolsonaro**. São Paulo: De Olho nos Ruralistas, 2022. Disponível em: https://deolhonos-ruralistas.com.br/wp-content/uploads/2022/09/Um-Pais-sob-Censura-2022-ptbr-1.pdf.

RODOTÀ, S. La dignità della persona. **Scuola di Cultura Costituzionale**, v. 14, 2011.

SCHAEFER, E. Protection Against Invasion of Privacy in Communications: The Olmstead Case Sustained. **Wash. & Lee L. Rev.**, v. 3, p. 270, 1941.

SILVA, V. A. **Direito Constitucional Brasileiro**. São Paulo: Editora da Universidade de São Paulo, 2021.

TEPEDINO, G. **Temas de Direito Civil**. Tomo II. Rio de Janeiro: Renovar, 2006.

TORRES, I. M. A importância da implementação da Autoridade Nacional de Proteção de Dados. **Revista Eletrônica da PGE-RJ**, v. 4, 2021.

TREIN, P.; VARONE, F. Citizens' agreement to share personal data for public policies: trust and issue importance. **Journal of European Public Policy**, p. 1-26, 2023.

VALENTE, M. G.; NERIS, N.; FRAGOSO, N.. Presa na Rede de Proteção Social: Privacidade, gênero e justiça de dados no Programa Bolsa Família. **Novos estudos CEBRAP**, v. 40, p. 11-31, 2021.

VERGILI, G.; SALIBA, P. **Políticas ambientais, transparência pública e proteção de dados: a viabilidade jurídica para compartilhamento de dados pessoais no âmbito do Cadastro Ambiental Rural**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2023.

WESTIN, Alan F. **Computers, personnel administration, and citizen rights**. US Department of Commerce, National Bureau of Standards, 1979.

WESTIN, A. F. Privacy, technology, and regulation. In: **Proc. of a symposium to explore the computer's impact on society on The computer culture**. 1985. p. 136-148.

WIMMER, M. O regime jurídico do tratamento de dados pessoais pelo poder público. In: MENDES, L. S. *et al.* **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

WHITMAN, J. Q. The two western cultures of privacy: Dignity versus liberty. **Yale Law Journal**, v. 113, p. 1151, 2003.

ZANATTA, R. A. F. **A proteção coletiva dos dados pessoais no Brasil: vetores de interpretação**. Belo Horizonte: Letramento, 2023.