NATALIA LANGENEGGER

PUBLICAÇÃO E COMPARTILHAMENTO DE DADOS PELO PODER PÚBLICO: EQUACIONANDO TRANSPARÊNCIA, EFICIÊNCIA E PRIVACIDADE

Tese de Doutorado

Orientador: Professor Dr. Marcos Paulo Veríssimo

UNIVERSIDADE DE SÃO PAULO

FACULDADE DE DIREITO

São Paulo - SP

2023

NATALIA LANGENEGGER

PUBLICAÇÃO E COMPARTILHAMENTO DE DADOS PELO PODER PÚBLICO: EQUACIONANDO TRANSPARÊNCIA, EFICIÊNCIA E PRIVACIDADE

Versão Original

Tese apresentada à Banca Examinadora do Programa de Pós-Graduação *Stricto Sensu* da Faculdade de Direito da Universidade São Paulo, como requisito para obtenção do título de Doutor em Direito, na área de concentração Direito do Estado, sob a orientação do Professor Dr. Marcos Paulo Veríssimo.

UNIVERSIDADE DE SÃO PAULO

FACULDADE DE DIREITO

São Paulo - SP

2023

Catalogação da Publicação
Serviço de Biblioteca e Documentação
Faculdade de Direito da Universidade de São Paulo

Langenegger, Natalia
Publicação e compartilhamento de dados pelo poder público: equacionando transparência, eficiência e privacidade ; Natalia Langenegger ; orientador Marcos Paulo Veríssimo -- São Paulo, 2023.
470 p.
Tese (Doutorado - Programa de Pós-Graduação em Direito do Estado) - Faculdade de Direito, Universidade de São Paulo, 2023.

1. Compartilhamento e Publicação de Dados Pessoais. 2. Interesse Público. 3. Transparência e Acesso à Informação. 4. Eficiência Governamental. 5. Privacidade e Proteção de Dados Pessoais. I. Veríssimo, Marcos Paulo , orient. II. Título.

RESUMO

LANGENEGGER, Natalia. **Publicação e compartilhamento de dados pelo poder público**: equacionando transparência, eficiência e privacidade. 2023. 470 p. Tese Doutorado em Direito do Estado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2023.

A adoção de tecnologias de informação e comunicação e de conectividade por governos nas últimas décadas tem permitido maior eficiência e transparência na prestação de serviços públicos. Ela também permite que governos ampliem sua capacidade de coletar e processar dados, muitos dos quais são referentes a uma pessoa natural, acabando por impor riscos aos direitos fundamentais de privacidade e proteção de dados pessoais de cidadãos. Nesses casos, os direitos de privacidade e proteção de dados pessoais entram em conflito com o direito de acesso à informação e os princípios da publicidade e transparência governamental. Diante desse cenário, o objetivo desta tese é apresentar meios para equacionar a transparência e a eficiência governamental com a privacidade e proteção de dados pessoais na publicação e no compartilhamento de dados pessoais por governos. Além disso, em vista da ausência de parâmetros legais claros, na prática, a privacidade e proteção de dados pessoais têm sido manejadas de formas distintas para o compartilhamento e para a publicação de dados pelo poder público, que são modalidades de divulgação a terceiros de dados pessoais mantidos por governos. Assim, esta tese também busca assegurar que o equacionamento proposto observe alguma uniformidade, respeitadas as particularidades dos casos concretos. Para tanto, foi realizada pesquisa dogmático-jurídica para apresentar procedimento capaz de acomodar os interesses supostamente conflitantes. Com o apoio da legislação e de exemplos extraídos de experiências estrangeiras, o procedimento proposto conta com três principais etapas: a definição do escopo da publicação ou do compartilhamento, a identificação do interesse público nessa atividade, e a adoção de medidas para o compartilhamento ou a publicação em observância à privacidade e à proteção de dados pessoais. Na primeira etapa, o agente público deverá identificar a presença de dados pessoais, assim como as finalidades e necessidade da publicação, e do compartilhamento proposto. Diante disso, será possível seguir para a identificação do interesse público no caso concreto, que exige a mediação de interesses conflitantes, por meio do teste de balanceamento. O resultado desta etapa poderá determinar tanto a restrição de acesso a dados como a sua publicação ou compartilhamento, observadas medidas previstas na legislação e a adoção de medidas de mitigação de riscos. Com isso, é possível o compartilhamento e a publicação de dados pessoais pelo poder público, sempre que isso for de interesse público, em respeito à privacidade e proteção de dados pessoais.

Palavras-chave: Compartilhamento e Publicação de Dados Pessoais. Interesse Público. Transparência e Acesso à Informação. Eficiência Governamental. Privacidade e Proteção de Dados Pessoais. Tratamento de Dados Pessoais pelo Poder Público.

ABSTRACT

LANGENEGGER, Natalia. **Publication and sharing of data by public authorities: balancing transparency, efficiency and privacy** 2023. 470 p. Tese Doutorado em Direito do Estado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2023.

The adoption of information and communication technologies and of connectivity by governments in recent decades has allowed greater efficiency and transparency in the provision of public services. It also allows governments to expand their ability to collect and process data, much of which relates to a natural person, ultimately posing risks to the fundamental rights of privacy and protection of personal data of citizens. In these cases, the rights of privacy and protection of personal data conflict with the right of access to information and the principles of government transparency and publicity. Given this scenario, the objective of this thesis is to present means to balance transparency and government efficiency with privacy and protection of personal data in the publication and sharing of personal data by governments. In addition, in view of the absence of clear legal parameters, in practice, the privacy and protection of personal data have been handled in different ways for the sharing and publication of data by the public authorities, which are genres for disclosing to third parties' personal data held by governments. Thus, this thesis also seeks to ensure that the proposed balancing observes some uniformity, respecting the particularities of concrete cases. Therefore, dogmatic-legal research was carried out to present a procedure capable of accommodating these supposedly conflicting interests. With the support of legislation and examples drawn from foreign experiences, the proposed procedure has three main steps: defining the scope of the publication or sharing, identifying the public interest in this activity, and adopting measures for sharing or publishing data in compliance with privacy and protection of personal data. In the first stage, the public agent must identify the presence of personal data, as well as the purposes and need for the proposed publication and sharing. Given this, it will be possible to proceed to the identification of the public interest in the concrete case, which requires the mediation of conflicting interests, by means of a balancing test. The result of this step may determine the restriction of access to data or its publication or sharing, observing the requirements provided for in the legislation and the adoption of risk mitigation measures. With this, it is possible for public authorities to share and publish personal data, whenever this is in the public interest, with respect for privacy and protection of personal data.

Keywords: Sharing and Publication of Personal Data. Public interest. Transparency and Access to Information. Government Efficiency. Privacy and Personal Data Protection. Processing of Personal Data by the Government.

RÉSUMÉ

LANGENEGGER, Natalia. Partage et Publication des Données Personnelles par le gouvernement: assimiler transparence, efficacité et confidentialité. 2023. 470 p. Tese Doutorado em Direito do Estado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2023.

L'adoption des technologies de l'information et de la communication, bien comme de la connectivité par les gouvernements au cours des dernières décennies, a permis plus d´efficacité et de transparence dans la cadre de la prestation des services publics. Cela permet également aux gouvernements de comprendre leur capacité à collecter et à traiter des données, dont une grande partie concerne des personnes physiques, ce qui, à terme, pose des risques pour les droits fondamentaux à la vie privée et à la protection des données personnelles des citoyens. Dans ces cas, les droits à la vie privée et à la protection des données personnelles entrent en conflit avec le droit d'accès à l'information et les principes de publicité et de transparence gouvernementale. Compte tenu de ce scénario, l'objectif de cette thèse est de présenter des moyens d'assimiler la transparence et l'efficacité du gouvernement à la confidentialité et à la protection des données personnelles dans la publication et le partage des données personnelles par les gouvernements. En outre, compte tenu de l'absence de paramètres juridiques clairs, dans la pratique, la confidentialité et la protection des données personnelles ont été traitées de différentes manières pour le partage et la publication des données par les autorités publiques, qui sont des modalités de divulgation des données personnelles détenues par les gouvernements. Ainsi, cette thèse cherche également à s'assurer que l'équation proposée respecte une certaine uniformité, en respectant les particularités des cas concrets. Pour ce faire, une recherche dogmatico-juridique a été menée afin de présenter une procédure capable de concilier les intérêts supposés contradictoires. S'appuyant sur la législation et des exemples tirés d'expériences étrangères, la procédure proposée comporte trois grandes étapes: définir le périmètre de publication ou de partage, identifier l'intérêt public de cette activité, et adopter des mesures de partage ou de publication en le respectant la vie privée et la protection des données personnelles. Dans un premier temps, l'agent public doit identifier la présence de données personnelles, ainsi que les finalités et nécessités de publication, et le partage proposé. Compte tenu de cela, il sera possible de procéder à l'identification de l'intérêt public dans le cas concret, qui nécessite la médiation d'intérêts conflictuels, par le test d’equilibre. Le résultat de cette étape peut déterminer à la fois la restriction de l'accès aux données et leur publication ou partage, en respectant des mesures prévues par la législation et l'adoption de mesures d'atténuation des risques. Avec cela, il est possible pour les autorités publiques de partager et de publier des données personnelles, chaque fois que cela est dans l'intérêt public, en respectant la vie privée et de la protection des données personnelles.

Mots-clés: Partage et Publication des Données Personnelles. Intérêt public. Transparence et accès à l'information. Efficacité du gouvernement. Confidentialité et protection des données personnelles. Traitement des données personnelles par le gouvernement.

AGRADECIMENTOS

A conclusão desta pesquisa de doutorado não teria ocorrido sem o carinho e suporte da minha família e amigos. Em especial, destaco o amor e suporte da minha família, Henrique, Leigh, Patrícia e Ramiro, as palavras de apoio oferecidas pelos meus sogros Silvana e José Luís, e a alegria garantida pelos meus sobrinhos Denise, Martin, Martin, Raul e Otto. Agradeço também minha avó, tio Paulinho, tia Berenice, e minhas primas Paula e Ana Clara, que me acompanharam nas temporadas de estudo na fazenda, e à minha família do Canadá, pela compreensão com meus estudos natalinos mesmo após três anos separados pela pandemia.

Sobretudo, não consigo descrever a gratidão que sinto pela paciência, amor e participação ativa do meu marido Ivan durante todas as etapas desse processo doutoral. Ele me ajudou na delimitação do objeto de pesquisa, esteve ao meu lado nos momentos de estudo, e discutiu e revisou o conteúdo deste trabalho.

Em seguida, agradeço o professor Marcos Paulo Veríssimo pela orientação, e aos professores Ronaldo Lemos, Carlos Affonso, Mário Viola, Dennys Antonialli, Miriam Wimmer e Virgílio Afonso da Silva pelo diálogo sobre essa pesquisa. Suas contribuições foram centrais para desatar nós da tese e me oferecer segurança no caminho a ser percorrido. Lembro também do estímulo da professora Gisele Craveiro para eu aprofundar no doutorado tema de artigo elaborado em conjunto com Ivan e com o apoio de Francisco Brito Cruz, Mariana Valente e Dennys Antonialliinstitucional do InternetLab.

Finalmente, sou também muito grata ao suporte emocional assegurado por amigos, em especial Ariane Gomes, Fabiano Harada, Vivian Ferreira, Maria Camila Florêncio, Luciana Mattar, Marina Montes Bastos, Marina Jacob, Juana Pulido, Guilherme Moraes-Rego e Rafaela Frade Reis. Aos amigos Sofia Lima Franco, Juliana Ruiz, Marina Cardoso de Freitas, Diego Canabarro, Ricardo Dalmaso Caio César de Oliveira, Ramon Alberto, Paula Ponce, Juana Pulido, Francisco Brito Cruz, Mariana Valente, Nathalie Fragoso, Mateus Piva, Bruno Bioni, Flávia Parra, Isabela Parisio, Andréa Gobbato, Leonardo Chaim, Iasmine Favaro, Laura Matta, Gabriela Sanches, Eduarda Costa, Lívia Torres, Gabriela Moribe, Andréa Gobbato, Leonardo Chaim, Caio César de Oliveira, Ramon Alberto, Ricardo Dalmaso, Mateus Piva, Sarah Marinho, Patrícia Alencar, Francisco Brito Cruz, Mariana Valente, Nathalie Fragoso, Bruno Bioni, Rafael Zanatta, Pedro de Paula e Eduardo Spanó dedico um agradecimento destacado por terem, cada um à sua forma, contribuído com a elaboração desta

pesquisa, seja pela reflexão sobre o objeto de estudo, envio de materiais, ou revisão da escrita e conteúdo. Aos queridos Nikolay Bispo, Luiz Fernando Esteves, Ana Laura Martins, Rodrigo Nitrini e Milene Cristina agradeço por dividirem comigo as angústias do percurso do doutorado.

LISTA DE SIGLAS E ABREVIATURAS

Abin - Agência Brasileira de Inteligência

ANATEL - Agência Nacional de Telecomunicações

Art. – Artigo

ADI – Ação Direta de Inconstitucionalidade

ADPF – Ação de Descumprimento de Preceito Fundamental

ANPD - Autoridade Nacional de Proteção de Dados Pessoais

API - *Application Programming Interface*

BNDES - Banco Nacional de Desenvolvimento Econômico e Social

BNDESPAR - BNDES Participações S.A.

CADE - Conselho Administrativo de Defesa Econômica

Cafir - Cadastro de Imóveis Rurais

CCGD - Comitê Central de Governança de Dados

CDC - Código de Defesa do Consumidor

CDRD - *Consumer Data Research Center*

CEF - Caixa Econômica Federal

CEGE - Comitê Executivo de Governo Eletrônico

CF - Constituição da República Federativa do Brasil de 1988

CFOAB - Conselho Federal da Ordem dos Advogados do Brasil

CGU - Controladoria Geral da União

CIRMO - *Corporate Information and Records Management Office*

CMRI - Comissão Mista de Reavaliação de Informações

CNH - Carteira Nacional de Habilitação

CNJ – Conselho Nacional de Justiça

CNPJ - Cadastro Nacional da Pessoa Jurídica

CNPQ - Conselho Nacional de Desenvolvimento Científico e Tecnológico

COMAER - Comando da Aeronáutica

COMPAS - *Correctional Offender Management Profiling for Alternative Sanctions*

CPF - Cadastro de Pessoas Físicas

CRAS - Centros de Referência de Assistência Social

C4DC - Contracts for Data Collaboration

DEA - Digital Economy Act

Denatran - Departamento Nacional de Trânsito

DOI - Declaração de Operações Imobiliárias

EBC - Empresa Brasil de Comunicação S.A.

ECHR - *European Court of Human Rights*

EDPB - *European Data Protection Board*

EDPS - *European Data Protection Supervisor*

E-Digital - Estratégia Brasileira para a Transformação Digital

EGD - Estratégia de Governo Digital

E-Gov - Programa Governo Eletrônico

ENEM - Exame Nacional do Ensino Médio

e-PING - Padrões de Interoperabilidade do Governo Eletrônico

FCRB - Fundação Casa de Rui Barbosa

Febraban - Federação Brasileira de Bancos

FIPP - *Fair Information Principles*

FOI - *Freedom of Information Act*

FPF - *Future of Privacy Forum*

FTC - *Federal Trade Commission*

GDPR - *General Data Protection Regulation*

GSI - Gabinete de Segurança Institucional da Presidência da República

GSS - *Government Statistical Service*

GTI - Grupo de Trabalho Interministerial

G2G - Governo-Governo

G2B - Governo-Empresa

G2C - Governo-Cidadão

IBGE - Instituto Brasileiro de Geografia e Estatística

ICO - *Information Commissioner's Office*

IoT - *Internet of Things*

INAI - *Instituto Nacional de Transparência, Accesso à la Información y Proteção de Datos Personales*

INDA - Infraestrutura Nacional de Dados Abertos

Inep - Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira

INSS - Instituto Nacional do Seguro Social

IPC - *Information and Privacy Commissioner*

ITA - Instituto Tecnológico de Aeronáutica

LAI – Lei de Acesso à Informação (Lei n° 12.527/2011)

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

MCI - Marco Civil da Internet (Lei n° 12.965/2014)

MDS - Ministério de Desenvolvimento Social

MJ - Ministério da Justiça

MP - Medida Provisória

MPDFT - Ministério Público do Distrito Federal e dos Territórios

MPF - Ministério Público Federal

MPO - *Ministry Privacy Officers*

MRE - Ministério da Relações Exteriores

MRI - Comissão Mista de Reavaliação de Informações

MS - Mandado de Segurança

MTE - Ministério do Trabalho e Emprego

NF-e - Nota Fiscal Eletrônica

NIS - Número de Identificação Social

NSDEC - *National Statistician's Data Ethics Advisory Committee*

OAB - Ordem dos Advogados do Brasil

OAIC - *Office of the Australian Information Commissioner*

OCDE - Organização para Cooperação e Desenvolvimento Econômico

OEA - Organização dos Estados Americanos

ONS - *Office for National Statistics*

ONU - Organização das Nações Unidas

OPC - *Office of the Privacy Commissioner of Canada*

PBF - Programa Bolsa Família

PEC - Proposta de Emenda à Constituição

PET - *Privacy Enhancing Technologies*

PGR - Procuradoria-Geral da República

PL – Projeto de Lei

PLC - Projeto de Lei da Câmara

PR - Presidente da República

Prodeb - Companhia de Processamento de Dados do Estado da Bahia

Prodemge - Companhia de Tecnologia da Informação do Estado de Minas Gerais

Prodesp - Companhia de Processamento de Dados do Estado de São Paulo

Rais - Relação Anual de Informações Sociais

RE - Recurso Ordinário

RFB - Receita Federal do Brasil

RIPD - Relatório de Impacto à Proteção de Dados Pessoais

Renape - Registro Nacional de Pessoas Naturais

SCDP - Sistema de Concessão de Diárias e Passagens

Senacon - Secretaria Nacional do Consumidor

SERPRO - Serviço Federal de Processamento de Dados

Setur - Secretaria de Turismo do Espírito Santo

SIAFI - Sistema Integrado de Administração Financeira do Governo Federal

Siape - Sistema Integrado de Administração de Pessoal

SIORG - Base Referencial de Integração dos Sistemas

SIPE - Sistema Integrado de Administração de Pessoal

SISA - Sub-comitê de Integração de Sistemas Administrativos

SISBN - Sistema Brasileiro de Inteligência

SISP - Sistema de Administração de Recursos de Tecnologia da Informação

SNT - Sistema Nacional de Trânsito

STF – Supremo Tribunal Federal

STI - Subsecretaria de Tecnologia da Informação

STJ - Superior Tribunal de Justiça

STN - Secretaria do Tesouro Nacional

TCU - Tribunal de Contas da União

TIC - Tecnologias de Informação e Comunicação

TJUE - Tribunal de Justiça da União Europeia

ToS - Termos de Serviço

ToU - Termos de Uso

TSE - Tribunal Superior Eleitoral

UFG - Universidade Federal de Goiás

UFMG - Universidade Federal de Minas Gerais

YODA - *Yale University Open Data Access*

WP 29 - *Working Party 29*

LISTA DE QUADROS

Quadro 1: possíveis conceitos abrangidos pela divulgação de dados pessoais

Quadro 2: Tratamento de dados pelo poder público nas versões do Anteprojeto de Lei

Quadro 3: Conceitos de compartilhamento de dados nas versões do Anteprojeto de Lei

Quadro 4: Mudanças promovidas ao Projeto de Lei pelo Congresso Nacional

Quadro 5 - Emendas Parlamentares à MP nº 869/2018

Quadro 6: Comparativo das soluções apontadas pelas autoridades sobre privacidade na publicação e o compartilhamento de dados pessoais

Quadro 7: comparativo de conceituação legal de dado pessoal

Quadro 8: comparativo das bases legais previstas na LGPD

Quadro 9: Semelhanças e diferenças no direito de acesso a dados pessoais entre a Lei de Habeas Data, LAI, Lei nº 13.460/2017 e LGPD

SUMÁRIO

PARTE I TENSÕES ENTRE O COMPARTILHAMENTO E A PUBLICAÇÃO DE DADOS PELO PODER PÚBLICO COM A PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS DE CIDADÃOS 33

1 O PAPEL CENTRAL DO TRATAMENTO DE DADOS PARA AS ATIVIDADES DO PODER PÚBLICO 33

1.1 Evolução da tecnologia e tratamento de dados para novos modelos de governos 34

1.2 Benefícios do tratamento de dados pelo poder público 40

2 O PAPEL DO COMPARTILHAMENTO E DA PUBLICAÇÃO PARA AS ATIVIDADES DO PODER PÚBLICO 45

2.1 Publicação de dados: conceito e benefícios 46

2.2 Compartilhamento de dados: conceito e benefícios 50

2.3 Semelhanças e diferenças entre compartilhamento e publicação 53

3 RISCOS À PRIVACIDADE DECORRENTES DO TRATAMENTO DE DADOS PELO PODER PÚBLICO 59

3.1 A publicação e o compartilhamento de dados e os riscos à privacidade 61

3.2 Origem conceitual da proteção à privacidade e dados pessoais 67

4 CONCLUSÃO PARCIAL: NECESSIDADE DE MAIOR DIÁLOGO ENTRE TEORIAS 77

PARTE II PANORAMA DA LEGISLAÇÃO BRASILEIRA SOBRE O COMPARTILHAMENTO E A PUBLICAÇÃO DE DADOS PELO PODER PÚBLICO EM OBSERVÂNCIA À PROTEÇÃO DE DADOS PESSOAIS 83

5 REGULAÇÃO BRASILEIRA SOBRE COMPARTILHAMENTO E PUBLICAÇÃO DE DADOS 83

5.1 Fundamentos constitucionais da publicação e do compartilhamento de dados 85

5.2 Regulação sobre publicação de dados 91

5.3 Regulação sobre compartilhamento de dados 96

6 REGULAÇÃO BRASILEIRA SOBRE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS 111

6.1 Proteção constitucional à privacidade e proteção de dados pessoais 111

6.2 Regulação sobre privacidade e proteção de dados pessoais 120
6.3 Debates legislativos sobre o tratamento de dados mantidos pelo poder público 125
6.4 Regulação pela LGPD do tratamento de dados mantidos pelo poder público 139
7 INCOERÊNCIAS PRÁTICAS NA INTERFACE ENTRE O COMPARTILHAMENTO E A PUBLICAÇÃO DE DADOS COM A PROTEÇÃO DE DADOS PESSOAIS 147
8 CONCLUSÃO PARCIAL: NECESSIDADE DE PROMOVER MAIOR DIÁLOGO ENTRE NORMAS 157
PARTE III DEFINIÇÃO DO ESCOPO DA PUBLICAÇÃO OU DO COMPARTILHAMENTO DE DADOS PELO PODER PÚBLICO 167
9 EXPERIÊNCIA ESTRANGEIRA SOBRE O COMPARTILHAMENTO E NA PUBLICAÇÃO DE DADOS 167
9.1 Guias sobre reuso de dados publicados ou compartilhados 169
9.2 Guias sobre publicação de dados 174
9.3 Guias sobre compartilhamento de dados 182
9.4 Aprendizados com a experiência estrangeira 188
10 PARÂMETROS PARA A DECISÃO SOBRE COMPARTILHAR E PUBLICAR DADOS PESSOAIS 195
10.1 Verificação sobre a presença de dados pessoais 195
10.2 Definição da finalidade da publicação e do compartilhamento 210
10.3 Identificação de receptores da informação que se deseja publicar ou compartilhar 228
11 CONCLUSÃO PARCIAL: NECESSIDADE DE DELIMITAR COM PRECISÃO O ESCOPO DA PUBLICAÇÃO E DO COMPARTILHAMENTO DE DADOS PELO PODER PÚBLICO 239
PARTE IV IDENTIFICAÇÃO DO INTERESSE PÚBLICO NO COMPARTILHAMENTO E NA PUBLICAÇÃO DE DADOS PELO PODER PÚBLICO 245
12 MÉTODO PARA A IDENTIFICAÇÃO DE INTERESSE PÚBLICO 245
12.1 Interesse público segundo a teoria administrativista 247
12.2 Identificação do interesse público com apoio do teste de proporcionalidade 249

12.3 Exemplos estrangeiros de identificação do interesse público 254
13 SITUAÇÕES CONCRETAS DE IDENTIFICAÇÃO DE INTERESSE PÚBLICO NA RELAÇÃO DO COMPARTILHAMENTO E DA PUBLICAÇÃO DE DADOS COM A PRIVACIDADE 265
13.1 Decisões sobre proteção à privacidade na publicação de dados 265
13.1.1 Dados sobre servidores públicos 266
13.1.2 Despesas relacionadas ao desempenho de função pública 270
13.1.3 Dados de particulares em relação a verbas e funções públicas 273
13.1.4 Dados pessoais de particulares mantidos pelo governo 280
13.2 Decisões sobre proteção à privacidade no compartilhamento de dados 282
13.2.1 Dados e microdados sobre sistema de ensino 283
13.2.2 Envio de dados por entes privados para o governo 287
13.2.3 Compartilhamento de dados para fins de fiscalização 289
13.3 Análise sobre interesse público nos julgados analisados 293
14 PROPOSTA: INTERESSE PÚBLICO ENQUANTO PONDERAÇÃO ENTRE PRIVACIDADE E EFICIÊNCIA E/OU TRANSPARÊNCIA GOVERNAMENTAL 299
PARTE V O COMPARTILHAMENTO E A PUBLICAÇÃO DE DADOS PELO PODER PÚBLICO EM OBSERVÂNCIA À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS 307
15 ESTRUTURA DE GOVERNANÇA, GESTÃO DE RISCOS E TRANSPARÊNCIA 307
15.1 Estrutura de governança para a proteção de dados pessoais 308
15.2 Prestação de contas e responsabilização 312
15.3 Assegurar transparência sobre o compartilhamento e a publicação de dados 320
16 FUNDAMENTOS LEGAIS PARA O COMPARTILHAMENTO E A PUBLICAÇÃO DE DADOS 329
16.1 Limites do consentimento no uso de dados mantidos por governos 334
16.2 Cumprimento de obrigação legal e execução de políticas públicas 346
16.3 Legítimo Interesse do controlador e de terceiros 359
17 DIREITOS DE CIDADÃOS SOBRE O COMPARTILHAMENTO E PUBLICAÇÃO DE DADOS 365

17.1 Direitos tradicionalmente assegurados: acesso aos dados, e a correção de dados incompletos, inexatos ou desatualizados 368
17.2 Atualização dos direitos: anonimização, bloqueio, eliminação, oposição e portabilidade 379
18 SALVAGUARDAS NA PUBLICAÇÃO E NO COMPARTILHAMENTO DE DADOS 389
18.1 Regulação sobre reuso de dados como primeiro elemento de proteção 389
18.2 Pseudonimização e anonimização como possíveis soluções 396
18.3 Divulgação de dados com restrição de acesso e de usos secundários 401
19 CONCLUSÃO PARCIAL: DIÁLOGO ENTRE LGPD E NORMAS APLICÁVEIS AO PODER PÚBLICO PARA A CONCRETIZAÇÃO DA PUBLICAÇÃO E DO COMPARTILHAMENTO DE DADOS EM OBSERVÂNCIA À PRIVACIDADE 411
REFERÊNCIAS 435

INTRODUÇÃO

A adoção de tecnologias de informação e comunicação e de conectividade por governos nas últimas décadas tem permitido maior eficiência e transparência na prestação de serviços públicos. Esse processo de adoção de tecnologias pelo poder público foi marcado primeiramente pela digitalização de documentos físicos e pela informatização de procedimentos administrativos, e depois viabilizou medidas como a prestação de serviços públicos em tempo real[1] e a automatização de determinadas decisões. Ele também oferece mecanismos para que órgãos e entidades públicas possam mais facilmente divulgar informações sobre suas atividades e para que cidadãos possam participar mais ativamente na gestão dos atos públicos.

Além disso, essa adoção de tecnologias por governos amplia sua capacidade de coletar e processar dados, de tal forma que passam a organizar robustas bases de dados sobre eventos diversos e que contam com elevado grau de confiabilidade, justamente por serem produzidos por órgãos e entidades públicas. Em vista disso e das múltiplas possibilidades de reuso desses dados por terceiros, são cada vez mais comuns as práticas de compartilhamento e publicação de dados,[2] cujos benefícios são inúmeros e muitas vezes atrelados aos princípios de transparência e eficiência governamental. Como exemplo, destacam-se melhorias à prestação de serviços públicos, o acesso da população a informações de interesse público, a qualificação de práticas verticais e horizontais de *accountability*,[3] e a contribuição com práticas de inovação.

No entanto, parte dos dados publicados ou compartilhados por governos são dados pessoais (ou seja, permitem que uma pessoa natural seja identificada), de tal forma a impor riscos aos direitos fundamentais de privacidade e proteção de dados pessoais de cidadãos. Por exemplo, a reunião de grande quantidade de informações sobre uma pessoa ou comunidade pode permitir que governos ou particulares exerçam práticas discriminatórias ou de vigilância em relação a eles e que podem limitar liberdades, como as de expressão e circulação. Além

---

[1] Um exemplo interessante desse processo consiste na utilização de dispositivos que fazem comunicação máquina-a-máquina por municipalidades para gerenciar o trânsito local, visto que permitem a coleta de dados em tempo real sobre a circulação de veículos e pessoas na malha urbana. Referidos dados são, por vezes, cruzados com informações de outras origens, como as reclamações recebidas em *call center* sobre a infraestrutura urbana ou dados sobre a situação climática nos diferentes bairros da cidade obtidos em centrais meteorológicas.

[2] Juntos, esses termos serão referidos nesta tese como divulgação de dados, conforme será mais bem detalhado.

[3] Conforme conceito de O'Donnel (1998), *accountability* horizontal e vertical envolvem práticas de fiscalização internas e externas ao governo.

disso, indivíduos podem perder a capacidade de decidir sobre como informações sobre si são utilizadas por terceiros (ou seja, pode-se criar um cenário de autodeterminação informativa limitada).

Assim, a privacidade e a proteção de dados pessoais são comumente apresentadas como conflitantes com práticas de publicação e compartilhamento de dados (e, por consequência, com os objetivos de eficiência e transparência governamental), na medida em que essas atividades de divulgação de dados pessoais poderão provocar consequências negativas para a intimidade e autonomia de indivíduos, ao passo que o extremo da privacidade e proteção de dados pessoais pode resultar na generalização do sigilo governamental e no enfraquecimento das capacidades de inovação e de controle social da coisa pública. É justamente esse o nó que a presente pesquisa de doutorado busca desatar: **como harmonizar práticas de compartilhamento e de publicação de dados por governos com a privacidade e a proteção de dados pessoais de cidadãos?**

No Brasil, o compartilhamento e a publicação de informações governamentais possuem respaldo constitucional no direito de acesso à informação (art. 5º, XIV) e nos princípios de publicidade e eficiência, aplicáveis à atuação da administração pública direta e indireta (art. 37). Da mesma forma, a privacidade e proteção de dados pessoais são reconhecidos como direitos fundamentais (art. 5º, X e LXXVIII). Esses direitos e princípios possuem proteção em outras disposições constitucionais, a exemplo do direito de *habeas data*, que protege tanto o direito de acesso à informação como a privacidade de cidadãos (art. 5º, LXXII).

Tais direitos e princípios são concretizados por normas infralegais que, inclusive, preveem exceções que estabelecem limites para seu alcance. Por exemplo, a Lei de Acesso à Informação (LAI) e o Decreto nº 10.046/2019, que estão entre as principais normas reguladoras da publicação e do compartilhamento de dados pelo poder público, prevêem a privacidade e a proteção de dados pessoais como exceção à sua consecução, salvo nos casos de interesse público. Por outro lado, a Lei Geral de Proteção de Dados Pessoais (LGPD) reconhece que dados pessoais poderão ser publicados e compartilhados pelo poder público.

No entanto, essas normas não estabelecem parâmetros claros capazes de informar o gestor público sobre como assegurar a privacidade dos cidadãos quando da divulgação dos dados que mantém. De um lado, a LAI e o Decreto nº 10.046/2019 fazem referências genéricas à privacidade e à proteção de dados pessoais de indivíduos e, de outro, a LGPD é

uma norma nova, principiológica, e o capítulo de tratamento de dados pelo poder público enfrenta problemas de técnica legislativa que dificultam sua compreensão.

Soma-se a isso o fato de que, a despeito da existência de jurisprudência judicial e administrativa sobre o tema, a edição da LGPD tem sido utilizada por alguns agentes públicos de forma arbitrária, por vezes sendo empregada para limitar práticas de transparência governamental ou sendo facilmente superada em casos de compartilhamento de dados por governos, para agentes públicos ou privados. Por isso, essa tese também busca responder à seguinte pergunta: **como assegurar que essa harmonização da publicação e do compartilhamento de dados pelo poder público à privacidade e a proteção de dados pessoais ocorra de forma uniforme, respeitadas as particularidades do caso concreto?**

Assim, nesta pesquisa se argumenta que, embora não ausentes de complexidade e nuances diversas, o compartilhamento e a publicação de dados pessoais por governos poderá ocorrer com observância à privacidade e à proteção de dados pessoais dos cidadãos. Essa tarefa exige compreender quais são os interesses em conflito em atividades de compartilhamento ou publicação de dados pessoais pelo poder público, bem como por avaliar níveis aceitáveis de divulgação e privacidade, que poderão ser variáveis entre comunidades e gerações. Perpassa também por debates sobre quais dados pessoais podem ser divulgados, em qual modalidade e para quais finalidades, mas também por mecanismos e salvaguardas capazes de assegurar sua proteção.

Além disso, argumenta-se que, ainda que práticas de compartilhamento e de publicação de dados pessoais tenham suas particularidades e sejam (em princípio) respaldados por bens jurídicos distintos, deverão ser harmonizados com a privacidade de forma coerente entre si. Em outras palavras, essa atividade de compatibilizar a privacidade e a proteção de dados pessoais com o compartilhamento e com a publicação de dados por governos deve observar as particularidades da situação concreta, mas não seguir lógicas diametralmente opostas para avaliar quando o uso de dados poderá ser restrito em benefício da privacidade.

Para tanto, e tendo em vista a legislação vigente, a jurisprudência administrativa e judicial brasileira, assim como a experiência internacional, esta tese propõe procedimento e identifica critérios para auxiliar agentes públicos a determinar, na avaliação do caso concreto, a presença de interesse público na publicação e no compartilhamento de dados pessoais (ou, ao contrário, se ele resulta na restrição de acesso aos dados). No entanto, os cuidados não se encerram na decisão sobre divulgar dados pessoais, devendo a publicação ou o

compartilhamento de dados pessoais por governos ocorrer segundo princípios, direitos e salvaguardas estabelecidos na legislação aplicável. Diante da abertura ou imprecisão textual da legislação vigente, essa atividade exige a interpretação conjunta das normas de direito administrativo e de privacidade e proteção de dados pessoais, para a qual esta tese realizou um esforço inicial que merece complementação por pesquisas futuras

Metodologia adotada nesta pesquisa de doutorado

Para responder às perguntas de pesquisa propostas, esta pesquisa de doutorado foi conduzida utilizando dois principais esforços: *estudos teórico* e *documental*. No entanto, cumpre esclarecer que esta pesquisa é essencialmente jurídico-dogmática, de modo que não serão avaliados fenômenos sociais com fins de confirmação de teorias e tampouco serão apresentadas soluções técnicas para o problema diagnosticado. Além disso, embora o conflito da privacidade e da proteção de dados pessoais com a publicação e o compartilhamento de dados por governos alcance também atividades como as de segurança pública e investigação e persecução criminal, elas não serão objeto deste estudo. Como se denota pela leitura desta introdução, o foco será a divulgação para fins de transparência e eficiência.

Dito isso, inicialmente, foi realizado **estudo teórico** com o objetivo de identificar o estado da arte da literatura e trabalhos empíricos já desenvolvidos sobre privacidade e proteção de dados pessoais quando da publicação e do compartilhamento de dados. Para tanto, observaram-se as literaturas nacional e estrangeira sobre: **(i)** transparência, dados abertos, governo eletrônico, governo aberto, governo digital e *smart cities*, e **(ii)** privacidade e proteção de dados pessoais. Como se verificou, há extensa literatura sobre o uso de dados por governos e sobre a proteção à privacidade e proteção de dados pessoais, mas ainda são escassos textos que buscam estabelecer o diálogo entre essas duas abordagens.

Especificamente, pesquisas nacionais têm sido conduzidas para identificar a observância de obrigações de transparência pelos distintos órgãos públicos dos três poderes e das distintas esferas federativas no Brasil (NÓBREGA, 2017; TEIXEIRA, 2017; FRANCO *et al*., 2015). No entanto, são poucas as pesquisas nacionais que estudam práticas de compartilhamento de dados pelo governo ou que observam a publicação e o compartilhamento[4] de dados à luz da proteção de dados pessoais. Há também pesquisas

[4] Como será mais detidamente abordado adiante, nesta tese o conceito de publicação de dados será compreendido como a atividade realizada pelo poder público de viabilizar acesso e uso posterior pela sociedade a informações de interesse público para, entre outros, promover a consecução da transparência

nacionais sendo desenvolvidas sobre a proteção de dados pessoais na Internet (MENDES, 2008; DONEDA, 2011; LEONARDI, 2012), especialmente em virtude da edição da LGPD em 2018 (Artigo 19, 2016; Internet Lab, 2016). Todavia, o debate está normalmente centrado no tratamento de dados por entidades privadas, sendo poucas as pesquisas sobre proteção de dados pessoais com o olhar direcionado ao poder público. Em 2010, Danilo Doneda escreveu sobre o conflito entre privacidade e política de transparência, mas não havia à época marcos regulatórios importantes para o tema no Brasil. Mais recentemente, Miriam Wimmer tem se dedicado mais ativamente ao tema, com publicações sobre tratamento de dados pelo poder público (2020) e sobre o reuso de dados mantidos por governos (2021). Outros autores também passaram a discutir o tema, como Laura Schertel Mendes (2022) e autores diversos no livro LGPD & Administração Pública, coordenado por Augusto Neves Dal Pozzo e Ricardo Marcondes Martins (2020).

No cenário internacional, práticas de compartilhamento e publicação de dados são abordadas em pesquisas diversas sobre o conceito, a implementação e a efetividade de governos eletrônicos (e.g., DUNLEAVY *et al*., 2001; TITAH, BARKI, 2006; YILDIZ, 2007; Hiller, Bélanger, 2001; VAN DEN BRAAK *et al*., 2012) e governos abertos (e.g. YU, ROBINSON, 2011; Geiger, Von Lucke, 2012; JANSSEN *et al.*, 2012; UBALDI, 2013; KASSEN, 2019; CLARKE, 2019). No entanto, ainda são poucas as pesquisas que abordam a relação entre o uso de dados nesses modelos de governo com a necessidade de garantir a privacidade e a proteção de dados pessoais de cidadãos. Mas que isso, muitos dos textos que abordam o tema se limitam a identificar a necessidade de compatibilizar esse uso de dados com a privacidade e proteção de dados pessoais, mas não apresentam soluções concretas para a questão (JANSSEN; VAN DEN HOVEN, 2015; MEIJER *et al.,* 2014; O'HARA, 2011; WU, 2014; JAATINEN, 2016; GREEN *et al.*, 2017).

De todo modo, esses e outros textos mobilizados nesta tese foram usados para qualificar os conceitos centrais e os problemas enfrentados nesta tese, assim como para propor soluções a esses problemas e construir pontos de diálogo entre as literaturas sobre o uso de dados pessoais por governos e sobre privacidade e proteção de dados pessoais.

---

governamental. Já o compartilhamento de dados será considerado por esta tese como a divulgação de dados pelo poder público com terceiros para finalidades específicas, que poderá ocorrer pela troca recíproca ou unilateral de dados entre organizações, pela autorização de acesso, integral ou parcial, a determinada base de dados por poucos interessados e pela reunião de dados fornecidos por diversos agentes para consumo desses mesmos atores ou por terceiros.

Já a **análise documental** foi realizada com base em decisões judiciais e administrativas, assim como em guias e relatórios elaborados por autoridades estrangeiras com competências relacionadas à proteção de dados pessoais. Essa análise buscou identificar debates relacionados à compatibilização entre privacidade e proteção de dados pessoais com relação ao tratamento de dados pelo poder público, buscando trazer contribuições ao debate teórico e as propostas de interpretação normativa ora realizadas. Assim, este estudo foi desenvolvido com vistas a colaborar com a formulação do *corpus* teórico do trabalho, de forma a qualificar o sobre a exposição ou proteção de informações e dados pessoais contidos em arquivos ou bases de dados públicas.

Para tanto, foi realizado **estudo não exaustivo de experiências internacionais** de proteção de dados pessoais no âmbito de políticas de transparência e abertura de dados, com o objetivo de identificar soluções debatidas em outros países para auxiliar na reflexão sobre possíveis interpretação das normas existentes sobre o tema no Brasil. Embora o intuito não tenha sido realizar estudo comparado ou replicar a experiência estrangeira à realidade brasileira, os guias e relatórios analisados, de autoria de autoridades e entidades da Europa e dos Estados Unidos, foram selecionados considerando o pioneirismo do estudo ou a influência que as autoridades e entidades autoras exercem sobre a prática brasileira de proteção de dados pessoais.

Também foi realizado **levantamento não exaustivo de decisões do Supremo Tribunal Federal (STF) e da Controladoria-Geral da União (CGU)**. Esse estudo não buscou observar tendências jurisprudenciais, mas tão somente identificar critérios capazes de mapear situações nas quais há interesse público na publicação ou no compartilhamento de dados pessoais pelo poder público. Vale ressaltar que a escolha por realizar análise de decisões do STF e da CGU se justifica por sua competência para julgar conflitos entre princípios constitucionais ou recursos denegatórios a pedidos de acesso à informação formulados em face de órgãos ou entidades da administração pública federal, e que, portanto, encontra forte afinidade com as principais questões debatidas neste trabalho. Por sua vez, os julgados foram selecionados considerando aspectos como o tipo de divulgação realizada (i.e., publicação ou compartilhamento), suas características (e.g., quem são os titulares de dados), e a repercussão e relevância do julgamento.

Estrutura desta pesquisa de doutorado

Diante do exposto, para responder à pergunta de pesquisa formulada, além desta introdução, o caminho percorrido para o desenvolvimento desta tese foi segmentado em cinco partes. A **primeira parte** buscou identificar como a teoria enfrenta o desafio do compartilhamento e da publicação de dados (que, nesta tese, são qualificados como categorias de divulgação de dados que, por sua vez, envolve a circulação de informações) pelo poder público em respeito à privacidade e proteção de dados pessoais. Conforme se verificou, há pouco debate teórico destinado a responder essa reflexão específica, visto que a literatura sobre divulgação de dados por governos está focada em romper sigilo governamental com viabilizar a modernização do aparato estatal por meio do uso de tecnologia, e a literatura sobre privacidade e proteção de dados pessoais, embora sua origem esteja atrelada a abusos cometidos por governos viabilizados por informações que reúnem sobre cidadãos, está atualmente focada em regular o tratamento de dados pessoais por particulares ou para a prática de atividades como as de segurança pública e persecução penal.

De fato, a utilização e divulgação de dados pessoais por governos é essencial para a garantia de direitos aos cidadãos e para o desempenho de suas atribuições legais de forma eficiente e transparente. Por outro lado, muitos dos dados mantidos por governos se referem a pessoas naturais e sua utilização oferece riscos a direitos e liberdades, inclusive na sua capacidade de se manifestar ou se organizar. Por isso, faz-se necessário ampliar o diálogo teórico e prático entre as literaturas dedicadas à circulação de dados por governos e à proteção de dados pessoais, e aprofundar análises específicas sobre meios de assegurar os benefícios dessa divulgação com o menor prejuízo possível a direitos e liberdades de cidadãos.

Já a **segunda parte** foi destinada a identificar como a legislação brasileira, constitucional e infraconstitucional, enfrenta o conflito entre privacidade e proteção de dados pessoais em relação à transparência e eficiência governamental. De forma similar ao encontrado na literatura, enquanto a legislação sobre o compartilhamento e a publicação de dados por governos está centrada em romper com paradigmas de burocracia e sigilo, a legislação sobre privacidade e proteção de dados pessoais é principiológica e conta com problemas de técnica legislativa que dificultam a sua aplicação para fins de tratamento de dados pelo poder público. Em todos os casos, ainda que a legislação preveja o interesse público como parâmetro de conduta do agente público (e uma autorização à publicação de dados pessoais), faltam parâmetros claros para auxiliar na sua identificação em casos

concretos envolvendo a divulgação de dados pelo poder público. Diante disso, é possível observar inconsistência prática na publicação e compartilhamento de dados por governos, motivo pelo qual se faz necessário identificar interpretações e estabelecer parâmetros para assegurar que dados pessoais serão divulgados em observância a direitos e liberdades de cidadãos.

Por sua vez, a **terceira parte** apresenta proposta de procedimento para a publicação ou o compartilhamento de arquivos ou bases de dados governamentais que contenham dados pessoais. Para tanto, são observados exemplos de soluções jurídicas apresentadas em outros países para a publicação e para o compartilhamento de informações mantidas por governos em observância à privacidade e à proteção de dados pessoais de cidadãos. De uma forma geral, tanto para o compartilhamento quanto para a publicação deve-se identificar com precisão os objetivos almejados, avaliar o interesse público na divulgação, e instituir estrutura de governança que conte com medidas de *accountability*, assegurem direitos aos titulares de dados e prevejam salvaguardas aos riscos decorrentes da divulgação pretendida. Diante dos aprendizados da prática estrangeira e em vista das balizas legais aplicáveis, esta parte da tese também apresentou proposta para a definição, no caso concreto, dos objetivos da divulgação de arquivos ou bases de dados governamentais. Essa tarefa exige compreender se há dados pessoais identificáveis nos arquivos ou bases de dados que se pretende divulgar, estabelecer a finalidade da publicação ou do compartilhamento (que deverá ser legítima, ter respaldo legal, e ser compatível com a atribuição legal do ente público divulgador), avaliar a necessidade da atividade para o alcance da finalidade estabelecida, e quem são os sujeitos interessados em receber esses dados.

Após, a **quarta parte** da tese aborda o próximo passo no procedimento de publicação e de compartilhamento de dados pelo poder público em observância à privacidade e proteção de dados pessoais, consistente na identificação do interesse público no caso concreto. Como se verificou, pela análise de modernas teorias de direito administrativo e constitucional, o interesse público consiste no resultado da ponderação pública e motivada entre interesses sociais conflitantes, que, no objeto desta tese, são os princípios da eficiência e transparência governamental, de um lado, e a privacidade e proteção de dados pessoais, de outro. Com isso, e considerando que poderá haver interesse público em assegurar a privacidade e proteção de dados pessoais, sua qualificação no caso concreto poderá resultar tanto na divulgação quanto na restrição de acesso aos dados. Além disso, tendo em vista a avaliação não exaustiva da experiência em outros países e de decisões do Supremo Tribunal Federal e da Controladoria-

Geral da União, foi possível identificar situações em que, a depender das particularidades do caso concreto, geralmente haverá interesse público na publicação ou no compartilhamento de dados pessoais por governos, a exemplo do fomento ao *accountability*, participação social e proteção do processo democrático, da tomada qualificada de decisão por órgãos públicos, e da garantia do melhor uso de dinheiro público. Por outro lado, não será de interesse público a informação de interesse para o público quando houver cláusula legítima de confidencialidade ou sigilo, e se a divulgação impuser elevados riscos à privacidade e proteção de dados pessoais.

Finalmente, a **quinta parte** busca apresentar procedimento para que seja possível ao poder público, nos casos em que houver interesse público na divulgação, compartilhar ou publicar dados em observância à privacidade e proteção de dados pessoais. Em verdade, alguns desses cuidados devem ser considerados quando da avaliação sobre a presença de interesse público na publicação ou no compartilhamento de dados pessoais pelo poder público, como a avaliação de riscos da divulgação e as salvaguardas adotadas para mitigá-los. De todo modo, será primeiro necessário ao agente público instituir estrutura de governança que estabeleça prioridades, atribua responsabilidades, estabeleça políticas e procedimentos para o tratamento de dados pessoais em conformidade com a legislação, e assegure direitos aos titulares. Além disso, o controlador deverá assegurar prestação de contas e transparência sobre a divulgação, que poderão ser instrumentalizados por documentos como o Relatório de Impacto à Proteção de Dados Pessoais e a Política de Privacidade. Em seguida, deverão ser determinadas as bases legais que justificam o tratamento de dados, com destaque ao cumprimento de obrigação legal e à execução de políticas públicas (visto que a atuação governamental é regida pelo princípio da legalidade do ato administrativo), e assegurados meios para que cidadãos possam exercer seus direitos em relação aos dados pessoais, como os exemplos dos direitos de acesso, retificação e oposição ao tratamento. Finalmente, deverão ser adotadas salvaguardas destinadas a mitigar os riscos da publicação ou do compartilhamento de dados pessoais por governos, a exemplo da adoção de práticas de anonimização de dados, do estabelecimento de cláusulas contratuais, ou da implementação de Conselhos e Códigos de Ética destinados a assegurar que a divulgação observará direitos e liberdades de cidadãos.

PARTE I TENSÕES ENTRE O COMPARTILHAMENTO E A PUBLICAÇÃO DE DADOS PELO PODER PÚBLICO COM A PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS DE CIDADÃOS

1 O PAPEL CENTRAL DO TRATAMENTO DE DADOS PARA AS ATIVIDADES DO PODER PÚBLICO

Historicamente, diversos governos realizaram cadastros de cidadãos para fins inerentes ao desenvolvimento das suas funções, como a condução de arrecadação de tributos ou o registro de propriedades. Foi justamente nesse contexto que, no século XIX, ocorreu uma primeira ampliação na coleta de dados[5] de cidadãos em virtude de fatos como o crescimento de cidades industriais e da burocracia governamental (WIMMER, 2020).

Com o consequente aumento do papel do Estado na promoção de direitos individuais, políticos e sociais, houve também uma intensificação na coleta de dados. Afinal, para que os cidadãos possam exercer os seus direitos, é necessário que realizem cadastro perante o órgão público competente. Por exemplo, para a matrícula de uma criança em uma instituição de ensino pública, será necessário coletar dados do menor de idade e dos seus representantes legais (e.g., nome, idade, identidade e local de residência). O mesmo ocorre para o exercício de liberdades políticas, tendo em vista que, para votar e desempenhar outras atividades da vida pública, o cidadão precisará se cadastrar perante a instituição eleitoral.

Além disso, a efetiva garantia de direitos civis, sociais e políticos exige dos governos maior e mais acurado conhecimento sobre a população, o que pode ser obtido de maneira mais precisa com base em dados a ela referentes. Assim, o desenvolvimento de novas formas de governar, em especial por meio de Estados de bem-estar social, que envolvem maiores esforços por parte da administração pública para prestar serviços e assegurar acesso aos direitos, requer maior coleta de dados para conhecer a população e executar suas atribuições com maior eficiência (DONEDA, 2020).

Dados também são obtidos pelos governos por motivos ainda mais diversos, como a gestão de registros públicos e de documentação básica, a elaboração de estatísticas oficiais e a prestação de serviços distintos. Eles poderão também ser recebidos de outros órgãos públicos

[5] Dados são, por vezes, resultado da ação humana e podem ser agregados de inúmeras maneiras para serem transformados em informação que, por sua vez, consiste em um recorte de dados agregados ao qual foi atribuído algum conteúdo (DAVIES, 2010).

ou de particulares em razão de fatores como: **(i)** determinação legal (como o envio, por empresas, de dados de seus funcionários para o eSocial); **(ii)** prestação por particulares de serviços públicos (como a coleta de dados cadastrais e de deslocamento em determinado transporte público por concessionárias de ônibus e metrô); e **(iii)** por força de cooperação entre órgãos públicos ou com particulares para o alcance do interesse público (como parcerias realizadas pelo poder público com empresas fornecedoras de tecnologia capazes de medir a quantidade de pessoas que estão descumprindo determinações de distanciamento social).

Logo, a utilização de dados é inerente ao desempenho de capacidades governamentais do Estado contemporâneo. Mais que isso, essa expansão das atividades estatais associada ao emprego de novas tecnologias potencializa sua capacidade de processamento de dados.

A seguir se demonstrará como a adoção por governos de tecnologias diversas vem permitindo o aprimoramento na execução de suas atribuições legais, inclusive viabilizando o desenvolvimento de novos modelos de governo que, por sua vez, radicalmente modificam a relação entre governos e cidadãos. Além disso, será demonstrado que esse fenômeno de adoção de tecnologias modernas por governos anda de mãos dadas com a ampliação na coleta e no processamento de dados, assim como na organização de relevantes bases de dados, cuja publicação ou compartilhamento com terceiros possui benefícios diversos à sociedade.

1.1 Evolução da tecnologia e tratamento de dados para novos modelos de governos

Para além da ampliação do papel do Estado ocorrida desde o século XIX, a adoção de novas tecnologias por governos também ampliou a sua capacidade de coletar, processar e armazenar dados de cidadãos. De fato, na origem, o manuseio de informações pelo Estado se dava por meio de sistemas baseados no papel (*paper-based systems*), o que dificultava a extração de análises em larga escala a partir das informações mantidas. Assim, nesse momento, os dados acabavam restritos a determinado órgão ou entidade pública e não eram utilizados para compreender fenômenos e aprimorar a atividade governamental.

Essa tendência se modificou em meados de 1960, com o surgimento de computadores e a digitalização de sistemas governamentais (KRAEMER; KING, 2003), que permitiram a automatização de operações e sistematização no registro de informações em bases de dados públicas. Nesse momento, que perdurou até o início da década de 2000, governos adotaram o que se chamou de *New Public Management* (NPM) ou Nova Gestão Pública, que tinha entre seus pressupostos a desagregação de estruturas organizacionais governamentais, resultando na

manutenção de informações em silos. De todo modo, por meio da utilização de Tecnologias de Informação e Comunicação ("TIC"), governos puderam melhorar suas práticas de análises de dados e de gestão (DUNLEAVY; MARGETTS, 2010), resultando em ganhos na eficiência, eficácia e responsividade da prestação de serviços públicos.[6]

Em seguida, com a introdução de conectividade aos órgãos públicos e com a possibilidade de prestação de serviços *online*,[7] o uso de dados pelo governo foi ainda mais potencializado (DUNLEAVY; MARGETTS, 2000), promovendo amplos benefícios, como uma significativa redução de custos operacionais e do distanciamento entre governo e cidadãos.[8]

Modernas tecnologias também afetaram o uso de dados pelos governos, a exemplo do uso de dispositivos de Internet das Coisas ("*Internet of Things*" ou "IoT"),[9] que pressupõem a comunicação máquina-a-máquina e possuem a capacidade de promover interação em tempo real, e da contratação de serviços de nuvem ("*cloud services*"),[10] que permitem o armazenamento de grandes quantidades de dados e o acesso remoto a eles. Com o apoio dessas e de outras tecnologias, é possível que haja a geração de *big data*[11] que, especialmente quando associado à adoção de mecanismos de inteligência artificial, permite a pesquisa, a

---

[6] Artigo interessante de Vydra e Klievink (2019) afirma que existem os tecno-otimistas e os tecno-pessimistas, que apresentam expectativas diferentes sobre a adoção de tecnologia pelo governo. Segundo afirma, enquanto os tecno-otimistas se focam nos dados e nos ganhos analíticos que podem ser alcançados pela adoção de tecnologias pelo governo, os tecno-pessimistas observam o processo humano em transformar esses *insights* em tomada de decisões e estruturas burocráticas.

[7] Embora em minha pesquisa eu utilize o termo ***online***, é questionável a segmentação entre *online* e ***offline*** (MILLER; SLATER, 2004). O *online* em minha pesquisa diz respeito ao espaço onde as informações são armazenadas, divulgadas ou acessadas. Não diz respeito ao local em que os dados são coletados ou onde será majoritariamente desenvolvido o estudo empírico da minha pesquisa.

[8] Entre as possibilidades de aproximação do governo com a sociedade estão a criação de canais *online* de atendimento, a alimentação de portais na internet com informações a respeito da prestação de serviços ou políticas públicas, ou a disponibilização de repositório de documentos ou bases de dados contendo informações de interesse público.

[9] Em inglês, o termo é cunhado de *Internet of Things*. O conceito se refere ao conjunto de serviços e dispositivos que reúnem ao menos três pontos elementares: conectividade, uso de sensores/atuadores, e capacidade computacional de processamento e armazenamento de dados. Sobre o tema, vide: https://www.jota.info/opiniao-e-analise/artigos/plano-nacional-de-internet-das-coisas-mais-um-passo-para-o-desenvolvimento-da-iot-no-brasil-02072019. Acesso em 05.07.2019.

[10] Para mais informações sobre o uso de computação em nuvem por governos, vide: LEMOS, Ronaldo et al. GovTech e computação em nuvem: o Brasil precisa de uma agenda digital. Jota, 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/govtech-e-computacao-em-nuvem-o-brasil-precisa-de-uma-agenda-digital-12042019. Acesso em 12.06.2019.

[11] Para fins deste trabalho, adotarei o conceito de *big data* de Laney (2001), consistente na massiva quantidade de dados ("high volume"), que cresce exponencialmente em alta velocidade ("high velocity") e de tipos e fontes diversas (*high variety*). Isso significa que o termo big data será considerado não somente pelo seu elemento "big", mas também pelo fato de viabilizar a pesquisa, agregação e análise de grandes quantidades de dados organizados (SMITH *et al*, 2012).

agregação e a análise de grandes quantidades de dados organizados (SMITH *et al*, 2012),[12] os quais ajudam na compreensão de fenômenos e na tomada de decisões de agentes públicos ou privados.

Nesse momento, houve nova mudança de paradigma, na medida em que empresas e cidadãos passaram a inovar de forma mais rápida do que os Estados. Foi, portanto, necessário aos governos se adequarem a modelos de gestão descentralizados e colaborativos (DUNLEAVY; MARGETTS, 2010), abrindo espaço para um novo modelo de gestão pública, o chamado de *Digital Era Governance* (DEG) ou Era da Governança Digital. Entre seus pressupostos estão a digitalização governamental e a reintegração de estruturas antes fragmentadas, de forma a integrar serviços e desestimular a atuação governamental em silos, e entre seus resultados a reorganização de processos para melhor atender ao público e a disponibilização de local centralizado para que cidadãos possam acessar o governo (DUNLEAVY; MARGETTS, 2020).

Relacionada a essa mudança de paradigma de gestão organizacional, a adoção de similares tecnologias pelos governos tem permitido o desenvolvimento de novas modalidades de prestação de serviços públicos, a exemplo do governo eletrônico, do governo digital, do governo aberto e das *smart cities.* Embora possam existir outros conceitos de governo baseados no uso de dados e tecnologias, são essas as terminologias mais frequentemente estudadas pela literatura e adotadas por governos.

O **governo eletrônico** (também conhecido pelos termos em inglês "*e-government"* ou *"electronic government"*) é o termo muitas vezes utilizado para qualificar a utilização da internet e a incorporação pelo governo de TICs em procedimentos internos, no desenvolvimento de políticas e na prestação de informações e serviços aos cidadãos (MARGETTS; DUNLEAVY, 2002).[13]-[14] Entre as tendências em governos eletrônicos estão

[12] A análise de *big data* permite a promoção de benefícios diversos, especialmente ao fornecer substrato de análises para a compreensão de fenômenos naturais e sociais que, por sua vez, auxiliam na tomada de decisão e na solução de problemas diversos. Mais que isso, a tomada de decisão com base em dados, em áreas diversas e por *player*s variados, produz resultados mais efetivos e oportunos, além de possibilitarem alguma redução de gastos (TENE; POLONETSKY, 2012; KIM; TRIMI; CHUNG, 2014).

[13] Como problematiza Yildiz (2007), o conceito de *e-government* não é uníssono, sendo usado para explicar situações que incluem, mas não se limitam a: (i) uso da internet para fornecer informações governamentais e prestar serviços a cidadãos (UN; ASPA, 2002); (ii) uso conjunto da internet e de TIC pelo governo (Jaeger, 2003); (iii) uso de tecnologias, especialmente integradas à internet, para aumentar o acesso e a eficiência na prestação de informações e serviços governamentais (BROWN; BRUDNEY, 2001).

[14] Importante ressaltar que é possível falar em governo eletrônico mesmo que determinados serviços públicos ainda não contem com informatização e digitalização de procedimentos. Trata-se de movimento progressivo e que alcança os serviços que já estão sendo agregados com similares tecnologias.

(i) a promoção de interoperabilidade entre sistemas,[15]-[16] (ii) a prestação de serviços de forma integrada, e (iii) a oferta de serviços multiportas. Essas tendências pressupõem a integração de sistemas e processos, e objetivam a prestação facilitada de serviços públicos aos cidadãos.

Isso porque a interoperabilidade permite que sistemas distintos interajam entre si para alcançar objetivos comuns mutuamente benéficos por meio do compartilhamento de informações, sem que para tanto seja necessária a criação de uma nova solução, mas apenas de sistemas que permitam esse intercâmbio. Por sua vez, a prestação de serviços públicos integrados resulta no desenvolvimento de interfaces destinadas a promover aos cidadãos acesso facilitado a informações e serviços públicos, bem como eximi-los da necessidade de fornecer a determinado órgão ou entidade pública documentos ou informações produzidas ou mantidas por outros órgãos públicos. Já a oferta de canais multiportas permite que o governo ofereça ao cidadão escolhas sobre como acessar o governo (pela internet, pelo telefone, presencial etc.), conforme sua preferência,[17] e assim também culminando na facilitação do acesso do cidadão aos serviços públicos.

Mais recentemente, foi desenvolvido o conceito de **governo digital**, que estende o conceito de governo eletrônico para colocar em destaque os benefícios da transparência e abertura de prestação de serviços públicos com a colaboração da sociedade e do mercado (OCDE, 2014). O pressuposto é que, com o desenvolvimento de novas tecnologias, torna-se cada vez mais possível permitir que distintos atores possam acessar dados mantidos pelo governo e, com isso, contribuir com soluções de interesse público.

Assim, embora intimamente relacionado com governos eletrônicos, o conceito de governo digital exige uma mudança de perspectiva com relação à prestação de serviços públicos: a definição de prioridades deixa de ser realizada preferencialmente pelo governo e passa a ser compartilhada com atores sociais relevantes (e.g., sociedade civil, mercado e academia). O desafio da integração de novas soluções tecnológicas às práticas

---

[15] A interoperabilidade consiste na capacidade de diferentes sistemas se comunicarem e usarem essas informações entre si para obterem resultados esperados pelos seus operadores. No entanto, o conceito de interoperabilidade também não é uníssono, sendo ainda qualificado como (a) habilidade de dois ou mais sistemas ou elementos de trocar informações entre si; ou (b) capacidade para unidades de equipamentos em trabalhar junto para realizar funções úteis. Vide: IEEE. The Authoritative Dictionary of IEEE Standards Terms, Seventh Edition, **IEEE Std 100-2000**, p. 1–1362, 2000, p. 582.

[16] Esse conceito pressupõe pluralidade de atores, sistemas e equipamentos, e possui dimensões organizacionais, técnicas e semânticas (VERNADAT, 2010), como a colaboração entre organizações para padronizar processos e realizar a troca de informações, a coordenação de requisitos tecnológicos para que os sistemas possam se comunicar, e a uniformização de significados de dados trocados.

[17] Também se debatem os interesses desses atores em utilizar serviços de e-government (ROWLEY, 2011; NEAMTU, 2013), como comunicação, coordenação, comércio, transparência, *accountability*, padronização de informações e serviços, dentre outros interesses.

governamentais é, portanto, associado à adoção de processos que sejam porosos à participação destes diferentes *stakeholders* (OCDE, 2014).

Relacionado ao governo digital está o conceito de **governo aberto** (bastante conhecido pela terminologia em inglês *open government*), que consiste na adoção de medidas para que o governo tenha como prioridades a transparência, a prestação de contas e a responsabilização de agentes públicos (SABO *et al.*, 2020). Mais que isso, como destacam Maier-Rabler e Huber (2011), governos abertos também possibilitam meios para que a sociedade desenvolva iniciativas em colaboração com o poder público.

Como mencionado, entre os pressupostos dessa modalidade de governo estão a transparência e a participação social. Com a adoção de novas tecnologias de conectividade e pela persecução de objetivos de transparência, os órgãos públicos conseguem coletar e divulgar um aporte enorme de informações em diferentes áreas, como, por exemplo, finanças, transporte, meio ambiente etc. Essas iniciativas possuem a capacidade de reduzir a assimetria de informação entre órgãos públicos e os diferentes interessados em consumir dados para finalidades diversas de interesse público.

Embora muitos conjuntos de dados sejam encontrados em sua forma bruta e por si próprios não tenham necessariamente muito valor informativo, os órgãos públicos podem alavancar empresas e cidadãos para contribuir com a inovação dos serviços governamentais por meio da reorganização, reempacotamento e síntese de informações de várias fontes (DIFRANZO *et al*., 2011). Entre essas iniciativas está a adoção de portais dedicados à transparência e dados abertos, que ampliam a capacidade de cidadãos e demais interessados em encontrar, acessar e compreender dados diversos.

Finalmente, também a noção de **cidades inteligentes** (conhecida pelo termo em inglês *smart cities*) é bastante disputada, especialmente considerando que o agregador "inteligente", que indica o objetivo a ser alcançado nessas cidades, poderá possuir significados diversos (e.g., cidade conectada, sustentável e/ou segura).[18] Com suas origens no final da década de 1990,[19] o termo ganhou espaço novamente a partir de 2010, após uma reorientação do modelo

[18] Como apontado no relatório *Mapping smart cities in the EU*, publicado pelo Parlamento Europeu em 2014. Vide: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf. Acesso em 02.08.2020.

[19] A literatura reconhece os textos de Van Bastelaer (1998) e Mahizhnan (1999) como as primeiras referências no tema.

de negócio de grandes empresas, como a IBM,[20] que deixaram de focar na venda de *hardwares* e *softwares* para focar na oferta de serviços (MOROZOV; BRIA, 2019).

O conceito vem sendo amplamente discutido, especialmente quando utilizado o vocabulário inteligente para referenciar as relações entre cidade e tecnologia (ALIZADEH, 2021),[21] e tem assumido significados distintos. Por exemplo, Glasmeier e Christopherson (2015) definem cidades inteligentes a partir da coordenação de instalações urbanas fragmentadas usando novas tecnologias capazes de proporcionar nova realidade para os moradores. Já Khatoun e Zeadally (2016) definem a cidade inteligente como aquela que utiliza tecnologias diversas para promover eficiência no planejamento urbano.

Apesar dessa variedade de definições, o conceito de cidades inteligentes é comumente atrelado à adoção de TIC para melhorar a qualidade de vida dos cidadãos, e pode assumir formas como: **(i)** a inserção de soluções tecnológicas na infraestrutura urbana; **(ii)** a circulação de informações na cidade; ou **(iii)** o desenvolvimento de verdadeiros laboratórios urbanos (*living labs*).[22] De todo modo, o interesse desta tese nas cidades inteligentes está na sua no fato de promover a circulação de dados dentro do poder público ou com particulares.

Embora distintos, esses conceitos de governo (i.e., governo eletrônico, digital, aberto e *smart cities*) são intimamente relacionados. Por exemplo, sistemas de governo eletrônico (ou digital) oferecem o suporte (YAN; ELISA; ELIOT, 2019) necessário para auxiliar cidades inteligentes ou governos abertos no alcance dos seus objetivos (ANTHOPOULOS; REDDICK, 2016) - que são variáveis a depender do conceito adotado e das prioridades escolhidas, como conectividade, sustentabilidade ou transparência. Além disso, todas essas novas modalidades de governo pressupõem a circulação de informações e dados mantidos por entidades públicas com terceiros, públicos ou privados. Essa circulação poderá ser de dados

---

[20] Uma cidade inteligente desenvolvida originalmente pela IBM ilustra uma cidade harmonizada onde a tecnologia orientada a TIC aprimora os serviços da cidade, como negócios, transporte, saúde, comunicação e suprimentos de energia (BATTY *et al*., 2012). Em 2010, 130 cidades em todo o mundo aceitaram o desafio das cidades mais inteligentes proposto pela IBM. Uma investigação conduzida por Alizadeh (2021) revela que o governo eletrônico, transporte e meio ambiente são as três áreas mais importantes no desejo das cidades participantes. Com análises emergentes de big data de rápido crescimento, Kitchin (2014) resume que uma cidade rica em dados pode usar análises de dados sofisticadas para entender, monitorar, regular e planejar.

[21] Para uma análise entre a interligação entre o conceito de cidades inteligentes e políticas públicas urbanas, Fábio Ferraz afirma que "novas tecnologias de informação e comunicação devem se tornar parte indissociável das políticas públicas de segurança, de mobilidade, de saneamento, de habitação, de desenvolvimento econômico, educação, saúde, mas não podem incidir apenas pontualmente em determinado sistema urbano". Vide: https://www.nexojornal.com.br/ensaio/2017/As-cidades-inteligentes-devem-ser-reflexo-de-uma-sociedade-inteligente?utm_campaign=a_nexo_2017823&utm_medium=email&utm_source=RD+Station. Acesso em 09.10.2017.

[22] Termo primeiramente cunhado por pesquisadores do Massachusetts Institute of Technology (MIT): William J. Mitchell, Kent Larson e Alex Pentland.

ou informações (DAVIES, 2010), em formatos diversos (MATHEUS; JANSSEN, 2015), a exemplo de resposta a solicitações de informação, da entrega de documentação em papel, ou disponibilização de informações em formatos eletrônicos diversos, como *websites*, bases de dados ou APIs (*Application Programming Interface*).[23] Esses dados ou informações poderão ser mantidos de forma fechada (*closed data*), ser compartilhados com terceiros em formatos diversos (*shared data*) ou serem divulgados em formato aberto (*open data*).

A seguir se demonstrará que essa circulação de dados organizados por governos, por meio da sua coleta viabilizada pela adoção de modernas tecnologias e de novas modalidades de governo, em diferentes formatos (como a publicação e o compartilhamento de dados), oferece benefícios diversos para o poder público e para a sociedade, na medida em que viabilizem práticas, por exemplo, de transparência e eficiência governamental, bem como de inovação.

1.2 Benefícios do tratamento de dados pelo poder público

Essas e outras tecnologias ampliam a capacidade de coleta, estruturação e processamento de dados em tempo real, de modo que o material coletado como resultado da adoção de tecnologias para a prestação de serviços públicos é capaz de revolucionar a prestação desses serviços.[24] Esse uso de novas tecnologias por governos para a tomada de decisão conta com a coleta e o processamento de grandes quantidades de dados (OCDE, 2019).

Com isso, governos acabam por organizar bases de dados de particular riqueza, na medida em que reúnem grande contingente de dados, inclusive sobre pessoas que não possuem acesso à internet,[25] obtidos em decorrência da prestação de serviços públicos e que

---

[23] APIs são uma série de rotinas, protocolos e instrumentos disponibilizados por determinado ambiente para que programadores possam desenvolver aplicações consistentes com aquele ambiente. Isso permite com que serviços possam se comunicar e aproveitar dados e funcionalidades do outro dentro de uma interface documentada. Vide: https://www.wired.com/2010/02/api/ e https://www.ibm.com/cloud/learn/api. Acesso em 14.03.2022.

[24] Um exemplo interessante desse processo consiste na utilização de dispositivos de IoT por municipalidades para gerenciar o trânsito local, visto que permitem a coleta de dados em tempo real sobre a circulação de veículos e pessoas na malha urbana. Sobre o tema, vide o seguinte relatório do Estudo para o Plano Nacional de Internet da Coisas: https://www.bndes.gov.br/wps/wcm/connect/site/f9582d36-4355-4638-b931-e2e53af5e456/8B-relatorio-final-plano-de-acao-produto-ambiente-regulatorio.pdf?MOD=AJPERES&CVID=m7tyLs1 e https:www.jota.info/opiniao-e-analise/artigos/internet-das-coisas-e-mobilidade-urbana-03042018. Acesso em 12.06.2019.

[25] Como se sabe, há ainda no Brasil muitos órgãos públicos pendentes de informatização, de modo que muitos dados e informações seguem sendo produzidos e armazenados em formato físico. Não obstante isso, há clara tendência dos órgãos públicos brasileiros em informatizar processos, digitalizar informações originárias do

contam com maior grau de confiabilidade por serem produzidos ou custodiados por órgãos públicos.

Em função disso, são cada vez mais comuns as práticas de compartilhamento e publicação de dados com interessados diversos, para finalidades distintas, como a promoção de transparência ou até mesmo o fornecimento de subsídios para o desenvolvimento de novos ou existentes mercados. O uso desses dados, seja pelo próprio órgão público ou por terceiros, permite aprimorar a prestação de serviços públicos, que tende a ser realizada de forma mais proativa, direcionada e baseada em evidências (VERHULST; YOUNG, 2018).

Entre os benefícios da utilização de dados mantidos pelo poder público estão, *primeiro*, o uso dos referidos dados para o aprimoramento da prestação de serviços públicos e para o desenvolvimento de políticas públicas, desde a definição de prioridades e desenho das políticas até a sua implementação, *enforcement* e avaliação (VERHULST *et al*., 2019). Esse uso figura como um dos principais benefícios porque o cruzamento de maior quantidade de dados seria capaz de resultar em novas ou mais precisas análises,[26] além de permitir a gestão da infraestrutura e serviços públicos em tempo real.

Mais detalhadamente, esse benefício envolveria **(a)** a desburocratização e o aumento de eficiência nos serviços públicos, por meio da redução na quantidade de interações entre cidadãos e órgãos públicos viabilizada pela interoperabilidade de bases de dados; e **(b)** a existência de substratos de informação, decorrente da maior disponibilidade de dados, para **(b.1)** análises mais oportunas e precisas para a construção, fiscalização e aprimoramento de políticas; e **(b.2)** inovação no setor público, que pode ocorrer de forma independente ou em colaboração com terceiros.

---

formato físico e desenvolver sistemas e procedimentos para criar e reproduzir documentos digitais. Assim, mesmo informações produzidas *offline* poderão ser disponibilizadas no ambiente *online*. Além disso, embora seja elevado o número de cidadãos brasileiros sem acesso à internet, há dados e informações sobre essas pessoas no ambiente *online*. Suas informações podem ser incluídas no espaço digital de maneiras diversas, como pela coleta de dados por dispositivos distribuídos pela malha urbana e em decorrência da prestação de serviços públicos. Também podem ser incluídas informações sobre esses indivíduos em bases de dados governamentais *online* por consequência de parcerias firmadas com entidades privadas. Desse modo, ainda que indivíduos estejam desconectados ou adotem proativamente medidas para assegurar sua privacidade *offline* e *online*, fato é que há dados desses indivíduos em bases de dados governamentais *online* (*shadow profiles*). Nesse sentido, falar em privacidade nos tempos atuais invariavelmente requer a reflexão sobre a privacidade no espaço virtual.

[26] Esse pressuposto é, todavia, questionado pela literatura por motivos diversos que serão tratados nesta tese de doutorado. Exemplificativamente, análises de *big data* não necessariamente resultam em melhor tomada de decisão pelo poder público porque as escolhas analíticas podem ser enviesadas e os resultados produzidos pelos dados podem não ser devidamente absorvidos no processo de tomada de decisão. Mais sobre o tema, vide Vydra e Klievink, 2019.

Embora ideais de inovação estejam geralmente focados no setor privado, os governos também se envolvem em iniciativas de inovação (ASSAR; BOUGHZALA; ISCKIA, 2011). Por exemplo, iniciativas de dados abertos governamentais viabilizam práticas de inovação capazes de beneficiar agências de governo, empresas e também a sociedade, com base em recursos que poderiam estar congelados em um banco de dados controlado pelo governo. Trata-se de prática da chamada inovação aberta,[27] que utiliza de entradas e saídas intencionais de conhecimento para acelerar a inovação interna e expandir os mercados para o uso externo da inovação (CHESBROUGH, 2003). Ela se contrapõe ao paradigma de inovação fechada, no qual as organizações contam com funções internas para a descoberta de novos negócios.

Segundo, dados mantidos pelo poder público, se publicizados, auxiliam na promoção de **transparência governamental**, que, além de consistir em uma qualidade em si, viabiliza o exercício de *accountability* sobre as práticas e performance de órgãos públicos e qualifica a participação de cidadãos no governo (JELENIC, 2019). Assim, a divulgação de dados mantidos pelo governo permite que a população compreenda melhor o que fazem os órgãos e entidades públicos e possa exercer de forma mais qualificada contribuições ou fiscalização sobre atividades públicas. Com isso, a transparência auxilia na responsabilização de agentes públicos e na avaliação sobre o interesse público das ações realizadas, bem como contribui para a confiança dos cidadãos em relação ao governo e ao regime democrático (HARRISON; SAYOGO, 2014).

Além disso, a divulgação ou confirmação de informações pela administração pública também permite o combate a práticas de fraudes ou de desinformação *online*. Por exemplo, durante a pandemia de COVID-19, a divulgação de dados por governos locais permitiu o fomento de ecossistemas de checagem de conteúdo e, com isso, conter o espalhamento de informações falsas sobre os efeitos e formas de evitar o contágio pelo vírus.[28]

Apesar disso, a transparência não deve ser determinada de forma fixa e estática. É preciso determinar quais informações são efetivamente relevantes ao público e contribuem para a promoção da transparência governamental (HARRISON; SAYOGO, 2014). Assim, a

[27] O conceito de inovação aberta foi introduzido por Chesbrough (2003) para descrever a mudança de paradigma calcado em inovação fechada para um modelo onde a inovação reside dentro e fora de uma organização.

[28] Vide, por exemplo, o caso de Guiné-Bissau em parceria com a ONU. O PNUD e o Ministério da Saúde apoiaram o desenvolvimento de um site de verificação de fatos, que ajuda os cidadãos lusófonos a ter acesso a informações confiáveis sobre a COVID-19. Ao construir uma ampla comunidade de jornalistas, médicos e economistas de verificação de fatos da Guiné-Bissau e de todo o mundo, o site visa combater a desinformação em torno da pandemia, fornecendo fatos e notícias verificadas. Para mais informações, vide: https://www.undp.org/content/undp/en/home/news-centre/news/2020/Governments_must_lead_against_coronavirus_misinformation_and_disinformation.html. Acesso em 09.10.2020.

transparência não exige a divulgação de todo e qualquer dado, mas sim que as informações fornecidas por meio de políticas de transparência e governo aberto devem buscar atender o interesse público e observar a legislação pertinente - como as que regulam a transparência, a proteção de dados pessoais ou outros objetivos (FUNG; GRAHAM; WEIL, 2007).

Terceiro, dados custodiados por órgãos públicos possuem grande **potencial econômico**, na medida em que fornecem elementos que contribuem para práticas de inovação, para o desenvolvimento de mercados existentes ou para a criação de novos serviços.[29] Além disso, esses dados são utilizados também para fundamentar decisões comerciais (ZUIDERWIJK *et al*., 2015),[30] enriquecer bases de dados e evitar práticas de fraude ou incidentes de segurança.

Em relação aos benefícios econômicos da divulgação de dados mantidos pelo poder público, por exemplo, a divulgação de dados por tribunais no Brasil vem permitindo o surgimento de empresas especializadas na utilização de inteligência artificial em material divulgado em bases de dados de Tribunais para desenvolver produtos e serviços inovadores para o mercado jurídico e aprimorar a atuação do Poder Judiciário. Chamadas de *Law Techs* e *Legal Techs*,[31] essas empresas desenvolvem produtos capazes de diminuir o número de litígios, facilitar o acesso a dados, gerir documentos e apoiar o trabalho de juízes, promotores e advogados, gerando maior eficiência judicial e maior acesso à justiça.

Outro exemplo consiste no uso, por empresas de transporte individual privado, dos serviços oferecidos pelo Serviço Federal de Processamento de Dados (empresa pública denominada de Serpro) de validação de documentação para fins de assegurar segurança na prestação de seus serviços. Chamado de Datavalid, o serviço remunerado realiza consulta em bases de dados governamentais para verificar a validade de dados ou imagens enviados por um interessado. Essa validação pode ser feita por meio de verificação biométrica (digital e facial) ou cadastral e biográfica (dados cadastrais, sexo, filiação, CNH).[32]

---

[29] Vide listagem de estudos sobre impacto econômicos de políticas de dados abertos adotadas em países membros da União Europeia, organizada pela Comissão Europeia, constante do seguinte link: https://ec.europa.eu/digital-single-market/en/news/economic-analysis-psi-impacts. Acesso em 12.06.2019.

[30] O estudo de Zuiderwijk, *et al*., (2015) argumenta, todavia, que não basta a disponibilização de dados, sendo necessário que as empresas desenvolvam determinadas capacidades e possuam recursos específicos.

[31] *Legal Tech* (abreviação de *Legal Technology*) geralmente descreve o uso de tecnologias em aconselhamento jurídico. O uso varia de suporte simples baseado em plataforma (tele-advogado) a soluções parcial ou totalmente automatizadas que usam análises de big data e abordagens de aprendizado de máquina.

[32] Em 2019, a solução Datavalid oferecida pelo Serpro foi alto de um processo aberto pelo Ministério Público do Distrito Federal (MPDFT) no Tribunal de Contas da União (TCU) por uso ilegal de dados pessoais, apontando que, com a plataforma, o Serpro estaria violando uma série de dispositivos legais, entre eles o Marco Civil da Internet (Lei n. 12.965/2014) e a Lei Geral de Proteção de Dados (LGPD - Lei n.

Além disso, a circulação de determinadas informações também possui o potencial de estimular a inclusão social e práticas de empreendedorismo social. Isso significa que dados poderão ser utilizados com propósitos econômicos, mas de forma a beneficiar ou focar em população negligenciada ou desfavorecida, desprovida de meios financeiros ou influência política para alcançar o benefício transformador por conta própria (MARTIN; OSBERG, 2007).

Com isso, fica claro que a utilização responsável de dados mantidos pelo poder público possui a capacidade de gerar benefícios diversos, como a melhoria dos serviços públicos oferecidos aos cidadãos e promovida por esforços de eficiência e coordenação.[33]

Por certo, não se pressupõe que a manutenção ou divulgação de dados por entidades públicas ou a organização de *websites* com informações públicas por parte de órgãos da administração pública tenha como efeito natural todos os apontados benefícios. É necessário estimular o desenvolvimento de um ecossistema de agentes capazes de encontrar, utilizar e divulgar os dados mantidos pelo governo de forma responsável, em observância aos direitos fundamentais dos cidadãos e ao interesse público.

13.709/2018). Por outro lado, se se demonstrar a legalidade e conformidade com a Lei Geral de Proteção de Dados e leis setoriais, a ferramenta pode tanto tornar as aplicações mais seguras para os usuários, quanto gerar receita para a estatal, sem que se haja a necessidade de realizar o uso compartilhado de bancos de dados governamentais. Vide https://www.mpdft.mp.br/portal/pdf/comunicacao/junho_2019/Representacao_TCU_-_SERPRO_-_PGJ.pdf. Acesso em 27.03.2021.

[33] Relatório divulgado pelo Centre for Data Ethics and Government do Governo Inglês, que apresenta casos em que a divulgação de dados pode gerar benefício público. Vide: https://www.gov.uk/government/publications/cdei-publishes-its-first-report-on-public-sector-data-sharing/addressing-trust-in-public-sector-data-use?utm_source=Digest&utm_campaign=7063bf665b-RSS_EMAIL_CAMPAIGN&utm_medium=email&utm_term=0_d90a01c7ff-7063bf665b-87770509#introduction--context. Acesso em 26.07.2020.

2 O PAPEL DO COMPARTILHAMENTO E DA PUBLICAÇÃO PARA AS ATIVIDADES DO PODER PÚBLICO

Os benefícios apontados, embora digam respeito ao tratamento de dados pelo poder público de uma forma geral, estão em grande medida atrelados à circulação de dados custodiados por órgãos e entidades públicas para terceiros, públicos e privados. Por exemplo, a eficiência assegurada pela interoperabilidade ou do sistema multiportas resulta do compartilhamento de dados entre órgãos e entidades públicas (e por vezes com particulares), de forma a evitar que o mesmo dado seja coletado diversas vezes. Da mesma forma, a transparência pública exige que dados e informações mantidos pelo poder público sejam publicados para acesso e uso posterior pela sociedade ou sejam compartilhados com solicitantes de acesso à informação. Também o uso de dados para finalidades de inovação e desenvolvimento de mercados exige a publicação ou compartilhamento de dados.

De fato, como mencionado, o desenvolvimento de novos modelos de governo (e.g., governo eletrônico, governo digital e governo aberto) envolve a circulação de dados, e essas trocas são comumente classificadas pela literatura, observando também outros aspectos,[34] como Governo-Governo (G2G), Governo-Empresas (G2B) e Governo-Cidadãos (G2C).

Essa circulação de dados será referida como a divulgação de dados que, por sua vez, será tido como um termo guarda-chuva, que envolve situações diversas de circulação de informações, como o compartilhamento de dados, entre órgãos públicos ou com particulares, e a publicação de dados em políticas de transparência ou de dados abertos. Já os termos *compartilhamento* e *publicação* também serão utilizados de forma ampla, podendo contemplar uma série de outros conceitos. Em particular, o compartilhamento será considerado como a divulgação (ou a comunicação, acesso, uso compartilhado etc.) de dados entre duas ou mais partes (sendo o governo o responsável por enviar os dados para o terceiro) para finalidades específicas, e a publicação significará a disponibilização (ou a difusão, transferência, acesso etc.) à coletividade por força de normas de transparência e dados abertos. Com isso, entende-se que os dois conceitos utilizados envolvem o deslocamento ou o acesso de dados a terceiros que não o detentor original da base de dados.

[34] Esse modelo pode ser complementado (Yildiz, 2007) pelo relacionamento entre Governo-Sociedade Civil (G2SC) e Cidadãs-Cidadãos (C2C). Há também o modelo C2G, no qual cidadãos fornecem feedback para órgãos públicos, ou o modelo de C2G2C, em verdadeiro diálogo entre cidadão e poder público (JOHNSON; SIBER, 2013; CAVALLO *et al*., 2014).

A seguir, serão abordados em maior detalhe os conceitos de compartilhamento de dados, com entes públicos ou particulares, e a publicação de dados em políticas de transparência e dados abertos, assim como serão demonstrados seus fundamentos jurídicos, e apontadas as suas semelhanças e diferenças. Ao final, será argumentado que, a despeito de suas diferenças, o compartilhamento e a publicação de dados por governos possuem semelhanças suficientes, especialmente porque envolvem a circulação de dados e seu posterior reuso por terceiros, para justificar a adoção de procedimentos semelhantes para assegurar que sejam realizadas em observância à proteção de dados pessoais.

2.1 Publicação de dados: conceito e benefícios

Nesta tese de doutorado, o termo publicação será compreendido como a atividade realizada pelo poder público de viabilizar acesso e uso posterior pela sociedade a informações de interesse público para, entre outros, alcançar a garantia da transparência governamental.

Por sua vez, como aponta Ann Florini (1999), o termo transparência governamental é raramente utilizado com rigor, mas os conceitos apresentados geralmente estão atrelados à consecução do direito à informação e ao conceito de *accountability*. Assim, a transparência governamental é essencial a um Estado republicano[35] e democrático,[36] visto que exige-se que sejam tornadas públicas informações essenciais ao exercício qualificado e independente da liberdade de expressão, da responsabilização de agentes públicos e do direito ao voto (UBALDI, 2013). De fato, a participação de cidadãos na gestão e fiscalização do governo é fundamental para uma democracia (RODRIGUES, 2014).

Assim, entre os benefícios da publicação de dados pessoais mantidos por órgãos e entidades públicas, em políticas de transparência e dados abertos, estão sua essencialidade

[35] Nesse sentido se manifestou o Ministro do Supremo Tribunal Federal, conforme se verifica: "Ato que indefere acesso a documentos relativos ao pagamento de verbas públicas. [...] A regra geral num Estado Republicano é a da total transparência no acesso a documentos públicos, sendo o sigilo a exceção. [...] As verbas indenizatórias para exercício da atividade parlamentar têm natureza pública, não havendo razões de segurança ou de intimidade que justifiquem genericamente seu caráter sigiloso (grifo nosso). Supremo Tribunal Federal (STF). Mandado de Segurança 28.178. Impetrante: Empresa Folha da Manhã. Impetrado: Presidente do Senado Federal. Relator: Ministro Roberto Barroso. Brasília, 04 de mar. de 2015. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=8399320. Acesso em 31.08.2022.

[36] De forma bastante sucinta, a transparência é pressuposto para que se configure uma das características-chave da democracia apontadas por Robert Dahl, consistente na responsividade contínua do governo em relação às preferências de seus cidadãos. Isso porque, segundo aponta o autor, para que um governo seja reiteradamente responsivo, todos os cidadãos devem possuir plenas oportunidades para (i) formular suas preferências; (ii) expressar suas preferências à sociedade e ao governo por meio de ação individual ou coletiva; e (iii) ter suas preferências igualmente consideradas pelo governo (DAHL, 2005). Esses requisitos somente são possíveis se aos cidadãos forem fornecidas informações e dados sobre a atuação governamental.

para a democracia (RUIJER *et al.*, 2017; HARRISON; SAYOGO, 2014), transparência e *accountability* governamental, além da promoção de aumento na confiança dos cidadãos em instituições públicas e o fomento à inovação (MEIJER *et al*., 2014). Ela é, em outras palavras, condição para o exercício de outros direitos e liberdades (Rodrigues, 2014) e permite: **(i)** maior visibilidade sobre as práticas e procedimentos governamentais; **(ii)** encontrar informações sobre ocupantes ou candidatos a cargos públicos e/ou políticos; **(iii)** facilitar determinadas transações, como a troca de propriedade, ou **(iv)** acessar informações para uma série de finalidades (SOLOVE, 2002).

A transparência pode ser assegurada de formas diversas, com destaque para a divulgação, ativa ou passiva, de informações produzidas ou mantidas pelo poder público por meio de políticas de transparência ou de dados abertos. As informações que estão contempladas no dever de transparência são as produzidas ou mantidas pelo governo e que estão relacionadas com atividades como o dispêndio de recursos públicos ou estabelecimento de contratos, mas que também podem ser coletadas por meio de sensores e outros dispositivos que coletam e armazenam grande quantidade de dados sobre fenômenos diversos, sociais (e.g., circulação de pessoas na cidade) ou não (e.g., nível de água em determinado reservatório). São, portanto, todos os dados mantidos pelo poder público, independentemente do meio (e.g., documento ou base de dados) ou da origem (se coletados diretamente pelo órgão público ou por terceiros), ainda que possa haver exceções legalmente estabelecidas à sua divulgação.

Embora a primeira norma de transparência tenha sido editada na Suécia em 1774, foi somente após a segunda Guerra Mundial, com a expansão da burocracia estatal, e a Guerra Fria, com a ampliação de práticas de sigilo para a garantia de segurança nacional, que foram editadas outras leis de transparência (FLORINI, 2004), a exemplo da edição do *Freedom of Information Act* nos Estados Unidos, em 1966, e da sua atualização em 1974 (FROST, 2003). A próxima onda de leis de transparência ocorreu na década de 1990 com apoio de organismos internacionais (a exemplo do Banco Mundial) e diante da redemocratização de governos e do fortalecimento de organizações da sociedade civil (ROBERTS, 2007).

Adiante, no final da década de 2000, ao lado das medidas de transparência iniciaram discussões acadêmicas sobre governos abertos. Esses debates se intensificaram após a publicação em 2009 pelo então Presidente dos Estados Unidos, Barack Obama, da iniciativa

de governo aberto.[37] Assim como a transparência, o termo possui uma multiplicidade de definições, mas que geralmente associam a utilização de tecnologias da informação e comunicação a três pilares: transparência, participação e colaboração (WIRTZ; BIRKMEYER, 2015). Sob a perspectiva tecnológica, governos abertos são comumente associados à adoção de dados governamentais abertos.

O conceito de dados abertos supõe a divulgação de ampla gama de dados, por meio da Internet, de forma atualizada, em formato não proprietário, e com a possibilidade de serem reutilizados indefinidamente (UBALDI, 2013). Dados governamentais abertos,[38] por sua vez, são produzidos e/ou mantidos por órgãos governamentais e disponibilizados com os parâmetros dos dados abertos. Em outras palavras, o substrato das políticas de dados abertos consiste em dados brutos de acesso, uso e compartilhamento irrestritos por qualquer pessoa, sendo, no máximo, obrigatório creditar sua autoria e compartilhá-los pela mesma licença.[39]

Assim, enquanto a ideia de transparência é historicamente utilizada para fundamentar o dever de governos divulgarem a cidadãos informações sobre suas práticas, as políticas de dados abertos são mais recentes e possuem finalidades mais amplas - podendo incluir desde a transparência até o reuso de dados para finalidades econômicas - e exigem que governos não apenas divulguem os dados que dispõem, mas também que o façam em formatos abertos.

Além disso, nas políticas de dados abertos, o objeto de divulgação são bases de dados abertas, e, nas práticas de transparência, o escopo de publicação poderá ser mais amplo, incluindo bases de dados e/ou repositórios de documentos. A divulgação de bases de dados em formato aberto permite sua reutilização e manipulação por máquina, o que não ocorre com informações divulgadas em repositórios de documentos, que são armazenadas de forma não sistematizada, em formato proprietário ou até em imagem.

Dessa forma, entre outras diferenças, as políticas de transparência **(i)** não compartilham dos mesmos pressupostos de políticas de dados abertos, como a ampla disponibilidade de dados e a ausência de licenças para sua reutilização; e **(ii)** estão intimamente relacionadas com a manutenção do estado democrático de direito, por meio da

[37] Desde o lançamento do primeiro portal de dados abertos (data.gov) pelo governo dos Estados Unidos em 2009 para fornecer um único ponto de acesso aos dados de várias agências públicas, um número crescente de países lançou iniciativas de dados abertos semelhantes (por exemplo, Cingapura, Austrália, Chile). O projeto incluiu oitenta e quatro programas diferentes de Big Data que fazem parte de seis departamentos diferentes.

[38] Note que os conceitos de dado governamental aberto e de governo aberto são distintos, pois o segundo nem sempre será conduzido pelos princípios de dados abertos. O governo aberto, como mencionado, envolve a utilização de tecnologia para promover transparência e participação social – o que poderá envolver ou não a divulgação de dados abertos.

[39] Vide: http://opendefinition.org/. Acesso em 10.01.2021.

promoção de acesso à informação e no fornecimento de subsídios para a fiscalização da atividade pública, enquanto as políticas de dados abertos podem também almejar contribuir com finalidades econômicas.

No entanto, mesmo que políticas de transparência e dados abertos sejam distintas, com características próprias (e.g., material divulgado e forma de publicação), elas são comumente abordadas em conjunto ou vistas como parceiras porque possuem entre seus objetivos a circulação de informações governamentais e poderão ter como fundamento leis de acesso à informação (UBALDI, 2013). Por exemplo, no Brasil, a LAI recomenda a adoção de certos padrões da divulgação de dados abertos quando da promoção de transparência ativa (art. 8º, § 3º, II e III), ainda que não sejam de observância mandatória, e que outros padrões de dados abertos não estejam igualmente mencionados (BURLE *et al*, 2015).

Assim, práticas de transparência e dados abertos possuem o condão de reduzir a assimetria de informações entre indivíduos e governo, permitindo a colaboração cidadã na promoção de gestão pública mais eficiente (STIGLITZ, 1999). Por exemplo, dados publicados a respeito da contaminação por COVID-19 permitiram a institutos de pesquisa realizar estudos sobre como a pandemia afetou de formas diferentes comunidades, ou identificar os momentos adequados para o encerramento de políticas de distanciamento social e os novos focos de infecção após essa reabertura.

Elas também contribuem para a tomada de decisão com base em *data analytics*, em áreas diversas e por *player*s variados, que é capaz de gerar resultados mais efetivos e a redução de gastos (TENE; POLONETSKY, 2011). Além disso, embora de comprovação ainda controvertida (GRIMMELIKHUIJSEN; MEIJER, 2012), outro benefício da publicação de dados por governos consiste na maior confiança nas instituições em razão do aumento da capacidade investigativa e probatória de órgãos atuantes no *enforcement* de leis (MEIJER *et al*., 2014). Por exemplo, a divulgação de dados eleitorais na Indonésia e em Burkina Faso tem auxiliado cidadãos a confiar mais no sistema eleitoral e nos representantes eleitos. Essa maior confiança está associada à possibilidade de acionar autoridades com base em informações divulgadas.

Esses benefícios da disponibilização de dados governamentais também podem gerar valor para o setor privado. Isso porque a disponibilidade de informações fornece substrato para o desenvolvimento de novos negócios ou o aprimoramento de mercados existentes, visto que permite *players* diversos a tomar decisões de maneira mais orientada, eficiente e

inovadora (JANSSEN; DEN HOVEN, 2015; KIM; TRIMI; CHUNG, 2014), o que pode reverter no aprimoramento de processos, produtos e serviços (JANSSEN *et al*., 2012; ZUIDERWIJK; JANSSEN, 2014).

No entanto, não se pode pressupor que políticas de transparência e dados abertos possuem como efeito natural a melhoria no processo democrático, sendo necessária a ampliação do alcance das informações governamentais disponibilizadas e a promoção de capacitação de agentes com habilidades técnicas específicas para ler, sistematizar e traduzir as informações para o público em geral (JANSSEN; DEN HOVEN, 2015). Isso porque a simples ampliação de informações e dados disponíveis não significa que cidadãos saberão onde encontrá-las ou como avaliá-las (FILGUEIRAS, 2011). Por exemplo, possuir o conhecimento e os recursos necessários para utilizar as informações publicadas se mostra essencial ao sucesso de políticas de dados abertos.

2.2 Compartilhamento de dados: conceito e benefícios

Na origem, órgãos e entidades públicos possuem suas próprias bases de dados, organizadas para que possam exercer atividades relacionadas às suas atribuições legais. Esses dados, que muitas vezes são mantidos e utilizados somente pelo ente público que os coletou, possuem grande valor social e econômico, motivo pelo qual são compartilhados com terceiros.

Como mencionado, o compartilhamento de dados consiste em atividades de tratamento de dados que contemplam a autorização integral ou parcial de acesso a dados, a troca recíproca ou unilateral de dados, ou a reunião de dados fornecidos por diversos agentes para consumo próprio ou por terceiros. Ele pode ocorrer de formas diversas, como ilustrado pelos seguintes exemplos: **(i)** troca recíproca ou unilateral de dados entre organizações; **(ii)** autorização de acesso, integral ou parcial, a determinada base de dados por poucos interessados e para finalidades específicas; **(iii)** reunião de dados fornecidos por diversos agentes (*data pooling*) para consumo desses mesmos atores ou por terceiros; **(iv)** troca de dados realizada de forma frequente ou apenas uma única vez (ICO, 2019).[40] Essas práticas poderão ou não envolver dados pessoais, sendo necessário ao gestor público avaliar

[40] Vide Relatório sobre compartilhamento de dados divulgado pela Autoridade Inglesa de proteção de dados pessoais, a ICO disponível em: https://ico.org.uk/media/2615361/data-sharing-code-for-public-consultation.pdf. Acesso em 07.03.2021.

previamente se há a presença de identificadores ou a possibilidade de associação dos dados a indivíduos específicos.[41]

Algumas dessas atividades podem ser ilustradas pela regulação do Denatran a respeito do acesso às suas bases de dados por terceiros interessados. A Portaria Denatran nº 15/2016 regula o acesso aos seus sistemas e subsistemas, concedendo a apenas algumas entidades a possibilidade de solicitar acesso às bases de dados de trânsito, a saber: **(a)** órgãos e entidades componentes do Sistema Nacional de Trânsito ("SNT"); **(b)** órgãos e entidades públicas não integrantes do SNT; e **(c)** entidades privadas credenciadas ou atuantes no mercado de trânsito (art. 6º).[42] Referidas entidades deverão obedecer procedimento de solicitação de acesso, integral ou parcial, à base de dados que, caso julgado procedente, culmina na assinatura de contrato com o Serpro,[43] entidade que realiza a gestão das bases de dados do Denatran e que concederá o acesso às bases de dados.[44] Como se verifica, nessa relação há algumas das referidas modalidades de compartilhamento de dados com entidades públicas ou entidades privadas que conseguirem demonstrar a relevância de acesso aos dados para a prática de suas atividades: **(i)** envio de bases de dados do Denatran para gestão pelo Serpro; **(ii)** acesso integral ou parcial às bases de dados pelo solicitante; e **(iii)** acesso aos dados realizado de forma frequente ou uma única vez.

Independente do formato, o compartilhamento de dados é peça essencial para o fomento a modelos de governo baseados no uso de novas tecnologias, como os já mencionados exemplos do governo eletrônico, governo digital, cidades inteligentes ou

---

41 O conceito e regulação de dado pessoal serão abordados mais adiante.

42 Nos termos da Portaria: "Art. 6º [...] III - Entidades privadas, devidamente credenciadas para desempenhar serviços estabelecidos no Código de Trânsito Brasileiro – CTB, normativos do Conselho Nacional de Trânsito – CONTRAN ou do Denatran, quando a informação for indispensável ao exercício de suas atividades; IV - Entidades privadas cuja atividade esteja relacionada ao trânsito, transporte, fabricação e comercialização de veículos, segurança veicular, financiamento, seguros, registros e outras atividades necessárias ao funcionamento do trânsito e transporte, desde que a entidade comprove a necessidade de acesso aos sistemas e subsistemas do Denatran para desempenho de suas atividades".

43 O Serpro é uma empresa pública brasileira vinculada ao Ministério da Fazenda, criada pela Lei nº 4.516/1964 e atualmente regulada pela Lei nº 5.615/1970. Suas atividades têm por objeto "a execução de serviços de tratamento de informações e processamento de dados, através de computação eletrônica ou eletromecânica, e a prestação de assistência no campo de sua especialidade" (art. 1º, Lei nº 5.615).

44 Para obter essa autorização, os solicitantes devem demonstrar o interesse e a necessidade em obter acesso aos dados. Para as entidades privadas interessadas, será necessário demonstrar que exercem, entre outras, atividades relacionadas ao trânsito, transporte, ou que precisem dos dados para a validação de Carteira Nacional de Habilitação ("CNH") ou de Certificação de Registro de Veículo ("CRV"). Deferido o pedido, as entidades autorizadas a acessar as bases de dados do Denatran deverão firmar contrato com o Serpro e assinar Termo de Compromisso de Manutenção de Sigilo, pelo qual se comprometem a não copiar ou reproduzir o conteúdo dos sistemas que acessar, assim como preservar e não compartilhar com terceiros as informações de acesso restrito. A portaria nº 15/2016 está disponível no seguinte link: https://infraestrutura.gov.br/images/Portarias-Denatran/2016/Portaria0152016_nova3.pdf. Acesso em 10.07.2019.

governo aberto. Enquanto nos governos eletrônicos e digitais a interoperabilidade de sistemas é peça essencial, nas *smart cities* a complexidade das soluções oferecidas muitas vezes exige o envolvimento de atores diversos em atividades de agregação e análise dos dados.[45] Além disso, a promoção de governos digitais e/ou abertos, que envolve maior engajamento do cidadão, requer a coordenação de sistemas e bases de dados para fornecer informações em maior granularidade e atualização.[46]

São diversas as finalidades que justificam o compartilhamento de dados mantidos pelo poder público, mas é possível apontar as seguintes como as mais comuns: (a) assegurar ao indivíduo serviços mais céleres e personalizados - esse era o caso do Programa Bolsa Família, cuja execução envolvia a coleta de dados por parte do município, que são divididos com o Ministério da Economia para avaliação de elegibilidade do solicitante e com a Caixa Econômica Federal para fins de pagamento do benefício; (b) planejar, executar e monitorar a prestação de serviços públicos - como exemplo, o serviço de transporte público envolve o compartilhamento frequente de dados entre governo local e concessionárias; (c) a criação, execução, monitoramento e avaliação de políticas públicas - é o caso do serviço fornecido pelo Serpro aos órgãos da administração pública federal para serviços de apoio ao desenho de novas políticas, tendo como base análises realizadas com dados constantes das diversas bases

[45] "Por exemplo, um aplicativo de reserva de estacionamento reúne dados de ocupação de garagem, dados históricos de tráfego, dados meteorológicos atuais e informações sobre os próximos eventos públicos para determinar os custos de estacionamento em tempo real. Também analisamos um conjunto mais amplo de potenciais aplicações futuras e descobrimos que 40% adicionais também exigirão agregação de dados entre as indústrias. [...] Como as soluções inteligentes atuais são frequentemente patrocinadas por departamentos municipais individuais, muitas aplicações habilitadas para o IoT dependem de dados limitados e em silos. Mas dado o valor potencial das aplicações que requerem agregação entre fontes, não é surpresa que muitas cidades estejam buscando parcerias com provedores de tecnologia para desenvolver plataformas e outras iniciativas que integrem dados de múltiplas fontes. Por exemplo, Huawei é o arquiteto chefe de soluções smart-city na cidade de Shenzhen's Longgang District, trabalhando com centenas de parceiros para acessar dados. Mesmo um projeto com escopo relativamente limitado – o programa LinkNYC em Nova York, que substituiu os telefones públicos por quiosques com Wi-Fi – exigiu que três empresas diferentes fornecessem os dados, o hardware e as capacidades de rede necessários. As cidades estão se tornando os gerentes das plataformas de dados e os orquestradores dos ecossistemas digitais em expansão.. (tradução nossa) (Veja "High-Impact Solutions Depend on Sharing Data.") Vide: https://www.bcg.com/publications/2020/smart-cities-need-to-understand-the-risks-and-rewards-of-data-sharing-part-3. Acesso em 07.03.2021.

[46] "Reconhecendo que soluções centradas no cidadão requerem mais compartilhamento de dados dentro do governo, as cidades estão começando a investir no intercâmbio interno de dados. Elas estão construindo plataformas abertas e diretórios de dados que dão a todos os departamentos e agências maior acesso aos dados disponíveis. Cerca de 40% das cidades inteligentes que analisamos têm plataformas de dados abertos com bancos de dados back-end integrados que permitem o acesso por aplicativos externos, um pré-requisito para o fácil compartilhamento e uso dos dados. Outros 15% incluíram a construção de conectividade back-end como uma prioridade em seus planos estratégicos digitais. Por exemplo, Portland (Oregon) e Seul (Coréia do Sul) estão construindo seus próprios repositórios de dados internos: Portland Urban Data Lake e Smart Seoul Data. O compartilhamento de alguns dados é intrinsecamente problemático." (tradução nossa) Vide: https://www.bcg.com/publications/2020/smart-cities-need-to-understand-the-risks-and-rewards-of-data-sharing-part-3. Acesso em 07.03.2021.

de dados que gerencia;[47] (d) fiscalização das atividades realizadas por entidades públicas e seus parceiros, como a realizada pelos Tribunais de Contas, Ministério Público ou até mesmo pelo cidadão; e (e) realização de pesquisas por órgãos públicos, pesquisadores independentes ou instituições privadas - como a análise por pesquisadores de dados detidos pelo Ministério da Saúde sobre a contaminação COVID-19 com a finalidade de compreender tendências do vírus e auxiliar em medidas de enfrentamento da pandemia.

Nesse sentido, o compartilhamento de dados mantidos pelo poder público, com outras entidades públicas ou com particulares, está geralmente associado a objetivos de cumprimento de atribuições legais ou de modernização do aparato estatal que, por sua vez, almeja assegurar ideais como eficiência, desburocratização, e participação popular. Poderá também almejar a transparência governamental, a exemplo do que ocorre quando da resposta a solicitações de acesso à informação ou no acesso controlado a dados de interesse público, mas cuja divulgação possa oferecer elevado risco a direitos e liberdades individuais.

Em outras palavras, o compartilhamento de dados fornece instrumentos para aprimorar políticas públicas, caso dados sejam efetivamente reunidos para a obtenção de melhor compreensão sobre determinada política, e permite que o próprio governo desenvolva novos negócios (VAN DEN BRAAK *et al.*, 2012). Além disso, permite a melhoria da experiência do cidadão quando do uso de serviços públicos, na medida em que reduz a necessidade de interações com diversos órgãos ou entidades públicas, fornecendo informações pessoais menos vezes e recebendo respostas com maior especificidade.[48] Finalmente, fornece substrato para o desenvolvimento de novos negócios, a execução compartilhada de políticas públicas, o fomento à execução direta de atividades de interesse público.

2.3 Semelhanças e diferenças entre compartilhamento e publicação

Como se verifica, nesta tese estão sendo analisadas as situações em que os dados são divulgados a terceiros, com foco no: **(i)** compartilhamento com outros órgãos públicos ou com particulares; e **(ii)** publicação em políticas de transparência e de dados abertos. Esses parâmetros tomam como pressuposto estudos sobre governo eletrônico (*e-government*) e governo aberto (*open government*), que apresentam modelos de interação do governo com

[47] O Serpro desenvolveu uma solução de lago de dados para promoção de políticas públicas. Vide: https://serpro.gov.br/menu/noticias/noticias-2018/data-lake-serpro-uma-nova-forma-de-prover-politicas-publicas-para-a-sociedade. Acesso em 07.03.2021.

[48] Todavia, faz-se necessário observar a implementação de tais serviços sem que se criem ou intensifiquem segmentações sociais (CAVALLO *et al.*, 2014).

distintos *stakeholders* (YILDIZ, 2007; BROWN; BRUDNEY, 2001).[49] Nesta tese, será privilegiado o modelo simplificado de interação de governos com distintos *stakeholders*: Governo-Governo (G2G), Governo-Empresas (G2B) e Governo-Cidadãos (G2C), na medida em que se está observando a divulgação de dados realizada pelo poder público a terceiros, que podem ser agrupados nessas três categorias (governos, empresas e cidadãos), e não o recebimento pelo poder público de dados enviados por terceiros, públicos ou privados.

Além disso, a publicação e o compartilhamento de dados são tratados nesta tese como passíveis de serem comparadas e submetidas a soluções jurídicas semelhantes, na medida de suas diferenças, por consistirem em atividades de tratamento que resultam na circulação de dados pessoais e viabilizam o reuso desses dados por terceiros. No entanto, para que se possa estabelecer os pontos de convergência e divergência nas soluções jurídicas propostas, é importante ter clareza sobre seu escopo, assim como sobre quais são as semelhanças e diferenças entre essas duas atividades de tratamento de dados.

Nesta tese, a publicação de dados seria a atividade de tratamento de dados realizada pelo poder público para viabilizar acesso e uso posterior de informações de interesse público por meio de sistemas de transparência e dados abertos. Já o compartilhamento consiste em atividades de tratamento de dados realizadas pelo poder público que contempla a autorização integral ou parcial de acesso a dados, a troca recíproca ou unilateral de dados, ou a reunião de dados fornecidos por diversos agentes para consumo próprio ou por terceiros. Os terceiros receptores desses dados podem ser cidadãos ou entes públicos ou privados.

Especificamente, nas políticas de transparência e dados abertos são disponibilizados ao público, ativamente ou mediante solicitação, documentos e dados custodiados por órgãos públicos com o objetivo de fomento à transparência, *accountability*, inovação e benefício econômico (RUIJER, GRIMMELIKHUIJSEN, HARRISON, SAYOGO, 2014; MEIJER *et al.*, 2014). Já nas práticas de compartilhamento de dados com o poder público ou com particulares haverá a divulgação, integral ou restrita, de documentos ou dados para sujeitos específicos. No compartilhamento com outros órgãos públicos, o objetivo reside na promoção de eficiência, redução de custos, desburocratização e aprimoramento na prestação de serviços público (VEN DEN BRAAK *et al.*, 2012; GIL-GARCIA *et al*., 2019), e no compartilhamento

[49] Esse modelo pode ser complementado (YILDIZ, 2007) pelo relacionamento entre Governo-Sociedade Civil (G2SC) e Cidadãs-Cidadãos (C2C). Há também o modelo C2G, no qual cidadãos fornecem feedback para órgãos públicos, ou o modelo de C2G2C, em verdadeiro diálogo entre cidadão e poder público (JOHNSON; SIBER, 2013; CAVALLO *et al*., 2014).

com particulares o objetivo está em viabilizar a execução descentralizada de serviços públicos, o estímulo à inovação e o fomento a execução de certas atividades.

Assim, tanto o compartilhamento como a publicação de dados mantidos pelo poder público são formas pelas quais governos interagem com os seus distintos *stakeholders*, por meio de divulgação (e.g., envio, publicação e permissão de acesso) de dados a terceiros para o alcance de finalidades diversas. Por outro lado, entre as principais diferenças entre essas atividades de tratamento estão quem são os receptores dos dados, as finalidades de divulgação e os riscos oferecidos aos titulares dos dados divulgados.

Em relação aos receptores dos dados, a publicação e o compartilhamento diferem porque a publicação é direcionada a sujeitos indeterminados, na medida em que deve ser acessível por toda a sociedade, e o compartilhamento é direcionado a sujeitos determinados, que poderão ser cidadãos, entes privados ou órgãos e entidades públicas. De todo modo, há alguma sobreposição em relação aos receptores do compartilhamento e da publicação. Embora a publicação seja direcionada a uma quantidade maior de possíveis interessados, ela alcança receptores que poderiam solicitar acesso a esses mesmos dados pelo compartilhamento. Inclusive, a publicação de informações em portais de transparência e dados abertos pode, em privilégio à eficiência e à isonomia, substituir o compartilhamento de dados solicitados por vias administrativas diversas, até mesmo por pedidos de acesso à informação.

Quanto às finalidades, no compartilhamento entre órgãos públicos, a divulgação do dado se dá, por exemplo, em função de determinação legal (e.g., decreto federal de compartilhamento de dados), para gestão de bases de dados (e.g., compartilhamento de dados com Serpro ou DataPrev), quando o desenvolvimento de uma determinada política pública envolver diversos órgãos ou entidades (e.g., compartilhamento de dados com a Caixa Econômica Federal para fins do programa Minha Casa Minha Vida). No compartilhamento com particulares, o dado será enviado ou recebido por particulares, em função de situações como o desempenho de atividades delegadas (e.g., bilhete único de ônibus), o estabelecimento de parcerias para o aprimoramento de políticas públicas (e.g., Zona Azul e parceria com *Waze*), ou para viabilizar ou colaborar com a devida prestação de serviços privados (e.g., acesso a bases de dados do Denatran por empresas atuantes no setor de transportes). Por fim, na publicação em políticas de transparência e/ou de dados abertos, órgãos ou entidades públicas divulgam dados (em formato aberto ou não) ao público - o que poderá contemplar

cidadãos, empresas, comunidade científica etc. -, com a finalidade de transparência, *accountability*, estímulo ao desenvolvimento e inovação, entre outros.

Assim, idealmente, o compartilhamento de dados pessoais tem como fundamentação jurídica a observância ao princípio da legalidade, a busca da eficiência governamental e a promoção de inovação e desenvolvimento econômico, e a publicação tem como fundamentação jurídica a transparência governamental, a garantia de acesso à informação e o fornecimento de substrato para o exercício de *accountability*. No entanto, atualmente (e em vista dos novos modelos de governo) as finalidades da publicação e do compartilhamento por vezes se confundem, de forma que a publicação poderá almejar promover a inovação ou o desenvolvimento econômico e o compartilhamento poderá assegurar o acesso à informação e fornecer subsídios para práticas de *accountability*.[50]

Por sua vez, em relação aos potenciais danos à privacidade de indivíduos, como será mais detidamente abordado a seguir, enquanto em políticas de transparência os dados são divulgados ao público, podendo ser sempre acessados por grande quantidade de sujeitos, no compartilhamento de dados a divulgação será realizada, uma única vez ou frequentemente, de forma direcionada a determinados sujeitos. Disso decorre que, na publicação, dados estão mais disponíveis do que no compartilhamento, de modo a oferecer maiores chances para que agentes maliciosos os utilizem de forma inadequada. Por isso, o compartilhamento de dados pessoais pode oferecer menores riscos à privacidade, se comparado com a publicação.

No entanto, essa presunção nem sempre será verdadeira. A depender de como é realizado, o compartilhamento de dados poderá privilegiar determinados *stakeholders*, entes públicos ou privados, que possuem acesso a dados que não estão disponíveis ao restante da sociedade. Para além dessa possível ausência de isonomia no acesso a dados mantidos e geridos pelo poder público, se realizados sem as devidas salvaguardas, o compartilhamento poderá permitir abusos por agentes públicos ou privados.

Adicionalmente, o risco da publicação ou do compartilhamento não pode ser medido somente em relação à quantidade de sujeitos que podem acessar os dados. Deve-se levar em

[50] Isso é confirmado pelo excerto do voto do Ministro Gilmar Mendes no julgamento conjunto da ADI 6649 e da ADPF 695: "O regulamento impugnado [Decreto n 10.046/2019] desempenha a delicada missão de sistematizar regras e princípios aplicáveis ao compartilhamento de dados entre órgãos públicos federais, em uma tentativa de fundar balizas para aplicação harmônica dos dispositivos da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) e a Lei de Acesso à Informação (Lei 12.527/2011). A complexidade do assunto é evidenciada pela existência de conflitos aparentes entre normas que impõem transparência absoluta na condução dos negócios públicos, de um lado, e aquelas que estabelecem limites rigorosos para o fluxo de dados pessoais coletados ou produzidos pelo Estado, de outro."

conta quais são os dados divulgados, a forma e frequência de sua divulgação, e as salvaguardas adotadas na divulgação. Por exemplo, a publicação do CPF de servidores públicos para fins de transparência, com tarjas em parte do número e em formato não legível por máquina, ofereceria menos risco à privacidade, se comparado com o compartilhamento de dados de saúde de cidadãos em formatos interoperáveis e para fins econômicos. Assim, o compartilhamento e a publicação de dados devem ter seus riscos avaliados no caso concreto e tendo em vista **(a)** quais dados são divulgados; **(b)** a quem os dados são divulgados; **(c)** para quais finalidades os dados serão utilizados; **(d)** o formato e frequência de divulgação dos dados; e **(e)** salvaguardas e restrições ao posterior uso dos dados.

Portanto, como se verifica, o compartilhamento e a publicação de dados pelo poder público, embora sejam atividades de tratamento distintas, com diferenças importantes entre si, resultam na circulação de dados pessoais e no reuso de dados por terceiros. Além disso, embora estejam originalmente fundamentados em regimes jurídicos distintos, em vista da evolução da tecnologia e do surgimento de novas modalidades de governo, o compartilhamento e a publicação podem por vezes ser utilizados para o alcance de finalidades similares e serem respaldadas por regimes jurídicos similares. Por isso, nesta tese se argumenta que essas atividades devem ser submetidas a similares procedimentos e parâmetros que assegurem a proteção da privacidade e dos dados pessoais em uma coerência mínima na sua prática, respeitadas as suas diferenças.

3 RISCOS À PRIVACIDADE DECORRENTES DO TRATAMENTO DE DADOS PELO PODER PÚBLICO

Como se verificou nas seções anteriores, o tratamento de dados pessoais pelo poder público é essencial à execução de suas atribuições legais, ao desenvolvimento de políticas públicas, à garantia de direitos, à adoção de medidas para garantir eficiência, inovação e publicidade governamentais, e até mesmo para viabilizar o desenvolvimento econômico. No entanto, entre os dados divulgados pelo poder público, há dados pessoais,[51] identificados ou que permitirão a posterior identificação do titular quando associados a outros dados.

Para fins ilustrativos, o Departamento Nacional de Trânsito ("Denatran") possui bases de dados com informações como fotografia de cidadãos, quantidade e tipos de infrações por eles cometidas, número do Cadastro de Pessoas Físicas ("CPF") dessas pessoas e veículos utilizados. O Instituto Nacional do Seguro Social ("INSS"), por sua vez, reúne dados como atividades profissionais desempenhadas pelos cidadãos, histórico de remuneração por eles auferida e condição de saúde atual e pretérita. Já a base de dados do Tribunal Superior Eleitoral ("TSE") possui dados pessoais como a residência, a biometria e a filiação partidária dos cidadãos. Isso sem falar de dados coletados pelo poder público quando da conexão em rede de *wi-fi* pública,[52] pelo uso de aplicativos de serviços públicos (por exemplo, CNH Digital, Caixa e FGTS),[53] ou por dispositivos espalhados pela malha urbana para finalidades diversas. Por exemplo, é cada vez mais comum o uso de sensores e de dispositivos de reconhecimento facial por órgãos públicos em todo o país, em setores como educação, transporte, controle de fronteiras e segurança pública.[54]

Além disso, a medição de fatores diversos, e muitas vezes não diretamente relacionados ao comportamento de uma pessoa específica, podem resultar no tratamento de dados pessoais. Por exemplo, a coleta de dados sobre a circulação de pessoas na malha urbana ou a avaliação sobre o consumo de energia elétrica são capazes de revelar dados pessoais (como dados de mobilidade, que podem identificar a rota utilizada por determinados

---

[51] Como será apresentado mais adiante, a legislação brasileira qualifica o dado pessoal como aquele que identifica ou permite a identificação de uma pessoa natural.

[52] Por exemplo, o prefeito do Município de São Paulo buscou estabelecer parcerias nas quais dados pessoais de cidadãos seriam oferecidos a parceiros comerciais (como os dados do bilhete único e dados do uso de *wifi* público). Vide: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/expansao-do-wi-fi-publico-as-custas-de-dados-pessoais-17072017. Acesso em 15.07.2018.

[53] Sobre o tema, vide: http://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-apps-do-governo/ Acesso em 29.06.2019.

[54] Vide estudo desenvolvido pelo Instituto Igarapé disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em 29.06.2019.

indivíduos para seu trabalho, ou dados de consultor de energia elétrica, os quais permitem identificar a quantidade de eletrodomésticos que uma pessoa usa).

Fato é que governos passaram a possuir quantidades massivas e sem precedentes de dados pessoais sobre comportamento, características, pertences e crenças de seus cidadãos (CATE, 2008). Mais que isso, referidos dados pessoais são, por diversas vezes, utilizados por órgãos públicos para finalidades que extrapolam a motivação de sua coleta (por exemplo, dados sobre encarceramento serem utilizados para a seleção de famílias beneficiárias de programas sociais), além de serem cada vez mais compartilhados com terceiros para finalidades diversas (por exemplo, dados biométricos coletados pelo TSE são compartilhados com a Polícia Federal com o intuito de promover eficiência à gestão pública).[55] Conforme será detalhado abaixo, essas e outras atividades podem implicar em danos consideráveis aos indivíduos aos quais se referem, especialmente pelo potencial desvio de finalidade no tratamento dos dados.

Assim, a despeito dos benefícios do tratamento de dados mantidos por órgãos públicos, há também **riscos associados aos direitos fundamentais de privacidade e de proteção de dados pessoais**, seja pelas atuais ou pelas futuras tecnologias (DONEDA, 2020).

A seguir serão apresentados alguns dos possíveis riscos relacionados à circulação de dados pessoais, especialmente de dados que são coletados pelo poder público em função de suas atribuições legais e/ou como condição ao exercício de direitos por cidadãos. Além disso, será apresentado como a evolução da tecnologia exigiu uma releitura do direito à privacidade, anteriormente compreendido em uma perspectiva essencialmente negativa de evitar a intervenção do Estado à individualidade dos cidadãos, para uma perspectiva positiva em que se reconhece autonomia dos indivíduos, entendidos enquanto coletividade, sobre como seus dados pessoais serão utilizados. Nesse momento, se verá a centralidade da preocupação com o uso de dados pelo Estado nessa evolução teórica e legislativa.

[55] Em 2017, o TSE e a Polícia Federal assinaram um Acordo Técnico para compartilhamento de dados biométricos entre as duas entidades públicas. Vide: https://www.tse.jus.br/imprensa/noticias-tse/2017/Novembro/tse-e-policia-federal-vao-compartilhar-banco-de-dados-biometricos. Acesso em 19.12. 2020.

3.1 A publicação e o compartilhamento de dados e os riscos à privacidade

De fato, o avanço das tecnologias resulta no constante aumento da capacidade de transformar fatos e coisas em dados - que, por sua vez, são compreendidos como o produto da abstração do mundo em categorias, medidas e outras formas de representação (KITCHIN, 2014). Esse processo, que tem sido denominado de datificação (MAYER-SCHONBERGER; CUKIER, 2013), aplica-se a qualquer fenômeno, mas tem sido também muito frequente na avaliação ou medição, direta ou indireta, de aspectos diversos da vida humana (MEJIAS, 2019).

Esses dados podem ser tanto dados propriamente ditos quanto metadados (ou seja, informações sobre outros dados, como a data de envio de determinada mensagem) e são utilizados por empresas e entidades governamentais de forma cada vez mais abrangente. Com o advento da internet e a proliferação de serviços digitais, como *internet banking*, redes sociais e aplicativos de locomoção, muitos aspectos da vida social que nunca haviam sido quantificados (por exemplo, amizades, interesses, conversas casuais, buscas de informações, expressões de gostos e respostas emocionais) passaram a ser codificados. Assim, a datificação pode ser uma forma de acessar e monitorar o comportamento de pessoas (VAN DIJCK, 2014), mas também permite influenciar e prever ações de indivíduos ou grupos.

O aumento da quantidade de dados produzidos e o aprimoramento de tecnologias capazes de segmentar e cruzar informações aprofunda, portanto, as chances de restringir direitos dos titulares desses dados. Por exemplo, podem ocorrer novas formas de vigilância pública e privada sobre indivíduos, a facilitação de práticas de discriminação em diversos serviços, a superexposição de indivíduos na internet, e a negativa de acesso a direitos desses indivíduos.

O problema assume contornos próprios quando envolve dados pessoais coletados e armazenados em bases de dados públicas. Como demonstrado, governos possuem enorme quantidade de dados, coletados para a execução de suas competências legais e para a prestação de políticas públicas, entre os quais há também dados pessoais. Embora esses dados possam ser utilizados para viabilizar e aprimorar a prestação da atividade pública, eles poderão também ser utilizados para finalidades não desejadas pelos cidadãos.

Primeiro, e na origem dos debates sobre proteção de dados pessoais, está a possibilidade de governos exercerem fiscalização dos cidadãos (ou **vigilância**), podendo lhes extrair direitos entre os mais caros à democracia, como as liberdades de expressão,

manifestação e de circulação (IGO, 2018). Embora com nuances diferentes, é possível que práticas de vigilância e manipulação possam ser exercidas também por particulares (ZUBOFF, 2019).

Em particular, a organização de *data lakes*, cadastros unificados com informações diversas de cidadãos ou interoperabilidade de sistemas, pode acentuar a capacidade de vigilância estatal, se não for devidamente regulamentada. Por exemplo, o Ministério da Justiça e Segurança Pública vem trabalhando com uma ferramenta da empresa Cortex, que, com o apoio de inteligência artificial, realiza a leitura de placas de veículos e cruza esses dados com informações de outras bases de dados públicas para a prevenção e combate ao crime, como a Relação Anual de Informações Sociais (Rais), o Sistema Nacional de Informações de Segurança Pública, o Cadastro Nacional de Foragidos, além de dados do Denatran e o Sistema Integrado Nacional de Identificação de Veículos em Movimento.[56]

Outro exemplo consiste na publicação, em março de 2020, do Termo de Autorização nº 7/2020-A, firmado entre o Denatran e a Agência Brasileira de Inteligência (Abin), que permitia o acesso e disponibilização eletrônica de dados do Denatran, inclusive dos dados pessoais e fotos contidos na Carteira Nacional de Habilitação (CNH). Contra essa medida, foi proposta perante o STF a Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 695. Às vésperas do dia em que estava previsto o julgamento do pedido liminar, o Ministério da Infraestrutura revogou o termo e o Advogado-Geral da União pediu que a ação fosse extinta por perda de objeto. No entanto, o Ministro Relator, Gilmar Mendes, apreciou o objeto da ação, tendo julgado como inconstitucional referido compartilhamento de dados entre Abin e Denatran. Esse entendimento foi posteriormente confirmado pelo pleno do STF.

Segundo, outra preocupação no tratamento de dados pelo poder público atrelada à privacidade consiste na remoção da capacidade de cidadãos controlarem os possíveis usos de seus dados pessoais. Diversas das teorias e leis relacionadas à proteção de dados pessoais se fundamentam nessa possibilidade de o indivíduo exercer alguma forma de controle sobre seus dados (BORGESIUS; GRAY; VAN EECHOUD, 2015). No entanto, especialmente em cenário de interoperabilidade de bases de dados públicas, é cada vez mais comum verificar o estímulo ao fluxo de dados sob o argumento de interesse público, mas sem qualquer ingerência dos indivíduos sobre a proteção de dados pessoais.

[56] O sistema de inteligência do Ministério da Justiça correlaciona dados de veículo com CPF e endereço de residência do proprietário, além de outras informações pessoais. Vide: https://nic.br/noticia/na-midia/sistema-de-inteligencia-do-ministerio-da-justica-correlaciona-dados-de-veiculo-com-cpf-e-endereco-de-residencia-do-dono/. Acesso em 10.11.2022.

Por exemplo, o já mencionado serviço DataValid oferecido pelo Serpro fornece serviço de validação de documentos com base em dados e documentos do Denatran ou da Receita Federal, que foram coletados de cidadãos quando do exercício de seus direitos ou em função de obrigação legal. Atualmente, o cidadão não possui ciência ou opção em relação a essa forma de monetização de seus dados pessoais por entidade pública, em clara mudança de finalidade de tratamento de dados em relação àquela que justificou sua coleta.

Outros exemplos consistem em medidas da iniciativa Cidade Digital do município de São Paulo. Uma primeira proposta era ofertar a base de dados do Bilhete Único[57] - que possui dados como CPF, RG, filiação, foto do rosto, endereço e trajetos de aproximadamente 5,6 milhões de usuários, avaliada em R$ 40 milhões - em um pacote de bens do município a serem privatizados.[58] O mesmo município buscou emplacar o projeto "Wi-Fi Livre Sampa", que, em sua primeira versão, envolvia a contratação não onerosa de empresas que ofertaram a infraestrutura de conectividade à internet em troca dos dados de navegação dos usuários, como registro dos sites acessados.[59] Nas duas propostas, os usuários das políticas públicas não teriam escolha ou informações claras sobre a disponibilização de seus dados para entidades particulares para fins econômicos. As críticas recebidas levaram o município a modificar elementos centrais à execução do programa em parceria com a iniciativa privada.[60]

Nesse tema, há especial preocupação com dados de pessoas beneficiárias de programas sociais. A vulnerabilidade daqueles que dependem desses programas é acentuada em vista da necessidade que eles têm em informar seus dados para agentes públicos a fim de acessarem os benefícios, além da falta de condição para questionar a forma de tratamento de dados na garantia de seus direitos. Com isso, governos por vezes acabam por coletar maior quantidade de dados de pessoas que dependem de serviços públicos e políticas públicas, que acabam por ter sua privacidade mais exposta do que de pessoas que não se utilizam na mesma medida das atividades oferecidas pelo poder público (PRIVACY INTERNACIONAL, 2019).

---

[57] O programa de governo de João Doria durante as eleições para prefeitura de São Paulo previa aprimoramento do Bilhete único por meio de soluções de interoperabilidade. Vide: http://estaticog1.globo.com/2016/10/26/proposta_governo1471620086520.pdf. Acesso em 10.04.2021.

[58] Em 2017, foi publicada notícia que Doria havia planos para privatizar a gestão do Bilhete único. Vide https://www1.folha.uol.com.br/cotidiano/2017/02/1856747-doria-vai-privatizar-o-bilhete-unico-e-espera-economizar-r-456-mi-por-ano.shtml. Acesso em 10.04,2021.

[59] O tema foi objeto do Projeto de Lei 228/2015 apresentado na Câmara Municipal de São Paulo. Vide http://documentacao.camara.sp.gov.br/iah/fulltext/projeto/PL0228-2015.pdf. Acesso em 10.04.2021.

[60] De forma exemplificativa, pode-se citar textos de opinião de Bruno Bioni e Ronaldo Lemos, disponíveis em: https://genjuridico.jusbrasil.com.br/artigos/544067877/expansao-do-wi-fi-publico-as-custas-de-dados-pessoais e https://www1.folha.uol.com.br/colunas/ronaldolemos/2017/02/1860214-proposta-de-doria-de-vender-os-dados-do-bilhete-unico-e-ilegal.shtml Acesso em 10.04.2021.

Em terceiro lugar, dados coletados na utilização de serviços públicos ou do espaço público poderão ser utilizados, sem a autorização ou ciência do cidadão, para finalidades discriminatórias e/ou que resultem em afronta a direitos. Por exemplo, dados compartilhados pelo governo podem ser utilizados para a valoração de serviços (como aumento no valor do plano de saúde para mulheres vítimas de violência doméstica)[61] ou para verificar antecedentes criminais (por vezes de forma ilegal e discriminatória) de candidatos para trabalhar em determinada empresa (BORGESIUS; GRAY; VAN EECHOUD, 2015).

Caso conhecido é o emprego de algoritmos de análise de risco em processos criminais, avaliando a chance de reincidência de um réu, servindo de base para juízes concederem ou não a liberdade condicional, tal como o COMPAS - em inglês, *Correctional Offender Management Profiling for Alternative Sanctions* (ZHANG; ROBERTS; FARABEE, 2014). A partir de uma série de perguntas aos indivíduos condenados criminalmente, o sistema promete avaliar o risco de o cidadão voltar a cometer um crime no futuro. Esta avaliação resulta em um sistema de pontos que apoia a determinação da sentença judicial. Apesar da pretensão de tornar as condenações mais objetivas e matemáticas, investigações encontraram evidências de que réus negros eram sistematicamente discriminados, recebendo avaliações que indicavam um risco maior de reincidência, o que indica um indesejado viés no mecanismo[62].

Ainda que essa modalidade de análise de risco não necessariamente corresponda ao resultado da decisão tomada (ou seja, apenas constitui um dos elementos que serão avaliados pelo juiz quando estiver proferindo sua decisão), há grandes chances de impactar consideravelmente a decisão tomada pelo magistrado. Esse e outros impactos da virada computacional sobre a atividade governamental estão longe de ser triviais. A constante adaptação de decisões aos perfis individuais e coletivos produzidos por tecnologias como a inteligência artificial resulta em um modo de governo sem precedentes, que pode reforçar ainda mais as desigualdades (sociais, de gênero, étnicas etc.) já existentes.

Assim, além dos danos individuais advindos de processos discriminatórios, há preocupação também sobre como o uso de soluções guiadas pelo tratamento de dados, quando não abertas ao escrutínio público, podem intensificar a exclusão de grupos vulneráveis. Um caso exemplar é o aplicativo Boston's Street Gaps lançado em 2012 pela cidade de Boston,

---

[61] Sobre esse respeito, foram identificados casos em que vítimas de violência doméstica, em vista dessa condição, não conseguiam contratar seguro de vida e saúde nos Estados Unidos..Vide: https://itsrio.org/wp-content/uploads/2017/05/algorithm-transparency-and-governance-pt-br.pdf . Acesso em 06.072019.

[62] Vide relatório "Machine Bias" publicado pela ProPublica. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em 22.04.. 2021.

cujo objetivo era detectar problemas relacionados ao asfaltamento das ruas. Os dados produzidos por este aplicativo determinariam o recapeamento realizado pelo poder público municipal.[63] No entanto, conforme relata Bioni, o resultado foi que buracos e falhas nas ruas de áreas mais pobres da cidade não eram relatados, pois os cidadãos que ali circulavam não possuíam *smartphones* (RAUB, 2018). Logo, no caso analisado, a política pública se mostrou enviesada, reforçando desigualdades sociais e espaciais.

Verifica-se que o uso de soluções guiadas pelo tratamento de dados não necessariamente coloca em risco apenas a capacidade de cada indivíduo de controlar o uso de seus dados, mas também sua liberdade política, capacidade decisória e até mesmo sua inserção no contexto social como um todo (COHEN, 2013). Particularmente em relação à automatização plena de processos decisórios, como através da implementação de políticas públicas para estímulo à inovação, há o risco de se resultar na exclusão de grupos e até mesmo reforçar desigualdades através dos vieses reforçados pelos próprios algoritmos (SIMÃO; FRAGOSO; ROBERTO, 2020).[64]

Uma quarta preocupação está relacionada a aspectos técnicos da modernização do aparato estatal. Por exemplo, um dos desafios está relacionado à forma como são desenhadas as bases de dados, indexados os dados e programados os mecanismos que intermedeiam a relação com os consumidores de dados, produzindo efeitos na forma de exposição de indivíduos.

Enquanto a indexação consiste na forma de ordenar a informação e de descrever um documento ou base de dados de acordo com seu conteúdo, mecanismos de busca dizem respeito ao instrumento por meio do qual o usuário efetua a pesquisa de conteúdos em determinado *website*. Esse instrumento, por sua vez, é intermediado por um algoritmo, consistente em regras técnicas para atribuir respostas padronizadas a perguntas formuladas, e que promove escolhas sobre quais informações serão disponibilizadas e em qual ordem (GRANKA, 2010). O algoritmo de mecanismos de busca procura identificar as páginas, documentos ou bases de dados que melhor se relacionam ao aparente objetivo do usuário

---

[63] Sobre este respeito, vide artigo "Street Bump: Crowdsourcing Better Streets, but Many Roadblocks Remain". Disponível em: https://digital.hbs.edu/platform-digit/submission/street-bump-crowdsourcing-better-streets-but-many-roadblocks-remain/. Acesso em 23.03.2021

[64] Nesse sentido, Dados do PNAD de 2014 mostram que somente 38,5% das pessoas brancas não usam a internet no Brasil, contra 60,5% da população negra, o que, a depender de quais sejam as fontes informacionais dos algoritmos utilizados, pode, por exemplo, excluir parte da população negra de determinada decisão tomada pelo Poder Público, ou apontar para resultados inadequados que poderão ser utilizados nos processos decisórios estatais. Vide: https://www.nexojornal.com.br/grafico/2016/05/30/Quem-%C3%A9-a-popula%C3%A7%C3%A3o-sem-acesso-%- C3%A0-internet-no-pa%C3%ADs. Acesso em 23.03.2021.

quando lhe apresenta determinadas palavras-chave. Dessa forma, acaba-se por determinar o que deverá ser conhecido e como identificar suas partes mais relevantes (GILLESPIE, 2014).

A questão que deve ser observada é como essas decisões são tomadas, de modo a evitar que a informação seja moldada apenas pelo seu detentor, seja ele o governo ou um ator de mercado (INTRONA; NISSENBAUM, 2000). É necessário saber as escolhas por trás da decisão sobre o que será indexado e quais critérios são utilizados para determinar o que é relevante, visto que elas acabam direcionando o conteúdo que será acessado, a forma como o usuário se porta diante de algoritmos e a sua percepção sobre a realidade em razão da informação que lhe é efetivamente disponibilizada (GILLESPIE, 2014).

Esses e outros possíveis riscos são potencializados quando se trata do compartilhamento ou da publicação de dados pelo poder público, na medida em que mais sujeitos terão acesso aos dados e poderão utilizá-los, de formas nem sempre esperadas ou desejadas pelas pessoas sobre quem os dados se referem. Nesse sentido se posicionou Laura Schertel Mendes (2022):

> Sabe-se que o compartilhamento envolve um risco mais elevado para o direito fundamental à proteção de dados, por diversos motivos. Primeiramente, além de aumentar o número de órgãos ou entes públicos que têm acesso, o compartilhamento de dados em geral está associado a uma mudança de finalidade em relação àquela para a qual os dados foram inicialmente coletados. Essa mudança de finalidade, também identificada muitas vezes com uma mudança de contexto de utilização dos dados, está associada à percepção de danos ao titular, visto que este não tinha expectativa de ter seus dados tratados em contextos diferentes, podendo sofrer consequências negativas a partir de tal mudança. Ademais, o compartilhamento também pode expor os dados pessoais a riscos de segurança da informação, como vazamentos e acesso não autorizado. Essas características aumentam o risco de uso inadequado e ilegítimo dos dados pessoais e exige maior atenção ao regime jurídico de proteção de dados.

Diante do exposto, fica claro que a ideia de risco à privacidade ainda é muito incipiente porque os danos são comumente tratados a partir da perspectiva individual e tangível, embora possuam também consequências intangíveis ou coletivas (SOLOVE, 2021). O risco com relação à privacidade, ainda que possa parecer menor quando visto isoladamente - com pequenos incômodos, como *e-mails* ou ligações indesejadas - aumenta consideravelmente quando realizado por diversas empresas em relação à sua coletividade de consumidores (SOLOVE, 2021). Quando se trata do poder público, esses riscos assumem uma perspectiva diferente, em vista da quantidade e sensibilidade dos dados que possui, bem como considerando o contexto que justifica a coleta e o processamento de dados de cidadãos.

Assim, por custodiar quantidades massivas de dados pessoais que são obtidos, analisados e mantidos independentemente da vontade de seu titular, é crucial que o poder

público observe normas específicas destinadas a proteger a privacidade dos cidadãos e a garantir a segurança da informação coletada, seja nos casos em que esse tratamento seja feito unicamente pelo poder público ou em parceria com agentes privados. Por isso, a reflexão sobre uso de dados mantidos pelo poder público deve perpassar sobre a forma de construção da base de dados, a indexação de conteúdo e o desenvolvimento dos algoritmos dos mecanismos de pesquisa e a acessibilidade do conteúdo disponibilizado.

3.2 Origem conceitual da proteção à privacidade e dados pessoais

A literatura nacional sobre privacidade e proteção de dados pessoais geralmente inicia sua análise apresentando a evolução do tema no contexto do direito à privacidade (CUEVA, 2017; ZANATTA, 2017; WIMMER, 2020, por exemplo). Nela, a privacidade era primeiro entendida como o direito de não ser perturbado em sua intimidade (BRANDEIS; WARREN, 1890), passando pela compreensão de controle e da possibilidade de indivíduos exercerem com liberdade escolhas sobre quais circunstâncias e de que maneira se expor (WESTIN, 1967), até chegar ao direito de autodeterminação informacional, conforme estabelecido pela Corte Constitucional Alemã em 1983 e amplamente aceito nos julgamentos recentes pelo STF.

Como apontam esses autores, na época em que Brandeis e Warren escreveram, o mundo vivia a primeira expansão na massificação da mídia, que resultou no diagnóstico sobre a necessidade de proteger a imagem, a honra e a intimidade de indivíduos. Foi diante dessas preocupações que se desenvolveu o conceito de privacidade, consistente no reconhecimento de uma liberdade negativa para cidadãos, e que foi amplamente aceito e adotado pela Declaração Universal dos Direitos do Homem (art. 12) e pela legislação de diversos países (CUEVA, 2017), a exemplo do Brasil, que estabeleceu como direito fundamental a inviolabilidade da vida privada, honra e imagem das pessoas (art. 5º, X).

Em seguida, a tendência de governos criarem registros unificados de dados sobre cidadãos iniciou nova fase no debate a respeito da proteção de dados pessoais a nível global.[65] Por exemplo, em 1965, pelo governo dos Estados Unidos, que propôs o *National Data Bank*, consistente no resultado da consolidação de bases de dados detidas pelo governo federal. A

[65] Conforme exposto na manifestação de *amicus curiae* da Associação Data Privacy Brasil de Pesquisa ("Data Privacy Brasil") sobre a Ação Direta de Inconstitucionalidade nº 6.649, que analisa a constitucionalidade da instituição do Cadastro Base do Cidadão. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755538665&prcID=6079238#. Acesso em 26.11.2022.

base contaria com informações pessoais referentes aos cidadãos, presentes no censo e em registros feitos por órgãos atuando na esfera da regulação trabalhista, fiscal e previdenciária.[66]

À época, houve o receio de que a concentração de dados nas mãos da administração pública implicasse um aumento relevante do poder do governo (DONEDA; ZANATTA, 2022), motivo pelo qual a proposta não foi implementada.[67] Entre as objeções suscitadas à época, destaca-se a redução de incentivo à minimização da coleta de dados, o descontrole sobre as finalidades para o tratamento dos dados, o aumento nas chances de perfilamento dos cidadãos que poderia resultar em iniquidade na prestação de serviços públicos a partir do perfil de cidadão, e riscos de segurança da base, na medida em que dificultaria a proteção contra acesso não autorizado e outros incidentes acidentais ou ilícitos.

Foi neste contexto que Alan Westin (1967) desenvolveu sua tese em meio à expansão do uso de computadores como instrumentos de guerra e à composição de bases de dados sobre cidadãos por governos, muitas para o monitoramento e a contenção de grupos opositores ao regime estabelecido. Com vistas a combater a utilização dessas tecnologias e dados para fins opacos e abusivos, o autor argumentou a necessidade de expansão do conceito de privacidade para compreender também a possibilidade de indivíduos exercerem controle sobre a coleta de suas informações. No mesmo sentido, Arthur Miller (1969) apontou para a perda de controle dos indivíduos sobre suas informações pessoais, relacionando as restrições de controle de acesso e revisão dos dados por parte dos indivíduos e o uso da cibernética como forma de vigilância pelo governo. Para esses autores, a privacidade estaria associada a uma pretensão pelo indivíduo de exercer algum grau de controle sobre quais informações coletadas ou oferecidas a terceiros seriam circuladas e em quais condições.

---

[66] Entre as vantagens citadas para a constituição do *National Data Bank*, estariam (i) a economia às entidades governamentais quanto à gestão dos bancos de dados independentes, que não mais seria necessária; (ii) a união inédita de informações diversas, que permitiria análises científicas e estudos baseados em amostragem mais ampla e rica do que anteriormente; (iii) a redução dos processos independentes de coleta de dados pessoais pelas entidades governamentais, que poderiam ser unificados em apenas um; (iv) devido à economia relacionada aos procedimentos para composição e gestão do banco, maior aproveitamento dos recursos públicos para análise dos dados; (v) maior reprodutibilidade dos estudos feitos com base em bancos de dados públicos, devido à unificação e validação das informações por diversas instituições.

[67] Interessante notar que, já à época, cientistas sociais - interessados no valor do banco de dados como base para estudos sociais de maior amplitude e acurácia - relatavam que a anonimização dos dados (ou mesmo a consideração exclusiva dos dados agregados) reduziria em muito a sua utilidade. Na verdade, ainda que fossem omitidos dados mais diretamente relacionados à identificação dos indivíduos (tais como nome ou número de documento de identificação), a riqueza informacional do banco dependeria ainda, em grande medida, da capacidade de associação dos dados com determinados perfis de titular, o que inevitavelmente levaria a algum grau de identificação dos indivíduos - e este cenário certamente teria maior impacto sobre a privacidade dos titulares envolvidos.

Em função dessas preocupações, no início da década de 1970 foram instituídos dois comitês, um na Inglaterra (*Younger Committee*)[68] e outro nos Estados Unidos (*Health, Education and Welfare Committee*),[69] destinados a construir propostas para compatibilizar a privacidade e tratamento de informações pessoais (GELLMAN, 2017). Embora independentes entre si, os dois comitês apresentaram princípios que são até hoje basilares no debate sobre privacidade e proteção de dados pessoais, consistentes nas *Fair Information Principles* ("FIPPs"),[70] que possuem em sua centralidade os conceitos de transparência, consentimento e acesso a dados. Com isso, e de forma alinhada à teoria construída nessa mesma época, para as FIPPS, a privacidade estaria fundamentada na ideia de fornecimento de informações para que os indivíduos exerçam controle sobre como seus dados são utilizados por terceiros.

Na mesma época, foram publicadas as primeiras leis destinadas a assegurar proteção a dados pessoais de cidadãos, como nos estados alemães de Hessen (1970) e Rheinland-Pfalz (1974), bem como na Suécia e na Áustria (KORFF; GEORGES, 2019).[71] Nesse momento, constituiu-se o que se chama de a primeira geração de leis destinadas a regular o tratamento de dados pessoais, que estavam preocupadas em conter a criação por governos de bases de dados centralizadas, com quantidade massiva de dados sobre cidadãos. Essa geração de leis foi, por isso, marcada por esforços em regular o desenvolvimento de novas tecnologias, na tentativa de evitar um processo de vigilantismo (MILLER, 1971), além de voltar-se especialmente para o setor público, que seria o principal agente capaz de assumir o papel de agente de vigilância. Ao cidadão eram assegurados determinados direitos, como o acesso ou correção aos seus dados mantidos por governos, mas sem possuir qualquer controle sobre como eles seriam efetivamente tratados.

Esse debate teve reflexos no cenário brasileiro da época.[72] Em função da tentativa pelo governo militar de criar bases de dados com informações detalhadas sobre indivíduos, o

---

[68] O comitê editou, como resultado de seus trabalhos, os seguintes relatórios:https://api.parliament.uk/historic-hansard/lords/1973/jun/06/privacy-younger-committees-report e https://api.parliament.uk/historic-hansard/commons/1973/jul/13/privacy-younger-report. Acesso em 07.06.2022.

[69] O comitê editou, como resultado de seus trabalhos, o seguinte relatório: https://www.justice.gov/opcl/docs/rec-com-rights.pdf. Acesso em 07.06.2020.

[70] As *Fair Information Principles* serão mais detidamente abordadas adiante nesta tese.

[71] Essas leis são qualificadas pela literatura como as normas de proteção de dados pessoais de primeira geração (Mayer-Schneberger, 1997), na medida em possuíam um mesmo racional por serem produzidas como reação a essa mencionada tendência de criação de grandes bases de dados nacionais e corporativas com informações diversas de cidadãos.

[72] Embora o debate brasileiro estivesse em grande medida relacionado ao debate ocorrido sobre o tema na França. Segundo Mayer-Schonberger (1997), a lei francesa de proteção de dados pessoais corresponde à segunda geração das leis sobre o tema. Diferentemente das normas de primeira geração, que se opunham à criação de bases de dados centralizadas e possuíam como foco a regulação da tecnologia, as leis de segunda

chamado Registro Nacional de Pessoas Naturais - Renape (1975), foram debatidas no Congresso Nacional propostas normativas para regular o uso de dados pessoais. Referido repositório seria destinado a unificar vários registros - Registro Geral, Cadastro de Pessoa Física e inscrição no Instituto Nacional de Seguridade Social - em um banco de dados unificado com informações biométricas sobre todos os cidadãos (DONEDA; ZANATTA, 2020). No entanto, houve grande mobilização contra a composição do registro, que contou com iniciativas como a tentativa de criar uma Lei Geral de Proteção de Dados em 1977.[73] Embora essas propostas legislativas não tenham avançado, as iniciativas do governo de criar o Renape foram contidas com sucesso à época.[74]

No entanto, com o passar do tempo e o desenvolvimento de novas tecnologias, ficou evidente a necessidade de dar um passo à frente no cenário regulatório internacional. Com a ampliação do acesso a computadores e outras tecnologias emergentes, ampliou-se a quantidade de sujeitos capazes de coletar e manter bases de dados sobre indivíduos. Dessa forma, iniciou-se a segunda geração de leis de proteção de dados pessoais. Sua principal diferença em relação à geração anterior foi a compreensão de que seria necessário não somente focar na regulação do setor público (MAYER-SCHONBERGER, 1997), visto que atividades realizadas por particulares também poderiam oferecer riscos aos direitos dos cidadãos.

Como consequência dessa mudança de paradigma regulatório, o controle sobre o fluxo de dados pessoais saiu das mãos do Estado e passou a ser exercido pelo próprio cidadão, ao qual passou a ser assegurado o direito à privacidade e a possibilidade de ter ingerência sobre os processos aos quais suas informações seriam submetidas (MAYER-SCHONBERGER, 1997). Nesse momento, o consentimento se consolidou como mecanismo protagonista na garantia ao devido tratamento de dados pessoais (BIONI, 2021).

Posteriormente, no ano de 1983, a Corte Constitucional Alemã (*Bundesverfassungsgericht*) proferiu decisão a respeito de lei sobre recenseamento

---

geração (datadas de meados-final da década de 1970) buscavam proteger o cidadão contra a criação de múltiplas bases com seus dados pessoais e lhes asseguravam mais voz em relação ao uso de seus dados.

[73] O Projeto de Lei exigia que o tratamento de dados deveria ser precedido do consentimento necessário dos cidadãos. O Projeto de Lei também adotou um conjunto de princípios para o processamento de dados pessoais tanto do setor privado quanto do público. Também propôs a criação de uma Autoridade de Proteção de Dados.

[74] O mesmo ocorreu nos Estados Unidos, em 1965, quando o Escritório do Orçamento norte-americano (https://www.cbo.gov) idealizou a criação do *National Data Center*, consistente em uma central única de armazenamento de informações pessoais, especialmente voltada para as informações coletadas pelo censo. À época, houve o receio de que a concentração de dados nas mãos da administração pública implicasse em um aumento relevante do poder do governo (DONEDA, 2021), motivo pelo qual a proposta não foi implementada.

populacional,[75] que passou a ser considerado um marco nos debates sobre proteção de dados pessoais, na medida em que reconheceu a existência de um direito fundamental à autodeterminação informativa. Em síntese, o parlamento alemão aprovou por unanimidade lei que exigia dos cidadãos responderem a centenas de perguntas, cujas respostas seriam utilizadas para fins estatísticos e para a comparação e o aprimoramento dos cadastros de residentes. O parlamento sofreu grande pressão para não aprovar a referida norma, sob o risco de facilitar a ocorrência de práticas de vigilância por parte do aparato estatal. No entanto, a lei foi aprovada e, como consequência, foram propostas ações judiciais que resultaram na declaração de inconstitucionalidade da lei e no reconhecimento do direito de autodeterminação informativa.

Segundo argumentou a Corte Constitucional Alemã no julgamento, a autodeterminação informativa consiste na garantia ao indivíduo de determinar as condições com base nas quais ocorrerá o uso de seus dados pessoais, determinando quando e sob quais limites informações sobre a sua vida privada podem ser utilizadas e comunicadas a outros. Ela seria baseada nos direitos da dignidade da pessoa humana e ao livre desenvolvimento da personalidade, mas também objetivava assegurar a igualdade entre indivíduos (MENDES, 2018).

Entre as inovações oferecidas pela decisão estão o reconhecimento da privacidade como um fenômeno destinado também à proteção do coletivo, contemplando tanto liberdades negativas ("*right to be left alone*") como liberdades positivas ("autodeterminação informativa"). Mais que isso, ela impactaria o bem comum, na medida em que seria condição elementar de uma sociedade democrática livre baseada na capacidade de seus cidadãos de agir e cooperar.

Segundo a Corte Constitucional Alemã, esse direito mereceria proteção particular, visto que dados pessoais podem ser rapidamente recuperados em bancos de dados e ser agrupados por sistemas integrados, reduzindo a capacidade de indivíduos realizarem controle sobre os processos feitos com seus dados. A impossibilidade de prever com certa precisão quais de suas informações são divulgadas e de estimar a quem elas são comunicadas, portanto, removeria dos indivíduos sua liberdade de planejar e decidir sobre o destino de suas informações pessoais.

[75] Essa decisão, que será mais detidamente abordada ao longo deste estudo, é considerada um símbolo da chamada terceira geração de normas de proteção de dados pessoais, na medida em que reconhece o direito de titulares de dados serem informados e se envolverem em todas as etapas do tratamento de dados pessoais (Mayer-Schonberger, 1997).

Com essa decisão, consolidou-se a chamada terceira geração de leis de proteção de dados pessoais, que influenciou a prática jurídica alemã e resultou na modificação de leis em países como Áustria, Noruega e Finlândia (KOSTA, 2013). Ela colocou o indivíduo no cerne da tomada de decisão sobre como serão manejados dados pessoais durante todo o processo de tratamento de dados (MAYER-SCHONBERGER, 1997). Com isso, o foco das normas passa a ser assegurar a participação e autodeterminação informativa aos indivíduos.

No entanto, a capacidade de indivíduos exercerem efetivamente o controle sobre o fluxo de seus dados pessoais se mostrou limitada. A ideia do consentimento como a expressão do direito à privacidade foi ofuscada pelas próprias relações sociais (BIONI, 2021), especialmente nas relações com o Estado, em que o cidadão não possui efetiva liberdade de escolha, na medida em que a coleta de dados pessoais é necessária para assegurar o exercício de direitos, prestar serviços públicos ou implementar políticas públicas.

É nesse contexto que surge a quarta geração de leis de proteção de dados, na tentativa de suprir a lacuna apresentada pela base legal do consentimento, bem como à tomada de decisão centrada quase exclusivamente no indivíduo (MAYER-SCHONBERGER, 1997). Também é nesse momento que são instituídas autoridades de proteção de dados pessoais, responsáveis pela criação de regras que levam em consideração os diferentes interesses envolvidos no processamento de dados pessoais, relativizando a centralidade do consentimento (BIONI, 2021). Importante notar que a autodeterminação informativa segue com a mesma relevância, havendo apenas uma evolução na forma como é assegurada. Entre as medidas legais que caracterizam essa geração de leis de proteção de dados pessoais estão o reconhecimento de outras bases legais (isto é, outras hipóteses legítimas de tratamento), em adição ao consentimento, como o cumprimento de obrigação legal e do legítimo interesse.

De todo modo, no cerne das modernas normas sobre proteção de dados pessoais estão os chamados FIPPs (SCHWARTZ, 1999a) que, como mencionado, são uma série de princípios norteadores das práticas de entidades que se utilizam de dados pessoais. Ainda que eles assumam particularidades a depender da versão adotada (e.g..: a OCDE, o FTC, a União Europeia e o Canadá adotam versões distintas desses princípios),[76] possuem um mesmo fio

[76] "Como a discussão anterior sugere, um problema inicial de basear um regime de proteção de dados no FIPPS é determinar qual conjunto de FIPPS deve ser aplicado. As Diretrizes da OCDE fornecem oito, a diretiva de proteção de dados da UE onze e os princípios da FTC apenas cinco (ou quatro). As diferenças são muitas vezes bastante substanciais. [...] O resultado final são diferenças significativas entre vários conjuntos de FIPPS, com a diretiva da UE em um extremo do espectro, fornecendo limites generalizados sobre o processamento de dados pessoais com poucos interesses compensatórios explicitamente reconhecidos; as Diretrizes da OCDE e a APEC Privacy Framework no meio, com reconhecimento explícito da necessidade de

condutor: partem do pressuposto de informação e controle ("*notice-choice*"), segundo o qual é necessário assegurar aos indivíduos maior informação e controle sobre o uso de seus dados.

Esses princípios têm sido utilizados no desenho das mais diversas normas locais, sendo apresentados em formatos de regras ou parâmetros interpretativos (BYGRAVE, 2014).[77] Por exemplo, na União Europeia, as FIPPS podem ser encontradas nos princípios e regras estabelecidos pela GDPR.[78] O mesmo ocorre no Brasil, sendo possível identificar com facilidade as FIPPs nas regras e princípios estabelecidos na LGPD e em outras normas aplicáveis, direta ou indiretamente, ao tratamento de dados pessoais.

Isso se dá, em grande medida, por conta da publicação pela OCDE de dois documentos: as *privacy guidelines* (1980) e o *transborder data flows* (1985), ambos voltados a estabelecer princípios diretivos para toda a comunidade internacional, a fim de criar um ambiente regulatório uniforme para a privacidade e garantir o fluxo de informações entre os países-membros (BIONI, 2019). Esses documentos (revisitados em 2013), referidos como *Fair Information Principles*, estimularam a edição de normas de proteção de dados pessoais em diversos países e asseguraram uma certa padronização do conteúdo das normas nacionais sobre o tema (BIONI, 2019).

Assim, leis de proteção de dados pessoais normalmente possuem uma estrutura similar, em grande medida espelhadas nas disponíveis versões das FIPPs. Isso significa que essas normas são geralmente estruturadas de maneira a estabelecer princípios que deverão ser observados no uso de dados, delimitar situações nas quais o tratamento de dados será considerado lícito, estabelecer direitos aos titulares de dados e instituir autoridade para normatizar, orientar, fiscalizar e sancionar atividades realizadas com base no tratamento de dados pessoais.

---

equilíbrio e proporcionalidade; e os princípios da FTC no outro extremo do espectro, com as menores restrições substantivas (embora talvez as mais rigorosamente aplicadas) sobre os processadores de dados. Os defensores da criação de regimes nacionais ou regionais de proteção de dados com base no FIPPS precisam ter cuidado para esclarecer qual FIPPS eles se referem." (tradução nossa) (CATE, 2006).

[77] Para se ter uma ideia, mais de cem das vigentes leis nacionais de proteção de dados pessoais estão baseadas nas orientações das *Fair Information Principles* (BORGESIUS GRAY; VAN EECHOUD, 2015).

[78] Segundo a GDPR, o tratamento de dados pessoais deverá ser: **(a)** lícito legal e transparente em relação ao titular de dados; **(b)** observar finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de forma incompatível com a finalidade original da coleta dos dados - salvo no caso de arquivos de interesse público ou para fins de investigação científica, histórica ou estatísticas; **(c)** adequado, pertinente e limitado ao que é necessário para o alcance de suas finalidades; **(d)** observar a exatidão e atualização dos dados; **(e)** conduzido de forma a assegurar que dados sejam conservados de forma a identificar os titulares de dados apenas quando necessário para as finalidades para as quais são tratados; e **(f)** realizado de forma a garantir a segurança dos dados, evitando seu tratamento não autorizado ou ilícito e contra sua perda, destruição ou danificação acidental.

De todo modo, destaca-se a existência de críticas à regulação da privacidade e proteção de dados pessoais com base nas FIPPs, na medida em que a prática tem demonstrado: **(a)** de um lado, elevados custos monetários e burocráticos para sua implementação; e **(b)** de outro lado, uma baixa efetividade das práticas de transparência e na garantia de controle ao indivíduo sobre o fluxo de seus dados pessoais (CATE, 2006).

De fato, a tentativa de garantir proteção de dados pessoais por meio da prestação de informações para que o titular de dados possa exercer escolhas livres e conscientes possui diversas limitações. Empresas e governos (embora a transparência sobre atividades de tratamento de dados pelo poder público ainda seja incipiente) têm divulgado extensas e complexas políticas de privacidade (que muitas vezes sequer são lidas) e que podem ser aceitas pelos usuários sem qualquer reflexão, para que utilizem um serviço prestado *online*. Sendo assim, o propósito informacional dos documentos exigidos pela legislação de proteção de dados, em boa parte das vezes, não é atingido - sendo que as formalidades impostas pela legislação se demonstram, muitas vezes, ineficientes em promover maior ingerência dos titulares sobre o uso de seus dados pessoais.

Diante dessas e outras críticas, leis de proteção de dados pessoais vêm sendo constantemente reavaliadas e aprimoradas. Por exemplo, há estudos sobre a inclusão de novos elementos de confiança no ciclo de vida dos dados e sobre a regulação de dados pessoais enquanto um interesse coletivo. Na primeira situação, há propostas de regulação de agentes de tratamento para que performem como fiduciários dos dados pessoais (*data trusts*) (RICHARDS; HARTOG, 2021) ou de inclusão de agentes intermediários na relação entre detentores e consumidores de bases de dados (como propõe o *Data Governance Act* da Europa).

De imediato, verifica-se que o debate sobre a compatibilização entre privacidade e o uso de dados pessoais não é novo, tendo sido objeto de amplo debate desde o final da década de 1960, momento no qual computadores passaram a ser mais amplamente utilizados por governos e entidades privadas para finalidades diversas. Além disso, vê-se que a preocupação com o uso de dados pessoais esteve intimamente relacionada ao recente histórico de uso de dados por governos para perseguir determinados grupos populacionais durante a época da segunda guerra mundial (KORFF; GEORGES, 2019). Assim, na origem dos debates e normas de proteção de dados pessoais esteve, em alguma medida, a preocupação com o uso indevido de dados pessoais de cidadãos por governos.

Portanto, na origem da regulação sobre proteção de dados pessoais está a imposição de limites às práticas de vigilância exercidas por governos sobre os cidadãos (WIMMER, 2019). No entanto, ainda que debates sobre a regulação de dados mantidos pelo poder público não sejam recentes, eles devem certamente ser retomados e revisitados por consequência da adoção de novas tecnologias por governos e por aqueles que acessam esses dados em função das políticas de transparência ou porque colaboram com o poder público.

4 CONCLUSÃO PARCIAL: NECESSIDADE DE MAIOR DIÁLOGO ENTRE TEORIAS

Como se verificou, governos historicamente coletam informações de cidadãos para fins inerentes ao desenvolvimento das suas funções, o que se intensificou com a ampliação do papel do Estado na promoção de direitos individuais, políticos e sociais. Além disso, governos recebem dados e informações, enviadas por entes públicos ou privados, para finalidades como o cumprimento de determinação legal, a prestação por particulares de serviços públicos, e para a cooperação entre órgãos públicos ou com particulares para o alcance do interesse público. Assim, a utilização de dados e informações é inerente ao desempenho de capacidades governamentais do Estado contemporâneo.

Essa tendência foi largamente potencializada com a adoção pelo poder público de TIC, conectividade, dispositivos e sensores de IoT, serviços de nuvem e inteligência artificial, que permitem a coleta, agregação e análise de grandes quantidades de dados e informações, de forma ajudar na compreensão de fenômenos e na tomada de decisões de agentes públicos ou privados. Mais que isso, a adoção de similares tecnologias pelos governos tem permitido o desenvolvimento de novas modalidades de prestação de serviços públicos, a exemplo do governo eletrônico, do governo digital, do governo aberto e das *smart cities.* Embora distintos, esses conceitos de governo são intimamente relacionados e pressupõem a circulação de dados e informações mantidas por entidades públicas com terceiros, públicos ou privados.

Com isso, governos acabam por organizar arquivos e bases de dados de particular riqueza, na medida em que reúnem grande contingente de dados e informações que contam com maior grau de confiabilidade por serem produzidos ou custodiados por órgãos públicos. Por essa razão, são cada vez mais comuns as práticas de compartilhamento e publicação de dados com interessados diversos, para finalidades distintas, como a promoção de transparência ou o fornecimento de subsídios para o desenvolvimento de novos ou existentes mercados.

Entre os benefícios da utilização de dados e informações mantidos pelo poder público estão: **(i)** o aprimoramento da prestação de serviços públicos e para o desenvolvimento de políticas públicas; **(ii)** promoção de transparência governamental, além de viabilizar *accountability* sobre as atividades de órgãos e entidades públicas e substrato para a participação de cidadãos no governo; e **(iii)** fornecimento de elementos que auxiliam com práticas de inovação, para o desenvolvimento de mercados existentes ou para a criação de

novos serviços. Esses benefícios, embora digam respeito ao tratamento de dados pelo poder público de uma forma geral, estão em grande medida atrelados à circulação de dados e informações mantidos por órgãos e entidades públicos para terceiros, especialmente por meio do compartilhamento e da publicação de dados e informações, a entes públicos ou privados.

A publicação de dados, para fins desta tese, é compreendida como a atividade realizada pelo poder público de viabilizar acesso e uso posterior pela sociedade a informações de interesse público para, entre outros, promover a consecução da transparência governamental. Ela estará comumente atrelada à garantia do direito à informação, dos princípios de publicidade e prestação de contas governamental, além de apoiar medidas destinadas a ampliar a confiança dos cidadãos no governo e de fomento ao desenvolvimento econômico e à inovação. A publicação poderá ocorrer de formas diversas, com destaque para a divulgação, ativa ou passiva, de informações produzidas ou mantidas pelo poder público por meio de políticas de transparência ou de dados abertos. Assim, práticas de transparência e dados abertos possuem o condão de reduzir a assimetria de informações entre indivíduos e governo, permitindo a colaboração cidadã na promoção de gestão pública mais eficiente, além de permitir a geração de valor para o setor privado.

Já o compartilhamento de dados será considerado por esta tese como a divulgação de dados pelo poder público com terceiros para finalidades específicas, que poderá ocorrer pela troca recíproca ou unilateral de dados entre organizações, pela autorização de acesso, integral ou parcial, a determinada base de dados por poucos interessados e pela reunião de dados fornecidos por diversos agentes para consumo desses mesmos atores ou por terceiros. Em relação às finalidades que justificam o compartilhamento de dados estão, ainda que não somente, assegurar ao indivíduo serviços mais céleres e personalizados: planejar, executar e monitorar a prestação de serviços públicos; criar, executar, monitorar e avaliar políticas públicas; fiscalização das atividades realizadas por entidades públicas e seus parceiros; e realização de pesquisas por órgãos públicos, pesquisadores independentes ou instituições privadas. Assim, o compartilhamento de dados é comumente associado ao cumprimento de atribuições legais ou de modernização do aparato estatal, que buscam atingir a eficiência, desburocratização, transparência e participação popular, além de fornecer substrato para o desenvolvimento de novos negócios e inovação no setor privado.

Diante disso, a publicação e o compartilhamento de dados são tratados nesta tese como passíveis de serem comparados e submetidos a soluções jurídicas semelhantes por consistir em atividades de tratamento que resultam na circulação de dados mantidos pelo poder público

e viabilizam o reuso desses dados por terceiros. Portanto, tanto o compartilhamento como a publicação de dados são formas pelas quais governos interagem com os seus distintos *stakeholders*, por meio de divulgação de dados a terceiros para o alcance de finalidades diversas. Por outro lado, entre as principais diferenças dessas atividades de tratamento estão: quem são os receptores dos dados, as finalidades de divulgação e os riscos oferecidos aos cidadãos. Por isso, essas atividades devem ser submetidas a procedimentos e parâmetros semelhantes que assegurem uma harmonia na sua prática, respeitadas suas particularidades.

Em seguida, é importante ressaltar que, entre os dados divulgados pelo poder público, há dados pessoais (e.g., foto, digital, endereço e número de CPF), que podem ser identificados ou permitir a identificação de um cidadão. Mais que isso, deve-se ter em mente que sua utilização de forma irregular oferece riscos a direitos fundamentais, como a perda de autonomia do cidadão sobre como suas informações são usadas por terceiros ou o reforço a práticas discriminatórias a indivíduos ou grupos sociais.

De fato, a disponibilização indiscriminada de dados permite que governos desenvolvam práticas de fiscalização de cidadãos e acabam por lhes extrair direitos entre os mais caros à democracia, como as liberdades de expressão, manifestação e de circulação. Ao lado desses direitos que se vêem fragilizados pelo uso indiscriminado de dados pelo poder público está a autonomia do cidadão em decidir como seus dados serão usados por terceiros, especialmente em práticas de interoperabilidade e abertura de dados. Esse é o exemplo do compartilhamento pelo governo brasileiro de dados atrelados à CNH de motoristas para outros órgãos e entidades públicas, como o TSE, a Receita Federal e a Abin, sem a ciência dos cidadãos.

Já a manipulação desses dados sem balizas legais e éticas claras pode permitir, de forma voluntária ou involuntária, reforços a vieses sociais discriminatórios, como o exemplo da utilização do sistema COMPAS pelo Poder Judiciário nos Estados Unidos que, em virtude das perguntas formuladas e dados utilizados, acaba por sugerir que indivíduos negros teriam maiores probabilidades de cometer crimes. Esse fenômeno pode ser reforçado também pela forma como sistemas governamentais são estruturados e as bases de dados são indexadas, de modo que a determinação de quem participa da sua construção deve ser socialmente avaliada.

Essa evolução da tecnologia e surgimento de novos riscos a direitos fundamentais resultou em uma releitura do direito à privacidade, anteriormente compreendido como o direito de não ser perturbado em sua intimidade, para uma perspectiva positiva que assegura

aos indivíduos certa autonomia de controle sobre definir em quais circunstâncias e condições seus dados e informações poderão ser utilizados. Essa preocupação esteve intimamente relacionada a uma tendência global, iniciada na época da segunda guerra mundial, de governos criarem registros unificados de dados sobre cidadãos e, em consequência, aumentarem sua capacidade de exercer controle e até mesmo praticar abusos contra indivíduos e sociedade.

Essas preocupações (bem apontadas por autores como WESTIN, 1967 e MILLER, 1969) deram origem às *Fair Information Principles* (princípios destinados a estabelecer diálogo entre privacidade e uso de informações pessoais) e às primeiras leis de proteção de dados na década de 1970. Essas leis voltaram-se especialmente para regular o uso de novas tecnologias pelo setor público e para assegurar aos cidadãos determinados direitos sobre o uso de seus dados, como os direitos de acesso ou correção aos seus dados mantidos por governos.

Com o desenvolvimento de novas tecnologias e da quantidade de sujeitos capazes de coletar e processar dados pessoais, as leis ampliaram seu escopo de atuação para regular entes privados e para assegurar aos indivíduos certo grau de escolha sobre os processos aos quais suas informações seriam submetidas, sendo o consentimento, transparência e direitos de titulares os principais instrumentos para tanto. Nesse momento, decisão proferida pela Corte Constitucional Alemã sobre Lei que regulava o recenseamento populacional, se reconhece a existência do direito fundamental à autodeterminação informativa, que permite aos indivíduos determinar as condições com base nas quais terceiros poderão usar seus dados pessoais. Com isso, a privacidade deixou de ser vista como uma liberdade exclusivamente negativa (de não sofrer interferências indesejadas do Estado em sua intimidade) para ser também uma liberdade positiva (de exercer controle sobre a circulação de suas informações).

No entanto, a limitação do consentimento para exercer o controle sobre toda a ampla gama de atividades de tratamento de dados pessoais, especialmente nas relações com o Estado (em que o tratamento de dados é necessário para a garantia de direitos e o exercício de suas atribuições legais), a regulação da proteção de dados pessoais passou a contar também com outras hipóteses autorizativas ao tratamento de dados pessoais, como o cumprimento de obrigação legal e legítimo interesse. Foi nesse momento também que foram instituídas as primeiras autoridades destinadas a regular e fiscalizar práticas de tratamento de dados pessoais.

Diante desse movimento regulatório global, em grande medida estimulado por organismos internacionais como a OCDE, a maioria das leis globais se fundamenta nos *Fair Information Principles* e possuem alguma medida de similaridade em suas disposições. Elas são geralmente pautadas por certos princípios fundantes, estabelecem situações em que será lícito tratar dados pessoais e asseguram direitos aos titulares de dados. Em seu recente desenho, as leis de proteção de dados pessoais sofrem críticas em relação aos elevados custos monetários e burocráticos de implementação, assim como pela limitada efetividade das medidas de transparência e na garantia de controle ao indivíduo sobre o fluxo de seus dados pessoais.

De todo modo, nesta Parte se verificou que esforços de compatibilização da privacidade com o uso de dados pessoais não são novidade e que os primeiros esforços de regulação do tratamento de dados pessoais buscavam limitar o uso inadequado de dados por governos. A despeito disso, a literatura recente sobre modernização e abertura governamental e a literatura dedicada à privacidade e proteção de dados pessoais ainda possuem diálogo escasso (tal como também diagnosticado por ALTMAN *et al.*, 2015). De um lado, a literatura sobre novos modelos de governo (e.g., governos eletrônicos e abertos) está dedicada à promoção de transparência e eficiência governamental e de cooperação intersetorial para o fomento de inovação, e, de outro lado, a literatura sobre privacidade e proteção de dados passou a preocupar-se mais com o uso de dados pessoais por agentes privados ou com atividades desenvolvidas por governos para fins de persecução penal e segurança do Estado.

Para tanto, é necessário ampliar o diálogo entre estas literaturas, especialmente com vistas a encontrar soluções para assegurar os benefícios dessa divulgação com o menor prejuízo possível a direitos e liberdades de cidadãos. Nos próximos capítulos se buscará avaliar as balizas legais existentes e apresentar uma proposta dogmático-jurídica para a harmonização prática entre divulgação de dados por governos e a privacidade e proteção de dados pessoais.

PARTE II PANORAMA DA LEGISLAÇÃO BRASILEIRA SOBRE O COMPARTILHAMENTO E A PUBLICAÇÃO DE DADOS PELO PODER PÚBLICO EM OBSERVÂNCIA À PROTEÇÃO DE DADOS PESSOAIS

5 REGULAÇÃO BRASILEIRA SOBRE COMPARTILHAMENTO E PUBLICAÇÃO DE DADOS

Neste tópico serão abordadas normas que regulam a publicação e o compartilhamento de dados pessoais no âmbito do governo federal brasileiro, para identificar como elas abordam a compatibilização entre essas práticas e a proteção de dados pessoais de cidadãos.

Importante ressaltar que, em vista da grande quantidade de normas existentes sobre o tema nas diferentes esferas federativas (especialmente quando se trata do compartilhamento de dados que muitas vezes é regulado de forma difusa, por intermédio de contratos ou outros instrumentos jurídicos), somente serão analisadas normas aplicáveis à administração pública federal. Além disso, não se propõe aqui realizar análise exaustiva das normas aplicáveis, sendo relevante para os propósitos ora almejados a delimitação do cenário normativo com base no qual são realizadas práticas de divulgação de dados mantidos pelo poder público.

Além disso, destaca-se que não há no Brasil definição legal clara para os conceitos abordados nesta tese, a exemplo dos termos publicação e compartilhamento. Por exemplo, na LGPD não há referência aos termos compartilhamento ou publicação, havendo apenas o conceito de uso compartilhado (que, nos termos do art. 5º, VI da LGPD, envolve uma multiplicidade de atividades, como a comunicação, a difusão e a transferência internacional) e referência à disponibilização de dados, que os atribui a característica de acessível ao público (art. 7º, § 3º). Igualmente, no art. 4º da LAI e no art. 2º, XII do Decreto nº 10.046/2019, há o conceito de disponibilidade, que consiste em uma qualidade da informação que teria sido disponibilizada por possuir interesse público. Já o termo compartilhamento é qualificado no Decreto nº 10.046/2019 como a disponibilização de dados pelo seu gestor para determinado recebedor de dados. Por sua vez, o conceito de disponibilização não é qualificado, mas é utilizado pela LAI, LGPD e pelo Decreto como uma ação que permite a terceiros (sujeitos limitados ou toda a coletividade) tratarem os dados.

Outros conceitos assemelhados foram propostos quando da deliberação do Anteprojeto de Lei de Proteção de Dados Pessoais, submetido a consulta pública pelo Ministério da Justiça

em 2015, e em guia sobre o tratamento de dados pelo poder público elaborado pelo Comitê de Governança de Dados (CCGD), constituído pelo Decreto nº 10.046/2019:

Quadro 1: possíveis conceitos abrangidos pela divulgação de dados pessoais

Terminologia	**Anteprojeto de Lei de Proteção de Dados Pessoais**	**Guia do Comitê de Governança de Dados**
Comunicação	divulgação de dados pessoais a um ou mais sujeitos **determinados** diversos do seu titular, sob qualquer forma;	transmitir informações pertinentes a políticas de ação sobre os dados;
Interconexão	divulgação de dados pessoais de um banco a outro, mantido ou não pelo mesmo proprietário, com finalidade semelhante ou distinta;	Não há
Difusão	divulgação de dados pessoais a um ou mais sujeitos **indeterminados**, diversos do seu titular, sob qualquer forma;	ato ou efeito de divulgação, propagação, multiplicação dos dados;
Distribuição	Não há	ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
Recepção	Não há	ato de receber os dados ao final da transmissão;
Divulgação	Não há	mudança de dados de uma área de armazenamento para outra, ou para terceiro;
Transmissão	Não há	movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc;
Uso compartilhado	comunicação, difusão, divulgação internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos.	Não há

Nos tópicos seguintes, quando descrevendo determinada legislação, se utilizará os termos por ela adotados. No entanto, análises autorais sobre os contornos da legislação privilegiaram os conceitos divulgação, publicação e compartilhamento, tal como esclarecidos anteriormente.

A seguir se abordará a legislação federal aplicável ao compartilhamento e à publicação de dados mantidos pelo poder público. O objetivo é compreender, de forma não exaustiva[79] (especialmente no caso de compartilhamento de dados, que possui uma grande quantidade de normas esparsas aplicáveis), os esforços que vêm sendo desenvolvidos pelo governo brasileiro para potencializar os benefícios decorrentes do compartilhamento e da publicação de dados com terceiros, públicos ou privados, bem como os cuidados exigidos para que essa prática ocorra em observância à privacidade de indivíduos.

5.1 Fundamentos constitucionais da publicação e do compartilhamento de dados

A ideia de **transparência governamental** é inovação no ordenamento jurídico brasileiro, prevista na Constituição de 1988, atrelada ao movimento de redemocratização, que buscou romper com o anterior paradigma de sigilo e opacidade, para permitir à sociedade ter acesso a informações que lhes permita confiar nas instituições e, ao mesmo tempo, exercer controle sobre eventuais desvios na gestão da coisa pública (MARTINS, 2012).[80] Ela está em linha com tratados internacionais aos quais o Brasil é signatário, que possuem entre seus pontos centrais o direito de acesso à informação, a exemplo do Pacto de San José da Costa Rica, e está resguardada por organismos internacionais dos quais o Brasil é parte, tal qual a Organização das Nações Unidas (ONU) e a Organização dos Estados Americanos (OEA).

Na Constituição Federal de 1988 ela não aparece de forma expressa, mas está presente especialmente por força dos arts. 5º, XXXIII e 37, *caput* e § 1º, sob a roupagem do direito de acesso à informação e do princípio da publicidade governamental. Dos referidos dispositivos constitucionais decorre que todo cidadão possui o direito de obter informações sobre si ou de interesse público provenientes de órgãos públicos, salvo em hipóteses prescritas em lei, e que os órgãos e entidades públicos possuem o dever de ativamente e passivamente, sem custos aos cidadãos, tornar público o máximo de informações possível sobre sua atuação. Em outras palavras, o Estado deverá receber e atender a pedidos de informação que lhe são enviadas por

---

[79] Como se poderá notar, as normas que regulam o compartilhamento de dados mantidos pelo órgão público são difusas e estão em constante modificação, o que dificulta a realização de pesquisa exaustiva.

[80] Corrobora esse entendimento a manifestação do Ministro Eros Grau quando do julgamento sobre a constitucionalidade da chamada Lei de Anistia: Lei 6.683/1979, a chamada "Lei de Anistia". Art. 5º, caput, III e XXXIII, da Constituição do Brasil [...]. Circunstâncias históricas. [...] Acesso a documentos históricos como forma de exercício do direito fundamental à verdade. [...] Impõe-se o desembaraço dos mecanismos que ainda dificultam o conhecimento do quanto ocorreu no Brasil durante as décadas sombrias da ditadura." Supremo Tribunal Federal (STF). Arguição de Descumprimento de Preceito Fundamental 153. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Intimado: Presidente da República e Congresso Nacional. Relator: Ministro Eros Grau. Brasília, 29 de abril de 2010. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=612960. Acesso em 31.08.2022.

cidadãos, como proativamente e frequentemente divulgar informações atualizadas (mas também históricas) que possam contribuir com a transparência governamental e/ou para o direito de acesso à informação pelos cidadãos.

Em particular, a publicidade governamental é pressuposto à consecução do direito de acesso à informação, visto que a publicidade das atividades governamentais permite ao cidadão receber informações sobre si mantidas pelo Estado e informações de interesse particular ou geral que lhe permitem compreender melhor a gestão da coisa pública.[81] Por sua vez, o exercício do direito de acesso à informação provê cidadãos de munição para qualificadamente participar, monitorar e fiscalizar os atos da administração pública. Portanto, juntos, referidos dispositivos constitucionais respaldam o direito fundamental à transparência, que deve ser realizado na maior medida possível.

Assim, a transparência governamental guarda origem no princípio republicano e na ideia de democracia participativa, visto que fornece à sociedade, de quem emana a legitimidade da atuação Estatal republicana e democrática, informações para escolher seus

[81] Por exemplo, o Ministro Alexandre de Moraes argumentou pela necessidade de publicidade de dados mantidos pelo Estado sobre os números de pessoas infectadas pelo vírus do COVID-19: "A gravidade da emergência causada pela COVID-19 exige das autoridades brasileiras, em todos os níveis de governo, a efetivação concreta da proteção à saúde pública, com a adoção de todas as medidas possíveis para o apoio e manutenção das atividades do Sistema Único de Saúde, entre elas o fornecimento de todas as informações necessárias para o planejamento e o combate à pandemia. A interrupção abrupta da coleta e divulgação de informações epidemiológicas, imprescindíveis para a análise da série histórica de evolução da pandemia (COVID-19), caracteriza ofensa a preceitos fundamentais da Constituição Federal e fundamenta a manutenção da divulgação integral de todos os dados que o Ministério da Saúde realizou até 4 de junho 2020, e o Governo do Distrito Federal até 18 de agosto passado, sob pena de dano irreparável. Supremo Tribunal Federal (STF). Arguição de Descumprimento de Preceito Fundamental 690. Requerente: Rede de Sustentabilidade e outros. Intimado: Presidente da República e Ministro de Estado da Saúde. Relator: Ministro Alexandre de Moraes. Brasília, 15 de março de 2021. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755586015. Acesso em 31.08.2022. No mesmo sentido se posicionou o Ministro Ricardo Lewandowski em julgamento sobre a divulgação de critérios estabelecidos pelo governo para estabelecer a ordem de preferência entre grupos prioritários para receber a vacina contra COVID-19: "Na 2ª edição Plano Nacional de Operacionalização da Vacinação contra a COVID-19 estabeleceu-se a população que será imunizada prioritariamente, sem, no entanto, detalhar adequadamente, dentro daquele universo de cerca de setenta e sete milhões de pessoas, qual a ordem de cada grupo de pessoas. O perigo decorrente da alegada omissão sobre a discriminação categorizada dos primeiros brasileiros a serem vacinados – uma vez que a quantidade de vacinas disponíveis até o momento em solo nacional é muito inferior ao número das pessoas incluídas como prioritárias –, é evidente, e compromete o dever constitucional da proteção da vida e da saúde. O direito à informação e o princípio da publicidade da Administração Pública constituem verdadeiros pilares sobre os quais se assenta a participação democrática dos cidadãos no controle daqueles que gerenciam o patrimônio comum do povo, seja ele material ou imaterial, com destaque para a saúde coletiva, sobretudo em período de temor e escassez de vacinas. Medida cautelar referendada pelo Plenário do Supremo Tribunal Federal para determinar ao Governo Federal que divulgue, no prazo de 5 (cinco) dias, com base em critérios técnico-científicos, a ordem de preferência entre os grupos prioritários, especificando, com clareza, dentro dos respectivos grupos, a ordem de precedência dos subgrupos nas distintas fases de imunização contra a COVID-19." Supremo Tribunal Federal (STF). Referendo Segunda em Tutela Provisória Incidental na Arguição de Descumprimento de Preceito Fundamental 754. Requerente: Rede Sustentabilidade. Intimado: Presidente da República. Relator: Ministro Ricardo Lewandowski. Brasília, 01 de março de 2021. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755295024. Acesso em 31.08.2022.

representantes, fiscalizar sua atuação e eventualmente contribuir com a gestão da coisa pública. É por isso que a transparência deve ser assegurada em sua máxima extensão, sendo o sigilo excepcional, tal como bem apresentado pelo Ministro Edson Fachin no julgamento da ADPF 129:

> O Estado Democrático de Direito instaurado pela Constituição de 1988 estabeleceu, como regra, a publicidade das informações referentes às despesas públicas, prescrevendo o sigilo como exceção, apenas quando imprescindível à segurança da sociedade e do Estado. Quanto maior for o sigilo, mais completas devem ser as justificativas para que, em nome da proteção da sociedade e do Estado, tais movimentações se realizem. Os tratados internacionais e a própria Constituição Federal convergem no sentido de se reconhecer não apenas a ampla liberdade de acesso às informações públicas, corolário, como visto, do direito à liberdade de expressão, mas também a possibilidade de restringir o acesso, desde que (i) haja previsão legal; (ii) destine-se a proteger a intimidade e a segurança nacional; e (iii) seja necessária e proporcional.

Assim, a transparência governamental possui ao menos três efeitos para o fomento de uma democracia republicana: **(i)** melhoria no processo decisório, na medida em que a maior transparência auxilia com a confiança do cidadão no Estado e incita sua participação na gestão da coisa pública e no desenvolvimento de políticas públicas; **(ii)** favorecimento de um ambiente de respeito a direitos fundamentais, na medida em que a possibilidade de fiscalização social fomenta o dever do agente público de pautar sua atuação pela moralidade e interesse público; e **(iii)** colaboração com a redução de burocracias e fomento a ambiente de inovação e desenvolvimento econômico (MAROUBO, 2018).

De fato, a evolução da tecnologia tem ampliado essa capacidade de abertura do governo, seja pela ampliação da quantidade de informações que passam a ser divulgadas, pelas novas formas em que elas podem ser oferecidas (e.g., arquivos em papel, documentos em pdf, bases de dados em formato aberto, integrações de sistemas), por facilitar a linguagem em que informações podem ser comunicadas, ou pela maior facilidade de acesso das informações pela população (RODRIGUES, 2014). Por outro lado, essa maior facilidade também tem exigido do agente público maior atenção sobre a sensibilidade das informações divulgadas.

Isso porque, assim como reconhecido pela própria Constituição, o direito à transparência não é absoluto, podendo ser flexibilizado diante do conflito com outros direitos quando houver interesse público preponderante. Por exemplo, a transparência poderá ser limitada em casos nos quais a divulgação de informações imponha riscos à segurança nacional ou à intimidade, vida privada e honra de outros cidadãos (art. 5º, XXXIII, Constituição Federal). Além disso, a transparência também poderá ser limitada quando sua consecução

impuser custos demasiados ao poder público, tal como será abordado mais adiante nesta tese.[82]-[83]

Por sua vez, o **princípio da eficiência** foi contemplado no ordenamento jurídico brasileiro a partir da reforma administrativa do Estado, promovida pela Emenda Constitucional nº 19/1998, que modificou o art. 37 da Constituição Federal. Nesse momento, a eficiência governamental passou a ser considerada um princípio da administração pública, ao lado da legalidade, impessoalidade, moralidade e publicidade.[84] O princípio se explica a partir do desenvolvimento dos conceitos de administração pública gerencial, acentuando a noção de pragmatismo do direito anglo saxônico no direito brasileiro (MOREIRA NETO, 2015).

A depender da interpretação atribuída a esse princípio, o agente público deve atuar para o alcance dos objetivos estabelecidos em lei, em busca do melhor custo-benefício nos gastos de recursos públicos e/ou para a superação do formalismo típico da burocracia governamental (MORAIS, 2004). Em sua concepção tradicional, o princípio da eficiência exige do agente público atuar para o alcance de resultados esperados em lei (GABARDO,

---

[82] O Poder Público não estará sujeito a medidas excessivas ou abusivas que prejudiquem o funcionamento da administração pública enquanto agente de concretização de direitos. Foi nesse contexto que o STF declarou a inconstitucionalidade de uma Lei do Estado do Rio Grande do Sul que determinava a publicização do custo para os cofres públicos referentes a veiculação e publicação de atos do poder executivo estadual nos jornais e outros veículos de imprensa. Segundo o STF, a obrigação de publicização prevista na referida Lei acarretava custos adicionais desnecessários ao erário, de tal forma a não observar o princípio da economicidade (art. 37, Constituição Federal). STF, ADI 2247, Relator Marco Aurélio, Julgamento em 11.11.2004

[83] Entre os instrumentos previstos na constituição para promover a transparência, seja na forma de publicidade governamental ou no direito de acesso à informação, a Constituição também prevê o o o Habeas Data (art. 5º, LXXII), certidão (art. 5º, XXXIV, "b") e petição (art. 5º, XXXIV, "a"), na medida em que assegura ao cidadão meios para se dirigir aos órgãos públicos e formular requerimento ou postulação a respeito de informações produzidas e/ou mantidas pelo poder público. Esses e outros dispositivos constitucionais atinentes à transparência governamental foram regulamentados pelo legislador infraconstitucional, que garantiu ainda outros meios de concretização desse direito, com destaque à edição da Lei de Acesso à Informação, que será mais detidamente abordada a seguir.

[84] Segundo Morais (2004) "Ressalte-se, preliminarmente, que a EC 19/98 não tem unanimidade na doutrina corno instrumento jurídico de modernização da administração pública, havendo autores que a consideram corno inócua neste sentido e outros que a consideraram corno violadora dos princípios em que está assentada a ordem jurídica brasileira à época. Em que pese a respeitabilidade da opinião dos referidos autores, verifica-se, por um exame menos superficial das alterações produzidas pela EC 19/98 no cenário jurídico da administração pública brasileira, que houve um considerável avanço no campo da atuação estatal/administrativa brasileira. Vejamos. A EC 19/98, dentre outros dispositivos constitucionais, produziu alterações nos artigos 37, XI, XIII a XVII, §§§ 30, 80e 90,39, § 10,41, §§§§ 10 a 40,70, parágrafo único, 169, § 40, e 247 da Constituição da República à época em vigor. (...) Verifica-se, portanto, que a Emenda Constitucional 19/98 inovou o juspublicismo brasileiro permitindo a criação de diversos instrumentos jurídicos, através dos quais se permitiu a avaliação do desempenho do servidor público, a expansão da atuação estatal para a sociedade civil organizada, a agilização dos procedimentos de licitação adotados pela administração pública, bem como a criação de cultura de responsabilidade fiscal, com o fim de equilibrar as contas públicas, através da fixação de regras e princípios oponíveis ao administrador público na gestão dos recursos do erário, bem como de adequada responsabilização pelo descumprimento das referidas normas."

2022), motivo pelo qual é comumente associado à idéia de boa administração e aos princípios da finalidade e da legalidade (BANDEIRA DE MELLO, 2015).[85]

Mais recentemente, o princípio passou a assumir também um significado econômico, segundo o qual não bastaria à administração pública atuar para produzir resultados esperados por lei, mas também buscar a otimização das suas atividades (MARTINS CARDOZO; LOPES QUEIROZ; BATISTA DOS SANTOS, 2006). Com isso, a gestão de interesses públicos não deve apenas ser adequada aos fins perseguidos, como também acarretar o menor custo para a sociedade e ocorrer da forma mais célere possível, de tal forma a consistir em um atributo técnico da administração e um dever ético dos gestores públicos (BANDEIRA DE MELLO, 2015; MOREIRA NETO, 2015).[86] De fato, segundo estudo desenvolvido em 2018, o princípio da eficiência vem sendo utilizado pelo STF para avaliar se a gestão dos recursos públicos está adequada em vista do emprego de mínimos recursos para máxima efetividade de políticas públicas (LANIUS; GICO JUNIOR; STRAIOTTO, 2018).[87] Esse racional pode ser percebido, por exemplo, no voto do Ministro Luís Roberto Barroso no Recurso Extraordinário 631.240:

> [...] o interesse em agir é uma condição da ação especialmente ligada aos princípios da economicidade e da eficiência. Partindo-se da premissa de que os recursos públicos são escassos, o que se traduz em limitações na estrutura e na força de trabalho do Poder Judiciário, é preciso racionalizar a demanda, de modo a não permitir o prosseguimento de processos que, de plano, revelem-se *inúteis*, *inadequados* ou *desnecessários*. Do contrário, o acúmulo de ações inviáveis poderia comprometer o bom funcionamento do sistema judiciário, inviabilizando a tutela efetiva das pretensões idôneas.[88]

---

[85] Exemplo desse entendimento pode ser verificado no voto do Ministro Gilmar Mendes no julgamento da ADI nº 6649: "É impensável que, na sociedade moderna, as repartições públicas operam com instrumentos defasados, renunciando à tecnologia, às ferramentas digitais, e desprezando as melhores práticas gerenciais. Ou seja, não é dado ao Estado virar as costas para o progresso tecnológico, tampouco permanecer amarrado ao passado. Cuida-se de mais cristalina aplicação do princípio da eficiência administrativa, ou daquilo que os italianos chamam de princípio da boa administração."

[86] Além disso, o princípio da eficiência vincula a atuação do agente público tanto na tomada de decisões vinculadas, quanto discricionárias, na medida em que há sempre margem para o cotejamento daquela medida que se revela como sendo a ótima, ou seja, que produza os melhores resultados, valendo-se dos meios menos custosos (GABARDO, 2022). Sobre o tema, José dos Santos Carvalho Filho aduz que "a eficiência transmite sentido relacionado ao modo pelo qual se processa o desempenho da atividade administrativa; a ideia diz respeito, portanto, à conduta dos agentes" (DOS SANTOS CARVALHO FILHO, 2015).

[87] Além disso, a pesquisa de 2018 identificou que o STF considera que princípio da eficiência: **(i)** não se confunde e possui autonomia em relação aos demais princípios aplicáveis à administração pública; **(ii)** pode ser utilizado para exercer controle sobre a discricionariedade administrativa; e **(iii)** está relacionado ao conceito científico de eficiência produtiva, que exige à administração pública, na gestão dos escassos recursos públicos, reduzir desperdícios por meio do emprego do mínimo de recursos possível e alcance da máxima efetividade das políticas públicas. Assim, de forma geral, o princípio da eficiência é utilizado para avaliar se a gestão dos recursos públicos está adequada em vista do emprego de mínimos recursos para máxima efetividade de políticas públicas (LANIUS; GICO JUNIOR; STRAIOTTO, 2018).

[88] Nesse julgado, o STF entende que o compartilhamento de dados entre o fisco e a Advocacia Geral da União é medida **necessária** à defesa em juízo da entidade fiscalizatória. Segundo o Tribunal, para que se promova

De todo modo, segundo explica Odete Medauar (2017), o princípio da eficiência não pode se opor a outros princípios aplicáveis à administração pública, na medida em que não será possível a eventual conduta do gestor público ser, ao mesmo tempo, ótima e contrária ao disposto na lei. Por isso, o princípio da eficiência deve ser sempre avaliado em conjunto com outros princípios e mandamentos aplicáveis à atuação da administração pública (MEDAUAR, 2017). De todo o modo, o princípio da eficiência pode ser invocado para legitimar a atuação da administração pública que vise assegurar uma atuação ótima, seja na condução das atividades de administração, seja na própria organização do Estado, para uma melhor prestação de serviços públicos (ZANELLA DI PIETRO, 2015).[89]

Finalmente, nos últimos anos, tem sido possível identificar decisões em que o STF prevê a eficiência da administração pública como elemento no teste de proporcionalidade realizado para justificar a limitação a direitos fundamentais, a exemplo da privacidade. Assim, no julgamento da ADI nº 2859, o Ministro Luís Roberto Barroso argumentou o seguinte:

> Portanto, a possibilidade de acesso aos dados bancários dos contribuintes sem prévia autorização judicial é medida plenamente *adequada* às novas finalidades de promover uma fiscalização eficiente e que possa alcançar a todos os contribuintes, indistintamente, mesmo aqueles sem acesso aos mais sofisticados meios de estruturação financeira. Ela confere maior efetividade à fiscalização, contribuindo para estimular a adimplência voluntária, incrementar a arrecadação e promover a justiça fiscal. Também torna mais difícil a vida dos devedores contumazes, que pretendem extrair vantagens competitivas indevidas da sonegação de tributos, da evasão fiscal e da omissão de receitas.

Por sua vez, no julgamento sobre a constitucionalidade do Decreto n. 10.046/2019, a ADI nº 6649 analisou o uso de tecnologias para melhoria da eficiência das atividades do poder público. Nesse caso, todavia, o princípio da eficiência esteve no centro da ponderação realizada pelo STF sobre a possibilidade de restringir os direitos à privacidade e proteção de dados pessoais. Nas palavras do Ministro Gilmar Mendes:

> [...] mesmo que ausentes os referidos comandos legais, é certo que a Constituição Federal impõe ao Estado o dever de desenvolver a atividade administrativa de modo mais eficiente, mais econômico e mais adequado ao interesse público. Naturalmente, o cumprimento da determinação constitucional pressupõe o emprego das mais modernas tecnologias e soluções computacionais, sobretudo em um contexto de amplo desenvolvimento de ferramentas digitais, de modernas aplicações de

---

uma fiscalização eficiente sobre as atividades do contribuinte, é adequado acessar os dados bancários dos contribuintes sem prévia autorização judicial. Dessa forma, o princípio constitucional da eficiência é analisado como ferramenta balizadora da adequabilidade das práticas de controle fiscal.

[89] Exemplo desse entendimento pode ser verificado no voto do Ministro Gilmar Mendes no julgamento da ADI nº 6649: "Isso não quer dizer que o dever de eficiência sirva de manobra para o descumprimento do princípio da legalidade nem que constitua um chefe em branco para o administrador público. Revela, apenas, a assunção de um compromisso de eficiência e busca dos melhores resultados pelo Estado brasileiro, o que de modo algum representa uma licença para o desatendimento, entre eles os mecanismos de proteção de dados pessoais."

> informática e de computação em nuvem (*cloud computing*). [...] A partir de agora, a administração pública se valerá de mecanismos menos intrusivos, como o compartilhamento de dados, para evitar pagamentos indevidos a pessoas falecidas e combater fraudes no âmbito da seguridade social. Por meio de integração de bases de dados, informações que já se encontram em posse de órgãos públicos federais serão utilizadas para dispensar a prova de vida. Basta que o cidadão tenha sacado dinheiro em agências bancárias, solicitando renovação de carteira de identidade ou habilitação, passaporte ou registro de votação, para que seja considerado vivo. Deparamo-nos, aqui, com exemplo real de legítima utilização do compartilhamento de dados em benefício do cidadão.[90]

5.2 Regulação sobre publicação de dados

Neste momento serão apresentadas as formas de publicação (transparência e dados abertos) de dados mantidos por governos e será realizada análise sobre como a legislação a elas aplicáveis regula a relação entre a divulgação de informações mantidas em bases de dados públicas e a proteção de dados pessoais de cidadãos.

Como mencionado, a publicação de dados pessoais na Constituição se faz presente pelos arts. 5º, IV e XXXIII e 37, *caput* e § 1º, sob a roupagem do direito fundamental de acesso à informação e do princípio da publicidade dos atos administrativos. No entanto, mesmo com referida previsão constitucional, nos primeiros anos após a redemocratização ainda foi possível verificar uma preponderância do sigilo sobre as atividades governamentais.

Diante disso, foram editadas leis que buscavam tornar efetivo o direito de acesso à informação, como a Lei n° 8.159/1991,[91] que dispõe sobre a política nacional dos arquivos públicos, e da Lei n° 11.111/2005,[92] posteriormente revogada pela LAI, que regulava a exceção ao acesso à informação por motivos de segurança da sociedade e do Estado. Todavia, essas normas foram percebidas como insuficientes à época para garantir os direitos fundamentais previstos na Constituição, motivo pelo qual foram apresentadas propostas normativas adicionais para suprir essa lacuna normativa. Em 2009, foi constituída uma Comissão Especial na Câmara dos Deputados para analisar e proferir parecer sobre um projeto de lei que versava sobre o acesso à informação, o PL nº 219/2003, do Deputado

---

[90] E o Ministro Gilmar Mendes complementa com o seguinte: "A partir de agora, a administração pública se valerá de mecanismos menos intrusivos, como o compartilhamento de dados, para evitar pagamentos indevidos a pessoas falecidas e combater fraudes no âmbito da seguridade social. Por meio de integração de bases de dados, informações que já se encontram em posse de órgãos públicos federais serão utilizadas para dispensar a prova de vida Basta que o cidadão tenha sacado dinheiro em agências bancárias, solicitando renovação de carteira de identidade ou habilitação, passaporte ou registro de votação, para que seja considerado vivo. Deparamo-nos, aqui, com exemplo real de legítima utilização do compartilhamento de dados em benefício do cidadão."

[91] Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8159.htm. Acesso em 12.10.2022.

[92] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/lei/l11111.htm. Acesso em 12.10.2022.

Federal Reginaldo Lopes (PT-MG),[93] ao qual foram apensados o Projeto de Lei n° 1019/2007, do Deputado Federal Celso Russomano (PP-SP), o Projeto de Lei n° 1924/2007, do Deputado Federal Chico Alencar (PSOL-RJ), e o Projeto de Lei n° 5228/2009, proposto pelo Poder Executivo e proposto na Câmara por intermédio da Mensagem nº 316/2009.

Com isso, foi formada uma Comissão Especial para analisar os projetos apensados, que contou com a participação de outros atores por meio de audiências públicas, integradas pela Associação Brasileira de Jornalismo Investigativo, Artigo 19, Ordem dos Advogados do Brasil e outros. O relator, Deputado Federal Mendes Ribeiro, em fevereiro de 2010, emitiu parecer pela aprovação do projeto com substitutivo, que foi aprovado pelo plenário da Câmara em abril de 2010. Em seu voto, o relator destaca que "a lei permitirá, igualmente, o desenvolvimento do controle social, mecanismo ínsito ao exercício da cidadania, e que constitui um dos mais eficazes instrumentos de combate à corrupção. Que fique claro, no entanto, que o controle social será mera ficção se não houver farta oferta de informação".[94]-[95]

Em 2011, o texto tramitou no Senado Federal, como o Projeto de Lei da Câmara (PLC) n° 41/2010. Na Comissão de Relações Exteriores e Defesa Nacional, o Relator emitiu parecer propondo um substitutivo[96] para aproximar a proposta ao Projeto de Lei da Câmara dos Deputados nº 5228/2009, de autoria da Presidência da República. O substitutivo foi rejeitado pelo plenário do Senado em 2011, mas o texto do projeto tal como aprovado na

---

[93] Ainda em 2003, o PL 219/2003 foi apresentado sob motivação de que o cidadão alcance "pleno conhecimento das ações do governo, da estrutura, missão e objetivos de seus órgãos, e sobre qual é o resultado final da equação representativa da aplicação de recursos públicos em confronto com os benefícios reais advindos à comunidade". O projeto passou pelas Comissões de Trabalho, Administração e Serviço Público e de Constituição e Justiça, em que houve parecer favorável ainda em 2004, porém o projeto ficou parado até 2009, quando foi apresentado o PL sobre o mesmo tema pelo Presidente da República, Luíz Inácio Lula da Silva. https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=115054&filename=PL+219/2003. Acesso em 12.10.2022.

[94] Vide: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=736307&filename=PRL+2+PL021903+%3D%3E+PL+219/2003. Acesso em 12.10.2022.

[95] Vide: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=736307&filename=PRL+2+PL021903+%3D%3E+PL+219/2003. Acesso em 12.10.2022.

[96] Na avaliação do relator, o PL aprovado na Câmara é excessivo em determinar níveis de publicidade e transparência ativa por parte da Administração, mesmo sem requerimento dos cidadãos, inclusive de informações de natureza sigilosa. Um exemplo seria as informações "oriundas de comunicação entre a chancelaria e as missões diplomáticas, as produzidas no âmbito da Defesa e das Forças Armadas (como os planos militares e a doutrina de emprego das Forças), os dados sensíveis na área de pesquisa tecnológica de ponta e o conhecimento produzido pelos serviços secretos". Ainda, o substitutivo entendeu por suprimir o dispositivo do projeto que vedava "quaisquer exigências relativas aos motivos determinantes da solicitação de informações de interesse público". Vide: https://legis.senado.leg.br/sdleg-getter/documento?dm=3948161&ts=1630415836174&disposition=inline. Acesso em 12.10.2022.

Câmara dos Deputados foi aprovado no Senado Federal, sendo enviado à sanção presidencial e sancionado como Lei nº 12.527/2011.

Assim, a regulamentação dos referidos dispositivos constitucionais, sob a perspectiva de valorização da transparência em relação ao sigilo, foi realizada após mais de 20 anos da promulgação da Constituição e bastante estimulada pela participação do Brasil nos debates internacionais sobre dados abertos (BURLE *et al*., 2015). A iniciativa foi fruto de discussões realizadas no âmbito do Conselho de Transparência Pública e Combate à Corrupção, tendo sido apresentada ao Congresso Nacional pela Presidência da República em 2009, assumindo o formato do PL nº 5.229 na Câmara dos Deputados, que foi apensado ao PL nº 219/2003.[97] Após quase dois anos, a proposta foi sancionada e transformada na Lei Federal nº 12.527/2011, denominada de **Lei de Acesso à Informação** ("LAI").

A nova legislação apresenta como pressuposto a disponibilização gratuita de informações públicas e apresenta o sigilo como exceção. Em outras palavras, ela obriga que órgãos e entidades públicas se sujeitem aos deveres de publicidade e transparência, devendo fornecer aos cidadãos informações de interesse público. Em especial, estabelece parâmetros para a divulgação de informações em *websites* de órgãos públicos e determina procedimentos e prazos para que cidadãos possam requerer acesso a dados públicos. Além disso, determina que a transparência pode ser exercida de forma ativa ou passiva (LAI, arts. 8º e 10). A transparência ativa impõe aos órgãos e entidades públicos a obrigação de promover, independentemente de requerimento, a divulgação de informações de interesse público em local de fácil acesso (LAI, art. 8°). Já a transparência passiva prevê a possibilidade e os procedimentos para que cidadãos solicitem informações a órgãos e entidades públicas (LAI, art. 10). Assim, a LAI estabelece o direito e regulamenta o procedimento de publicização ativa e de fornecimento passivo de informações à comunidade.

No entanto, essa obrigação possui exceções, entre elas as disposições específicas a respeito das informações pessoais, destinadas a garantir que dados relativos a uma pessoa natural sejam protegidos contra perdas, alterações indevidas, acessos, transmissões e divulgações não autorizadas (LAI, art. 25). A proteção garantida consiste em não divulgar, salvo quando autorizado pelo titular dos dados ou pela legislação, tais dados pelo período de 100 anos. No entanto, como ocorre em relação a qualquer direito fundamental, a exceção à

[97] Vide Histórico da LAI disponível em: https://www.gov.br/acessoainformacao/pt-br/assuntos/conheca-seu-direito/historico-da-lai. Acesso em 20.09.2022.

transparência em função da proteção à privacidade não é absoluta e deve ser ponderada no caso concreto.

Tal qual estabelecidos pela LAI, será possível acessar informações pessoais mediante consentimento ou nos casos de prevenção e diagnóstico médicos, realização de estatísticas e pesquisas científicas, cumprimento de ordem judicial, defesa de direitos humanos e proteção do interesse público (LAI, art. 31, §3˚, I a V). Dentre essas exceções à possibilidade de utilizar a privacidade como argumento para a decretação de sigilo a informações mantidas pelo governo, destaca-se a hipótese de interesse público. Esse conceito não é definido na legislação e, como se verá em maiores detalhes adiante, exige a mediação no caso concreto de interesses sociais heterogêneos. Com isso, a LAI buscou estimular a ponderação entre interesses constitucionais (e.g., acesso à informação e publicidade governamental em face à privacidade e proteção de dados pessoais), autorizando a divulgação de informações pessoais quando o interesse geral da sociedade resultar na divulgação de dados. De forma similar se manifestou Laura Schertel Mendes (2014):

> [...] Ao fazer isso, percebe-se que a lei de acesso cumpre um importante papel em buscar delinear as fronteiras entre o direito à privacidade e o direito à informação, estabelecendo critérios determinados segundo os quais o acesso aos dados pode se dar sem o consentimento do titular. Naturalmente, por se tratar de uma exceção e de uma limitação ao direito fundamental à privacidade, esses critérios são numerus clausus e devem ser interpretados de forma restritiva. Do contrário, ter-se-ia a violação da privacidade e dos direitos da personalidade do indivíduo. A despeito do delineamento desses critérios pela lei, sabe-se que, muitas vezes, os conflitos entre a privacidade e o direito à informação não são passíveis de serem resolvidos a priori. Por se tratar de dois preceitos constitucionais, a solução somente pode ser encontrada com o adequado balanceamento entre ambos à luz dos detalhes de caso concreto.

Por sua vez, a LAI foi regulamentada pelo **Decreto nº 7.724/2012**, que dispõe sobre procedimentos para que órgãos da administração pública federal prestem acesso à informação de forma ativa e passiva. Por exemplo, determina que os referidos órgãos e entidades públicas deverão criar Serviço de Informação ao Cidadão - SIC, por meio do qual o cidadão poderá apresentar pedidos, obter informações de tramitação e obter resposta às suas demandas. Similar regulamentação no âmbito do Poder Judiciário foi conduzida pelo Conselho Nacional de Justiça (“CNJ”) somente em 2015, com a edição da Resolução nº 215/2015, de modo que o Poder Legislativo ainda precisa editar norma sobre o tema."

A política de transparência foi incrementada pela edição pelo governo federal do **Decreto nº 8.777/2016**, que estabelece a Política de Dados Abertos do Governo Federal e exige a publicação de dados na internet, de maneira atualizada e em formato não proprietário e reutilizável. Com isso, passou a ser recomendável a divulgação ativa de bases de dados

estruturadas e facilmente aproveitáveis por parceiros, o que diverge de prática de publicação de repositórios de documentos em formato Pdf (que pode impor óbices à leitura por máquina e requer a obtenção de licenças específicas para o processamento dos dados) ou com avaliações já realizadas (em contraposição à divulgação de substrato para que terceiros possam realizar suas próprias análises).

Mais recentemente foi editada a **Lei de Governo Digital** (Lei nº 14.129/2021) que, entre outros, estabelece a abertura de dados como requisito de governo como plataforma. Para tanto, reforça o preceito de publicidade como pressuposto e estimula a publicação de dados em formato aberto, com permissão irrestrita de uso de dados, sempre em observância ao disposto na LGPD. Além disso, estabelece certas informações que deverão ser publicadas, como os exemplos de: **(i)** o orçamento anual de despesas e receitas públicas do Poder ou órgão independente; **(ii)** a execução das despesas e receitas públicas; **(iii)** os convênios e as operações de descentralização de recursos; **(iv)** as licitações e as contratações realizadas; **(v) as** informações sobre os servidores e os empregados públicos federais como nome e detalhamento dos vínculos profissionais e de remuneração; **(vi)** as sanções administrativas aplicadas a pessoas, empresas, organizações não governamentais e a servidores públicos; e **(vii)** os currículos dos ocupantes de cargos de chefia e direção. A lei também estabelece procedimento para a solicitação de abertura de bases de dados, em adição ao disposto na LAI. Nos casos de abertura de bases de interesse público, não será permitido à administração pública exigir motivação ao seu pedido ou a apresentação de exigências de identificação do requerente, que inviabilizam o exercício do direito. As bases de dados que não possuem informações protegidas por lei serão consideradas automaticamente passíveis de abertura.

Assim, e de forma alinhada às tendências internacionais (MEIJER *et al*., 2014), nota-se que a LAI (e, mais recentemente, a Lei de Governo Digital) tem sido apresentada como substrato para a implementação de uma política de disponibilização de dados em formato aberto no Brasil. Inclusive, há na própria LAI previsão que permite ao cidadão gravar relatórios em formatos eletrônicos diversos, inclusive aberto e não proprietário, de forma a facilitar a análise de dados. Muito em razão disso, no Brasil, políticas de dados abertos têm sido fundamentadas na publicidade governamental e seus objetivos têm sido essencialmente destinados a aprimorar a transparência, fornecer informações aos cidadãos e promover a inovação nos serviços públicos, ainda que também incluam objetivos como o desenvolvimento tecnológico e a inovação no setor privado.

Diante do exposto, nota-se que, ainda que anterior aos recentes debates sobre proteção de dados pessoais, a Lei de de Acesso à Informação buscou desenvolver regramento capaz de assegurar a proteção de dados pessoais sem, todavia, prejudicar o interesse público. No entanto, a proteção conferida é genérica e não aborda suficientemente questões essenciais à plena consecução da obrigação de transparência, como **(a)** a identificação de situações em que o interesse público deve prevalecer sobre o direito individual à privacidade, **(b)** quais salvaguardas devem ser adotadas na publicação de dados - especialmente considerando a insuficiência de determinadas práticas de anonimização de dados, e **(c)** quais são os limites à utilização desses dados por terceiros.

5.3 Regulação sobre compartilhamento de dados

As iniciativas coordenadas de modernização e aprimoramento da prestação de serviços públicos com o apoio de tecnologias eletrônicas não são novas. Como já mencionado, por força da emenda Constitucional nº 19/1998, que modificou o *caput* do art. 37 da Constituição Federal, a eficiência governamental passou a ser considerada um princípio da administração pública, ao lado da legalidade, da impessoalidade, da moralidade e da publicidade.[98] Com isso, a depender da interpretação atribuída a esse princípio, o gestor público deve atuar com racionalidade (ie.: melhor custo benefício) nos gastos de recursos públicos em relação ao interesse público almejado ou em constante busca de superação do formalismo característico da burocracia governamental (MORAIS, 2004).

Entre as medidas adotadas de forma a concretizar esse princípio, destaca-se iniciativa de 2000, na qual se instituiu o **Programa Governo Eletrônico (E-Gov)**, realizada por

[98] Segundo Morais (2004) "Ressalte-se, preliminarmente, que a EC 19/98 não tem unanimidade na doutrina corno instrumento jurídico de modernização da administração pública, havendo autores que a consideram corno inócua neste sentido e outros que a consideraram corno violadora dos princípios em que está assentada a ordem jurídica brasileira à época. Em que pese a respeitabilidade da opinião dos referidos autores, verifica-se, por um exame menos superficial das alterações produzidas pela EC 19/98 no cenário jurídico da administração pública brasileira, que houve um considerável avanço no campo da atuação estatal/administrativa brasileira. Vejamos. A EC 19/98, dentre outros dispositivos constitucionais, produziu alterações nos artigos 37, XI, XIII a XVII, §§§ 30, 80e 90,39, § 10,41, §§§§ 10 a 40,70, parágrafo único, 169, § 40, e 247 da Constituição da República à época em vigor. [...] Verifica-se, portanto, que a Emenda Constitucional 19/98 inovou o juspublicismo brasileiro permitindo a criação de diversos instrumentos jurídicos, através dos quais se permitiu a avaliação do desempenho do servidor público, a expansão da atuação estatal para a sociedade civil organizada, a agilização dos procedimentos de licitação adotados pela administração pública, bem como a criação de cultura de responsabilidade fiscal, com o fim de equilibrar as contas públicas, através da fixação de regras e princípios oponíveis ao administrador público na gestão dos recursos do erário, bem como de adequada responsabilização pelo descumprimento das referidas normas."

recomendação do Grupo de Trabalho Interministerial ("GTI"),[99] coordenado pelo Ministério da Ciência e Tecnologia Secretaria Executiva da Casa Civil da Presidência da República,[100] segundo o qual seria necessário adotar uma política integrada capaz ampliar a disponibilidade e a qualidade dos serviços públicos.[101] Nessa oportunidade, o GTI recomendou que a política de E-Gov deveria ter como diretrizes a universalização do acesso aos serviços públicos, a integração de sistemas e bases de dados governamentais e a abertura de informações à sociedade, e, entre os objetivos de longo prazo, metas como a ampliação do acesso à informação aos cidadãos por meio da Internet e a integração entre sistemas de informação, redes e bancos de dados governamentais para permitir a troca de informações e a agilização de procedimentos.[102]

Da aprovação das sugestões do GTI pela Presidência da República foi editado o Decreto nº 18/2000, que instituiu formalmente o Programa E-Gov e atribuiu a definição e a supervisão das suas estratégias ao Comitê Executivo de Governo Eletrônico ("CEGE"), que possuía entre seus membros o Procurador-Geral da República, Secretários-Executivos dos Ministérios e o Chefe da Casa Civil.[103] O envolvimento de cargos de liderança estratégica do governo buscou justamente ressaltar a importância e assegurar a devida implementação do programa.[104]

Entre os projetos e ações do programa E-Gov, especificamente em relação ao objetivo de integração de sistemas e bases de dados, estiveram a: (i) adoção de rede multiserviço, que envolveria a integração entre redes existentes para ampliação e aperfeiçoamento de serviços; (ii) instituição de Base Referencial de Integração dos Sistemas (SIORG) com informações

---

[99] BRASIL. Decreto Presidencial de 3 de abril de 2000. Institui Grupo de Trabalho Interministerial para examinar e propor políticas, diretrizes e normas relacionadas com novas formas eletrônicas de interação. Disponível em: http://www.planalto.gov.br/ccivil_03/dnn/2000/dnn8917.htm#:~:text=Institui%20Grupo%20de%20Trabalho%20Interministerial,novas%20formas%20eletr%C3%B4nicas%20de%20intera%C3%A7%C3%A3o.&text=O%20PRESIDENTE%20DA%20REP%C3%9ªBLICA%2C%20no,que%20lhe%20confere%20º%20art..Acesso em 14.03.2021.

[100] Vide: Do eletrônico ao Digital. Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital. Acesso em 07.03.2022.

[101] Vide Avaliação do Programa Governo Eletrônico. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24F0A728E014F0ADD8CFB5E7B. Acesso em 07.03.2022.

[102] Vide: 2 Anos de Governo eletrônico: balanço de realizações e desafios futuros. Brasília: 02 de dezembro de 2002. Disponível em: https://portal.tcu.gov.br/biblioteca-digital/2-anos-de-governo-eletronico-balanco-de-realizacoes-e-desafios-futuros.htm. Acesso em 14.03.2021.

[103] Curadoria ENAP. Política de Governo Eletrônico e Modelo de Acessibilidade. p. 1. Disponível em: http://antigo.enap.gov.br/downloads/ec43ea4fresumo_20acessibilidade.pdf. Acesso em 14.03.2021.

[104] Vide: 2 Anos de Governo eletrônico: balanço de realizações e desafios futuros. Brasília: 02 de dezembro de 2002. Disponível em: https://portal.tcu.gov.br/biblioteca-digital/2-anos-de-governo-eletronico-balanco-de-realizacoes-e-desafios-futuros.htm. Acesso em 14.03.2021.

sobre estruturas e cargos de todos os órgãos da administração pública federal; e (iii) criação de inventário e catálogo de aplicações e bases de dados da administração pública federal. Nesse contexto, foi editada a resolução (nº 01/2001) sobre a implementação e gestão de sistemas de gestão destinados ao uso compartilhado por todos os órgãos e entidades públicas.

Após dois anos, em 2002, Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento elaborou um balanço sobre os dois anos de Governo Eletrônico,[105] no qual se descrevem os principais avanços e limitações do programa em relação à liderança e coordenação, formulação e avaliação da política, ambiente cultural e motivacional, e infraestrutura e padrões tecnológicos. Por exemplo, o relatório apontou que, embora tenha havido avanço na disseminação de equipamentos e programas computacionais no governo, não foi implementada Intranet para aprimorar a comunicação de serviços.

O relatório de balanço também apontou desafios do programa, de modo a orientar as medidas de continuidade e implementação do Governo Digital nos anos seguintes.[106] Entre os desafios apontados estavam o fortalecimento da penetração do programa na estrutura organizacional dos ministérios e a garantia de recursos orçamentários dedicados, mas também ações como a adoção de medidas capazes de assegurar a integração entre plataformas e sistemas.

Nesse contexto, o CEGE definiu as novas diretrizes gerais para o Programa e foram editadas diversas normas destinadas a acomodar essa redefinição de prioridades. Por exemplo, a Resolução nº 08/2002 criou o Sub-comitê de Integração de Sistemas Administrativos (SISA) no âmbito do CEGE e a Resolução nº 12/2002 que institui o Portal de Serviços e Informações de Governo e-Gov. Além disso, em 2003 foi editado o Decreto Presidencial de 29 de outubro de 2003[107], que instituiu oito Comitês Técnicos no âmbito CEGE para discutir e propor medidas relacionadas às novas diretrizes gerais, a saber: **(i)** implementação de *software* livre; **(ii)** inclusão digital; **(iii)** integração de sistemas; **(iv)** sistemas legados e licenças de *software*;

---

[105] Vide: 2 Anos de Governo eletrônico: balanço de realizações e desafios futuros. Brasília: 02 de dezembro de 2002. Disponível em: https://portal.tcu.gov.br/biblioteca-digital/2-anos-de-governo-eletronico-balanco-de-realizacoes-e-desafios-futuros.htm. Acesso em 14.03.2021.

[106] Curadoria ENAP. Política de Governo Eletrônico e Modelo de Acessibilidade. p. 1. Disponível em: http://antigo.enap.gov.br/downloads/ec43ea4fresumo_20acessibilidade.pdf. Acesso em 14.03.2021.

[107] BRASIL. Decreto Presidencial de 29 de outubro de 2003. Institui os Comitês Técnicos do Comitê Executivo do Governo Eletrônico e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/dnn/2003/dnn10007.htm#:~:text=Institui%20Comit%C3%AAs%20T%C3%A9cnicos%20do%20Comit%C3%AA,Eletr%C3%B4nico%20e%20d%C3%A1%20outras%20provid%C3%AAncias.&text=VIII%20%2D%20Gest%C3%A3o%20de%20Conhecimentos%20e%20Informa%C3%A7%C3%A3o%20Estrat%C3%A9gica. Acesso em 14.03.2021.

(v) gestão de sítios e serviços *online*; **(vi)** governo para governo; **(vii)** infra-estrutura de rede; e **(viii)** gestão de conhecimentos e informação estratégica.

Desse esforço surgiram diversas iniciativas, como a publicação em 2004 da primeira versão dos Padrões de Interoperabilidade do Governo Eletrônico (e-PING),[108] que regula sobre as condições técnicas mínimas que devem ser observadas para a troca em tempo real de dados mantidos pelo governo federal.[109] O e-PING é, portanto, direcionado ao intercâmbio de dados governamentais com terceiros, como cidadãos, empresas, outros entes públicos, sociedade civil e organismos internacionais.

Sua institucionalização é coordenada pelo Sistema de Administração de Recursos de Tecnologia da Informação ("SISP"), instituído pelo Decreto nº 10.048/1994 (substituídos pelo Decreto nº 7.579/2011), responsável pelo planejamento, coordenação, organização, operação, controle e fiscalização dos recursos de tecnologia da informação e comunicação (TIC) dos entes do governo federal. Embora ele seja produzido pelo governo federal (Portaria SLTI/MP n° 5/2005),[110] para uso obrigatório por órgãos e entidades da administração pública federal (segundo o e-PING versão 2004 e posteriormente pela Portaria SLTI/MP n° 92/2014), ele também pode ser utilizado como referência por outras instâncias governamentais.

O e-PING é segmentado em cinco áreas, que são: (i) interconexão, que possui normas técnicas para viabilizar a comunicação de serviços em rede; (ii) segurança, que regula aspectos de segurança de tecnologia utilizada pelo governo federal; (iii) meios de acesso, que prevê especificações e padrões técnicos para dispositivos de acesso a serviços; (iv) organização e intercâmbio de informações, que aborda a divulgação e o tratamento de informações nos serviços de governo eletrônico; e (v) áreas de integração de governo eletrônico, destinados à utilização ou construção de especificações técnicas que sustentem a troca de informações nas áreas transversais de atuação do governo.[111]

---

[108] Interoperabilidade pode ser definida como capacidade de dois ou mais sistemas distintos trabalharem em conjunto e trocarem e usarem estas informações entre si para obterem resultados esperados. Essa definição, entretanto, não é única e tampouco pode ser tomada como consenso (IEEE, 2000).

[109] ePING, Secretaria de Governo Digital, Ministério da Economia, 2004.

[110] https://www.gov.br/governodigital/pt-br/legislacao/Portaria_ePING_14_07_2005.pdf. Acesso em 12.03.2022.

[111] A relevância da interoperabilidade de sistemas governamentais é reconhecida inclusive pelo Marco Civil da Internet (Lei nº12.965/2014), que estabeleceu como objetivo do uso da internet no Brasil a "adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados" (art. 4, III). Além disso, o MCI requer que a atuação do poder público na internet busque a promoção da interoperabilidade tecnológica entre os sistemas e terminais diversos do governo, a partir da adoção de padrões e formatos abertos e livres (arts. 24, I e II).

Entre suas políticas gerais, o e-PING requer que sistemas adotados pelo governo contem com escalabilidade, de forma que permitam constante adaptação na demanda do sistema, adotem padrões preferencialmente abertos e softwares públicos ou livres, para ampliar o acesso aos sistemas governamentais por outras tecnologias que se mostrem adequadas em termos de segurança, e assegurem transparência sobre as informações que detém.[112] Na versão original, a privacidade de informações não estava diretamente referenciada no e-PING, mas foi incluída na lista de políticas gerais em versões mais recentes.

Alguns anos depois, a Presidência da República editou o **Decreto Cidadão** (nº 6.932/2009), destinado a adotar medidas capazes de simplificar o atendimento da população em guichês federais, por meio de ações destinadas a promover as diretrizes como o compartilhamento de informações entre órgãos públicos, a racionalização de métodos e procedimentos de controle, e a aplicação de soluções tecnológicas que visem a simplificar processos e procedimentos de atendimento ao cidadão.[113] Particularmente, estabeleceu que entes do governo federal devem disponibilizar orientações para que outros entes públicos pudessem acessar informações constantes de seus arquivos e bases de dados. Na prática, qualquer atividade consistente na divulgação ou acesso a dados pessoais mantidos pelo governo federal dependia da celebração de acordos e convênios.

Entre os benefícios do Decreto Cidadão, em conjunto com a publicação da Lei de Acesso à Informação (nº 12.527/2011), intensificaram-se medidas de promoção de participação social na gestão pública. Em particular, por meio do Portal Governo eletrônico, cidadãos puderam se cadastrar para enviar contribuições e receber atualizações sobre consultas públicas, e a partir da implementação da Infraestrutura Nacional de Dados Abertos (INDA) e do lançamento do Portal Brasileiro de Dados Abertos (IN nº 04/2012),[114] foram fortalecidas as condições de troca de informações entre órgãos de governo para viabilizar seu uso pela sociedade.[115]-[116]

---

[112] ePING, Secretaria de Governo Digital, Ministério da Economia, 2004.

[113] http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/decreto/d6932.htm. Acesso em 12.03.2022.

[114] https://dados.gov.br/pagina/instrucao-normativa-da-inda#:~:text=Institui%20a%20Infraestrutura%20Nacional%20de%20Dados%20Abertos%20%E2%80%93%20INDA.&text=X%20%E2%80%93%20promover%20a%20participa%C3%A7%C3%A3o%20social,de%20valor%20dos%20dados%20p%C3%BAblicos. Acesso em 18.03.2022.

[115] https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital. Acesso em 18.03.2022.

[116] Também foram adotadas medidas destinadas a padronizar os portais na internet de órgãos públicos federais com o objetivo de otimizar a comunicação com o cidadão, a exemplo da Identidade Digital de Governo (IGD).

Nesse contexto, a partir de 2015 o paradigma de governo eletrônico passou a ser substituído pela lógica de governo digital, que insere o cidadão como foco de medidas destinadas à informatização de processos internos ao governo. Com esse novo paradigma, a adoção de tecnologias por entes públicos deverá ser guiada pela busca de acessibilidade e eficiência na oferta de serviços e informações para o cidadão. Diante disso, foi publicada a **Estratégia de Governo Digital ("EGD")** para os anos de **2016 a 2019,**[117] aprovada pela Portaria nº 68/2016 do Ministério do Planejamento, Desenvolvimento e Gestão, e respaldada no **Decreto nº 8.638/2016**,[118] que revogou o Decreto Presidencial de 29 de outubro de 2003 e instituiu a Política de Governança Digital, destinada a promover a transformação digital do governo.

Entre os pilares da EGD estavam: **(i)** acesso à informação; **(ii)** melhoria na prestação de serviços públicos; e **(iii)** ampliação da participação dos cidadãos na gestão pública, por meio de medidas destinadas a intensificar a transparência. Com base nesses pilares, foram estabelecidos dez objetivos estratégicos, como a edição de normas destinadas a estimular a divulgação de dados abertos, a adoção de tecnologias inovadoras para ampliar a transparência e aprimorar a prestação de serviços públicos, e a promoção de compartilhamento e integração de dados governamentais.

Como parte da política, foi editado o **Decreto nº 8.789/2016,** que substituiu a anterior exigência de formalização das divulgações e/ou acessos a dados pessoais entre órgãos governamentais por um processo simplificado de divulgação de dados.[119] Determinou que órgãos ou entidades da administração pública Federal responsáveis pela gestão de dados seriam obrigados a compartilhar esses dados com outras instituições públicas para evitar a necessidade de reiteradas solicitações a cidadãos e empresas de documentos, de informações já fornecidas e possibilitar a atualização simultânea das bases de dados.

Especificamente, no caso de dados cadastrais (considerados como sendo: identificadores cadastrais em órgãos públicos, vínculo empregatício, nome civil e/ou social de

---

[117] Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/revisaodaestrategiadegovernancadigital20162019.pdf. Acesso em 05.03.2021.

[118] BRASIL. Decreto nº 8.638 de 15 de janeiro de 2016. Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8638.htm#art15. Acesso em 14.03.2021.

[119] Referido decreto possui a finalidade de estimular a utilização de TIC para gerar benefícios para a sociedade, bem como novas formas de participação social no desenvolvimento de políticas públicas. O Decreto nº 8.789/2016 foi alterado pelo Decreto nº 9.584/2018 para instituir a Rede Nacional de Governo Digital – Rede Gov.Br, a fim de promover o diálogo e cooperação de órgãos governamentais na criação de iniciativas inovadoras relacionadas ao governo digital.

pessoas naturais, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar e endereço),[120] passou a vigorar o pressuposto do compartilhamento automático. Para os demais dados, salvo os protegidos por sigilo, poderá ser autorizada a disponibilização integral ou parcial de bases de dados, mediante mecanismos próprios para a conferência de existência e manutenção dos requisitos de elegibilidade, dispensada a celebração de convênios e outros instrumentos similares.

Buscou-se, com isso, permitir a simplificação da prestação de serviços públicos, visto que não mais seria necessário aos órgãos públicos estabelecer parcerias com outras instituições e/ou solicitar reiteradamente os mesmos dados a um mesmo cidadão. Disso decorrem mudanças estruturais no fluxo de informações entre órgãos governamentais, na medida em que se reduz burocracia e se encurta o tempo de processos para trocas de dados.

No entanto, referido Decreto não apresentou cuidados específicos com a proteção de dados pessoais constantes dessas bases. Além de exigir genericamente que órgãos envolvidos adotem procedimentos que garantam a segurança, proteção e confidencialidade aos dados e informações divulgados, estabeleceu que o solicitante de dados deveria municiar seu pedido de acesso apenas com data da solicitação, nome e documento do solicitante, descrição dos dados solicitados e finalidade atribuída aos dados (art. 8º).[121]

O Decreto foi regulamentado pela **Portaria nº 58/2016** do Ministério do Planejamento, Desenvolvimento e Gestão, que estabelece procedimento unificado de solicitação de acesso às bases de dados com intermediação pela Secretaria de Tecnologia da Informação ("STI") do referido Ministério (posteriormente revogado pela Portaria da SGD nº 1.3420/2020). Esse maior detalhamento sobre os procedimentos garantia maior segurança e integridade aos dados, além de permitir ao detentor das bases de dados verificar a devida utilização dos dados pelo órgão solicitante (ainda que isso não fosse exigido expressamente na regulação).

Entre as disposições da Portaria, constava a possibilidade de o acesso às bases de dados ser autorizado a determinados órgãos ou entidades públicos, mas sempre mediante

---

[120] O conceito de dados cadastrais não é definido de forma uníssona, sendo o mais abrangente o estabelecido no Decreto nº 8.771/2016, que regulamenta a Lei nº 12.965/2014 (o Marco Civil da Internet ou "MCI"). Já o conceito de dados cadastrais no MCI (art. 11, § 2º, III) é mais restritivo (filiação, endereço e qualificação pessoal - nome, prenome, estado civil e profissão do usuário) e os dados contemplados poderão ser enviados a autoridades administrativas sem a necessidade de prévia autorização judicial.

[121] Como será abordado adiante, entre as medidas que deverão ser adotadas para proteger direitos de cidadãos, é necessário que o compartilhamento de informações pessoais seja precedido de ponderação por parte do gestor das bases de dados sobre os riscos associados e das possíveis medidas técnicas e/ou de governança que poderão ser adotadas.

autorização pelo órgão detentor das bases de dados cujo acesso é solicitado. Além disso, **(i)** o órgão solicitante deveria garantir a rastreabilidade dos dados disponibilizados e a STI poderia solicitar demonstração da utilização das bases de dados; e **(ii)** a autorização de acesso poderia ser suspensa em caso de impedimento legal ou de não observância a requisitos de segurança, de sigilo ou das finalidades informadas ao detentor das bases de dados.

A Portaria também instituiu o Catálogo de Bases de Dados, destinado a manter registro do conteúdo das bases de dados e práticas de compartilhamento vigentes. Tratava de medida relevante para garantir transparência sobre práticas de tratamento de dados entre órgãos e entidades públicos, de forma a assegurar ao titular de dados maior clareza sobre como seus dados são utilizados pelo governo e municiar a sociedade de maior capacidade fiscalizadora.

No mesmo período foram editadas outras normas para regular o compartilhamento de dados,[122] que assumiam o formato de: **(a)** autorizações genéricas emitidas por portarias ou simples permissões, casos em que não seria necessário observar o procedimento de autorização previsto na Portaria nº 58/2016; e **(b)** processos específicos adotados por órgãos diversos, como o Ministério de Desenvolvimento Social ("MDS") e a Receita Federal ("RFB").

Entre as autorizações genéricas, destaca-se a concedida pela Secretaria do Tesouro Nacional ("STN"), por meio da Portaria nº 141/2017 do Ministério da Fazenda (atual Ministério da Economia), para acesso ao Sistema Integrado de Administração Financeira do Governo Federal ("SIAFI").[123] Referido ato normativo determina que o acesso aos dados do SIAFI se dará mediante a celebração de contrato com o Serpro, sendo a disponibilização feita por meio de API, e que os dados deverão ser utilizados para atividades que estão entre as competências legais do órgão solicitante. Contudo, restam excluídos de acesso os dados classificados como ultrassecretos, secretos ou reservados, nos termos da LAI. Outros sistemas do Ministério da Economia podem ser acessados mediante similares autorizações genéricas, como o Sistema Integrado de Administração de Pessoal ("SIPE"), o Sistema de Concessão de Diárias e Passagens ("SCDP") e o Sistema de Informações Organizacionais do Governo Federal ("SIORG"). Em relação aos procedimentos especiais, para obter acesso aos dados do

[122] Informações sobre o compartilhamento de dados entre órgãos públicos podem ser acessados em: https://www.governodigital.gov.br/transformacao/compras/orientacoes/interoperabilidade/roteiro-de-acesso-a-dados. Acesso em 04.07.2019.

[123] Vide: http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/20815173/do1-2017-03-01-portaria-n-141-de-20-de-fevereiro-de-2017-20815101. Acesso em 04.07.2019.

MDS, o órgão ou entidade pública interessada deveria entrar em contato direto com o departamento da Secretaria Especial.

Já a Receita Federal editou a Portaria nº 1.384/2016[124], na qual estabeleceu procedimento para o compartilhamento de suas bases de dados[125], salvo quando houver dados protegidos por sigilo fiscal. Dentre as bases de dados passíveis de compartilhamento, encontram-se: CPF, CNPJ, Cadastro de Imóveis Rurais ("Cafir"), Nota Fiscal Eletrônica ("NF-e"), Consulta e Gerencial da Declaração de Operações Imobiliárias ("DOI"), dentre outras. Os órgãos ou entidades interessados deverão encaminhar à RFB solicitação contendo detalhamento sobre quais dados se deseja acessar, periodicidade, necessidade e para quais finalidades. Após o deferimento do pedido, deveria o solicitante firmar contrato com o prestador de serviços de tecnologia da RFB, assegurar rastreabilidade dos dados, sendo vedada a divulgação ou a disponibilização dos dados a terceiros.[126]

Em seguida, em 2018, o governo federal editou a Estratégia Brasileira para a Transformação Digital (E-Digital), com um balanço dos desafios a serem enfrentados e ações futuras para a transformação digital do governo, economia e sociedade, que incorporou a então vigente Estratégia de Governo Digital. Entre as metas da E-Digital estavam a ampliação de serviços digitais, a adoção de sistema de autenticação único ao cidadão, e a melhoria das plataformas digitais de participação social.[127] Para tanto, seria necessário, entre outras medidas, promover confiança no ambiente digital por meio da proteção a direitos de privacidade e da defesa e segurança do ambiente online. Destacou-se, portanto, a necessidade de complementar a legislação existente sobre direitos de cidadãos sobre o fluxo de dados pessoais - representado por normas como o Marco Civil da Internet (Lei nº 12.965/2014), o Código de Defesa do Consumidor, a Lei de Acesso à Informação e a Lei do Cadastro Positivo (Lei n° 12.414/2011) -, mas que mereceria ser complementada por lei específica, com regras

---

[124] Portaria disponível em: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=77256. Acesso em 04.07.2019.

[125] Art. 2º Serão disponibilizados dados constantes das seguintes bases: I - Cadastro de Pessoas Físicas (CPF); II - Cadastro Nacional da Pessoa Jurídica (CNPJ); III - Cadastro de Imóveis Rurais (Cafir); IV - Consulta e Gerencial da Declaração de Operações Imobiliárias (DOI); V - Nota Fiscal Eletrônica (NF-e); VI - créditos ativos de pessoas jurídicas de direito público; VII - sistemas de controle de débitos de pessoas jurídicas de direito público; VIII - créditos parcelados; IX - sistemas de controle de débitos parcelados; e X - sistema de emissão de Certidão de Regularidade Fiscal perante a Fazenda Nacional.

[126] Referida Portaria foi complementada pelo Portaria nº 1639/2016, disponível em: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=78818. Acesso em 05.07.2019.

[127] Vide https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital e https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/eDigital.pdf. Acesso em 18.03.2022.

transversais sobre o tema e que sejam adequadas e adaptáveis aos novos desafios tecnológicos.

Posteriormente, mas ainda dentro do escopo da EGD 2016-2019, foi editado o **Decreto nº 10.046/2019,**[128] que revogou o decreto Decreto nº 8.789/2016 e estabeleceu novas regras e estrutura de governança para o compartilhamento de dados entre órgãos e entidades da administração pública federal, com a finalidade de otimizar as diversas etapas de execução de políticas públicas. Para tanto, estabeleceu que qualquer informação será amplamente compartilhada (antes, esse pressuposto se aplicava apenas aos dados cadastrais), dispensada a necessidade de celebrar convênios ou instrumentos jurídicos similares, desde que observado o disposto na LGPD e as regras aplicáveis às informações sigilosas (art. 3º).

Especificamente, o compartilhamento de dados foi segmentado em três modalidades: **(i)** amplo, aplicado a dados públicos e não submetidos a qualquer restrição; **(ii)** restrito, incidente sobre dados sigilosos, podendo ser divulgados para fins de execução de políticas públicas, mediante procedimento simplificado a ser estabelecido pelo Comitê de Governança de Dados; **(iii)** especial, aplicável a dados sigilosos, caso em que serão acessíveis a órgãos e entidades públicos específicos, mediante procedimento definido pelo gestor de dados.[129] Dados classificados em amplos e restritos deverão ser utilizados para interoperabilidade.

A Resolução CCGD nº 02/2020 estabelece que, para o compartilhamento de **restrito**, o solicitante deverá enviar solicitação de acesso ao gestor dos dados, assinado por dirigente do órgão ou entidade pública, com a motivação da solicitação, que não poderá resultar na recusa de acesso aos dados. Além disso, o gestor e o solicitante de dados deverão estabelecer controles de acesso e segurança, de forma a impedir eventos de segurança. Já o compartilhamento **específico** de dados dependerá de autorização do gestor de dados e observar similares procedimentos de segurança.[130]

A definição da categoria dos dados entre restrito ou específico será feita pelo seu gestor (também chamado de custodiante dos dados), observando regras estabelecidas pelo Comitê Central de Governança de Dados (CCGD), órgão instituído pelo Decreto com

---

[128] http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em 18.03.2022.

[129] Segundo a Resolução CCGD nº 02/2020, os dados qualificados como acesso amplo são aqueles que deveriam ser publicados em política de transparência, motivo pelo qual seu compartilhamento entre órgãos públicos seria autorizado. Os dados de acesso restrito são regulados por normas que restringem sua ampla divulgação, mas podem ser cedidos a outros órgãos e entidades governamentais sem uma análise profunda de seu uso, devido ao seu baixo risco. Já os dados de acesso específico são aqueles que oferecem maiores riscos para seus titulares ou para o órgão ou entidade pública.

[130] Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-n-2-de-16-de-marco-de-2020-249025238. Acesso em 27.10.2022

composição exclusiva de representantes de governo[131]-[132] e com competência de fiscalização, criação de regras e intermediação de disputas entre órgãos públicos a respeito do compartilhamento de dados (art. 4º, § 3º).[133]-[134] A qualificação de dados como restrita ou específica dependerá da motivação do gestor da base de dados. Segundo a Resolução CCGD nº 02/2020, a qualificação do dado deverá ser realizada pelo gestor dos dados e observar o disposto na legislação e, nos casos em que houver ambiguidade, aplicar qualificação com restrição de acesso proporcional ao dano decorrente de um vazamento de informação.

Além disso, o Decreto dispensa a necessidade de órgãos públicos celebrarem convênios ou outros instrumentos jurídicos congêneres para a efetivação do compartilhamento de dados mantidos pelo governo (art. 5º), devendo os requisitos de privacidade e segurança estarem contemplados diretamente nas plataformas de interoperabilidade. Todo acesso aos dados deverá ser precedido de solicitação de interoperabilidade e de ciência pelo custodiante dos dados, além de ser necessário: **(i)** no compartilhamento restrito, o custodiante e solicitante de dados observarem regras adicionais de sigilo e segurança estabelecidas pelo CCGD, **(ii)** no compartilhamento especial, atender a regras e obter a autorização do gestor de dados.

Quanto ao reuso dos dados divulgados, o Decreto estabelece que os dados categorizados como de compartilhamento amplo deverão ser disponibilizados em formato aberto e serem catalogados no Portal de Dados Abertos[135] (art. 11, *caput* e §5º), os dados de compartilhamento restrito poderão ser compartilhados pelo solicitante de dados com outras entidades desde que comprovada a necessidade de acesso, salvo se o custodiante dos dados expressamente vedar ou revogar essa divulgação (art. 12, §4º), e os dados de

---

[131] O Comitê Central é composto por (i) dois representantes do Ministério da Economia (sendo um deles da Secretaria Especial de Desburocratização – que presidirá o Comitê Central, e outro da Secretaria Especial da Receita Federal do Brasil); (ii) um representante da Casa Civil da Presidência da República; (iii) um representante da Secretaria de Transparência e Prevenção à Corrupção da Controladoria-Geral da União; (iv) um representante da Secretaria Especial de Modernização do Estado da Secretaria Geral da Presidência da República; (v) um representante do Ministério Público Federal; e (vi) um representante do INSS.

[132] Como apontado por Langenegger e Mascarenhas (2020) "Isso significa que, diferentemente das recomendações internacionais para o compartilhamento de dados, não haverá órgão *multistakeholder* com capacidade de fiscalizar a regularidade das atividades realizadas por órgãos públicos em relação a dados pessoais.

[133] A atuação do CCGD, nos termos do Decreto nº 10.046/2019, possui alguma sobreposição às atividades da ANPD de estabelecer regras e parâmetros para o compartilhamento de dados entre órgãos públicos, como se ver adiante (SANTOS; ANASTÁCIO; VARON, 2020).

[134] Como apontado por Langenegger e Mascarenhas (2020) "Como se verifica, existe alguma sobreposição das atividades do CCGD e aquelas que serão desempenhadas pela Autoridade Nacional de Proteção de Dados Pessoais ("ANPD"), que possui competência para realizar consultas, elaborar normas e fiscalizar atividade de tratamento de dados pessoais realizadas por órgãos e entidades públicas.

[135] Acessível em: https://dados.gov.br/

compartilhamento específico não poderão ser compartilhados pelo solicitante de dados, salvo se o custodiante expressamente conceder essa permissão (art. 12, § 2º).

Além disso, o Decreto constituiu o Cadastro Base para atuar como fonte de consulta a dados cadastrais de cidadãos e, com isso, aumentar a confiabilidade de cadastros governamentais e aprimorar a gestão de políticas públicas por medidas como o cruzamentos de dados e a oferta de interface unificada de identificação de cidadãos.[136] O Cadastro Base é composto por base integradora e por componentes de interoperabilidade, que permitirão consulta a dados pessoais classificados como de acesso amplo ou restrito. Nele, há os dados que constam da base temática do CPF, tais como número de inscrição no CPF, nome completo, nome social, data de nascimento, sexo, naturalidade, filiação, indicador de óbito, e será acrescida de dados biográficos[137] e biométricos[138] provenientes de bases temáticas. A esses dados serão acrescidos os dados de outras bases temáticas, por meio do número do CPF. Com isso, o Decreto ampliou a quantidade de dados que são compartilhados entre órgãos públicos, visto que a norma anterior previa o compartilhamento facilitado somente de dados cadastrais.[139] Isso significa que órgãos públicos diversos terão acesso facilitado a uma maior quantidade de dados pessoais.[140] Caberá ao CCGD propor governança e adotar medidas para a implantação, operação e monitoramento do Cadastro Base.

No entanto, o Decreto, em sua redação original, não esclareceu como o compartilhamento de dados deveria ocorrer, em respeito à privacidade e proteção a dados

---

[136] Entre seus objetivos estão: **(i)** realizar o cruzamento de informações das bases de dados cadastrais oficiais a partir do número de inscrição do cidadão no CPF; **(ii)** viabilizar a criação de meio unificado de identificação do cidadão; **(iii)** disponibilizar interface unificada de atualização cadastral; **(iv)** facilitar o compartilhamento de dados entre órgãos e entidades governamentais; **(v)** a melhoria na gestão das políticas públicas, **(vi)** o aumento na confiança dos cidadãos nos registros mantidos pela administração pública, e **(vii)** viabilizar a criação de um mecanismo unificado para identificar os cidadãos no contexto da prestação de serviços públicos.

[137] "Atributos biográficos: dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios (art. 2º, I, Decreto 10.046/2019)." Atributos genéticos: características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas (art. 2º, IV, Decreto nº 10.046/2019).

[138] "Atributos biométricos: características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar"(art. 2º, II, Decreto 10.046/2019).

[139] "Dados cadastrais: informações identificadoras perante os cadastros de órgãos públicos, tais como (i) os atributos biográficos; (ii) o número de inscrição no CPF; (iii) o Número de Identificação Social ("NIS"); (iv) o número de inscrição no Programa de Integração Social ("PIS"); (v) o número do Título de Eleitor; dentre outros (art. 2º, III, Decreto nº 10.046/2019).

[140] O Cadastro Base, por sua vez, também se encontra em plena ampliação mediante disposições do Decreto nº 10.332/2020, o qual estabelece a Estratégia de Governo Digital. Isso ocorre na medida em que entre seus objetivos estão: (i) ampliar para vinte a quantidade de atributos de cada cidadão registrados até 2022; (ii) catalogar, no mínimo, as trezentas das principais bases de dados do Governo Federal, com previsão de publicação de uma primeira versão em 2021, segundo o Ministério da Economia.

pessoais (havia apenas referências esparsas e genéricas à LGDP). No entanto, em novembro de 2022, após julgamento pelo STF sobre a constitucionalidade do Decreto (no qual se estabeleceu qual interpretação do Decreto seria conforme a constituição), a Presidência da República editou o Decreto nº 11.266/2022 para incluir no texto do Decreto nº 10.046/2019 disposições sobre como promover a interoperabilidade em respeito à privacidade e proteção de dados pessoais. Por exemplo, seu art. 3º passou a exigir que o compartilhamento de dados pessoais deverá ser limitado ao mínimo necessário para o alcance de propósitos legítimos, específicos e explícitos, além de serem compatíveis com as finalidades apresentadas aos titulares de dados.

Mais adiante, por força do **Decreto nº 10.332/2020**, foi publicada a **Estratégia de Governo Digital para o período entre 2020 e 2022**, que busca promover o fornecimento de serviços públicos integrados, de políticas públicas baseadas em dados e evidências, e de serviços preditivos e personalizados para cidadãos.[141] Para tanto, a Secretaria de Governo Digital do Ministério da Economia estabeleceu seis prioridades temáticas (eg., governo centrado no cidadão, integrado, inteligente, confiável, transparente e eficiente) que se desdobram em dezoito objetivos estratégicos, entre os quais estão: o acesso unificado a serviços públicos, a promoção de serviço público integrado, o uso de dados para tomada de decisões e personalização do atendimento ao cidadão, o estabelecimento de método e adequação de órgãos públicos à LGPD, e a criação de plataforma de gestão do uso de dados pessoais.

Em 2020, em meio à pandemia de COVID-19, a Presidência da República editou a Medida Provisória nº 964/2020, que determinou às empresas de telefonia o envio para o Instituto Brasileiro de Geografia e Estatística (IBGE) os nomes, números de telefone e endereços de todos os seus consumidores para a finalidade de condução de pesquisas por parte da instituição. Segundo a MP, os dados deveriam ser tratados em caráter sigiloso e ser utilizados para a realização de entrevistas não presenciais e produção de estatística oficial. O IBGE não era autorizado a disponibilizar os dados a qualquer terceiro, público ou privado, além de possuir a obrigação de informar em seu sítio eletrônico as situações em que os dados foram utilizados e divulgar relatório de impacto à proteção de dados pessoais. No entanto, a

[141] Segundo explica ao *site* que divulga a estratégia: "A elaboração de diretrizes contou com 150 participantes de 32 organizações, públicas e privadas, além das mais de 320 contribuições da sociedade, recebidas em consulta pública realizada em novembro de 2019. Atualmente, apesar do país ser a 4ª população que mais tem acesso à internet mundialmente (cerca de 70%), ocupa apenas a 44ª posição quando se fala de *ranking* de governo digital (dados da ONU)." Disponível em https://www.gov.br/governodigital/pt-br/EGD2020 Acesso em 05.03.2021.

Medida Provisória foi declarada inconstitucional pelo Supremo Tribunal Federal, na medida em que não estava clara a necessidade do compartilhamento de dados, na forma como proposto, para o alcance das finalidades de realizar a produção de estatísticas oficiais. Diante disso e da ausência de procedimentos claros para salvaguardar os dados, a Corte entendeu que a norma resultava em afronta aos direitos fundamentais de privacidade e proteção de dados pessoais.

Após, foi editada a **Lei de Governo Digital** (Lei nº 14.129/2021) para estabelecer princípios, cujo objetivo é fomentar a eficiência da administração pública por meio de medidas como a promoção de serviços públicos no formato digital, da atuação integrada do poder público e do uso de dados abertos.[142] Entre os princípios da lei estão: **(a)** a desburocratização, modernização fortalecimento e simplificação das relações entre poder público e sociedade; **(b)** a transparência na execução dos serviços públicos; **(c)** a promoção de integração entre os órgãos públicos e entidades envolvidas na prestação e no controle dos serviços públicos por meio do compartilhamento de dados pessoais; e **(d)** a interoperabilidade de sistemas e a promoção de dados abertos. Para tanto, estimula a administração pública a adotar soluções digitais para a gestão de suas políticas e para o trâmite de processos administrativos. Na prestação digital de serviços públicos, estabelece que órgãos e entidades públicos devem, entre outros, eliminar as exigências desnecessárias ao usuário no fornecimento de informação e tornar os dados interoperáveis para composição dos indicadores. Para as plataformas de governo digital, será necessário oferecer ferramentas de transparência e exercício pelos cidadãos de seus direitos enquanto titulares de dados pessoais, como o acesso a informações sobre a finalidade específica do seu tratamento pelo órgão ou ente público e sobre os terceiros para quem seus dados foram compartilhados. Além disso, prevê a atuação da administração pública em modelo de governo como plataforma, que envolve práticas de abertura e a interoperabilidade de dados, assim como o estabelecimento de procedimentos de governança que contem com gestão e controles de riscos.

Durante a tramitação do Projeto de Lei que deu origem à Lei de Governo Digital (nº 7.843/2017), muito se discutiu se esse acesso a dados seria gratuito, tendo em vista os benefícios dos públicos dados abertos para inovação e desenvolvimento de novas soluções na

[142] Para alcançar estes objetivos, a Lei estabelece as seguintes diretrizes: (i) digitalização da administração pública e prestação digital de serviços públicos, por meio, também, do desenvolvimento de uma base nacional de serviços públicos; (ii) estabelecimento de apenas um número suficiente para identificação do cidadão; (iii) promoção da transparência ativa de dados e interoperabilidade de sistemas; (iv) estabelecimento de domicílio eletrônico para comunicações, notificações e intimações ao cidadão; (v) fomento a laboratórios de inovação; e (vi) implementação de sistemas de governança, gestão de riscos e mecanismos de controle.

prestação de serviços públicos. A gratuidade desse acesso foi defendida por entidades da sociedade civil e, com o veto presidencial, o dispositivo que determinava a cobrança não foi sancionado (ITS RIO, 2021). Em vista do veto presidencial a respeito da cobrança para o acesso a dados abertos, tramita no Congresso Nacional o Projeto de Lei nº 2224/2021,[143] que altera a Lei de Governo Digital para determinar a possibilidade de ressarcimento de custos ou de despesas relacionados ao fornecimento do serviço de interoperabilidade para a publicização dos dados abertos. A proposta normativa limita a possibilidade de cobrança apenas às hipóteses que esses dados estejam relacionados ao fomento de atividade econômica ou ao atendimento a demanda específica de uma determinada pessoa jurídica ou setor da economia, que oneram os custos de fornecimento ou requeiram investimentos por parte do órgão ou entidade. Para a cobrança, existem condições específicas que devem ser observadas, como quando os dados forem requisitados por instituições acadêmicas, organizações sem fins lucrativos ou startups. Nesse sentido, nota-se que a possibilidade de cobrança para acesso a esses dados ainda é um tema em disputa no contexto brasileiro.

[143] Vide: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2287424. Acesso em 28.08.2022.

6 REGULAÇÃO BRASILEIRA SOBRE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Nesse tópico serão abordados os contornos normativos oferecidos pela legislação brasileira para garantia da privacidade e da proteção de dados pessoais mantidos pelo poder público. Para tanto, se demonstrará que os direitos à privacidade e à proteção de dados possuem respaldo na constituição e, ainda, que a proteção de dados pessoais é assegurada pela legislação infraconstitucional pelo menos desde a edição do Código de Defesa do Consumidor, tendo sido respaldada por outras normas, a exemplo do Marco Civil da Internet, e, após amplo e democrático processo legislativo, conta com proteção abrangente assegurada pela LGPD.

Em seguida, serão apresentadas as soluções estabelecidas pela legislação para o tratamento de dados pessoais pelo poder público em observância à privacidade de cidadãos. Como se observará, embora a LGPD tenha regulado, de forma abrangente e inovadora no país, cuidados que deverão ser observados no tratamento de dados pessoais, suas disposições ainda deixam muito espaço para a interpretação no caso concreto, especialmente no que diz respeito ao tratamento de dados pessoais mantidos pelo poder público. Por isso, a prática e a edição de normas complementares por autoridades competentes assumirão papel importante na orientação de como a lei deverá ser interpretada nesses casos.

6.1 Proteção constitucional à privacidade e proteção de dados pessoais

Até recentemente, havia algum grau de incerteza jurídica a respeito do caráter constitucional da proteção de dados pessoais no Brasil. Isso porque a Constituição Federal de 1988 possuía normas que balizam a circulação de informação (MENDES, 2018), mas que não tratavam especificamente da proteção de dados pessoais, a exemplo do acesso à informação (art. 5º, XIV), da inviolabilidade da intimidade, vida privada, honra e imagem das pessoas (art. 5º, X) e do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (art. 5º, XII). Mais que isso, o direito à privacidade era entendido pela literatura e pela jurisprudência como uma liberdade negativa do cidadão em ver sua individualidade protegida em relação à atuação do Estado. Ou seja, era um direito de ser deixado só, de assegurar sigilo sobre sua intimidade e ser resguardado contra interferências alheias.

Na literatura brasileira, essa interpretação teve respaldo em artigo de Tércio Sampaio Ferraz Júnior (1993) intitulado "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado." Segundo o autor, o direito à privacidade consistiria na liberdade de negar a comunicação de seu pensamento e o sigilo seria uma faculdade atribuída ao cidadão e à sociedade de não ver sua liberdade e segurança devassadas. Tendo como base essa premissa, o autor argumenta que o sigilo previsto no art. 5º, XII, da Constituição Federal, visa proteger a comunicação realizada e não a modalidade tecnológica de comunicação (ie.: correspondência, telegrafia, dados, telefonia). Assim, os dados não seriam protegidos pelo sigilo estabelecido no art. art. 5º, XII, da Constituição Federal, salvo quando relacionados ao conteúdo previsto no art. 5º, X da Constituição, ou seja, a intimidade, vida privada, honra e imagem.[144]

No mesmo sentido, decisões do Supremo Tribunal Federal ("STF") asseguravam à sociedade e aos cidadãos a proteção à comunicação privada, mas não garantiam a mesma proteção aos dados pessoais. Isso se deu no contexto de decisões sobre interceptação telefônica que, na linha do argumentado por Tércio Sampaio Ferraz Júnior, levaram em conta a compreensão do direito à privacidade enquanto liberdade negativa do cidadão em ver sua individualidade protegida em relação à atuação do Estado. Diante disso, quando do julgamento de casos dessa natureza,[145] o STF entendeu que informações contidas em registros individuais não estariam protegidas pelo direito à privacidade ou pelo sigilo de comunicações (WIMMER, 2020).

Em função desse entendimento jurisprudencial, coube à doutrina construir o caminho para que fosse reconhecido o caráter constitucional da proteção de dados pessoais, com especial destaque para Marcel Leonardi, Danilo Doneda e Laura Schertel Mendes. Segundo

---

[144] Segundo o autor: "No que tange à intimidade, é a informação daqueles dados que a pessoa guarda para si e que dão consistência à sua pessoalidade - dados de foro íntimo, expressões de auto-estima, avaliações personalíssimas com respeito a outros, pudores, enfim dados que, quando constantes de processos comunicativos, exigem do receptor extrema lealdade e alta confiança, e que, se devassados, desnudariam a personalidade, quebrariam a consistência psíquica, destruindo a integridade moral do sujeito. [...] No que diz respeito à vida privada, é a informação de dados referentes às opções da convivência, como a escolha de amigos, a freqüência de lugares, os relacionamentos civis e comerciais, ou seja, de dados que, embora digam respeito aos outros, não afetam, em princípio, direitos de terceiros (exclusividade da convivência). [...] Por último, a honra e a imagem. A privacidade, nesse caso, protege a informação de dados que envolvam avaliações (negativas) do comportamento que, publicadas, podem ferir o bom nome do sujeito, isto é, o modo como ele supõe e deseja ser visto pelos outros." (Ferraz Júnior, 1993)

[145] A exemplo dos julgamentos do Mandado de Segurança nº 21.729/DF e do Recurso Extraordinário nº 418.416-8/SC. No julgamento do MS, o STF entendeu que o banco deve informar ao Ministério Público "o nome de beneficiários de empréstimos concedidos pela instituição, com recursos subsidiados pelo erário federal, sob invocação do sigilo bancário, em se tratando de requisição de informações e documentos para instruir procedimento administrativo instaurado em defesa do patrimônio público", não prevalecendo o direito de privacidade, como alegado pela defesa. No mesmo sentido, no julgamento do RE, o STF determinou não haver violação à proteção constitucional ao sigilo das comunicações de dados quando houver sido objeto de apreensão, em cumprimento de mandado judicial, a base física na qual se encontram dados

os autores, a concepção do direito à privacidade enquanto liberdade negativa merecia revisão para se alinhar aos avanços ocorridos na tecnologia nos últimos anos, tal como sugerido por autores europeus como Stefano Rodotà e na paradigmática decisão da Suprema Corte Alemã.

De acordo com essa leitura, o direito à privacidade estaria contemplado na Constituição Federal de 1988, e respaldado na dignidade da pessoa humana (LEONARDI, 2012), no direito fundamental de proteção à vida privada e no *habeas data* (MENDES, 2018).[146] Essa privacidade deveria possuir tanto os contornos de liberdade negativa como de liberdade positiva. Para tanto, argumentam que informações pessoais não necessariamente são íntimas ou privadas, assim como podem não ser comunicadas, mas seu uso inadequado poderá afrontar direitos fundamentais (MENDES, 2018). Esse é o motivo pelo qual a proteção constitucional baseada na vida privada e no sigilo de comunicação seria considerada insuficiente.

Finalmente, argumentam que essa interpretação extensiva ao direito à privacidade merece reconhecimento constitucional para impedir retrocessos iniciados pelo legislativo (DONEDA, 2019; MENDES, 2018). Esse receio teria como exemplo prático o ocorrido na Alemanha na década de 1980, pois, a despeito da existência de legislação destinada à proteção de dados pessoais desde a década de 1970 (MENDES, 2018), foi aprovada lei controversa que determina o recenseamento geral da população. Referida iniciativa foi questionada perante a Corte Constitucional do país, que reconheceu o caráter constitucional do direito de escolha por parte dos cidadãos a respeito de como seus dados seriam utilizados por terceiros.

Alinhado ao argumentado por esses autores, recentemente o STF, em três julgamentos distintos, reconheceu o respaldo constitucional à proteção a dados pessoais. Especificamente, isso se deu no momento do julgamento das ADIs nº 6387, nº 6388, nº 6389, nº 6390 e nº 6393, quando da análise da constitucionalidade da MP nº 954/2020, que impunha às empresas de telefonia a obrigação de envio de dados de seus clientes para o IBGE. Esse entendimento

---

[146] O STF, quando do julgamento do *Habeas Data* 22/DF em 1991, reconheceu a existência de um direito material de acesso aos dados pessoais protegido pela Constituição Federal, além da sua relação com direitos de intimidade, vida privada e autonomia individual. O caso versava sobre requerimento de acesso a dados pessoais constantes no arquivo do extinto Serviço Nacional de Informações. No julgamento, o Ministro Relator Celso de Mello, destacou que "[o tema da acessibilidade de registros existentes no extinto Serviço Nacional de Informações] tem suscitado grande discussão, especialmente porque envolve um dos aspectos mais expressivos da tutela jurídica dos direitos da personalidade. A garantia de acesso a informações de caráter pessoal, registradas em órgãos do estado, constitui um natural consectário do dever estatal de respeitar a esfera de autonomia individual, que torna imperativa a proteção da intimidade." STF, Recurso em Habeas Data 22-DF. Ministro Relator Marco Aurélio, relator para o acórdão Ministro Celso de Mello, julgado em 19 de setembro de 1991. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=362613.

foi reiterado pelos Ministros Edson Fachin e Rosa Weber no julgamento conjunto da ADPF nº 403 e da ADI nº 5527, que discutem a possibilidade de decisões judiciais solicitarem o acesso a mensagens criptografadas ponta-a-ponta, ainda em curso. O mesmo entendimento também foi apresentado pelo Ministro Gilmar Mendes quando da análise da Medida Cautelar à ADPF nº 695, na qual se questiona a constitucionalidade do compartilhamento de dados entre a Abin e o Serpro com relação a dados coletados pelo Denatran.[147]-[148]

Em seu voto quando da apreciação da Medida Cautelar na ADI 6387 (Caso IBGE),[149] a Ministra Relatora Rosa Weber declarou que os direitos fundamentais à inviolabilidade da vida privada, honra e imagem, pertencentes ao chamado direito à privacidade, reforçam a importância da proteção à personalidade e às liberdades individuais. Os dados pessoais, na medida em que relacionados a pessoas naturais, integram a proteção às liberdades individuais, à privacidade e ao desenvolvimento da personalidade. Com isso, a Ministra reconheceu que a autodeterminação informativa e a privacidade seriam decorrentes dos direitos de personalidade. Além disso, entendeu que o texto normativo questionado não observou o devido processo legal,[150] que o tratamento de dados pessoais teria como régua de análise a demonstração clara da finalidade,[151] adequação, necessidade e segurança[152] do referido tratamento intentado.

No mesmo sentido se manifestou o Ministro Gilmar Mendes,[153] ao reconhecer a necessidade de avançar ao debate sobre sigilo comunicacional e o fato de que o uso de

---

147 "Em primeiro lugar, é importante situar epistemologicamente que o parâmetro de controle invocado nesta ADPF está relacionado à afirmação do **direito à proteção de dados pessoais enquanto categoria autônoma de direito fundamental na ordem constitucional brasileira**, especialmente na forma de uma projeção alargada do direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, consagrado no art. 5º, inciso X, da CF." (STF, ADPF-MC nº 695-DF, Voto Min. Gilmar Mendes)

148 Voto disponível em: https://www.conjur.com.br/dl/gilmar-manda-plenario-analise.pdf. Acesso em 07.09.2020

149 Voto disponível em: https://www.conjur.com.br/dl/adi-6387.pdf. Acesso em 07.09.2020

150 Sobre o tema, vide artigo de opinião publicado por Bruno Bioni e Pedro Martins, disponível em http://genjuridico.com.br/2020/08/10/devido-processo-informacional/. Acesso em 07.09.2020.

151 "Observo que o único dispositivo da MP n. 954/2020 a dispor sobre a finalidade e o modo de utilização dos dados objeto da norma é o § 1º do seu art. 2º. E esse limita-se a enunciar que os dados em questão serão utilizados exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. Não delimita o objeto da estatística a ser produzida, nem a **finalidade específica**, tampouco a amplitude. Igualmente não esclarece a **necessidade** de disponibilização dos dados nem como serão efetivamente utilizados." (STF, ADI-MC 6387, Voto Min. Rosa Weber, julgado em 24.04.2020)

152 Nessa linha, ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP n. 954/2020 não oferece condições para avaliação da sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. Desatende, assim, a garantia do devido processo legal (art. 5º, LIV, da Lei Maior), em sua dimensão substantiva. (STF, ADI-MC 6387, Voto Min. Rosa Weber, julgado em 24.04.2020)

153 Voto disponível em: https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf. Acesso em 07.09.2020

informações possui a capacidade de afetar o sistema de proteção a direitos individuais, especialmente em vista das novas tecnologias disponíveis. Por isso, declarou a necessidade de se reconhecer a existência de um direito fundamental à proteção de dados pessoais na Constituição brasileira.[154] Para tanto, o Ministro realizou uma releitura sobre o princípio da privacidade, antes baseado na compreensão da privacidade enquanto direito de não intervenção por parte do Estado (*right to be left alone*).[155] Com a evolução da tecnologia, a privacidade teria passado a constituir também um elemento positivo, indutivo da cidadania e das liberdades individuais.[156] Tal como argumenta o Ministro, conforme reconhecido no julgamento do paradigmático caso do censo alemão, a proteção de dados pessoais seria elemento essencial da personalidade, além de estar também respaldada no direito ao sigilo. Essa proteção exigiria que indivíduos tenham o poder de decidir quando e dentro de quais limites seus dados podem ser utilizados (a chamada autodeterminação informativa).[157]

Diante disso, o Ministro argumenta que o direito fundamental à proteção de dados pessoais possui lastro no direito fundamental à dignidade da pessoa humana, na proteção à intimidade em sua compreensão atualizada e no reconhecimento do *habeas data* como

---

[154] "É claro que a proteção do sigilo em operações como essas é indispensável. Contudo, **a autonomia do direito fundamental em jogo na presente ADPF exorbita, em essência, a sua mera equiparação com o conteúdo normativo da cláusula de proteção ao sigilo**. A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do habeas data enquanto instrumento de tutela material do direito à autodeterminação informativa." (STF, ADI-MC 6387 - Voto Conjunto ADIs 6.388, 6.389, 6.390 e 6.393, Min. Gilmar Mendes, julgado em 07.05.2020)

[155] "Na doutrina pátria, os estudos voltados à identificação da autonomia do Direito à Privacidade parecem ter se vinculado inicialmente a essa abordagem formal de um direito negativo de não intervenção. Tal abordagem foi reproduzida em artigo clássico do Professor Tércio Sampaio Ferraz Júnior intitulado "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado", publicado em 1993 (FERRAZ JÚNIOR, Tércio. Sigilo de dados: o direito à privacidade e os limites da função fiscalizadora do estado. Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, p. 430-459, 1993)." (*ibid*)

[156] "A partir desses três elementos – valorização da dignidade humana, proteção constitucional à intimidade e vitalização do habeas data –, é possível identificar dupla dimensão do âmbito de proteção do direito fundamental à proteção de dados. [...] [E]m uma dimensão objetiva, a afirmação do direito fundamental à proteção de dados pessoais impõe ao legislador um verdadeiro dever de proteção (Schutzpflicht) do direito à autodeterminação informacional, o qual deve ser colmatado a partir da previsão de mecanismos institucionais de salvaguarda traduzidos em normas de organização e procedimento (Recht auf Organisation und Verfahren) e normas de proteção (Recht auf Schutz). Essas normas devem ser positivadas justamente para garantir o controle efetivo e transparente do indivíduo relativamente à circulação dos seus dados, tendo como chave-interpretativa da juridicidade desse controle a noção de consentimento." (ibid)

[157] "É justamente essa reconfiguração que possibilita a afirmação do direito à autodeterminação informacional como um contraponto a qualquer contexto concreto de coleta, processamento ou transmissão de dados passível de configurar situação de perigo. Nas palavras ilustres de Stefano Rodotà, a privacidade também passa ser definida como "o direito de manter o controle sobre suas próprias informações e de determinar como a privacidade é alcançada e, em última instância, como o direito de escolher livremente o seu modo de vida" (tradução livre) (RODOTÀ, Stefano. In diritto di avere. Roma: Laterza, 2012, p. 321)." (*ibid*)

instrumento de proteção do direito à autodeterminação informativa. Inclusive, reconhece que a proteção aos dados pessoais vem sendo paulatinamente incorporada ao ordenamento jurídico brasileiro, em normas como o Código de Defesa do Consumidor e do Marco Civil da Internet. Tais normas, por sua vez, seriam dotadas de uma natureza pré-constitucional, visto que apoiam a interpretação da própria Constituição Federal por meio da sua característica de lei formal sobre temas como a internet.[158]

Com base nisso, argumentou que a perspectiva constitucional da proteção de dados pessoais possui duas dimensões. De um lado, a dimensão subjetiva do direito de privacidade impõe ao legislador apresentar justificativa constitucional para qualquer intervenção que produza possíveis efeitos negativos sobre a autodeterminação informacional do indivíduo, o que se dará na observância do devido processo informacional e aos subprincípios de proteção de dados pessoais - que serão mais detidamente abordados adiante -, como a finalidade e a transparência.[159] De outro lado, na dimensão objetiva do direito, o legislador possui a obrigação de proteger a autodeterminação informacional, por meio da edição de normas de organização - que envolvem a constituição de autoridades independentes para a fiscalização.

Em seguida, no julgamento da ADPF nº 403, sobre a constitucionalidade de interpretações que permitem a juízes exigir acesso a mensagens criptografadas ponta-a-ponta, o Ministro Edson Fachin reconheceu que o direito à privacidade exige que o indivíduo tenha controle sobre sua própria informação e que possa escolher como construir sua esfera pública. Tal como os Ministros Rosa Weber e Gilmar Mendes, reconheceu que o direito à privacidade não mais se restringe ao *right to be left alone* dos titulares, englobando o direito às escolhas sobre o fluxo de seus dados e sendo essencial para a consecução de sua liberdade de

---

158 "Daí porque autores como Lex *et al*. chegam a afirmar que algumas leis formais sobre a internet, como o próprio Marco Civil da Internet brasileiro, embora se situem em um plano infraconstitucional, apresentam uma verdadeira natureza "pré" ou "proto-constitucional", uma vez que estabelecem verdadeiros blocos de construção intelectual para a interpretação das constituições (GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights. Research Publication No. 2015-15, 2015, v. 7641, 2015, p. 6). (STF, ADI-MC 6387, Voto Min. Gilmar Mendes, julgado em 07.05.2020)

159 "A partir da tradição norte-americana, também é possível identificar como corolário da dimensão subjetiva do direito à proteção de dados pessoais, a preservação de verdadeiro "devido processo informacional" (*informational due process privacy right*), voltado a conferir ao indivíduo o direito de evitar exposições de seus dados sem possibilidades mínimas de controle, sobretudo em relação a práticas de tratamento de dados capazes de sujeitar o indivíduo a julgamentos preditivos e peremptórios. Como destacado por Julie E. Cohen: "o caráter autônomo da privacidade sugere uma necessidade de repensar a concepção do devido processo como uma tomada de decisão individualizada. [...] O devido processo na era de computação abrangente deve pressupor limites à personalização nos processos administrativos públicos" (COHEN, Julie E. What Privacy is For. Harvard Law Review, v. 126, 2013, p. 1931). (STF, ADI-MC 6387, Voto Min. Gilmar Mendes, julgado em 07.05.2020)

expressão. Diante disso, o julgado estabelece ser a criptografia, que vem sendo cada vez mais adotada por empresas e governos, mecanismo adequado para proteger a privacidade *online*.[160]

Finalmente, no julgamento da Medida Cautelar na ADPF nº 695, que discute o respaldo constitucional de atos administrativos que autorizam o compartilhamento de dados entre o Denatran (que não compõe o Sistema Brasileiro de Inteligência)[161] e a Abin, o Ministro relator Gilmar Mendes reforçou[162] seu entendimento sobre a necessidade de reconhecimento da existência de um direito fundamental à proteção de dados pessoais.

Analogamente, o Ministro argumentou que a dimensão subjetiva do direito fundamental de proteção de dados pessoais impõe ao poder público, no geral, o ônus de apresentar as justificativas constitucionais e de interesse público para os casos nos quais sua atuação poderá restringir a autodeterminação informacional dos cidadãos, não bastando a declaração de que os dados serão mantidos em sigilo. Essa restrição deverá ser excepcional, e a sua justificativa deverá ser composta pela identificação da finalidade da restrição e pelo estabelecimento de limites à atividade de tratamento de dados pretendida.[163]

Diante desse novo paradigma constitucional, a preocupação se desloca do conteúdo dos dados para se centrar nos possíveis usos que lhe serão atribuídos - motivo pelo qual devem estar previstos tanto mecanismos de controle de finalidade do uso desses dados pelo poder público, quanto salvaguardas aos dados pessoais amplamente considerados (e não limitados à proteção de informações consideradas sensíveis).

No entanto, argumenta que, para além de garantir algum nível de autonomia ao indivíduo sobre como seus dados pessoais serão tratados, a privacidade, em casos de manejo de informações pelo poder público, não deve "partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em

---

[160] Voto disponível em: https://www.conjur.com.br/dl/fachin-suspensao-whatsapp-decisao.pdf. Acesso em 08.09.2020.

[161] Lei n° 9.883/1999, Art. 2°, caput. "Os órgãos e entidades da administração pública Federal que, direta ou indiretamente, possam produzir conhecimentos de interesse das atividades de inteligência, em especial aqueles responsáveis pela defesa externa, segurança interna e relações exteriores, constituirão o Sistema Brasileiro de Inteligência, na forma de ato do Presidente da República."

[162] Voto disponível em: https://www.conjur.com.br/dl/gilmar-manda-plenario-analise.pdf. Acesso em 08.09.2020.

[163] "Diferentemente do que ocorre com o direito fundamental ao sigilo, a dimensão subjetiva do Direito Fundamental à Proteção de Dados Pessoais impõe que o legislador e o Poder Público de modo geral assumam o ônus de apresentar uma justificativa constitucional para qualquer intervenção que de algum modo afete a autodeterminação informacional. Nesse aspecto, a autodeterminação do titular sobre os dados deve ser sempre a regra, somente afastável de maneira excepcional. A justificativa constitucional da intervenção deve ser traduzida na identificação da finalidade e no estabelecimento de limites ao tratamento de dados em padrão suficientemente específico, preciso e claro para cada área." (STF, MC na ADPF-MC nº 695-DF, Voto Min. Gilmar Mendes)

confronto com o valor constitucional da privacidade e proteção de dados pessoais." Segundo o Ministro, se a privacidade e a proteção de dados pessoais forem consideradas como sendo interesses meramente individuais, será mais simples encontrar uma justificativa para limitar sua aplicação para a execução de finalidades do poder público. Por isso, é necessário reconhecer seu conteúdo comunitário e constitucional.[164]

Diante disso, à luz da ideia de autodeterminação informativa, afasta-se a ideia de que o tratamento de dados pessoais menos críticos ou sensíveis - tal como os dados cadastrais - seria irrelevante para a tutela da privacidade e da proteção de dados pessoais, sendo central a avaliação sobre as finalidades e riscos do uso dos dados.[165]

Não obstante isso e com vistas a solidificar o entendimento de que os dados pessoais possuem proteção constitucional autônoma, foi aprovada, em 10.02.2022, no Congresso Nacional, a Proposta de Emenda à Constituição ("PEC") nº 17/2019[166], convertida na Emenda Constitucional nº 115/22[167], que: **(i)** incluiu a proteção de dados pessoais entre os direitos fundamentais dispostos na Constituição Federal; e **(ii)** estabeleceu a competência legislativa exclusiva da União para legislar sobre o tema da proteção de dados pessoais.

A proposta foi debatida em audiências públicas promovidas pelo Congresso Nacional, oportunidade na qual os participantes, de uma forma geral, argumentaram pela necessidade de reconhecer a proteção de dados pessoais como direito fundamental. Por exemplo, Tércio Sampaio Ferraz Jr. defendeu que a proteção de dados pessoais é direito autônomo que deveria ser incluído no rol do art. 5º da Constituição Federal. No mesmo sentido, Francisco Brito Cruz sustentou que o reconhecimento da proteção de dados pessoais enquanto direito fundamental cristaliza a visão de que a privacidade excede o direito individual de ser deixado sozinho. Outros diversos participantes reforçaram que a previsão expressa desse direito no texto constitucional assegura segurança jurídica, a exemplo de Laura Schertel Mendes, que também pontuou o caráter coletivo do direito.

---

[164] Mais detalhes sobre o julgamento serão apresentados adiante nesta tese.

[165] "Como bem destacado pela professora Laura Schertel Mendes, é decisivo para a concepção do direito à autodeterminação: "o princípio segundo o qual não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado dos danos", de modo que "o risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados mesmos (ou no fato que quão sensíveis ou íntimos eles são)" (MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. No Prelo). (STF, ADPF 696, Voto do Ministro Gilmar Mendes, proferido em 24.06.2020).

[166] Ver: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1620769236373&disposition=inline. Acesso em 20.07.2021

[167] Ver: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 02.05.2022.

A princípio, a PEC recebeu críticas no sentido de que seria redundante adicionar um inciso contendo o direito fundamental à proteção de dados, uma vez que os julgados do STF, de maneira conclusiva, o estabeleceram como diretamente dedutível dos demais direitos fundamentais já incluídos no texto constitucional. Em sentido contrário, Bruno Bioni[168] argumenta ser a sua positivação entre o rol de direitos fundamentais do artigo 5º benéfica para equacionar o direito com outros bens constitucionalmente reconhecidos, de maneira a favorecer o amadurecimento do debate a respeito da proteção de dados, para além da complexa formulação que encontrou nos julgados da Suprema Corte.

Como se verifica, por meio da jurisprudência do STF e do emendamento constitucional, o direito à privacidade deixou de ser compreendido apenas como um direito negativo do indivíduo em ter a sua intimidade protegida contra intervenções do Estado, passando a se qualificar como uma liberdade positiva de exercício de controle sobre como seus dados pessoais serão utilizados por terceiros. No entanto, como bem apontado pelo Ministro Gilmar Mendes, esse direito também deverá deixar de ser compreendido como uma liberdade de um indivíduo isolado, mas como sendo um interesse da coletividade. Similar formulação é apresentada por Charles Raab (2012), que argumenta ser a privacidade um interesse não individual, de interesse público e intimamente relacionado à complexidade do arranjo social.

Essa formulação, apoiada por esta tese, reconhece que a proteção assegurada pelos direitos à privacidade e proteção de dados pessoais deve extrapolar a esfera de pessoas individualmente consideradas para alcançar toda a coletividade, inclusive sendo um dentre os possíveis interesses conflitantes que compõem o significado de interesse público. Isso se deve, entre outros, à centralidade desses direitos para a democracia, mas também aos efeitos coletivos do tratamento de dados pessoais de grupos de indivíduos.

---

[168] "O julgamento se valeu de uma dogmática bastante sofisticada da Constituição para extrair um direito que nela não está explícito. Houve uma construção argumentativa no sentido de verificar quais eram os dispositivos do artigo 5º/CF que abririam espaço, no texto constitucional, para o reconhecimento da proteção de dados pessoais como um direito fundamental. Um avanço, sem dúvida, mas que necessita amadurecer para uma compreensão (e delimitação) do seu alcance em face da necessidade de equacionar outros bens constitucionalmente assegurados, como resultado de um processo de ponderação de direitos fundamentais." Ver: https://brunobioni.com.br/wp-content/uploads/2020/06/Jota_PEC-17-e-STF_final.pdf. Acesso em 20.07.2021

6.2 Regulação sobre privacidade e proteção de dados pessoais

Entre as primeiras normas que asseguram proteção a dados pessoais no ordenamento jurídico brasileiro estão o Código de Defesa do Consumidor ("CDC", Lei nº 8.078/1990), as já mencionadas Leis do *Habeas data* e de Acesso à Informação, bem como o Marco Civil da Internet ("MCI", Lei nº 12.965/2014) e seu Decreto regulamentador (Decreto nº 8.771/2016).

Em relação ao aspecto consumerista, o CDC estabelece como direito do consumidor o recebimento de informações adequadas e claras sobre os serviços que lhe forem prestados (art. 6º, III), o que se aplica também às bases de dados que possuam suas informações (art. 43). Mais que isso, o CDC apresenta princípios e direitos básicos que são aplicáveis também às atividades de tratamento de dados pessoais (MENDES, 2018), como o reconhecimento da vulnerabilidade do consumidor (art. 4º, I), a exigência de prestação de informação adequada e clara sobre produtos e serviços (art. 6º, II) e a proteção contra práticas abusivas (art. 6º, IV).

Segundo Laura Mendes (2018), a interpretação das normas do CDC permite concluir pela proteção de dados pessoais de consumidores, nas duas dimensões essenciais à proteção da sua personalidade e à garantia da sua autodeterminação informativa: **(i)** a dimensão objetiva, consistente na proteção do consumidor contra riscos oferecidos pelo uso indevido de seus dados por terceiros; e **(ii)** a dimensão subjetiva, que envolve o direito do consumidor em controlar o fluxo de seus dados. Esse entendimento foi respaldado pelo Superior Tribunal de Justiça ("STJ"), especialmente em relação ao reconhecimento da dimensão objetiva da proteção de dados pessoais (CUEVA, 2017).[169]

De fato, antes mesmo da entrada em vigor da Lei Geral de Proteção de Dados, a Secretaria Nacional do Consumidor ("Senacon") do Ministério da Justiça ("MJ"), investigou diversos casos relacionados ao tratamento de dados pessoais por entidades públicas ou privadas.[170] Além disso, unidades diversas do Ministério Público, com especial destaque para

[169] "Foi um processo muito complexo por que repentinamente foram chamados à mesa dezenas de órgãos públicos que tinham tido pouco ou nenhum envolvimento com o tema até aquele momento e obviamente a reação era... não vou dizer de pânico, mas era uma reação defensiva, tipo "essa lei vai impactar nesse, nesse, nesse aspecto, então vamos propor um monte de veto" e eu acho que foi muito revelador do grau de distanciamento que havia do poder executivo com relação a discussão no Congresso Nacional" Disponível em: https://www.youtube.com/watch?v=87kDGMwgoc0. Acesso em 12.10.2020.

[170] Entre 2019 e 2020, a Senacon analisou casos de comercialização de dados pessoais, uso de tecnologias de monitoramento, compartilhamento de dados pessoais e uso indevido de dados e falhas de segurança no tratamento dessas informações. A título exemplificativo, a Senacon investigou o uso de câmeras pela loja Hering para elaboração de mapa de calor que demonstrava os pontos mais frequentados da loja e a indicação de gênero, faixa etária e humor dos consumidores no ambiente da loja. A Secretaria entendeu que se tratava do uso de câmeras com tecnologia de reconhecimento facial que coletava dados dos consumidores sem que eles autorizassem, ou ao menos soubessem da prática. A loja foi condenada em processo administrativa a

a do Distrito Federal ("MPDFT"),[171] também atribuíram para si a proteção de dados pessoais, tendo em vista que a legislação até então vigente era essencialmente pautada em direitos do consumidor.

O direito de proteção a dados pessoais, antes reconhecido por força de interpretação da legislação consumerista, foi também reconhecido pelo **Marco Civil da Internet** (Lei nº 12.965/2014 ou "MCI").[172]-[173] A referida norma estabeleceu princípios, direitos e obrigações para o uso da Internet no Brasil, apresentando regras sobre o tratamento de dados *online*. Para tanto, o MCI estabelece que a disciplina e o uso da internet no país terão como princípio a proteção da privacidade e de dados pessoais, bem como garante aos usuários de internet o direito à **(a)** inviolabilidade da intimidade e da vida privada; **(b)** inviolabilidade e sigilo de suas comunicações privadas, salvo por ordem judicial.[174]

Por sua vez, em seu **Decreto regulamentador** (Decreto nº 8.771/2016), dados pessoais foram qualificados como qualquer dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa. O Decreto também estabeleceu diretrizes sobre padrões de segurança no tratamento de dados pessoais (art. 13) e

---

sanção pecuniária publicada no Diário Oficial da União em 14 de agosto de 2020. União. Diário Oficial da União - Seção 1. 2020. Disponível em: https://pesquisa.in.gov.br/imprensa/servlet/INPDFViewer?jornal=515&pagina=57&data=14/08/2020&captchafield=firstAccess. Acesso em 8.08.2022.

171 Ainda em 2020, o MPDFT propôs Ação Civil Pública 0736634-81.2020.8.07.0001 em face do Serasa Experian por indevida comercialização maciça de dados pessoais de brasileiros por meio dos produtos "Lista Online" e "Prospecção de Clientes" oferecidos pela ré. Em primeiro grau, o juiz de direito do Tribunal de Justiça de Brasília e Territórios (TJDFT) julgou procedente o pedido da autora para condenar a ré Serasa S.A. a se abster de comercializar dados pessoais dos titulares. Nos fundamentos, a sentença determinou que "mesmo para os dados públicos, exige-se o propósito legítimo e específico, a preservação dos direitos dos titulares e a observância das diretrizes básicas contidas na LGPD". O Serasa apelou e o TJDFT, em acórdão, negou provimento ao recurso, em vista da falta de transparência sobre o trâmite de coleta e tratamento dos dados.

172 "Ademais, o Marco Civil também traz um catálogo de direitos do usuário relacionados à privacidade e à proteção de dados (art. 7.°, I, II, III, VI, VII, IX, X e XI), que, interpretados em conjunto com os direitos do consumidor, acabam por formar um imponente arsenal de proteção da privacidade e dos dados pessoais do consumidor na internet." (MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, p. 37-69, 2018.)

173 Como apontam Carlos Affonso e Ronaldo Lemos (2016), à época o Brasil não possuía norma destinada especificamente à proteção de dados pessoais, motivo pelo qual "os dispositivos então inseridos no Marco Civil inauguravam o tratamento da tutela de dados no que diz respeito à rede no País. Até então se contava apenas com dispositivos ora muito genéricos, como o constante do artigo 21 do Código Civil, ora muito setoriais, como o artigo 43 do Código de Defesa do Consumidor."

174 No âmbito do Marco Civil da Internet, a proteção à privacidade é feita pela atribuição dos seguintes direitos aos usuários: "Art. 7º [...];" Trata-se, portanto, de norma que, não obstante sua natureza de legislação ordinária, densifica o comando constitucional e internacional sobre a privacidade do fluxo de comunicações. Ele é, substancialmente, a ponte que atualiza e adapta o alcance do direito à privacidade ao mundo digital. (Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental 403. Relator: Edson Fachin. Julgado em: 14/05/2020).

apresentou regras de minimização de dados (art. 13, § 2º, II). Com isso, o CDC e o MCI estabeleceram os fundamentos para a proteção de dados pessoais no país (MENDES, 2018).

Interessante notar que, alinhado a gerações anteriores de leis internacionais de proteção de dados pessoais, o MCI prevê o consentimento como pressuposto ao tratamento de dados pessoais. De fato, o art. 7º do MCI, que apresenta regulação voltada ao tratamento de dados pessoais, não foi fruto do mesmo nível de deliberação democrática que os demais dispositivos do Marco Civil, tendo sido incluído no texto da proposta pouco antes de sua aprovação e após a divulgação por Edward Snowden de que a Presidência da República teria suas conversas monitoradas pelo governo dos Estados Unidos.[175] Sobre isso relatam Ronaldo Lemos e Carlos Affonso Souza (2016):

> Mas, além das manifestações de 2013, outro fator foi especialmente determinante para o encaminhamento do Marco Civil da Internet. Trata-se das revelações feitas por Edward Snowden sobre o desenvolvimento de programas governamentais de espionagem, e em especial voltados para o governo brasileiro. De forma surpreendente, o Marco Civil foi escolhido como parte da resposta nacional aos escândalos envolvendo o aumento indiscriminado de vigilância e espionagem. Vale dizer que efetivamente havia pouco no Marco Civil da Internet que atacasse diretamente as questões envolvidas nos escândalos de espionagem, mas uma vez eleito pelo governo como uma ferramenta de resposta à situação colocada, o texto legal passou por algumas modificações. Duas foram as mudanças mais significativas empreendidas no texto do projeto de lei. A primeira dizia respeito ao incremento do atual artigo 7º, que trata da proteção da privacidade e dos dados pessoais. Compreensivelmente, ao Marco Civil foram acrescidos dispositivos que traziam para o corpo do projeto questões envolvendo a coleta e o tratamento de dados pessoais.

De todo modo, essa previsão do MCI está alinhada com normas de proteção de dados pessoais publicadas antes da edição do Regulamento Europeu de Proteção de Dados Pessoais (Regulamento 2016/679, também chamado de GDPR). Esse é, inclusive, padrão que prevalece na América Latina (mas também em países de outras regiões, como o Canadá),[176] em que leis destinadas à proteção de dados pessoais editadas antes de 2016 são centradas no consentimento dos titulares (ex.: Colômbia, México, Peru e Argentina). No entanto, como se verá adiante, esse desenho normativo focado no consentimento foi superado no Brasil pela LGPD, que prevê outras bases legais para o tratamento de dados pessoais e estabelece direitos aos titulares de dados. Esse mesmo movimento também é verificado nas mais recentes normas

[175] Vide: https://www12.senado.leg.br/emdiscussao/edicoes/espionagem-cibernetica/contexto-a-guerra-nao-declarada/denuncias-de-snowden-revelam-amplo-monitoramento. Acesso em 25.04.2021.

[176] Vide https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html. Acesso em 23.04.2022.

de proteção de dados pessoais, a exemplo da lei editada no Panamá[177] em 2019, na Tailândia[178] em 2019, no Equador[179] em 2021, na África do Sul[180] em 2013.

De todo modo, o Marco Civil da Internet tem sido utilizado para embasar investigações e ações relacionadas à proteção de dados pessoais. Por exemplo, em 2014 a Senacon sancionou a operadora Oi por monitorar a navegação de usuários na internet, compor e comercializar perfis de navegação dos mesmos para direcionamento de anúncios para melhorar a experiência de navegação.[181]

Em relação às informações de interesse público, a primeira norma a regular o tratamento de dados pessoais foi a **Lei nº 9.507/1997**, que prevê direitos de acesso e de retificação a informações pessoais e disciplina sobre o rito processual do *habeas data* (Constituição Federal, art. 5º, LXXII). Segundo dispõe a lei, o interessado poderá apresentar requerimento administrativo perante órgão ou entidade que detenha o registro ou banco de dados que se deseja acesso. Caso o pedido seja deferido e o solicitante verificar inexatidão de registro ou informação, poderá requerer sua retificação. Na hipótese de o pedido de acesso ou de retificação ser rejeitado, o interessado poderá ajuizar a ação judicial de *habeas data* para fazer valer o pedido rejeitado pela via administrativa.

No entanto, algumas de suas características impuseram desafios à efetividade da medida no Brasil. Como aponta Danilo Doneda (2008), a redação vaga do dispositivo constitucional exigiu do Poder Judiciário superar os entendimentos de que a ação seria personalíssima (ou seja, que só poderia ser apresentada pela pessoa sobre quem os dados se referem) e só poderia ser ajuizada contra entes públicos. Doneda também apontou que entre os fatores que limitaram a eficácia do *habeas data* foi a previsão de recurso ao poder judiciário nos casos de rejeição ao pedido administrativo previamente formulado, na medida em que o exercício de direitos por cidadãos seria condicionado a procedimento custoso e mediado por advogados.

---

[177] https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf. Acesso em 23.04.2022.

[178] https://www.dataguidance.com/legal-research/personal-data-protection-act-2019. Acesso em 23.04.2022.

[179] http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoicm8iLCJ1dWlkIjoiOTE1ZTIyMDQtY2Q1Zi00ZGMzLWFkYTAtNDE1OTRkNjgyNTEwLnBkZiJ9. Acesso em23.04.2022.

[180] https://www.dataguidance.com/sites/default/files/popia_2013.pdf. Acesso em 23.04.2022.

[181] Conforme o *release* da imprensa do Ministério da Justiça, a operadora possuía parceria com a empresa britânica Phorm. O foco era fornecer dados de perfis dos usuários para anunciantes, agências de publicidade e plataformas online. Considerou-se que a empresa violou a boa-fé e o princípio da transparência, já que os usuários não tinham qualquer informação sobre o uso de seus dados. Além disso, feriu o princípio da neutralidade de rede, por redirecionar o tráfego do consumidor e filtrar seus dados. Vide: https://www.justica.gov.br/news/ministerio-da-justica-multa-oi-por-monitorar-navegacao-de-consumidores-na-internet. Acesso em 23.04.2022.

Além disso, destaca que o procedimento regulado pela Lei de *habeas data* possui capacidade limitada de proteger os direitos à informação ou à intimidade porque apenas assegura ao indivíduo o acesso e retificação aos dados, sem ser garantido qualquer controle a respeito de como seus dados serão utilizados. Por esses motivos, Doneda (2008) argumenta que no Brasil o habeas data "não se presta absolutamente à proteção de dados pessoais". Como aponta, o *habeas data,* tal como construído pela legislação e prática brasileiras, não possui similar maleabilidade e adequação à sociedade da informação tal como verificado no *habeas data* de outros países sul-americanos. Por exemplo, na Colômbia, o instrumento é regulado de forma mais estruturada. Além de a lei claramente estabelecer que o *habeas data* pode ser oferecido contra entidades públicas e privadas, ela estabelece que a circulação de informações pessoais deve observar os princípios da confidencialidade, a finalidade e a segurança.[182]

Nesse cenário, e também focada no poder público, a **Lei de Acesso à Informação** (Lei nº 12.527/2011) foi editada com o intuito de superar as práticas de sigilo governamental e impor a divulgação de informações públicas como pressuposto, e acabou por estabelecer normas destinadas à proteção de dados pessoais de cidadãos quando da divulgação de dados mantidos por governos. Com esse intuito, determinou que o tratamento de informações pessoais,[183] consideradas como aquelas que permitem a identificação de uma pessoa natural, deve ser realizado de forma transparente e em respeito à privacidade e às outras liberdades e garantias individuais. Estabeleceu também que tais informações serão submetidas a acesso restrito, exceto diante de previsão legal ou de consentimento expresso da pessoa a que elas se referirem ou em casos como a realização de estatísticas, pesquisas científicas e diante do interesse público (LAI, art. 31 e Decreto nº 7.724/2012, arts. 55 a 58).

De fato, o art. 31 da LAI e os arts. 55 a 58 do Decreto nº 7.724/2012 vêm orientando as decisões a pedidos de acesso à informação em que os documentos solicitados possuem informações pessoais. Por exemplo, em caso paradigmático de 2015, a Controladoria Geral da União deu parcial provimento a recurso apresentado contra decisão da Fundação Casa de Rui Barbosa que, sob o argumento de proteção aos direitos autorais e à privacidade dos autores,

---

[182] Sobre o tema, vide publicação da Siperintendencia de Industria y Comercio (SIC), autoridade competente para a proteção de dados pessoais na Colômbia: https://www.sic.gov.co/manejo-de-informacion-personal. Acesso em 16.04.2022.

[183] Referida lei qualifica o dado como componente ou sinônimo de informação (art. 4, I da LAI). A informação pessoal, por sua vez, está "relacionada à pessoa natural identificada ou identificável", conceito similar àquele trazido pelo Decreto nº 8.771/2016, que regulamenta o Marco Civil da Internet (Lei nº 12.965/2014), na medida em que reconhece como pessoal o dado que, sozinho ou associado a outros dados, identifica ou permite identificar uma pessoa natural.

rejeitou pedido de acesso por pesquisador a poemas e cartas dos autores Manuel Bandeira e Vinícius de Moraes.[184] Segundo a Controladoria Geral da União (CGU), a reconstrução de fatos históricos com documentos mantidos pelo poder público qualifica-se como hipótese de interesse público capaz de excetuar o sigilo de informações pessoais previsto no art. 31 da LAI. Inclusive, o órgão argumentou que a não divulgação do conteúdo poderia se qualificar como medida de censura prévia e que eventual posterior lesão a direitos deverá ser pleiteada perante o poder judiciário.

6.3 Debates legislativos sobre o tratamento de dados mantidos pelo poder público

Neste tópico será abordado o processo normativo que culminou na aprovação da redação final da LGPD - lei de regência sobre tratamento de dados pessoais em geral. O objetivo será fornecer subsídios para a interpretação crítica dos dispositivos da LGPD sobre o tratamento de dados pessoais pelo poder público, que possuem grande imprecisão e cuja compreensão exige algum esforço interpretativo. De imediato, destaca-se que os contornos das regras aplicáveis ao uso de dados pessoais por governos foi fruto de divergência desde os primeiros textos legais que posteriormente viriam a se tornar a Lei de Proteção de Dados Pessoais.

Em 2010 foi publicada uma primeira minuta de Anteprojeto de Projeto de Lei de Proteção de Dados Pessoais.[185] No seu art 5º, a proposta determinava ser permitido o tratamento de dados pessoais por pessoas jurídicas de direito público para o cumprimento de suas funções institucionais e dentro dos limites da lei. A proposta também possuía capítulo dedicado a esse tratamento de dados (Capítulo IX), com dois dispositivos: um sobre a comunicação e interconexão de dados pessoais (art. 32) e outro sobre limites aos direitos de titulares de dados pessoais mantidos em bancos de dados públicos (art. 33).

Em síntese, o art. 32 determinava que a comunicação e interconexão de dados pessoais entre pessoas jurídicas de direito público somente seria permitido quando as competências dessas entidades fossem similares. No caso de pessoas jurídicas de direito público com

---

[184] Recurso disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/01590000162201501_CGU.pdf. Acesso em 24.04.2022.

[185] A primeira consulta pública realizada sobre dados pessoais pelo Ministério da Justiça ocorreu no ano de 2010. Disponível em: http://pensando.mj.gov.br/dadospessoais2011/debata-a-norma/. Acesso em 30.07.2022. Para mais informações, ver: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018. Acesso em 12.10.2020.

atribuições distintas, seria admitida a comunicação de dados quando houvesse previsão legal expressa ou quando necessária para a realização de suas competências institucionais. A comunicação era conceituada como "ato de revelar dados pessoais a um ou mais sujeitos determinados diversos do seu titular, sob qualquer forma" e a interconexão qualificada como "divulgação de dados de um banco de dados a outro, mantido ou não pelo mesmo proprietário, com finalidade semelhante ou distinta.".

Nesse sentido, o art. 32 apresentava maior restrição à divulgação de dados em comparação à revelação de dados, mas ambas as atividades deveriam ser realizadas para o cumprimento de obrigação legal expressa ou de atribuições institucionais das entidades públicas envolvidas. Por sua vez, o art. 33 autorizava os responsáveis por bancos de dados públicos a negar o cancelamento e a oposição de dados pessoais quando indispensável para a proteção da ordem pública, de direitos de terceiros, ou para não prejudicar a atuação judicial ou administrativa. Não havia norma sobre a comunicação ou interconexão de dados pelo poder público com entidades privadas.

Finalmente, os arts. 13 e 28 da proposta dispensavam a necessidade de obter consentimento para o tratamento de dados pessoais: (i) provenientes de registros, atos ou documentos públicos de acesso público irrestrito; e (ii) necessários para o exercício de funções próprias dos poderes do Estado. Por sua vez, o art. 21 estabelecia que dados sensíveis poderiam ser tratados quando: (i) manifestamente tornados públicos pelo seu titular; ou (ii) necessários para o exercício de funções próprias dos poderes do Estado.

Em 2015, quando da divulgação pelo MJ da segunda consulta pública para a elaboração de Anteprojeto de Lei de Proteção de Dados Pessoais, também havia regras específicas para o poder público,[186] ainda que não em capítulo específico para órgãos e entidades públicos. Em seu art. 2º, §3º, a proposta vedava aos órgãos e entidades públicas transferir para entidades privadas dados pessoais constantes de bases de dados que tenham acesso ou administram, salvo em casos de concessão e permissão de atividade pública que exija essa divulgação de dados e somente para essa finalidade. Em seguida, o art. 3º estabelecia que empresas públicas e sociedades de economia mista que atuem em regime de concorrência serão, para fins da proposta, equiparadas a pessoas jurídicas de direito privado.

[186] Por exemplo, vide os seguintes artigos: "**Art. 2º** Esta Lei aplica-se a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede e do país onde esteja localizado o banco de dados, desde que:". Disponível em: http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/. Acesso em 10.10.2020.

Por sua vez, os arts. 11 e 13 dispensavam a obtenção de consentimento quando o tratamento de dados, triviais ou sensíveis, fosse necessário para tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública. Já os arts. 24 e 25 regulavam a comunicação ou interconexão de dados pessoais mantidos por entidades de direito público.[187] Quando o receptor de dados fosse entidade privada, seria necessário o consentimento prévio do titular de dados, salvo (i) se aplicável outra base legal, (ii) nos casos de uso compartilhado de dados pessoais,[188] e (iii) quando houver prévia autorização de órgão competente, que avaliará o interesse público, adequação e necessidade da dispensa de consentimento, e desde que cumpridas obrigações complementares determinadas por órgão competente e que os titulares de dados sejam comunicados e permitidos a cancelar seus dados. Esses mesmos dispositivos dispensavam o consentimento para o tratamento de dados pessoais de acesso público irrestrito.

Dentro das sugestões apresentadas à Consulta Pública, que contou com mais de 1100 comentários (INTERNETLAB, 2016) de representantes de setores diversos, houve grande debate em torno da divulgação para entidades privadas de dados pessoais contidos em bases de dados públicas, com propostas que simplesmente removiam o poder público do escopo da proposta, que estabeleciam a anonimização por pressuposto, ou que abordaram a utilização da base legal do consentimento para as atividades de tratamento de dados pelo poder público.[189]

Após colhidas as manifestações oferecidas à consulta pública promovida pelo MJ, algumas das quais apontavam para a desigualdade nas regras aplicáveis aos setores público e privado,[190] a versão de Projeto de Lei encaminhada pela Presidência da República ao

---

[187] Segundo o APL, a comunicação consistia na "divulgação de dados pessoais a um ou mais sujeitos determinados diversos do seu titular, sob qualquer forma" e a interconexão na "divulgação de dados pessoais de um banco a outro, mantido ou não pelo mesmo proprietário, com finalidade semelhante ou distinta;". http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/. Acesso em 10.10.2020.

[188] Segundo o APL, o uso compartilhado de dados pessoais consiste em: "XVII – uso compartilhado de dados: a comunicação, a difusão, a divulgação internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos."

[189] https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf

[190] A exemplo das manifestações de: (i) Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação (GPOPAI), disponível em http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/07/07c449c076fabbb00f3d3b850e063417.pdf, (ii) da Câmara Brasileira de Comércio Eletrônico (Camara-e.net), disponível em: http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/07/c93b8d90f8a74403d2dd95c517059956.pdf; (iii) do Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal (Sinditelebrasil), disponível em: http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/07/eec2b997c68b9ce0f47dbddef376975a.pdf; (iv) da Telefônica do Brasil,

Congresso Nacional (na Câmara dos Deputados, PL nº 5.276/2016)[191] previa capítulo específico para regular tais atividades - em redação muito similar à final aprovada pelo Congresso Nacional no Projeto de Lei nº 4.060/2012,[192] ao qual o PL nº 5.276/2016 foi apensado.[193]

Em resumo, a proposta normativa enviada ao Congresso Nacional incluiu capítulo específico para regular o tratamento de dados pessoais pelo poder público (Capítulo IV), tal como previsto no texto apresentado para consulta pública em 2010. No capítulo constam: (a) regras gerais ao tratamento de dados pelo poder público, e (b) limitações e fiscalização ao uso compartilhado, comunicação e divulgação de dados pessoais pelo poder público.

Em relação às regras gerais, a proposta estabelece que qualquer tratamento de dados pessoais pelo poder público deverá ser realizado para o atendimento de sua finalidade pública, na persecução de um interesse público, tendo por objetivo a execução de competências legais ou o cumprimento de atribuições legais pelo poder público (art. 23). Essa redação se manteve na versão aprovada da LGPD e apresenta elementos importantes para orientar agentes públicos em suas atividades com dados pessoais. A proposta também determina que entes públicos divulguem, em local de fácil acesso informações claras e atualizadas sobre as atividades de tratamento de dados pessoais que realizam (art. 24). Além disso, esclarece que serão abrangidas pelas regras do Capítulo IV as pessoas jurídicas de direito público, sendo que as empresas públicas e sociedades de economia mista, naquilo que atuarem em regime de concorrência, serão equiparadas a entidades privadas (art. 25).

No que diz respeito ao uso compartilhado de dados pessoais, o anteprojeto dispõe que, quando realizado entre órgãos e entidades públicas, deverá atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas. Já

---

disponível em: http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/07/bd75964516e61608ae6d60d4924ea523.pdf, (v) da Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações (ABDTIC), disponível em: http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/07/ac4f4934b17b9c987a1edc9780f5d6d7.pdf, e (vi) da Escola de Direito de São Paulo da Fundação Getúlio Vargas (FGV Direito SP), disponível em: http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/07/ef64f4d964b58ecf1a9a5040efc25464.pdf. Acesso em 10.10.2020

[191] Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016. Acesso em 31.07.2022.

[192] CONGRESSO NACIONAL. Projeto de Lei 4060/2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências.Brasília, DF, 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=PL+4060/2012

[193] Interessante notar que, à época, já havia duas propostas normativas destinadas a regular o tratamento de dados pessoais (PL nº 4.060/2012 do Deputado Federal Milton Monti, e PL nº330/2013, do Senador Antônio Carlos Valadares).

a divulgação de dados a entidades privadas seria vedada, exceto em casos de descentralização de atividade pública que o exija, e exclusivamente para essa finalidade (art. 26). A comunicação de dados pessoais a outros órgãos públicos deverá ser publicizada (art. 28), e a divulgação e a comunicação de dados pessoais para particulares deverá ser informada à autoridade competente e não precisará de consentimento se: (a) houver outra base legal aplicável, e (b) nos casos de uso compartilhado de dados (art. 27).

A proposta não qualifica os conceitos de divulgação e comunicação, mas apresenta o conceito de uso compartilhado, que envolve leque amplo de atividades (art. 4º, XVII), incluindo a comunicação e a interconexão de dados (esse último conceito, nos textos enviados para consulta pública, era definido como a divulgação de dados). No entanto, a falta de conceito para comunicação e divulgação, bem como a forma em que esses conceitos são usados no Capítulo IV abrem espaços para dúvidas a respeito das regras aplicáveis ao uso compartilhado de dados pessoais.

Do que se depreende dessa proposta: (i) todo o uso compartilhado de dados pessoais entre órgãos públicos deveria buscar a execução de políticas públicas e as atribuições legais às respectivas entidades públicas; (ii) é vedada a divulgação (e não a comunicação) de dados a entes privados, salvo em situações restritas; (iii) a comunicação e divulgação de dados para particulares dependerá de consentimento quando não houver outra base legal aplicável (e em caso de uso compartilhado de dados pessoais, conceito que abrange a divulgação e a comunicação). Assim, em leitura seca da lei, parece ser permitida a comunicação de dados a particulares, desde que coletado o consentimento do titular de dados ou aplicável outra base legal. Já a divulgação somente será permitida para finalidades específicas e necessárias ao exercício de atividade pública descentralizada.

De todo modo, como se pode verificar, o Anteprojeto de Lei de Proteção de Dados Pessoais enviado pela Presidência da República ao Congresso Nacional, embora com similar racional das propostas iniciais, absorveu as contribuições apresentadas pelos participantes das consultas públicas realizadas em 2010 e 2015. A seguir consta quadro que mostra a evolução da regulação de tratamento de dados pessoais no âmbito do Poder Executivo:

Quadro 2: Tratamento de dados pelo poder público nas versões do Anteprojeto de Lei

	Texto da Consulta Pública de 2010	**Texto da Consulta Pública 2015**	**Texto enviado ao Congresso Nacional**
Bases legais	Dispensado o consentimento se dados forem usados para funções próprias do Estado (art. 13, III) para o cumprimento de obrigação legal (art. 13, I)	Dispensado o consentimento se tratamento e uso compartilhado for para observar leis ou regulamentos da administração pública (art. 11, II e 12, II, b) ou para o cumprimento de obrigação legal (art. 11, I e 12, I, a)	Tratamento ou uso compartilhado de dados triviais pode ser realizado pela administração pública para executar políticas públicas previstas em leis e regulamentos (art. 7º, III) ou para o cumprimento de obrigação legal (art. 7º, II). Para dados sensíveis, se aplicam as mesmas hipóteses, mas como dispensa de consentimento (art. 11, II, a e b)
Regras gerais para o uso de dados pelo poder público	Não há	Não há	Uso para o alcance de sua finalidade pública, para um interesse público, com objetivo de execução de competências e atribuições legais (art. 23). Necessidade de publicidade e indicação de encarregado (art. 24)
Compartilhamento com entes públicos	Comunicação e interconexão permitida quando entidades têm competências de matérias similares; ou Comunicação quando autorizado em lei ou necessária para cumprir com competências institucionais (art. 32)	Comunicação e interconexão sem consentimento se: - se aplicável outra base legal; - para uso compartilhado; - com autorização do órgão competente (art. 24)	Deve atender fim de execução de políticas públicas e atribuição legal, e observar os princípios da lei (art. 26). Publicidade da comunicação de dados (art. 28)
Compartilhamento com entes privados	Não dispõe.	Divulgação não autorizada, salvo se necessário para a execução descentralizada de atividades públicas (art. 2º, §3º)	Divulgação não autorizada, salvo se necessário para a execução descentralizada de atividades públicas (art. 26, pu). Consentimento dispensado para a **comunicação** e **divulgação** de dados se

			(art. 27): - houver outra base legal; - para uso compartilhado. Comunicação à autoridade (art. 27).
Uso de dados tornados públicos	Dispensado o consentimento para uso de dados em registros, atos ou documentos públicos de acesso público irrestrito (art. 13, III e 28, § 2º, I)	Dispensado o consentimento para dados triviais de acesso público irrestrito (art. 11 e art. 12, b, II)	Tratamento realizado de acordo com a lei e observando a boa-fé, finalidade e o interesse público que justificaram a divulgação (art. 7º, §4º)

A despeito dessa evolução das propostas normativas, especialmente no que diz respeito ao estabelecimento de balizas para o tratamento de dados pessoais pelo poder público, a terminologia utilizada na proposta enviada ao Congresso acabou por tornar confusa a redação dos dispositivos que regulam o uso compartilhado de dados pessoais com entes privados. Em especial, a proposta não conceitua os termos divulgação e comunicação, e não esclarece como eles se relacionam com as demais atividades contempladas no conceito de uso compartilhado de dados pessoais (e.g., o art. 27, II, apresenta o uso compartilhado de dados pessoais como uma exceção à necessidade de obter consentimento para a divulgação de dados para pessoas jurídicas de direito privado).

Para auxiliar na compreensão dos conceitos relacionados ao uso compartilhado de dados pessoais, seguir consta quadro com evolução dos conceitos:

Quadro 3: Conceitos de compartilhamento de dados nas versões do Anteprojeto de Lei

	Texto da Consulta Pública de 2010	**Texto da Consulta Pública 2015**	**Texto enviado ao Congresso Nacional**
Comunicação	Ato de revelar dados pessoais a um ou mais sujeitos determinados diversos do seu titular, sob qualquer forma (art. 4º, VIII)	Mesmo conceito (art. 5º, X)	Não há
Interconexão	Divulgação de dados de um banco de dados a outro, mantido ou não pelo mesmo proprietário, com finalidade semelhante ou distinta	Mesmo conceito (art. 4º, X)	Não há

	(art. 4º, X)		
Difusão	Ato de revelar dados pessoais a um ou mais sujeitos indeterminados diversos do seu titular, sob qualquer forma (art. 4º, IX)	Mesmo conceito (art. 4º, XII)	Não há
Uso compartilhado	Não há	A comunicação, a difusão, a divulgação internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos (art. 4º, XVII)	Mesmo conceito (art. 5º, XV)

Como mencionado, após a tramitação da proposta no Congresso Nacional (na Câmara dos Deputados, PL nº 5.276/2016, apensado ao PL nº 4.060/2012), o texto aprovado em 2018 possuía, no que diz respeito ao capítulo sobre o tratamento de dados pessoais pelo poder público, redação muito similar ao autógrafo enviado pelo Poder Executivo em 2016. Essa pequena modificação no texto originalmente proposto pela Presidência da República está relacionada, entre outros fatores, ao fato de ter havido disputa entre a Câmara dos Deputados e o Senado Federal em relação à condução da proposta normativa que viria a regular a proteção de dados pessoais no país (MOTA ALVES, 2020). De um lado, havia na Câmara dos Deputados ao menos duas propostas normativas sobre o tema (PLs nº 4060/2012 e nº 5.276/2016) e, de outro lado, no Senado Federal tramitou o PLS nº 330/2013.

Em geral, os debates legislativos foram realizados no escopo da Comissão Especial, instituída na Câmara dos Deputados para debater os PLs de proteção de dados pessoais. Além do trabalho de engajamento de diversos setores na construção de legislação com amplo apoio,

a referida Comissão promoveu em 2016 e 2017 onze audiências públicas e um seminário internacional sobre temas diversos relacionados à proteção de dados pessoais.[194]

No entanto, após a entrada em vigor da Regulação Europeia de Proteção de Dados Pessoais (*General Data Protection Regulation* ou GDPR), a ocorrência do escândalo de *Cambridge Analytica* e a perspectiva de o Brasil ser aceito na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), iniciou-se uma corrida entre as Casas legislativas para aprovar uma legislação de proteção de dados pessoais.[195] Nesse contexto, a Presidência passou a negociar com o Senado Federal os dispositivos sobre as atividades de tratamento de dados realizadas pelo poder público - com tentativas, inclusive, de excepcionar o poder público da regulação que se estava desenhando[196]-[197]. Diante da aprovação mais célere do

---

[194] https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018. Acesso em 12.10.2020.

[195] Nesse sentido, vide as manifestações – que em alguns pontos divergem – de Miriam Wimmer e de Fabrício Mota Pinto sobre essa corrida entre casas legislativas: "o que a gente percebeu ali na reta final da aprovação da lei é que havia uma verdadeira corrida entre as duas casas, a Câmara do Deputados e o Senado Federal. E havia dois projetos de lei que eram rivais embora não incompatíveis. Veja: o PLS 330 do senado havia sido relatado pelo ministro Aloysio Nunes que tinha tido um diálogo profícuo também com a Senacon na época e o PL5276 oriundo da própria Senacon. Então não eram projetos que apontavam direções diferentes mas eles tinham diferenças em termos da profundidade da abordagem. Talvez do grau de maturidade certas discussões, então 5276 claramente era o projeto muito mais detalhado, mais extenso que tinha já burilado alguns conceitos de uma maneira que o [PLS] 330 não havia não havia ainda feito e o governo federal naquele momento por razões políticas entendia que pega o PLS 330 era o caminho mais promissor, que era um projeto de lei com qual faria mais sentido dialogar em que apostava-se todas as fichas" (WIMMER, 2019) e "Com o fim do processo de impeachment e o afastamento da presidente Dilma e a posse efetiva do Temer como presidente, o governo Temer ele escolheu estrategicamente dialogar nesse assunto com o Senado. [...] Então o governo Temer dialogou com Ferraço até hoje eu sei que ele não dialogou com Orlando [PL 5276 da CD] para que se criasse um projeto que atendesse aos interesses da administração pública federal. Então o projeto do Ferraço [PLS 330 do Senado] começou a ganhar um corpo mais próximo de uma de uma junção de interesses tanto da academia (porque foi construído basicamente pela academia) e o setor empresarial e com o governo também, então era um projeto que tinha uma maturidade técnica e regulatória maior em relação ao setor público do que o próprio projeto do Orlando" MEMÓRIA DA LGPD. Observatório PPD – Miriam Wimmer – Video 05 em. 2020. Disponível em:https://www.youtube.com/watch?v=8eN9r9tcHKo. Acesso em: 12.12.2021. MEMÓRIA DA LGPD. Observatório PP– - Fabrici– - Video 10 EN. 2020. Disponível em: https://www.youtube.com/watch?v=nvhAEI2HJ7U. Acesso em 12.10.202.

[196] Nesse sentido se verifica manifestação de Renata Mielli: "Com a evolução da tramitação do 5276 na Câmara, houve um processo de acelerar também a tramitação do [PLS] 330, principalmente por parte de um setor do governo né que via no 330 a possibilidade de dizer: "olha temos um projeto de... temos uma lei de dados pessoais mas que não me envolve", então houve também um estímulo do governo para acelerar a tramitação do [PLS] 330 né... que teve uma tramitação muito [ela não termina a frase]... Se você for pegar lá o histórico da tramitação do [PLS] 330 é de um vai-e-vem imenso né, mas o último relator do projeto, que foi o Senador Ferraço, a gente tinha uma boa interlocução com ele, uma boa interlocução com assessoria tanto pro Aloysio como para o Fabrício, bom [...] a gente estabeleceu uma relação política importante com ele e não ignoramos o projeto" Disponível em: https://www.youtube.com/watch?v=_lFd-4UdUjI. Acesso em 12.10.2020

[197] O mesmo é sentido na fala do Senador Aloysio Nunes: "Houve na tramitação do lado de órgãos do governo [...] algum mau humor em relação à limitação de utilização de dados que são recolhidos por órgãos do governo. Houve isso sim. E a gente vê… você pode avaliar, por exemplo, o que pode fazer um governo manipulando ou tratando para traçar perfis de pessoas que têm acesso ao financiamento público (tipo minha casa minha vida, fies, o sistema previdenciário). Então havia bastante preocupação com esse tema... Havia a questão da segurança, o que fazer com a segurança... sempre paira essa questão da segurança como um álibi

texto da Câmara dos Deputados, essa negociação de dispositivos entre Presidência e Senado Federal não foi refletida no texto final da LGPD. Ressalte-se, todavia, como já mencionado, que os dispositivos sobre tratamento de dados pelo poder público foram alvo de debates desde a consulta pública promovida pelo Ministério da Justiça e em audiências públicas realizadas pela Câmara dos Deputados.

Em síntese, as mudanças, conforme especificadas no quadro abaixo são: (a) ampliação da base legal do art. 7º, III, de modo a permitir que o tratamento de dados triviais pela administração pública para a execução de políticas públicas seja respaldado em contratos, convênios ou instrumentos congêneres; (b) a previsão de proteção aos dados pessoais dos requerentes de acesso à informação, vedado o seu compartilhamento; (c) determinação que órgãos e entidades do poder público devem manter bases de dados em formato interoperável e estruturado para o uso compartilhado para a execução de políticas públicas, serviços públicos, a descentralização da atividade pública e a disseminação de dados; e (d) ampliação das exceções ao uso compartilhado de dados pessoais para incluir a existência de previsão legal, a divulgação respaldada em contratos, convênios ou instrumentos congêneres, e os casos em que dados forem acessíveis publicamente.

Quadro 4: Mudanças promovidas ao Projeto de Lei pelo Congresso Nacional

	Texto enviado ao Congresso Nacional	**Texto aprovado pelo Congresso Nacional**

para esconder alguns interesses que nem sempre são confessáveis". Disponível em: https://www.youtube.com/watch?v=ZXEiaKiJVqU. Acesso em 12.10.2020.

Bases legais	Tratamento ou uso compartilhado de dados triviais pode ser realizado pela administração pública para executar políticas públicas previstas em leis e regulamentos (art. 7º, III) ou para o cumprimento de obrigação legal (art. 7º, II). Para dados sensíveis, se aplicam as mesmas hipóteses, mas como dispensa de consentimento (art. 11, II, a e b)	Tratamento ou uso compartilhado de dados triviais pode ser realizado pela administração pública para executar políticas públicas previstas em leis e regulamentos **ou respaldada em contratos, convênios ou instrumentos congêneres** (art. 7º, III) ou para o cumprimento de obrigação legal (art. 7º, II). Para dados sensíveis, se aplicam as mesmas hipóteses, mas como dispensa de consentimento **não podendo ser fundamentado em contratos, convênios ou instrumentos congêneres** (art. 11, II, a e b)
Regras gerais para o uso de dados pelo poder público	Uso para o alcance de sua finalidade pública, para um interesse público, com objetivo de execução de competências e atribuições legais (art. 23). Necessidade de publicidade e indicação de encarregado (art. 24)	Uso para o alcance de sua finalidade pública, para um interesse público, com objetivo de execução de competências e atribuições legais (art. 23). Necessidade de publicidade e indicação de encarregado (art. 23, I e III) **Proteção de dados pessoais dos requerentes de acesso à informação, vedado o seu compartilhamento** (art. 23, II)**.**
Regras gerais ao compartilhamento	Não há	**Os dados devem ser mantidos em formato interoperável e estruturado para o uso compartilhado para a execução de políticas públicas, serviços públicos, à descentralização da atividade pública e à disseminação de dados (art. 25)**
Compartilhamento com entes públicos	Deve atender fim de execução de políticas públicas e atribuição legal, e observar os princípios da lei (art. 26). Publicidade da comunicação de dados (art. 28)	Deve atender fim de execução de políticas públicas e atribuição legal, e observar os princípios da lei (art. 26). Publicidade da comunicação de dados (art. 28)
Compartilhamento com entes privados	Divulgação não autorizada, salvo se necessário para a execução descentralizada de atividades públicas (art. 26, pu). Consentimento dispensado para a **comunicação** e **divulgação** de dados se (art. 27):	Divulgação não autorizada, salvo se necessário para a execução descentralizada de atividades públicas; **quando houver previsão legal e a divulgação seja respaldada em contratos, convênios ou instrumentos congêneres; ou nos casos em que dados forem acessíveis publicamente** (art. 26,

	- houver outra base legal; - para uso compartilhado. Comunicação à autoridade (art. 27).	pu). Consentimento dispensado para a **comunicação** e **divulgação** de dados se (art. 27): - houver outra base legal; - para uso compartilhado; **- nas exceções do art. 26**. Comunicação à autoridade (art. 28).
Uso de dados tornados públicos	Tratamento realizado de acordo com a lei e observando a boa-fé, finalidade e o interesse público que justificaram a divulgação (art. 7º, §4º)	Tratamento realizado de acordo com a lei e observando a boa-fé, finalidade e o interesse público que justificaram a divulgação (art. 7º, §3º). **Dispensa de consentimento para o tratamento de tornados manifestamente públicos pelo titular de dados (art. 7º, §4º)**.

Após a aprovação pela Câmara dos Deputados da versão final do Projeto de Lei nº 4.060/2012, o texto foi encaminhado para sanção presidencial, momento no qual sofreu veto em dispositivos sobre o uso de dados pelo poder público. Entre os dispositivos vetados pela Presidência da República estavam: (i) a vedação ao compartilhamento, para entidades públicas ou privadas, de dados sobre solicitantes de acesso à informação (art. 23, II);[198] (ii) a exigência de publicidade sobre as atividades de comunicação de dados pessoais entre órgãos e entidades de direito público ou com particulares (art. 28);[199]-[200] e (iii) a exceção à divulgação de dados com particulares consistente na existência de previsão legal ou o respaldo em contratos, convênios ou instrumentos congêneres (art. 26, II, § 1º).[201] Ao que consta, os

[198] A justificativa para tanto foi "O dispositivo veda o compartilhamento de dados pessoais no âmbito do Poder Público e com pessoas jurídicas de direito privado. Ocorre que o compartilhamento de informações relacionadas à pessoa natural identificada ou identificável é medida recorrente e essencial para o regular exercício de diversas atividades e políticas públicas. É o caso, por exemplo, do banco de dados da Previdência Social e do Cadastro Nacional de Informações Sociais, cujas informações são utilizadas para o reconhecimento do direito de seus beneficiários e alimentados a partir do compartilhamento de diversas bases de dados administrados por outros órgãos públicos. Ademais, algumas atividades afetas ao poder de polícia administrativa poderiam ser inviabilizadas, a exemplo de investigações no âmbito do Sistema Financeiro Nacional, dentre outras."

[199] Apesar do veto, tendo em vista que as atividades referidas estão compreendidas no conceito de tratamento de dados, consideramos que o poder público não está dispensado da obrigação de transparência em relação à previsão legal, à finalidade, aos procedimentos e às práticas do compartilhamento de dados que realiza.

[200] A justificativa para tanto foi: "A publicidade irrestrita da comunicação ou do uso compartilhado de dados pessoais entre órgãos e entidades de direito público, imposta pelo dispositivo, pode tornar inviável o exercício regular de algumas ações públicas como as de fiscalização, controle e polícia administrativa."

[201] A justificativa apresentada para tanto foi: "A redação do dispositivo exige que haja, cumulativamente, previsão legal e respaldo em contratos, convênios ou instrumentos congêneres para o compartilhamento de dados pessoais entre o Poder Público e entidades privadas. A cumulatividade da exigência estabelecida no

órgãos do governo federal convocados para manifestação sobre a proposta se mostraram reativos a diversos dispositivos, visto que não tinham se envolvido na construção da proposta aprovada no Congresso Nacional.[202]

Após cerca de oito anos desde a primeira consulta sobre o tema (2010), em agosto de 2018 foi aprovada a Lei de Proteção de Dados Pessoais (Lei nº 13.709/2018 ou LGPD). No entanto, isso não significou a estabilização dos dispositivos sobre tratamento de dados pelo poder público. Isso porque, pouco após, em dezembro de 2018, a Presidência da República editou a Medida Provisória (MP) nº 869/2018 que, entre outras disposições, modificou regras relacionadas ao tratamento de dados pessoais pelo poder público.

Em particular, a MP nº 869/2018 mudou os artigos 26 e 27 da LGPD para: **(a)** determinar a comunicação da Autoridade quando houver divulgação de dados pelo poder público com entes privados; e **(b)** inserir novamente no texto legal disposições sobre compartilhamento de dados por entes públicos removidas durante a tramitação do PL no Congresso Nacional ou por veto presidencial. Isso resultou na ampliação das hipóteses em que seria autorizada a divulgação de dados pessoais com entidades privadas, a saber: **(i)** indicação de encarregado para as operações de tratamento de dados pessoais (em versões anteriores da proposta, essa obrigação residia no art. 23 e era aplicável a qualquer ente público que trate dados pessoais); **(ii)** previsão legal ou a divulgação for respaldada em contratos, convênios ou instrumentos congêneres; **(iii)** casos em que a divulgação dos dados objetivar a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados (essa hipótese não esteve em outras versões da proposta); ou **(iv)** nos casos em que os dados forem acessíveis publicamente.

Interessante que os arts. 26 e 27 da LGPD, tal como aprovados pelo Congresso Nacional, apresentavam problemas de técnica legislativa que tornava de difícil compreensão as regras sobre uso compartilhado de dados pessoais pelo poder público. No entanto, as modificações feitas pela Medida Provisória não removeram essa ausência de clareza e acabaram por ampliar e intensificar as incertezas existentes. Por exemplo, a obrigação de

---

dispositivo inviabiliza o funcionamento da administração pública, já que diversos procedimentos relativos à divulgação de dados pessoais encontram-se detalhados em atos normativos infralegais, a exemplo do processamento da folha de pagamento dos servidores públicos em instituições financeiras privadas, a arrecadação de taxas e tributos e o pagamento de benefícios previdenciários e sociais, dentre outros."

[202] "Foi um processo muito complexo por que repentinamente foram chamados à mesa dezenas de órgãos públicos que tinham tido pouco ou nenhum envolvimento com o tema até aquele momento e obviamente a reação era... não vou dizer de pânico, mas era uma reação defensiva, tipo "essa lei vai impactar nesse, nesse, nesse aspecto, então vamos propor um monte de veto" e eu acho que foi muito revelador do grau de distanciamento que havia do poder executivo com relação a discussão no Congresso Nacional" Disponível em: https://www.youtube.com/watch?v=87kDGMwgoc0. Acesso em 12.10.2020.

nomeação de encarregado não deveria estar atrelada às atividades de divulgação de dados, mas ser uma obrigação aplicável a qualquer ente público que atue como controlador de dados pessoais.

Na tramitação da MP nº 869/2018 no Congresso Nacional, foram oferecidas cerca de 170 emendas à sua redação, muitas das quais propunham mudanças a respeito do tratamento de dados pelo poder público. O tema dessas emendas direcionadas pode ser agrupado em quatro focos, apresentados no quadro a seguir.

Quadro 5 - Emendas Parlamentares à MP nº 869/2018

Emendas parlamentares na MP nº 869/2018	**Número da emenda e proponente**
Art. 7º, § 7º. O tratamento de dado pessoal tornado manifestamente público pelo titular ou de acesso público poderá ser realizado para fim diverso daquele para o qual os dados pessoais foram coletados, se houver compatibilidade de finalidade, observados os propósitos legítimos e específicos do novo tratamento e a preservação dos direitos do titular previstos nesta Lei.	Nº 112 Dep. Eduardo Barbosa
Art. 23-A. Cabe às 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) a proteção e preservação dos dados pessoais de requerentes de acesso à informação, nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação). Parágrafo único. Fica vedado o compartilhamento de dados pessoais de requerentes de acesso à informação no âmbito do Poder Público e com pessoas jurídicas de direito privado.	Nº 69, 57, 16, 125, 141, 152, 194, 159, 51 Sen. Humberto Costa, Dep. Sergio Vidigal, Dep. Orlando Silva, Sen. Rogério Carvalho, Dep. Sâmia Bonfim, Dep. Marcelo Freixo, Dep. Talíria Petrone, Dep. Paulo Pimenta, Dep. Ivan Valente
Suprime o Art. 26, §1º, III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.	Nº 160, 23, 64, 153, 140, 109, 88, 52, 38 Dep. Paulo Pimenta, Dep. Orlando Silva, Sen. Humberto Costa, Dep. Marcelo Freixo, Dep. Sâmia Bonfim, Dep. Talíria Petrone, Dep. Alessandro Molon, Dep. Ivan Valente, Dep. Celso Russomano
"27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à Autoridade Nacional de Proteção de Dados e dependerá de consentimento do titular, exceto"	Nº 93, 122 Senador Izalci Lucas, Dep. Túlho Gadêlha

Como se verifica, um primeiro foco de emendas apresentadas à MP nº 869/2018 está no art. 26 da LGPD, que regula o compartilhamento de dados pessoais mantidos pelo poder público. Buscou-se, **(i)** determinar a obrigatória notificação à ANPD dos casos de compartilhamento de dados entre órgãos públicos e entidades privadas; e **(ii)** obter a supressão de dispositivo incluído na LGPD pela MP (art. 26, §1º, III) que permite a divulgação de dados

a particulares mediante a indicação de encarregado. Segundo a justificativa apresentada, o encarregado é pressuposto de todo tratamento de dados pessoais e não uma hipótese de permissão da divulgação a entidades privadas de dados pessoais mantidos pelo poder público. Um segundo foco de emendas buscou estabelecer entre as competências da ANPD o monitoramento das atividades de tratamento de dados pessoais realizadas pelo poder público.

Outros dois focos de mudança, mas propostos por menor quantidade de parlamentares, foi destinado a: **(a)** permitir o tratamento posterior para novas finalidades de dados pessoais manifestamente tornados públicos pelo titular de dados, desde que observados propósitos legítimos e específicos e a preservação do previsto na lei; e **(b)** reinserir na LGPD os cuidados ao tratamento de dados pessoais de cidadãos que formulam pedidos de acesso à informação com base na Lei n° 12.527/2011.

Ao final, a versão final da MP nº 869/2018, aprovada pelo Congresso Nacional em 29 de maio de 2019, na forma do Projeto de Lei de Conversão (PLV) nº 7/2019, foi convertida na Lei nº 13.853/2019. Entre as mudanças promovidas à LGPD, aquelas relativas ao tratamento de dados pessoais pelo poder público foram: **(a)** a obrigação de nomeação de encarregado foi restituída ao art. 23, sendo aplicável a qualquer ente público que atue como controlador de dados pessoais; **(b)** autorização da divulgação de dados pelo poder público a particulares quando: (b.i) houver previsão legal ou a divulgação for respaldada em contratos, convênios ou instrumentos congêneres; e (b.ii) objetivar a prevenção de fraudes e irregularidades, ou proteger a segurança e a integridade do titular de dados; **(c)** necessidade de regulamentação sobre a comunicação à autoridade competente a respeito do uso compartilhado de dados pessoais; e **(d)** possibilidade de a autoridade solicitar a entes públicos informações sobre os tratamentos realizados. Em relação aos dados de acesso público ou tornados manifestamente públicos pelo titular de dados, as mudanças realizadas autorizam seu tratamento posterior, desde que observados propósitos legítimos e específicos para o novo tratamento (art. 7º, §7º).

6.4 Regulação pela LGPD do tratamento de dados mantidos pelo poder público

Finalmente, a **Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/2018 ou "LGPD"), editada em 14 de agosto de 2018, trata da proteção de dados pessoais de forma abrangente e transversal, não estando restrita a determinadas políticas ou setores. Seus

dispositivos se aplicam a qualquer operação de tratamento de dados pessoais realizada,[203] por particulares ou pessoas jurídicas de direito público, de todas as instâncias federativas, em território nacional ou com dados de indivíduos localizados no território nacional, em meio digital ou físico.

A LGPD se aplica às operações de tratamento de dados pessoais (i) realizadas no território nacional; (ii) cuja atividade de tratamento vise a oferta ou o fornecimento de bens ou serviços no território nacional; (iii) realizadas em relação a dados de indivíduos localizados no território nacional; ou (iv) quando os dados pessoais objeto do tratamento tenham sido coletados no território nacional (art. 3º, I a III). Assim, considerando que atividades de tratamento de dados pessoais realizadas por órgãos ou entidades públicas brasileiras sempre serão realizadas, ao menos em parte, em território nacional e com dados de indivíduos localizados no território nacional, aplica-se sempre o disposto na LGPD.

Seus dispositivos se aplicam às operações de tratamento de dados realizadas por pessoas físicas ou jurídica, de direito privado ou público, salvo aquelas realizadas para finalidades (a) particulares e não econômicas, (b) jornalísticas, (c) acadêmicas, ou (d) de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Para essas últimas exceções, a LGPD estabelece que deverá ser editada legislação específica.[204] O conceito e alcance de certas exceções depende de esclarecimento.

De modo geral, essas atividades deverão estar contempladas em alguma das hipóteses legais para o tratamento de dados pessoais (e.g.: consentimento, obrigação legal ou regulatória, legítimo interesse etc.), observar a boa-fé e respeitar os princípios de tratamento de dados pessoais previstos na lei (e.g.: finalidade, necessidade, livre acesso, transparência,

---

[203] A definição de tratamento de dados pessoais envolve quaisquer operações realizadas com referidos dados, incluindo as atividades de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, divulgação e extração de dados.

[204] Para tanto, a Câmara dos Deputados constituiu, em novembro de 2019, comissão de juristas responsável pela elaboração de anteprojeto de lei sobre o tema. De todo modo, mesmo enquanto não forem editadas essas normas, aplicam-se as vigentes normas, como os arts. 13 e 15 da Lei nº 12.965/2014, que tratam da guarda e fornecimento de conexão à internet e de acesso a aplicações, além de regras como as que determinam o sigilo de comunicações, assegurado pelo art. 5º, XII da Constituição Federal, ou o sigilo bancário, nos termos da Lei Complementar nº 105/2001. Essa Comissão apresentou o anteprojeto de lei para o Presidente da Câmara dos Deputados, em novembro de 2020, mas ele não foi apresentado por nenhum dos deputados federais para que, então, fosse apreciado pela casa. Para além do texto apresentado pelo Comissão, o deputado Coronel Armando apresentou o PL 1515/2022, que regula a proteção de dados no âmbito penal e guarda semelhança com o anteprojeto em alguns dispositivos. Este projeto está tramitando na Câmara dos Deputados.

segurança, não discriminação e responsabilização e prestação de contas).[205] Além disso, a lei exige que esses agentes assegurem meios para o exercício de direitos por titulares de dados (ex.: acesso, portabilidade, correção e revisão de decisões automatizadas) e observem boas práticas de segurança da informação. Esses aspectos da lei serão abordados em maiores detalhes adiante.

Também recomenda aos agentes de tratamento de dados adotarem programa de governança em que estabeleçam as condições de organização e os procedimentos para assegurar aderência de suas práticas às exigências da lei. Nesse contexto, estabelece que os programas de governança deverão contar com medidas como a nomeação de um encarregado para atuar como canal de comunicação com indivíduos e autoridades, a observância de normas e padrões técnicos de segurança da informação, e a implementação de meios para que titulares exerçam seus direitos (art. 50).

Outra exigência ao controlador de dados pessoais consiste em elaborar **documentação para registrar as atividades** de tratamento de dados pessoais que realiza, bem como detalhar as condições em que ocorre e quais as salvaguardas adotadas para reduzir possíveis riscos a direitos fundamentais de titulares de dados pessoais. Esse registro de atividades pode seguir metodologias diversas e é comumente denominado de Record of Processing Activities (RoPA). Nesse momento, o controlador deverá avaliar se o tratamento realizado possui o potencial de gerar riscos à liberdade, intimidade ou privacidade dos titulares, inclusive de forma a impossibilitar ou prejudicar o exercício de qualquer um dos direitos previstos na LGPD. Caso esse elevado risco seja identificado, deverá ser elaborado **Relatório de Impacto à Proteção de Dados Pessoais** (ou RIPD), consistente em ferramenta para auxiliar na tomada de decisão sobre a forma em que o tratamento será realizado, por meio da identificação de possíveis riscos e desenvolvimento de plano para sua mitigação.

Para assegurar que essas regras serão observadas, a lei instituiu autoridade com capacidade normativa e sancionatória relacionada a dados pessoais (a **Autoridade Nacional**

---

[205] Esses princípios são expressamente referidos na LGPD, mas podem ser identificados em normas diversas, como a LAI, o CDC e o Marco Civil, e foram inspirados pelos princípios estabelecidos nas FIPPS e na GDPR. Ilustrativamente, a versão dos FIPPS da União Europeia determina que o tratamento de dados pessoais deverá observar os seguintes elementos: (i) transparência: titulares de dados devem ser informados sobre as atividades de tratamento realizadas com seus dados pessoais, (ii) escolha: titulares de dados devem poder escolher e consentir com o tratamento de seus dados pessoais; (iii) acesso e participação: titulares de dados devem ser assegurados mecanismos fáceis e gratuitos para ver quais dados são coletados e para contestar as atividades de tratamento realizadas; (iv) agentes de tratamento de dados devem assegurar a veracidade e segurança dos dados pessoais que coletam; (v) enforcement: para garantir que agentes de tratamento de dados pessoais observarão esses princípios, devem ser assegurados mecanismos de exequibilidade.

de Proteção de Dados Pessoais ou "ANPD"). Instituída por força da Lei nº 13.853/2019, a autoridade foi originalmente constituída como parte integrante da estrutura da Presidência da República, tendo assumido a forma de autarquia por força da Lei nº 14.460/2022, e possui entre suas competências a edição de normas, fiscalização e a aplicação de sanções administrativas.[206] Ela também deverá promover consultas públicas sobre temas relacionados à proteção de dados pessoais e coordenar sua atuação com órgãos públicos com competências complementares às suas. Especificamente em relação ao poder público, a LGPD atribui à ANPD competência para solicitar informações sobre as atividades de tratamento realizadas e emitir informe ou parecer destinado a assegurar o cumprimento da Lei ou o término de irregularidades. Inclusive, a ANPD elaborou guia sobre o tratamento de dados pelo poder público, em que apresenta interpretação inicial sobre a aplicação dos princípios e bases legais por órgãos e entidades públicas, assim como sobre os limites e possibilidades de compartilhamento de dados mantidos pelo poder público.[207] A LGPD também atribuiu à ANPD a possibilidade de normatizar e fiscalizar agentes públicos pelo descumprimento das normas de proteção a dados pessoais. Especificamente, atribui à autoridade competência para elaborar normas sobre o tratamento de dados por órgãos da administração pública e de solicitar às entidades públicas informações sobre as atividades de tratamento realizadas e emitir informe ou parecer técnico destinado a assegurar o cumprimento da Lei ou o término de práticas irregulares. [208]-[209]-[210]

---

[206] Conforme argumentado em artigo do Jota "Essa estrutura muito difere do modelo vetado pelo Presidente da República, que submetia a ANPD a regime autárquico especial e vinculada ao Ministério da Justiça e dotada de autonomia técnica – e, portanto, mais alinhado à experiência brasileira de agências reguladoras. Embora seja assegurada autonomia técnica à ANPD, o vínculo à Presidência da República representa um grave prejuízo à sua independência – apesar de regras de a MP prever a existência de mandato e condições de perda de cargo análogas às aplicáveis aos órgãos reguladores. Trata-se ainda de diferença marcante em relação ao texto original da LGPD, que determinava a independência administrativa e a ausência de subordinação hierárquica como algumas das características da natureza de autarquia especial conferida à ANPD." (LEMOS; *et. al*, 2018)

[207] Para mais informações, acesse: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico___defeso_eleitoral.pdf.

[208] Sobre isso, interessante notar que o Presidente da República, ao editar a Medida Provisória nº 869/2018 ("MP"), modificou a LGPD para remover a obrigação de comunicação dessas atividades à ANPD. No entanto, após a tramitação da MP pelo Congresso Nacional, a redação original da LGPD foi retomada e, com isso, também a obrigação de comunicação à Autoridade das práticas de compartilhamento de dados pessoais. De forma similar, ao sancionar a LGPD, o Presidente da República vetou dispositivo que exigia a publicidade no sítio eletrônico dos órgãos públicos que realizam o compartilhamento de dados pessoais entre órgãos e entidades de direito público. Esse dispositivo, embora não tenha sido realocado no texto legal, está em alguma medida contemplado pela obrigação de publicidade incidente sobre todas as atividades de tratamento de dados pessoais pelo governo.

[209] Texto legal original (e mantido): "Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto [...]". Texto legal conforme Medida Provisória nº 869/2018:

Essas regras e princípios estabelecidos pela LGPD, assim como as competências da ANPD, são direcionadas tanto a particulares como ao poder público, mas não de forma idêntica para cada um dos agentes (WIMMER, 2020). Essas disposições deverão ser interpretadas e aplicadas levando em consideração as particularidades dos serviços que prestam e tendo em vista as demais normas e princípios incidentes sobre suas atividades, a exemplo dos princípios constitucionais, aplicáveis à administração pública, da legalidade, impessoalidade e eficiência, como será mais detidamente analisado nesta tese. De todo modo, além das disposições gerais aplicáveis de forma transversal a qualquer agente de tratamento de dados pessoais, a LGPD possui capítulo destinado especificamente às atividades de tratamento de dados pelo poder público que, embora não resolva certas dúvidas sobre como interpretar a LGPD para esse setor, apresenta orientações relevantes para guiar suas atividades.

Esse capítulo basicamente **(i)** estabelece as condições dentro das quais poderá ocorrer o compartilhamento de dados mantidos pelo poder público (arts. 25 a 27), **(b)** exige que o poder público deverá orientar suas atividades de tratamento de dados pessoais ao alcance do interesse público e à execução de competências ou atribuições legais (arts. 23, 25 e 26); e **(c)** reforça a necessidade de transparência sobre essas atividades (art. 23, I, 26, § 2º e 27) e a capacidade fiscalizatória da ANPD sobre a atuação do poder público (27 a 30).

Em relação às condições para o uso compartilhado de dados pessoais, a LGPD requer aos entes públicos manter dados em formato interoperável e estruturado para o uso compartilhado entre órgãos públicos, para viabilizar a descentralização da atividade pública e o acesso das informações pelo público em geral. No entanto, reforça que o compartilhamento de dados entre entidades do poder público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal.[211] Assim, ao mesmo tempo em que a LGPD reconhece

---

"Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa jurídica de direito privado dependerá de consentimento do titular, exceto [...]"

[210] Nas razões de veto, o Presidente afirmou que: *"*A publicidade irrestrita da comunicação ou do uso compartilhado de dados pessoais entre órgãos e entidades de direito público, imposta pelo dispositivo, pode tornar inviável o exercício regular de algumas ações públicas como as de fiscalização, controle e polícia administrativa.*"*

[211] Essa solicitação de participantes da Consulta Pública realizada pelo Ministério da Justiça para a elaboração do Anteprojeto de Lei de Proteção de Dados Pessoais, como relatado pela associação InternetLab (2016) em relatório de acompanhamento do debate público realizado à época: " Joana Varon, Luiz Perin Filho, Proteste e Veridiana/Intervozes e GPoPAI sugeriram, no escopo da Consulta, que fosse delimitada a hipótese do consentimento com relação ao compartilhamento de dados para o exercício de direitos ou deveres em leis ou regulamentos da administração pública, exigindo-se um dever de anonimização e a observância de todos os princípios previstos na lei [inciso II]: "Trata-se de uma exceção ao consentimento muito ampla. Ela deve, explicitamente, sujeitar-se a todos os princípios elencados no artigo 6° desta lei, bem como prever a anonimização de dados, sempre que possível ou compatível com a finalidade da utilização do dado [Joana].

a importância do compartilhamento de dados entre órgãos e entidades públicos, ela exige que sejam estabelecidos procedimentos para assegurar a observância ao princípio da finalidade e ao alcance do interesse público, bem como para verificar a adequação da solicitação de acesso realizada em relação às atribuições legais do órgão ou entidade solicitante.

Para o compartilhamento com particulares, esclarece as situações em que será permitido ou quando dependerá de consentimento. Assim, o compartilhamento de dados pessoais com particulares é considerado vedado, salvo se presentes as seguintes exceções: **(i)** execução descentralizada de atividade pública que exija a divulgação, exclusivamente para esse fim específico e determinado, sendo exigida transparência sobre essas atividades; **(ii)** previsão legal ou a divulgação for respaldada em contratos, convênios ou instrumentos congêneres; **(iii)** casos em que a divulgação dos dados objetivar a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados; ou **(iv)** casos em que os dados forem acessíveis publicamente.

Na prática, a autorização para o compartilhamento de dados por parte do poder público, para entes públicos ou privados, é bastante ampla. Os limites a essas práticas recaem sobre os princípios (LGPD, art. 6º), bases legais (LGPD, arts. 7º e 11), que são igualmente aplicáveis a entes privados que realizam atividades de tratamento de dados pessoais, bem como à necessidade de observar o interesse público e as competências ou atribuições legais dos órgãos ou entidades públicos envolvidos (LGPD, art. 23).

De todo modo, verifica-se que a publicação e o compartilhamento, com entes públicos ou privados, de dados pessoais mantidos pelo poder público possuem como requisito em comum a avaliação prévia do interesse público (além das exigências aplicáveis a qualquer atividade de tratamento de dados pessoais, como a observância da finalidade e transparência). Tal como na LAI, a LGPD não estabelece parâmetros para auxiliar o gestor público a identificar a existência de interesse público no compartilhamento e publicação de dados pessoais.

Ainda que para as atividades da administração pública e realização de políticas públicas seja muitas vezes necessário o tratamento de dados sem consentimento específico do seu titular. Os riscos de mau uso que podem se desdobrar dessa compreensão inicial devem ser minimizados mediante tais mecanismos de controle. Sugeriram, ainda que a hipótese com relação ao compartilhamento de dados para o exercício de direitos ou deveres em leis ou regulamentos da administração pública, se submetesse aos princípios da necessidade do APL e da eficiência da administração pública [inciso II]:"Essa previsão é, extremamente genérica, devendo-se vincular aos princípios da necessidade do APL e da eficiência da administração pública. Isso, em tese, restringiria essa hipótese que, da forma como está redigida, é extremamente permissiva ao Estado."

A LGPD também apresenta normas que serão aplicáveis à publicação de dados pessoais pelo poder público. No art. 7º, §§3º e 7º, a LGPD reconhece que dados pessoais poderão ser publicados em políticas de transparência e dados abertos, e, em conjunto com o art. 23, estabelece balizas para o posterior tratamento dos dados tornados públicos, consistentes na determinação de que a utilização posterior desses dados deverá estar respaldada na boa-fé, buscar o interesse público, e ser destinada ao alcance de finalidades legítimas, além de estarem fundamentados em uma base legal e serem garantidos meios para que titulares de dados possam exercer seus direitos tais como previstos na lei.

A despeito do diálogo entre a LGPD e a LAI, e as atribuições da ANPD, há muitas lacunas na LGPD a respeito de sua aplicação por órgãos e entidades públicas. Por exemplo, como compatibilizar os princípios da finalidade e da necessidade com a interoperabilidade de bases de dados públicas? Quais bases legais são aplicáveis às atividades de tratamento de dados pessoais realizadas por particulares em benefício do interesse público? Nesse sentido, tem razão o Ministro Gilmar Mendes quando, no julgamento da ADPF 695, afirma que "há significativos pontos cegos sobre o regime de proteção de dados no que aplicável às relações firmadas com o Poder Público". Ou seja, elas não apresentam respostas claras a essas e outras perguntas relacionadas aos cuidados que deverão ser observados quando do tratamento de dados mantidos pelo poder público.

Diante desse cenário, após aprovada a LGPD, foi possível ver movimentações distintas por parte de órgãos e entidades públicos. Foram editadas **normas destinadas a estabelecer uma estrutura de governança** para a proteção de dados pessoais nas atividades do órgão público - a exemplo do Decreto nº 59.767/2020, que regulamenta a aplicação da LGPD no âmbito da administração municipal direta e indireta de São Paulo, do Decreto nº 42.036/2021, que dispõe sobre a aplicação da LGPD no âmbito da administração pública direta e indireta do Distrito Federal e do Decreto nº 55.647/2020, que regulamenta os procedimentos gerais, os prazos e as fases para implementação da LGPD no âmbito do Poder Executivo do Estado do Rio Grande do Sul. Esses decretos visam regulamentar as práticas para promoção da proteção de dados pessoais a nível estadual e municipal executadas pelo Poder Público. No âmbito do governo federal, como mencionado, a SGD publicou guias e editou normas para auxiliar entidades públicas na tarefa de adequar suas atividades à LGPD. [212]

[212] Disponível aqui: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em 10.01.2021.

Independente da movimentação realizada, as diversas interpretações apresentadas apenas reforçaram o diagnóstico de que ainda há grande dúvida sobre como interpretar os dispositivos da LGPD para o poder público. Por exemplo, ainda há incerteza sobre como órgãos e entidades públicos poderão assegurar os direitos de titulares de dados, como os de anonimização, bloqueio ou eliminação de dados desnecessários, especialmente em cenário no qual são criadas bases de dados centralizadas com informações de cidadãos. Outro exemplo reside em como compatibilizar os princípios da finalidade e da necessidade em casos de compartilhamento e publicação de dados entre órgãos públicos. Também foi possível identificar dificuldade na aplicação dos conceitos de controlador e operador para fins do poder público.[213] Caberá à ANPD importante papel nesse sentido.[214]

[213] Em algumas situações, esses conceitos foram interpretados como orientadores da distribuição interna à instituição de responsabilidade sobre as atividades de tratamento de dados realizadas (eg., enquanto ocupantes de cargos de liderança foram qualificados como controladores, assessores foram qualificados como operadores).

[214] Com efeito, além das autorizações previstas para tanto na LGPD, no Decreto que regulamenta a sua estrutura (Decreto nº 10.474/2020) há referências diversas sobre a competência da autoridade em normatizar e fiscalizar atividades de tratamento de dados pessoais pelo poder público (e.g.: art. 2º, XI e XVI e art. 4º, I, *c*, II, *e*, III, *b*, VI, *b*, VIII, *a* e IX).

7 INCOERÊNCIAS PRÁTICAS NA INTERFACE ENTRE O COMPARTILHAMENTO E A PUBLICAÇÃO DE DADOS COM A PROTEÇÃO DE DADOS PESSOAIS

Hoje no Brasil é possível observar dois movimentos distintos em paralelo: a ampliação de medidas de divulgação de dados mantidos em bases de dados governamentais e a restrição de medidas destinadas a promover o acesso à informação mantida por governos. Mais que isso, o compartilhamento e a publicação de dados mantidos por entes públicos foram afetados de formas distintas pela entrada em vigor da LGPD, que estabelece regras sobre como dados pessoais poderão ser manejados por terceiros e assegura direitos aos indivíduos sobre seus dados.

Divulgação de dados para fins de transparência

No que diz respeito à transparência, na década de 2010 o Brasil liderou debates sobre o tema. Em meados de 2010, o governo brasileiro atuou como co-fundador de Parceria Global para Governo Aberto[215] (Open Government Partnership ou OGP),[216] que possuía entre seus objetivos a ampliação da transparência e participação social em governos. Essa atuação do governo brasileiro foi fundamental para se criar pressão política para a aprovação pelo Congresso Nacional da Lei de Acesso à Informação (LAI) em novembro de 2011 (GUIMARÃES, 2014).

A entrada em vigor da LAI, bem como a edição dos decretos regulamentadores nº 8.638/2016, nº 8.777/2016 e nº 8.789/2016,[217] motivou uma mudança de paradigma, e governos das mais diversas instâncias federativas passaram a adotar medidas ativas e passivas de transparência e abertura de dados. No âmbito do governo federal, entre os esforços adotados estão a criação dos portais da transparência (transparência.gov.br) e de dados abertos (dados.gov.br), nos quais cidadãos podem encontrar informações diversas, desde gastos públicos (eg.: salários de servidores, benefícios sociais, emendas parlamentares, licitações e contratos) até o perfil de estudantes de escolas públicas. Assim, embora diversos relatórios acertadamente apontem para a necessidade de melhoria dos canais de transparência e dados

[215] O termo governo aberto não é sinônimo de transparência. Segundo a OCDE "Estratégias e iniciativas de governo aberto são baseadas nos princípios da transparência, integridade, *accountability* e participação de agentes" (tradução livre). Vide https://www.oecd.org/gov/open-government/. Acesso em 05.03.2022.

[216] Website da OGP: https://www.opengovpartnership.org/. Acesso em 05.03.2022.

[217] A LAI também foi regulamentada por outros entes federados e poderes de Estado. No entanto, o Poder Executivo Federal foi quem acelerou a implementação dos instrumentos previstos na LAI.

abertos (pelo formato, periodicidade, qualidade ou quantidade da informação divulgada), o governo brasileiro iniciou caminho de superação da cultura de sigilo governamental.[218]

No entanto, recentemente, é possível notar uma mudança de postura do governo em relação à promoção da transparência governamental.[219] Em diversas situações, o acesso a documentos ou a bases de dados passaram a ser rejeitados. Não somente se deixou de publicar determinadas informações, em portais da transparência e dados abertos ou em resposta a pedidos de acesso à informação, como foram modificadas normas que regulam a transparência governamental para reduzir obrigações do governo em relação ao tema.[220]

Um exemplo dessa recente mudança de postura do governo brasileiro consiste na edição, em 2019, pela Presidência da República, do Decreto nº 9.690/2019[221], que ampliou a quantidade de agentes públicos com poderes para decretar o sigilo de informações públicas. Com isso, buscou-se reduzir certos freios burocráticos à classificação de informações mantidas pelo poder público[222] como restritas ao público. De todo modo, diante de grande repercussão negativa e buscando evitar sofrer derrotas no Congresso Nacional, que já havia aprovado requerimento de urgência em proposta que buscava sustar os efeitos do Decreto, a Presidência revogou referido ato normativo.[223]

No ano seguinte, o Governo Federal editou a Medida Provisória (MP) nº 927/2020, que determinou a suspensão dos prazos para a resposta a pedidos de acesso à informação durante o período de pandemia do coronavírus. A medida, no entanto, foi derrubada pelo Supremo Tribunal Federal (STF) após o ajuizamento das Ações Diretas de Inconstitucionalidade (ADI) nº 6347, nº 6351 e nº 6353. Isso não impediu, no entanto, que pedidos de acesso a informações que buscavam acesso a dados relacionados ao COVID-19

---

[218] Vide: https://artigo19.org/2017/05/15/os-5-anos-da-lei-de-acesso-a-informacao-uma-analise-de-casos-de-transparencia/, https://artigo19.org/2019/05/16/7-anos-da-lei-de-acesso-a-informacao-relatorios-ineditos-analisam-avancos-e-desafios-em-relacao-a-transparencia-e-sistemas-eletronicos-de-informacao/ e http://www.internetlab.org.br/wp-content/uploads/2015/11/AcessoAInf_TJSP.pdf. Acesso em 05.03.2022.

[219] https://oglobo.globo.com/politica/transparencia-em-queda-maioria-dos-ministerios-de-bolsonaro-reduz-atendimento-pedidos-de-acesso-informacao-25258926. Acesso em 05.03.2022.

[220] Vide: https://www1.folha.uol.com.br/poder/2020/06/gestao-bolsonaro-acumula-ao-menos-13-medidas-para-reduzir-transparencia-oficial.shtml. Acesso em 05.03.2022.

[221] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9690.htm. Acesso em 20.04.2021.

[222] Nesta tese entende-se que o dado mantido pelo poder público, seja ele pessoal ou não, é aquele coletado (e.g., informações levantadas pelo IBGE na realização do censo demográfico) ou compartilhado com o poder público (e.g., dado coletado por uma concessionária de serviço público e enviado ao órgão ou entidade pública contratante). Em outras palavras, o dado mantido pelo poder público será aquele que, em determinado momento de seu ciclo de vida, esteve sob a posse do governo.

[223] Assim, a decretação de sigilo continua sendo regida pelos arts. 25 e seguintes do Decreto Nº 7.724/2012, sendo que a competência para classificação da informação consta do art. 30.

fossem rejeitados.[224] No mesmo ano, a CGU determinou a declaração de sigilo a todos os pareceres jurídicos emitidos pelos Ministérios para orientar a Presidência da República (PR) quando da sanção de propostas normativas aprovadas pelo Congresso Nacional.[225]

Ainda em meio à pandemia de COVID-19, o Governo Federal tomou medidas restringindo a publicidade de informações sobre danos provocados pelo vírus (e.g.,: removendo dados, atrasando sua divulgação, modificação da metodologia de contagem dos dados etc.). No entanto, o Ministro do STF Alexandre de Moraes proferiu decisão liminar na Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 690, determinando a retomada da publicação, pelo Ministério da Saúde, de dados epidemiológicos relativos à pandemia e ao número acumulado de mortes.

Não bastasse isso, houve aumento na quantidade de pedidos de acesso à informação negados, sob argumentos como os de que cidadãos estariam realizando *pescaria* de informações públicas (ou seja, buscando informações públicas para fins maliciosos) ou gerando ineficiência ao Estado, e promovendo custos ao contribuinte.[226] Pesquisas realizadas por associações independentes de jornalismo indicaram uma redução das concessões de acesso pela administração pública federal aos pedidos fundados na Lei de Acesso à Informação - observando uma queda de quase 25% na quantidade de acessos em 2020 em relação à média dos anos de 2016 a 2019.[227]

Outro argumento que vem sendo utilizado pelo governo federal para restringir o acesso a informações que possui é que a LAI escusa o dever de transparência quando a publicação de informações afronta a privacidade de indivíduos. Essa escusa teria sido reforçada pela edição da LGPD, destinada a proteger a privacidade de indivíduos. De fato, pesquisa publicada em agosto de 2021 pela organização Fiquem Sabendo identificou cerca de

---

[224] Vide: https://blog.transparencia.org.br/pandemia-foi-usada-para-negar-atendimento-a-pedidos-de-informacao-mesmo-apos-suspensao-da-mp-928/. Acesso em 02.02.2022.

[225] Vide: https://congressoemfoco.uol.com.br/area/governo/governo-reduz-transparencia-e-amplia-sigilo-de-pareceres-de-ministerios/. Acesso em 05.03.2022.

[226] Vide: https://apublica.org/2020/02/governo-bolsonaro-acusa-cidadaos-de-pescarem-dados-ao-negar-pedidos-de-informacao-publica/ e https://ultimosegundo.ig.com.br/politica/2020-02-08/lei-de-acesso-a-informacao-numero-de-pedidos-negados-quintuplicou-em-2019.html. Acesso em 13.04.2021.

[227] Vide: 149ransparência.org.br/blog/pandemia-foi-usada-para-negar-atendimento-a-pedidos-de-informacao-mesmo-após-suspensao-da-mp-928/ https://www.transparencia.org.br/downloads/publicacoes/Negativas_de_acesso_a_informacao_pioram_sob_governo_Bolsonaro.pdf. Acesso em 20.04.2021.

80 recursos oferecidos à CGU contra pedidos de acesso à informação negados com base na recém publicada LGPD, dos quais metade foi rejeitada pelo órgão recursal.[228]

Conforme a pesquisa, um exemplo recorrente de rejeição a pedido de acesso à informação com base na proteção da privacidade de cidadãos está relacionado ao controle de entrada de visitantes a prédios públicos, como os da Presidência da República e da Vice-Presidência da República. Entre os diversos pedidos feitos nesse sentido estão o registro de entrada e saída dos visitantes que se cadastrem para encontrar o Presidente da República ou das visitas do Deputado Federal Luís Miranda (envolvido em escândalos de corrupção relacionados à compra de vacinas contra a COVID-19) ao Palácio do Planalto entre janeiro e junho de 2021.[229]

Essa tendência também foi reconhecida pela própria Autoridade Nacional de Proteção de Dados Pessoais (ANPD) em Estudo Técnico publicado sobre "A LGPD e o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos por órgão de pesquisa".[230] Conforme o estudo indica, Tribunais[231] e Universidades[232], em vista de incertezas sobre como assegurar a privacidade de cidadãos à luz da nova legislação de proteção de dados pessoais, vêm rejeitando pedidos de acesso a documentos realizados para fins de pesquisas acadêmicas.

Esse argumento tem sido utilizado não somente para rejeitar pedidos de transparência passiva, mas também para restringir a publicação de informações em transparência ativa. Por exemplo, em meio a debates sobre a eficácia de iniciativas destinadas ao enfrentamento do

---

[228] Vide: https://fiquemsabendo.substack.com/p/veja-como-o-governo-vem-usando-a?utm_source=url. Acesso em 01.03.2021.

[229] Esses pedidos foram denegados pelo Gabinete de Segurança Institucional da Presidência da República (GSI-PR) sob o argumento de que as informações solicitadas possuem dados pessoais, cuja disponibilização é restrita pela LGPD.

[230] https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000810_2022_17.pdf. Acesso em 27.05.2022.

[231] "Assim, por exemplo, um órgão do Poder Judiciário informou à ANPD que "vem se manifestando pelo indeferimento de pedidos realizados por pessoa natural para o tratamento de dados pessoais para fins de pesquisa acadêmica". O mesmo órgão reconhece que esse posicionamento pode inviabilizar a realização de trabalhos acadêmicos, "razão pela qual se busca alternativas legais, alicerçadas pelo órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional"." Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000810_2022_17.pdf. Acesso em 27.05.2022.

[232] "Na mesma linha, uma Universidade Federal adotou, por cautela, a postura de negar pedidos de acesso à informação para fins de pesquisa, "por considerar a inexistência de ato normativo regulamentador" que disponha sobre a aplicabilidade do art. 7º, IV e do art. 11, II, c, da LGPD. Ainda segundo a mesma instituição, "o que se verifica é que a LGPD ao tempo que desejou não impedir o desenvolvimento de pesquisas no país, desejou preservar os dados pessoais [...]. Entretanto, consideramos que tais questionamentos precisam de uma melhor orientação [...] sobre o procedimento a se realizar com relação aos pedidos de acesso à informação de dados pessoais e/ou sensíveis para fins de pesquisas"." Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000810_2022_17.pdf. Acesso em 27.05.2022.

COVID-19, o Governo Federal decretou o sigilo por 100 anos da carteira de vacinação do Presidente da República, sob o argumento de proteção à sua privacidade.[233]

Outro caso emblemático consiste na remoção, do site do Ministério da Educação, de dados sobre o Censo Escolar da Educação Básica e sobre o Exame Nacional do Ensino Médio (Enem), antes divulgados pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep). Particularmente, os microdados do Enem de 2020 e do Censo Escolar da Educação Básica de 2021 foram divulgados de forma incompleta e os dados referentes aos anos anteriores foram suprimidos. Esses dados, que são amplamente utilizados para pesquisas e políticas públicas de educação, foram suprimidos sob o argumento de proteção de dados pessoais constantes das bases de dados.[234]

Esse uso da LGPD para restringir acesso a informações públicas foi tão frequente que motivou debate sobre o tema na Comissão de Fiscalização Financeira e Controle da Câmara dos Deputados. Nessa oportunidade, o Deputado Elias Vas afirmou que determinados órgãos públicos estariam "pegando carona na confusão da interpretação da LGPD e da LAI para impedir que a população tenha acesso à informação transparente", e o Dep. Kim Kataguiri afirmou que "o governo usa deliberadamente a legislação que foi feita para proteger dados privados, que foi feita para proteger o cidadão comum de um abuso, de uma exposição ou uso ilegal de seus dados privados para interferir na Lei de Acesso à Informação, umas das legislações mais importantes para trazer publicidade aos atos da administração pública".

Um ano depois, diante do aumento de respostas a pedidos de acesso à informação rejeitados com fundamento na LGPD, a Controladoria-Geral da União editou o Enunciado nº 04/2022[235] no qual esclareceu que a LGPD, a LAI e a Lei de Governo Digital são sistematicamente compatíveis entre si, motivo pelo qual não haveria antinomia entre seus dispositivos. De todo modo, estabeleceu que a LAI, por ser norma mais específica, deverá prevalecer no processamento de pedidos de acesso à informação.

Com efeito, como se verá ao longo desta tese de doutorado, o texto legal apresenta a privacidade como ressalva ao dever de publicidade governamental, mas somente quando não

---

[233] Vide: https://congressoemfoco.uol.com.br/area/governo/planalto-sigilo-cartao-vacinacao-bolsonaro/. Acesso em 01.03.2022.

[234] Vide: https://www.metropoles.com/colunas/guilherme-amado/inep-usa-lei-de-protecao-de-dados-para-censurar-informacoes-do-enem, https://educacao.uol.com.br/noticias/agencia-estado/2022/02/21/inep-exclui-microdados-do-censo-escolar-e-do-enem-e-oculta-informacoes-do-sistema.htm, https://www.uol.com.br/tilt/colunas/carlos-affonso-de-souza/2022/02/23/dados-enem-censo-escolar-lgpd-inep-acesso-a-informacao-educacao-brasil.htm. Acesso em 23.04.2023.

[235] Vide: https://www.in.gov.br/en/web/dou/-/enunciado-n-4-de-10-de-marco-de-2022-385474869. Acesso em 23.04.2022.

houver interesse público e geral preponderante nesse acesso a informações pessoais. Caso o interesse público esteja presente, dados pessoais poderão ser divulgados. O racional da legislação é assegurar a transparência como pressuposto e estabelecer o sigilo de dados mantidos pelo governo como exceção. Assim, a redução da transparência da administração pública não deverá ser uma consequência da preocupação com a proteção de dados pessoais. A despeito disso, a proteção à privacidade, de detentores ou não de cargos políticos, vem sendo utilizada como argumento para não observar a transparência.

Divulgação de dados para fins de eficiência governamental

De forma distinta, durante esse mesmo período, intensificaram-se medidas que ampliam a circulação de informações mantidas pelo poder público sob argumentos como o aumento de eficiência governamental e melhoria na prestação de serviços públicos. De fato, a troca de informações por entes públicos, com outras entidades públicas ou com particulares, é de suma importância na medida em que produz benefícios como o aprimoramento da prestação de serviços públicos e da execução de políticas públicas, além de estimular a inovação e o desenvolvimento de novos mercados.

Diante disso, práticas de compartilhamento de dados estão entre as medidas previstas para executar os princípios e objetivos das estratégias de governo digital que vêm sendo adotados pelo Brasil. Por exemplo, a estratégia de Governo Digital para o período de 2020 a 2022 possui entre seus objetivos o acesso digital único aos serviços públicos e a prestação de serviços públicos integrados.[236] Para tanto, é crucial a integração de sistemas governamentais e o compartilhamento de dados, pessoais ou não (como se vê pela iniciativa 6.1, que busca a interoperabilidade de sistemas do governo federal para que serviços públicos contem com o preenchimento automático de informações, ou pela iniciativa 4.4, que busca ampliar a utilização de login único de acesso gov.br para serviços públicos digitais).

No entanto, esse compartilhamento não tem sido realizado em observância à proteção de dados pessoais. Pesquisa realizada entre 2010 e 2012 pela autoridade do Reino Unido de proteção de dados pessoais (*Information Commissioner's Office* ou ICO) mostrou que autoridades públicas estavam menos adaptadas às exigências legais de proteção de dados

[236] Vide: https://www.gov.br/governodigital/pt-br/EGD2020. Acesso em 05.03.2022.

pessoais.[237] No Brasil, é possível notar similar cenário de ausência de adequação de órgãos públicos às normas de proteção de dados pessoais, como verificou o Tribunal de Contas da União (TCU) após realizar a avaliação das atividades de 386 órgãos públicos e diagnosticar que 76,7% deles não estão preparados para cumprir a lei (acórdão nº 1384/2022).[238]

Assim, ainda que as normas que regulam essa prática façam referências genéricas à legislação sobre proteção de dados pessoais, não observam suas regras e princípios norteadores. Pelo contrário, em determinados casos, determina-se o compartilhamento de dados por pressuposto, sem a demonstração ou exigência de que o ente público detentor da base de dados demonstre que essa atividade não irá impor riscos relevantes às pessoas sobre quem os dados se referem.

O primeiro e mais notável movimento nesse sentido consiste na edição do Decreto nº 10.046/2019, que revogou o Decreto nº 8.789/2016 e criou o Cadastro Base do Cidadão, destinado a aprimorar a interoperabilidade entre bases de dados do governo federal, o que facilita a troca de dados entre órgãos e entidades públicas federais. Embora a medida busque assegurar eficiência governamental, a norma ampliou sensivelmente a possibilidade de o governo federal compartilhar dados pessoais (inclusive dados biométricos) sem prever medidas para assegurar a privacidade dos cidadãos. Por isso, o decreto recebeu críticas e acabou por ter sua constitucionalidade questionada pela Ordem dos Advogados do Brasil (OAB) perante o STF, na ADI nº 6649, por não prever mecanismos de transparência ou que permitam controle sobre a forma como dados pessoais de cidadãos são compartilhados. A ação aguarda apreciação pelo Tribunal.

Casos como esse geram grandes preocupações em termos do nível de vigilância estatal que a construção de bases de dados enriquecidas por diversas entidades públicas permitirá. Além disso, ainda que o uso dessas informações seja devidamente regulado para evitar abusos por parte das entidades governamentais, com acesso a uma quantidade crescente de dados pessoais sobre a população, destaca-se o risco de segurança que a construção dessas bases pode representar, caso o tratamento de dados governamentais não seja conduzido com as devidas salvaguardas, já garantidas na legislação de proteção de dados.

---

[237] Vide "Private sector leads the way on data protection compliance but 'room for improvement' elsewhere". Disponível em. http://www.ico.gov.uk/news/latest_news/2012/private-sector-leads-the-way-on-data-protection- compliance-11102012.aspx. Acesso em 05.11.2022.

[238] Vide; https://capitaldigital.com.br/wp-content/uploads/2022/06/038.172-2019-4-AN-auditoria_Lei-Geral-de-Protecao-de-Dados.pdf. Acesso em 01.07.2022.

Outra medida foi tomada em meio a momentos críticos da Pandemia de COVID-19, quando a Presidência da República editou a Medida Provisória nº 954/2020, na qual se determinou o envio de dados de clientes de empresas de telecomunicações para o Instituto Brasileiro de Geografia e Estatística (IBGE). O objetivo final da proposta era viabilizar a realização de pesquisas e estatísticas oficiais pela instituição em momento de distanciamento social. Para tanto, a MP determinou que empresas de telefonia deveriam disponibilizar ao IBGE, em formato eletrônico, os nomes, números de telefone e endereços de todos seus consumidores. Os dados deveriam ser tratados em caráter sigiloso e serem utilizados somente para a realização de entrevistas e produção de estatística oficial, descartada a possibilidade de serem utilizados como meio de prova em processos administrativos, fiscais ou judiciais.[239]

Tal como o Decreto nº 10.046/2019, a MP também foi fruto de grande questionamento por não apresentar propostas concretas para assegurar observância aos princípios de proteção de dados pessoais, com particular destaque aos princípios da finalidade, necessidade e segurança. Em função disso, a norma teve sua constitucionalidade questionada perante o STF por diversas organizações, como a OAB e determinados partidos políticos. Ao final, a Medida Provisória foi julgada inconstitucional, haja vista o reconhecimento de um direito fundamental à proteção de dados pessoais, decorrente de interpretação conjunta e renovada dos direitos à privacidade e à dignidade da pessoa humana.

No mesmo ano, o Departamento Nacional de Trânsito (Denatran), vinculado ao Ministério da Infraestrutura, aprovou o Termo de Autorização nº 7, no qual concedeu à Agência Brasileira de Inteligência (Abin) acesso a dados dos sistemas e subsistemas do Denatran.[240] Entre as informações que seriam acessadas estão o nome, número da CNH, tipo de habilitação, fotografia, tipo e placa do carro ou a quantidade de infrações recebidas. No entanto, em vista da falta de informações a respeito da finalidade atribuída pelo órgão de inteligência aos dados coletados por órgãos de trânsito, o termo também teve sua constitucionalidade questionada perante o STF (ADPF nº 695).[241] Para tentar evitar a declaração de inconstitucionalidade do ato, o Ministério da Infraestrutura revogou o ato e a

[239] Segundo a MP, o IBGE também não poderá disponibilizar os dados a qualquer empresa pública ou privada ou órgãos ou entidades da administração pública direta ou indireta, além de possuir a obrigação de informar em seu sítio eletrônico as situações em que os dados foram utilizados e divulgar relatório de impacto à proteção de dados pessoais. Após a situação de emergência de saúde pública, as informações compartilhadas serão eliminadas das bases de dados do IBGE, salvo se necessários para concluir a produção de estatística oficial, caso em que poderá utilizar os dados por 30 dias após o fim da situação de emergência.

[240] Vide: https://www.in.gov.br/web/dou/-/extratos-de-autorizacao-246822072. Acesso em 03.03.2022.

[241] Petição inicial pode ser encontrada em: https://internetlab.org.br/wp-content/uploads/2020/06/psbcnhabin.pdf. Acesso em 03.03.2022.

Advocacia Geral da União (AGU) solicitou que a ação fosse retirada de pauta. No entanto, o Ministro Gilmar Mendes manteve o julgamento da ação sob o argumento de que a forma como dados são compartilhados entre entes públicos é tema de extrema relevância para a proteção da privacidade e para a garantia de uma sociedade democrática.[242] A ação aguarda julgamento pelo pleno do Tribunal.

De forma similar, o Denatran aprovou o Termo de Autorização nº 107/2017, que assegura ao Tribunal Superior Eleitoral (TSE) acesso a dados, especialmente dados biométricos, dos sistemas e subsistemas informatizados do órgão superior de trânsito.[243] O objetivo primordial do acesso a esses dados pelo TSE é evitar fraudes e garantir maior segurança na identificação de cidadãos durante as diferentes etapas do processo eleitoral,[244] mas os dados também são utilizados para outras finalidades, como a realização virtual da exigência de prova de vida feita pelo Instituto Nacional de Seguro Social (INSS) aos beneficiários de previdência social.[245]

Além disso, em virtude dos serviços que presta para diversos entes públicos, o Serpro vem sendo autorizado a, cada vez mais, utilizar para objetivos próprios e divulgar dados que acessa por consequência dos serviços que presta. Por exemplo, em 2016 o Ministério da Fazenda editou a Portaria nº 457,[246] regulada pela Portaria nº 2.189/2017 da Receita Federal do Brasil (RFB),[247] que autoriza o Serpro a permitir o acesso de terceiros a dados e informações sob gestão da RFB. Novamente, em 2022, a RFB publicou a Portaria nº 167, permitindo ao SERPRO disponibilizar acesso, para terceiros, dos dados e informações, inclusive pessoais[248]. As portarias não estabelecem procedimentos para determinar quem

---

[242] Nas palavras do Ministro: "o regime jurídico de compartilhamento de dados entre órgãos e instituições do Poder Público é matéria de extrema relevância para a proteção constitucional do direito constitucional à privacidade (art. 5º, caput e incisos X, da Constituição Federal), situando-se como garantia elementar de qualquer sociedade democrática contemporânea.". Vide: https://www.conjur.com.br/dl/gilmar-manda-plenario-analise.pdf. Acesso em 03.03.2022.

[243] Vide: https://www.tse.jus.br/imprensa/noticias-tse/2017/Agosto/tse-tera-acesso-ao-banco-de-dados-informatizados-do-denatran e https://www.gov.br/mdr/pt-br/noticias/denatran-disponibiliza-dados-biograficos-e-biometricos-de-condutores-para-o-tse. Acesso em 03.03.2022.

[244] Vide: https://www.tse.jus.br/imprensa/noticias-tse/2022/Fevereiro/90-anos-da-justica-eleitoral-biometria-impede-fraude-na-identificacao-do-eleitor-no-momento-da-votacao. Acesso em 03.03.2022.

[245] Vide: https://www.convergenciadigital.com.br/Gestao/Prova-de-vida-do-INSS-por-selfie-exige-biometria-cadastrada-no-TSE-ou-Denatran-56979.html?UserActiveTemplate=mobile. Acesso em 03.03.2022.

[246] Vide: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/22188323/do1-2016-12-09-portaria-n-457-de-8-de-dezembro-de-2016-22188268. Acesso em 04.03.2022.

[247] Vide: Disponível em: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=83517. Acesso em 04.03.2022.

[248] Vide: Disponível em:https://www.in.gov.br/web/dou/-/portaria-rfb-n-167-de-14-de-abril-de-2022-394181490. Acesso em 02.05.2022.

serão esses terceiros ou medidas concretas para assegurar a segurança dos dados e a privacidade de cidadãos.

A Portaria nº 457/2016 apenas determina que o acesso de dados: (i) dependerá de anuência do órgão detentor dos dados na qual se ateste não haver risco institucional ou de sigilo sobre dados de pessoas físicas ou jurídicas a quem se referem os dados; e (ii) somente poderá ocorrer pelo terceiro ou outras entidades que tenham autorização legal para tanto. Já a Portaria nº 2.189/2017 foi modificada pela Portaria RFB nº 4.255/2020 para determinar que a divulgação dos dados a terceiros dependerá de análise prévia de risco ao sigilo dos dados e à privacidade daqueles sobre quem os dados se referem, bem como deverá respeitar o disposto na LGPD. Para tanto, as autorizações de acesso ao conjunto de dados relativos à Nota Fiscal Eletrônica seriam revogadas a partir de julho de 2020, até que referida verificação de risco fosse realizada. No entanto, não foram estabelecidos procedimentos claros sobre como isso deverá ocorrer e o prazo de revogação das autorizações já concedidas foi prorrogado sucessivas vezes, estando atualmente previsto para junho de 2022.

Em agosto de 2022, a ANPD concluiu sua análise da Portaria RFB nº 167, especificando que o compartilhamento dos dados poderá ocorrer apenas com finalidade explícita da "complementação de políticas públicas voltadas ao fornecimento de informações à sociedade por meio de soluções tecnológicas complementares às oferecidas pela Receita Federal Brasileira"[249]. Nessa oportunidade, a Autoridade mencionou expressamente que o Serpro e a RFB não poderão, em qualquer caso, realizar a venda dos dados pessoais detidos nas bases - algo que não foi esclarecido no texto inicial da Portaria.

[249] Vide: https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/anpd-conclui-analise-sobre-tratamento-de-dados-pessoais-entre-receita-e-serpro. Acesso em 29/08/2022.

8 CONCLUSÃO PARCIAL: NECESSIDADE DE PROMOVER MAIOR DIÁLOGO ENTRE NORMAS

Neste capítulo se apresentou como a legislação brasileira regula as práticas de publicação e de compartilhamento de dados pelo poder público em observância à privacidade e proteção de dados pessoais de cidadãos. Como demonstrado, a despeito dos avanços legislativos dos últimos anos, ainda há incerteza sobre como compatibilizar na prática a divulgação de dados mantidos pelo poder público com a proteção de dados pessoais.

A **publicação de dados** mantidos pelo governo, no Brasil, possui respaldo constitucional no direito de acesso à informação e no princípio da publicidade dos atos administrativos (embora também possa contribuir com outros bens jurídicos constitucionalmente protegidos, como a eficiência governamental), tendo como sua principal expressão de concretização a Lei de Acesso à Informação (Lei nº 12.527/2011). Essa lei estabelece a divulgação proativa de informações de interesse público em *websites* de órgãos e entidades públicos e determina procedimentos e prazos para que cidadãos possam requerer acesso a dados públicos. No entanto, o dever de publicidade governamental possui exceções, a exemplo da não divulgação de documentos ou bases de dados com informações que possam prejudicar a privacidade de cidadãos. Essa exceção não se aplicará, todavia, em situações tais como a obtenção de consentimento do cidadão ou em casos nos quais houver interesse público na divulgação.

Assim, o interesse público assume o importante papel de limitar a decretação ampla de sigilo a documentos e bases de dados governamentais sob o argumento de proteção à privacidade.[250] Com isso, a LAI buscou assegurar determinado grau de proteção à privacidade, mas sem prejudicar o alcance do interesse público. No entanto, ela não estabeleceu contornos claros para a determinação sobre quais situações se qualificam como interesse público, de forma que restou à Controladoria-Geral da União e à Comissão Mista de Reavaliação de Informações, assim como ao poder judiciário, estabelecer jurisprudência no tema.[251]

---

[250] Especialmente considerando que: (i) a obtenção de consentimento muitas vezes será inviável, diante da necessidade de entrar em contato e obter autorização de cada um dos cidadãos listados nos documentos ou bases de dados; e (ii) as demais exceções possuem o escopo mais restrito, alcançando menos situações.

[251] Como se verá adiante, em vista da inexistência, entre os anos de 2011 e 2018, de legislação que estabelecesse parâmetros para o tratamento de dados pessoais, certas decisões proferidas pela CGU, MRI ou STF acabaram por determinar a publicação ou o compartilhamento de dados sem determinar como essas atividades poderiam ser realizadas de forma a assegurar determinado nível de proteção à privacidade de cidadãos.

De todo modo, a LAI foi regulamentada por normas diversas, com destaque ao Decreto nº 7.724/2012, que regula a LAI no âmbito da administração pública federal, e ao Decreto nº 8.777/2016, que estabelece a política de dados abertos do governo federal. Essas normas estabelecem procedimentos adicionais à concretização do acesso à informação pela administração pública, sendo que o Decreto nº 8.777/2016 exige a publicação de bases de dados em formato aberto (ou seja, não proprietário, legível por máquina e reutilizável sem licenças). Em relação ao Decreto nº 7.724/2012, ele estabelece informações que deverão ser publicadas ativamente, o que inclui certas informações pessoais, como os dados sobre salário e benefícios auferidos por servidores públicos. Além disso, em 2021 foi editada a Lei de Governo Digital (Lei nº 14.129/2021), que reforça as obrigações previstas na LAI, na medida em que reforça o dever de transparência, com destaque a práticas de dados abertos, e estabelece determinados documentos e bases de dados que deverão ser divulgados e que podem conter dados pessoais (e.g., currículos de ocupantes de cargos de chefia e de direção).

Já o **compartilhamento de dados** pelo poder público possui respaldo constitucional nos princípios da eficiência e da publicidade governamental, e no direito de acesso à informação. Sua realização é regulada por legislação esparsa, mas é muitas vezes atrelada a práticas de governo eletrônico e de governo digital. Por exemplo, no ano 2000, o governo federal adotou o inovador programa E-Gov com objetivos de universalização de acesso a serviços públicos, integração de sistemas governamentais e abertura informacional à sociedade, os quais são dependentes de práticas de compartilhamento de dados com entes públicos e privados.

Desde então, foram adotadas novas iniciativas com objetivos similares, mas sempre à luz de novas tecnologias ou demandas sociais, como a edição do Decreto Cidadão (nº 6.932/2009), que buscava simplificar o atendimento da população por meio da integração de sistemas e da racionalização de processos, ou a Estratégia de Governo Digital, que motivou a edição do Decreto nº 8.789/2016, que exigiu aos órgãos ou entidades da administração pública federal o compartilhamento de dados com outras instituições públicas para evitar a necessidade de reiteradas solicitações à sociedade de informações previamente fornecidas e possibilitar a atualização simultânea das bases de dados. Esse texto legal, por sua vez, foi substituído pelo Decreto nº 10.046/2019, que estabeleceu novas regras e estrutura de

---

Outras decisões estabeleceram a não existência de interesse públicos (e a consequente não divulgação de informações) diante da falta de mecanismos claros de garantia à privacidade e proteção de dados pessoais de cidadãos ou por considerar os dados como sendo dados sensíveis (em desacordo ao que a LGPD qualifica como dados sensíveis), cuja publicação implicaram grande risco a direitos dos indivíduos sobre quem os dados se referem.

governança para o compartilhamento de dados entre entes da administração pública federal, para otimizar a execução de políticas públicas.

Essas iniciativas sinalizam a tentativa do governo em assegurar transparência e modernizar o aparato estatal. No entanto, elas não esclarecem como compatibilizar a publicação e o compartilhamento de dados com a privacidade e proteção de dados pessoais de cidadãos, apenas prevendo obrigação genérica de observar o disposto na LGPD, e estabelecendo que informações pessoais somente poderão ser divulgadas em hipóteses específicas, como em casos de interesse público na divulgação.

Especificamente em relação ao Decreto nº 10.046/2019, tal como originalmente editado, acabava por permitir interpretações que vieram posteriormente a ser consideradas pelo STF como sendo contrárias à Constituição, a exemplo da autorização de compartilhamento amplo de dados cadastrais, sem a obrigação de que certos cuidados e procedimentos mínimos sejam observados. Por exemplo, não havia obrigação de fundamentar a atividade em base legal prevista na LGPD, demonstrar os motivos que justificam o acesso aos dados por terceiros, garantir direitos aos titulares de dados, ou fornecer informações aos cidadãos sobre quais interessados tiveram acesso às bases de dados. Além disso, o Decreto não exigia a adoção de medidas de *accountability* e salvaguardas para mitigar eventuais danos a direitos e liberdades dos titulares de dados. Com isso, era possível que princípios e obrigações basilares a um sistema de proteção a dados pessoais viessem a ser desconsiderados.[252]-[253]

No julgamento de ADI ajuizada para terminar a inconstitucionalidade do referido Decreto, o STF determinou que qualquer interpretação atribuída a esse texto legal que permita

[252] Nesse sentido se manifestou Laura Schertel Mendes (2022): "Qualquer sistema que busque viabilizar o fluxo de dados pessoais no âmbito da Administração Pública deve corrigir essas falhas, por meio de medidas básicas que estabeleçam: i) procedimentos de proteção que levem em conta o risco do tratamento de dados pessoais em geral e não apenas de dados sigilosos, especialmente a partir da mudança de finalidade intrínseca a todo compartilhamento; ii) procedimentos especiais que levem em conta o risco do tratamento de dados sensíveis; iii) mecanismos efetivos para o exercício dos direitos do titular, conforme o artigo 18 da LGPD; iv) a edição de ato normativo pelo órgão receptor como requisito para o acesso de dados pessoais, indicando as finalidades para as quais os dados são tratados no âmbito daquele órgão; v) instrumentos de transparência e de *accountability*, que possibilitem o controle do fluxo dos dados pessoais pelo cidadão e pelos órgãos competentes, a exemplo de convênios, atos autorizativos ou outros registros que permitam tal supervisão; vi) a necessidade de realização de relatórios de impacto prévios ao compartilhamento de dados de alto risco; e vii) um sistema de governança mais robusto, para além de um comitê central com composição restrita, conforme previsto no decreto."

[253] As críticas mencionadas ao Decreto nº 10.046/2019 se refletiram, inclusive, em respostas por parte do Congresso Nacional a partir de diversos Projetos de Decreto Legislativo ("PDL") que buscam sustar seu texto, tais como PDL 661/2019, PDL 673/2019, PDL 675/2019 e PDL 151/2020 (Santos; Anastácio; Varon, 2020). Essas propostas não foram apreciadas pelo Congresso Nacional, mas o Decreto foi submetido à apreciação pelo STF na ADI 6649. Vide: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em 16.07.2023.

a ampla e irrestrita divulgação de dados pessoais mantidos pelo poder público será contrária aos direitos fundamentais da privacidade e proteção de dados pessoais. Com isso, embora o STF tenha reconhecido a importância da interoperabilidade para a eficiente e transparente atuação do Estado, entende que essas práticas somente serão alinhadas à constituição quando contarem com procedimentos como aqueles que garantam, para a entidade interessada no acesso aos dados, o tratamento de dados para finalidades legítimas e informadas aos titulares de dados, assim como a limitação do compartilhamento ao mínimo necessário.

Por sua vez, a **privacidade e a proteção de dados pessoais** são direitos previstos na Constituição Federal Brasileira, regulados setorialmente por leis como o Código de Defesa do Consumidor (Lei nº 8.078/1990) e do Marco Civil da Internet (Lei nº 12.965/2014), mas com regulação abrangente editada em 2018, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Essa lei estabelece princípios, obrigações e procedimentos de governança que devem ser observados quando do tratamento de dados pessoais, e assegura aos titulares de dados direitos em relação ao uso de seus dados por terceiros.

Para o compartilhamento e publicação de dados pelo governo, a LGPD estabelece parâmetros gerais (e.g., os princípios da necessidade, finalidade e transparência e as bases legais de cumprimento de obrigação legal e execução de políticas públicas) e específicos, como os previstos nos art. 7º, §§3º e 7º e arts. 23 a 17. Em relação a dados publicados, a LGPD reconhece que dados pessoais poderão ser divulgados em políticas de transparência e dados abertos, e exige que seu tratamento posterior deverá estar respaldado na boa-fé, buscar o interesse público, e ser destinada ao alcance de finalidades legítimas, além de estarem fundamentados em uma base legal e serem garantidos meios para que titulares de dados possam exercer seus direitos tal como previstos na lei.

Quanto ao compartilhamento de dados entre órgãos e entidades públicas, estabelece que deve atender a finalidades específicas de execução de políticas públicas e atribuição legal. Já para o compartilhamento de dados com particulares, estabelece que somente será permitido em situações específicas, como **(i)** execução descentralizada de atividade pública que exija a divulgação, exclusivamente para esse fim específico e determinado, sendo exigida transparência sobre essas atividades; e **(ii)** previsão legal ou a divulgação for respaldada em contratos, convênios ou instrumentos congêneres. Essas duas formas de compartilhamento devem assegurar a observância ao princípio da finalidade e o alcance do interesse público.

No entanto, muitos de seus dispositivos pertinentes à divulgação de dados mantidos pelo poder público são principiológicos e/ou possuem imprecisões de técnica legislativa que dificultam sua implementação no caso concreto. Assim, a observância da LGPD por órgãos e entidades públicos apresenta desafios próprios, especialmente devido à necessidade de compatibilizá-las às demais leis e regulamentos aplicáveis ao poder público. Esse desafio é ainda maior porque, de um lado, governos armazenam quantidade massiva de dados pessoais sobre os indivíduos, coletados em função de obrigações legais e/ou quando da prestação de serviços públicos, e de outro, cidadãos, na maioria das vezes, não possuem a opção em fornecer e/ou recusar a utilização de seus dados.

De todo modo, a LGPD é inegavelmente uma conquista da sociedade brasileira, na medida em que apresenta parâmetros mínimos para o tratamento de dados pessoais no Brasil. Como apontado por Miriam Wimmer (2020), as disposições da LGPD podem ser vistas como uma oportunidade de construção de confiança social em relação ao Estado e de aproximação entre preocupações até então vistas como conflitantes nos esforços de modernização do governo. Isso porque suas regras, com destaque para as obrigações de transparência e para os direitos dos titulares de dados, exigem a adoção de estratégias e ferramentas tecnológicas capazes de assegurar transparência e maior protagonismo aos cidadãos sobre como seus dados são usados. Mais que isso, com base nesses parâmetros, muitos dos quais foram considerados pelo Supremo Tribunal Federal como proto-constitucionais, é possível tanto avaliar a adequação e suficiência de normas sobre compartilhamento e publicação de dados pelo poder público, quanto guiar as práticas de disponibilização de dados pessoais de interesse público de tal forma a assegurar a privacidade e proteção de dados pessoais.

Apresentado o racional das normas sobre transparência e dados abertos, modernização do aparato governamental e proteção de dados pessoais, fica claro que elas possuem pontos de contato relevantes, mas que não necessariamente dialogam na mesma língua. Ou seja, ainda que a Lei de Acesso à Informação possua regras sobre proteção de dados pessoais, ela está focada em determinar as situações nas quais dados poderão ser publicados ou deverão ser mantidos em sigilo, apresentando solução genérica e binária ao problema (i.e.: o dado pessoal deverá ser mantido em sigilo, mas poderá ser publicado se houver interesse público). Já as normas sobre governo eletrônico e governo digital, ainda que façam referências genéricas à privacidade e à LGPD, dedicam-se a promover a maior divulgação possível de dados para a finalidade de aprimorar a prestação de serviços públicos. Em outros termos, elas estão mais focadas em romper com os paradigmas históricos de burocracia e sigilo governamental.

Diante disso, ainda que apresentem exceções às práticas de compartilhamento e publicação de dados destinados, entre outros, a proteger a privacidade e proteção de dados de cidadãos, não apresentam critérios mais objetivos para assegurar essa proteção. Em nenhum dos casos há parâmetros claros capazes de informar o gestor público sobre como assegurar a privacidade dos cidadãos quando da divulgação dos dados que mantém. Essa tarefa foi assumida por legislação específica sobre proteção de dados pessoais,[254] mas que também possui ausência de parâmetros claros para auxiliar o gestor público na tomada de decisão sobre se, quais e como divulgar dados pessoais. Embora preveja base legal específica para o tratamento de dados pessoais necessários para a execução de políticas públicas e um capítulo dedicado a regular o tratamento de dados pessoais, não são claros os contornos normativos aplicáveis para o compartilhamento e para a publicação de dados pessoais. Como demonstrado, os artigos destinados a regular essas atividades sofrem de má técnica legislativa que não permite sua clara compreensão. Ao fim e ao cabo, o capítulo exige do agente público agir para o alcance do interesse público, segundo suas atribuições legais, privilegiando a interoperabilidade entre órgãos e entes públicos e observando a transparência pública.

No entanto, a LGPD também não estabelece parâmetros claros para se definir no caso concreto o que seria o interesse público na divulgação de dados pessoais por governos, de tal modo que recairá ao agente público ou ao judiciário identificar no caso concreto se há interesse público que resulte na divulgação de dados. Com isso, têm-se verificado, na prática, falta de coerência entre decisões sobre quais dados os governos devem publicar ou compartilhar com terceiros: de um lado, tem se utilizado a LGPD para restringir o alcance de políticas de transparência e dados abertos e, de outro, foram editadas novas medidas destinadas a ampliar práticas de compartilhamento de dados entre órgãos e entidades públicos sem a mesma preocupação com a privacidade e proteção de dados pessoais.

Esse cenário possui pelo menos três principais problemas. O primeiro consiste na falsa percepção de que a proteção de dados pessoais é conflitante com a divulgação de dados mantidos pelo poder público - seja para fins de transparência ou de eficiência. É por conta dessa falsa percepção de que não é possível compatibilizar privacidade e divulgação de dados

[254] De fato, antes mesmo da edição da LGPD, Laura Schertel Mendes (2014) ressaltou a importância e competência de uma norma de proteção de dados pessoais no estabelecimento de procedimentos para assegurar o direito à privacidade: "Ademais, a edição de uma lei geral de proteção de dados pessoais, nos moldes propostos pelo Ministério da Justiça, em muito ajudaria na construção de critérios para o adequado delineamento entre o direito de acesso e o direito à privacidade. Nesse sentido, consideramos que a mera regulamentação, conforme previsto pelo art. 31, § 5º, da lei de acesso, não seria suficiente, nem adequada, para solucionar essa lacuna. Afinal, por se tratar de direito fundamental, somente uma lei poderá tratar de forma abrangente sobre a proteção de dados pessoais."

mantidos por governos, que a proteção da privacidade de cidadãos vem sendo utilizada por governos de maneira meramente instrumental, mediante conveniência da situação, justificando a restrição à transparência e sendo superada nos casos de compartilhamento de dados a entidades específicas, sejam elas públicas ou privadas.

No entanto, a compatibilização desses interesses (privacidade e uso dos dados) é necessária. Isso porque o uso irrefletido de dados poderá provocar prejuízos graves para a intimidade dos indivíduos, ao passo que a extrema proteção da privacidade tende a viabilizar a generalização do sigilo governamental e a redução das capacidades de inovação e de controle social sobre a gestão pública. Assim, entende-se que os fundamentos para os usos de dados (eg.: princípios da publicidade e eficiência da administração pública) e para a garantia da privacidade são compatíveis entre si, e que a legitimidade de políticas governamentais poderá ser influenciada positivamente pela sua capacidade de proteger dados e informações pessoais.

Mais que isso, devido à sua natureza principiológica, esses interesses operam como mandamentos de otimização, que não comportam aplicação determinada, mas exigem sua execução na maior extensão possível. Disso decorre que a proteção de dados pessoais mantidos pelo governo envolve constante ponderação entre interesses de uma sociedade democrática (de um lado, a dignidade da pessoa humana, a privacidade e a proteção de dados pessoais, e, de outro, a publicidade, impessoalidade e eficiência governamentais).

O segundo, e já mencionado, problema consiste em proteger a privacidade de formas distintas em situações similares. Como demonstrado, no Brasil se tem visto, ao mesmo tempo, a redução da transparência governamental em vista da privacidade de cidadãos e o aumento de medidas de compartilhamento de dados com terceiros sem a devida preocupação com a privacidade. Quando se trata de compartilhamento de dados mantidos por governos, não há similar preocupação com a proteção de dados pessoais como a supostamente demonstrada em políticas de transparência governamental. Enquanto diversas práticas de transparência vêm sendo restringidas por conta da presença de dados pessoais (limitando-se acesso, integral ou parcial, a documentos e bases de dados), diversas normas vêm sendo editadas para autorizar o compartilhamento de dados pessoais sem apresentar medidas concretas destinadas a assegurar a proteção da privacidade das pessoas sobre quem os dados se referem.

Importante ressaltar que nesta tese não se defende a restrição ao compartilhamento de dados pessoais com terceiros. Em muitas situações, essa atividade não somente é desejada como necessária, seja para a transparência, para a melhoria na prestação de serviços públicos

e execução de políticas públicas ou na promoção de inovação e desenvolvimento de novos mercados. No entanto, esse compartilhamento deve ser realizado observando procedimentos destinados a assegurar que os direitos fundamentais dos titulares de dados sejam preservados. O mesmo racional se aplica às políticas de transparência: esta tese não defende a publicação indiscriminada de dados pessoais em políticas de transparência e dados abertos, mas rejeita o fechamento de bases de dados sob a justificativa irrefletida de que parte ou integralidade dos dados são pessoais. Os dados devem ser publicados observando-se procedimentos destinados a assegurar que direitos fundamentais dos titulares de dados não sejam desrespeitados.

Nesta tese, entende-se que deve haver certa harmonia (mas respeitando suas particularidades, como abordadas anteriormente) em relação à forma de interpretar a proteção de dados pessoais em políticas de transparência e em práticas de compartilhamento de dados pessoais com terceiros, públicos ou privados. Embora o compartilhamento e a publicação de dados possuam diferenças entre si, as duas atividades envolvem a divulgação de dados com terceiros, o que deverá em todo caso, apenas ocorrer em respeito a um procedimento específico, voltado à proteção da privacidade dos indivíduos afetados. Por isso, a ponderação feita para devidamente compatibilizar ambas as formas de divulgação de dados, de um lado, e a proteção da privacidade, de outro, deverá ser realizada de forma harmônica, ainda que os dois casos sejam motivados por diferentes princípios constitucionais. Ela deve observar as particularidades da situação concreta, mas não seguir lógicas diametralmente opostas para avaliar quando o uso de dados poderá ser restrito em benefício da privacidade.

Com efeito, essas práticas possuem diferenças entre si que devem ser consideradas no momento de tomada de decisão sobre quais e a forma de publicar ou compartilhar dados pessoais. Não é possível presumir de antemão que a publicação de dados promove maiores riscos que as práticas de compartilhamento de dados pessoais entre as entidades governamentais e também entre o governo e entidades privadas de sua escolha. Embora as políticas de transparência envolvam a divulgação de dados a uma quantidade maior de destinatários, é possível haver maior risco no compartilhamento de dados a depender de fatores como a natureza do tratamento a ser realizado ou da efetividade das salvaguardas adotadas. Além disso, os riscos decorrentes da publicação ou compartilhamento de dados devem ser contrapostos ao interesse público dessa divulgação. Por exemplo, ainda que haja riscos à privacidade, há inerente interesse público na divulgação de salários de servidores ou no compartilhamento de dados sobre contágio de COVID-19 para instituições de pesquisa.

O terceiro problema tem sido a utilização da LGPD (voluntariamente ou diante de incertezas sobre o escopo da proteção conferida pela lei) para frear políticas e atos do Poder Público para promoção da transparência ao negar informações. As políticas de transparência enfrentam desafios próprios e a preocupação com a proteção de dados pessoais não deve, de forma alguma, se colocar como mais uma motivação para a restrição na divulgação de informações em políticas de transparência.[255] Ainda que dados pessoais mantidos pelo governo devam ser protegidos contra indevida exposição, há meios de assegurar sua proteção ou de minimizar os riscos relacionados à sua utilização.

Nas próximas Partes desta tese se buscará promover maior diálogo entre as normas vigentes, tendo como ponto de partida as disposições da LGPD. Esse recorte analítico considera justamente o fato de que a LGPD apresenta, ainda que diante das limitações impostas, uma proposta de compatibilização do uso de dados e proteção de direitos dos cidadãos.

[255] Isso se agrava em países com regimes autoritários ou com governos menos afeitos à transparência, que realizam disponibilização seletiva de dados pessoais, cuja análise poderá levar a análises equivocadas (Carlitz & Mcllean, 2020).

PARTE III DEFINIÇÃO DO ESCOPO DA PUBLICAÇÃO OU DO COMPARTILHAMENTO DE DADOS PELO PODER PÚBLICO

9 EXPERIÊNCIA ESTRANGEIRA SOBRE O COMPARTILHAMENTO E NA PUBLICAÇÃO DE DADOS

Esse tópico apresentará como o debate sobre o tema tem sido enfrentado por autoridades de proteção de dados de outros países, com o objetivo de identificar os desafios e soluções já apresentadas. Ressalte-se que: **(i)** o levantamento de posicionamentos elaborados por autoridades estrangeiras não é exaustivo; e **(ii)** não será realizado estudo comparado entre a legislação brasileira e as de outros países. O objetivo será tão somente identificar soluções encontradas em outros países para auxiliar na reflexão e construção de um quadro analítico sobre o compartilhamento e a publicação de dados pessoais mantidos pelo governo. Com isso, espera-se encontrar subsídios para a interpretação e aplicação das normas existentes sobre o tema no Brasil, a exemplo da LGPD e da LAI.

Conforme indicado anteriormente, as primeiras leis de proteção de dados pessoais foram editadas por países europeus e a paradigmática decisão que reconheceu a existência de direito de autodeterminação informativa foi proferida pela Suprema Corte da Alemanha, em 1983. Em busca de maior padronização de normas na Europa, foi primeiro editada a Diretiva 95/46/EC, com base na qual foram proferidas opiniões que seguem guiando a prática de proteção de dados pessoais, e, posteriormente, a Regulação 2016/679, que tem influenciado a edição de normas e manifestações de autoridades de proteção de dados pessoais em diversos países do mundo. Também como já mencionado, o Brasil foi um dos países cuja legislação sobre proteção de dados pessoais foi fortemente influenciada pela prática europeia - inclusive, um dos fatores que impulsionou a aprovação do Projeto de Lei que culminou na LGPD foi a proximidade com a entrada em vigor da GDPR.[256] Mais que isso, em seus primeiros posicionamentos, a ANPD comumente faz referência a posicionamentos de autoridades europeias, a exemplo do Guia Orientativo para Definição dos Agentes de Tratamento de Dados Pessoais e do Encarregado (ANPD, 2021), que cita o conceito de controlador e operador do *European Data Protection Board* (EDPB), e do Guia Orientativo de Segurança

[256] Vide artigo sobre o tema: https://www.jota.info/opiniao-e-analise/artigos/gdpr-dados-pessoais-europa-25052018. Acesso em: 30 abr. 2021.

da Informação para Agentes de Tratamento de Pequeno Porte (ANPD, 2022.2), que oferece o entendimento da Comissão Europeia sobre anonimização de dados.

Além disso, a Europa segue sendo palco de debates sobre como viabilizar o potencial social e econômico do uso de dados, pessoais ou não pessoais, mantidos por governos. Por exemplo, já na década de 1990 ocorriam debates relacionados à edição de Diretiva sobre o tema (a chamada *Public Sector Information Directive*, Diretiva 2013/37/EU, que foi substituída pela Diretiva 2019/1024). Recentemente, estão sendo debatidas propostas para a criação de um espaço de dados europeus, capaz de impulsionar o uso benéfico desses dados. Todas essas iniciativas foram analisadas pelas autoridades europeias de proteção de dados pessoais.

Assim, não somente a prática europeia influenciou e segue influenciando o debate sobre proteção de dados no Brasil, como autoridades locais produziram materiais relevantes sobre o tema desta tese. Por isso, serão avaliados posicionamentos das principais autoridades da União Europeia, a saber, a Working Party 29 ("WP 29"), extinta autoridade consultiva criada por força da Diretiva 95/46/EC, a EDPB, autoridade consultiva com competência atribuída pela GDPR, e o *European Data Protection Supervisor* ("EDPS"), entidade com capacidade fiscalizatória.

Além disso, será avaliada também a iniciativa da cidade de Seattle, nos Estados Unidos, em elaborar relatório de análise de risco para seu programa de abertura de dados. O relatório foi elaborado pela *Future of Privacy Forum* (FPF) e contou com contribuições diversas, inclusive da Universidade de Washington e do Berkman Klein Center da Universidade de Harvard.[257] A escolha por avaliar também essa iniciativa se deve ao seu pioneirismo no que concerne ao tema do tratamento de dados abertos, ao fato de ter contado com contribuições de entidades diversas, e de apresentar uma perspectiva diferente da adotada na União Europeia. Isso porque, embora os Estados Unidos também tenham liderado o debate sobre proteção de dados pessoais na década de 1970, a edição de versão própria das *Fair Information Principles* culminou em particularidades na regulação sobre privacidade e proteção de dados pessoais.

[257] Vide a contribuição: https://privacytools.seas.harvard.edu/files/privacytools/files/fpf.pdf. Acesso em 30.04. 2021.

9.1 Guias sobre reuso de dados publicados ou compartilhados

União Européia, Diretiva sobre Informações do Setor Público

No final da década de 1990, o Working Party 29 (WP 29), **editou a Opinião nº 03/1999**,[258] no qual avaliou os cuidados que devem ser observados quando da publicação pelo poder público de bases de dados contendo dados pessoais. O documento foi uma reação à consulta pública lançada pela Comissão Europeia para debater a ampliação de acesso pelos cidadãos a dados mantidos pelo poder público ("*Public Sector Information: a key resource for Europe*").[259]

Além de esclarecer que dados disponibilizados ao público não perdem sua qualificação de dados pessoais, o documento esclarece que a utilização desses dados estaria sujeita à demonstração de uma **base legal** para o tratamento de dados e à observância das **finalidades** que justificaram a coleta ou a publicação dos dados. Sobre isso, a WP 29 reconhece que a aplicação do princípio da finalidade nesses casos apresenta desafios porque, como tais dados normalmente são obtidos por força de alguma obrigação legal ou enquanto condição para usufruir de determinado serviço público, os cidadãos não possuem a expectativa de que serão utilizados para finalidades distintas.

Sobre isso, a autoridade esclarece que há normas locais que, de maneira geral, impedem o uso de dados pessoais mantidos por órgãos e entidades públicos para finalidades comerciais. No entanto, se esses dados forem efetivamente utilizados para essas finalidades, devem ser observados certos parâmetros mínimos e ponderados no caso concreto. De todo modo, a WP 29 argumenta que os cidadãos **deverão ser informados** sobre a utilização de seus dados para finalidades comerciais e poderão se opor a similar tratamento. Por isso, recomendou que bases de dados públicas deveriam ser acompanhadas de informações sobre o **exercício de *opt-out*** para determinadas finalidades, bem como indicou ser necessário obter o **consentimento dos titulares** de dados para a prática de determinadas atividades.

Diante disso, a Autoridade argumentou que a **compatibilização da privacidade com o direito de acesso** a esses dados deveria considerar os seguintes fatores: **(i)** a análise no caso concreto sobre a possibilidade de publicar o dado e sob quais condições e em qual meio

---

[258] Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp20_en.pdf. Acesso em 04.03.2021.

[259] Disponível em: https://op.europa.eu/en/publication-detail/-/publication/599834ce-7a43-44fe-8cd8-334b3c19feba. Acesso em: 04.03.2021.

(digital, *online* etc.); **(ii)** os princípios da finalidade e da legitimidade; **(iii)** a obrigação de informar o titular de dados sobre essa divulgação de seus dados; **(iv)** a garantia do direito ao titular de dados de se opor ao tratamento; e **(v)** o emprego de técnicas e tecnologias atualizadas para assegurar a proteção da privacidade.

União Européia, Atualização da Diretiva sobre Informações do Setor Público

Alguns anos depois, a WP 29 editou a **Opinião nº 07/2003** em reação à proposta de Diretiva sobre o reuso de informações do setor público, levada a consulta pública pelo Conselho Europeu (a *Public Sector Information Directive*, "Diretiva PSI", numerada 2003/98/CE após a sua aprovação).[260] Adotada pela Comissão Europeia em junho de 2002, e votada pelo Parlamento Europeu em 25 de setembro de 2003 (com emendas que foram aceitas pelo Conselho em 27 de outubro), a Diretiva apresentou medidas para auxiliar na evolução para uma sociedade de informação e para oferecer novos meios de acesso à informação.[261]

A Opinião nº 07/2003, por sua vez, realiza uma diferenciação entre **(i)** o acesso de dados nos termos da **diretiva de dados pessoais**, caso em que a preocupação central está em garantir direitos fundamentais; **(ii)** o acesso a documentos do poder público por leis de acesso à informação, que busca assegurar **transparência e *accountability*** pelo governo, sem a necessidade de justificar sua solicitação; e **(iii)** a disponibilização desses dados para fins de reuso, com **finalidades comerciais**. De acordo com a Opinião nº 07/2003, essa diferenciação, embora nem sempre clara, terá consequências na prática quando da aplicação dos princípios de proteção de dados pessoais.

Conforme detalhado no documento, embora os dados objeto da Diretiva PSI sejam geralmente informações geográficas, comerciais, de trânsito ou dados estatísticos agregados, é possível que as bases de dados divulgadas possuam dados pessoais. Nesse caso, a WP 29 defende **a remoção dos dados pessoais das bases de dados** disponibilizadas, sempre que possível. Quando essa exclusão de dados não for possível, seria necessário adotar **salvaguardas técnicas** para assegurar o acesso limitado ou estruturado, de tal forma a evitar o tratamento ilícito de dados pessoais (e.g., impedir o *download* massivo de dados).

---

[260] A Diretiva 2003/98/EC está disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:345:0090:0096:en:PDF. Acesso em 16.10.2022.

[261] Dessa Diretiva originou-se o Open Data Portal da em ("EU ODP"), que fornece acesso crescente a dados públicos nemUE. O objetivo é prover acesso facilitado e gratuito a dados públicos, sempre que possível e quando não houver restrição para sua divulgação.

Além disso, a Opinião nº 07/2003 recomendou a adoção de cuidados adicionais quando da divulgação de **dados sensíveis**, bem como a observação dos **princípios de tratamento** de dados pessoais, com especial destaque aos princípios da **qualidade, minimização e finalidade.** Em relação ao princípio da finalidade, para a verificação da **compatibilidade** do novo tratamento em relação à finalidade original, são adotados distintos critérios interpretativos nos Estados-membros, como **(i)** observar as expectativas razoáveis dos indivíduos, **(ii)** verificar a presença de uma obrigação legal, e **(iii)** avaliar as circunstâncias do tratamento de dados, como a natureza do dado, a forma de coleta e as salvaguardas oferecidas ao titular de dados. No setor público, as regras de finalidade são invariavelmente determinadas pelas normas que estabelecem suas competências, de modo que certo órgão somente poderá tratar dados para finalidades contempladas entre suas atribuições legais. No entanto, a avaliação da compatibilidade pelo órgão público nem sempre será viável, visto que determinados pedidos de acesso a dados não exigem a identificação da finalidade.

Ainda, a Opinião nº 07/2003 indicou que há outros critérios que devem ser observados na avaliação de compatibilidade: **(i)** a **justificativa para a coleta** de dados - consentimento, cumprimento de obrigação legal, atuação em benefício do interesse público ou execução de contrato; **(ii)** se a **disponibilização foi obrigatória** (e.g.,: cumprimento de obrigações tributárias) ou condição para a utilização de serviço público (para a utilização de políticas de assistência) - nesses casos, o exame de compatibilidade é particularmente desafiador porque o cidadão não possui a expectativa desse uso ou a possibilidade de facilmente evitar que seus dados sejam utilizados para outras finalidades; **(iii)** conhecer o **receptor dos dados** ajuda na avaliação da finalidade, que poderá ser o exercício de algum direito fundamental, a exemplo do direito de informação; e **(iv)** a **natureza do dado** influencia na avaliação da compatibilidade na medida em que determinados dados, como os dados sensíveis, merecerão maior cuidado.

No caso em que os dados forem oriundos de **registros públicos**, a sua disponibilização será autorizada em menos casos, na medida em que sua constituição ocorre para finalidades muito específicas. Já nos casos de reuso para **comercialização**, consideradas como as finalidades de gerar receita ou realizar *marketing*, é necessário realizar uma ponderação entre direito fundamental do titular de dados e os interesses comerciais do solicitante. De todo modo, argumenta que essas finalidades geralmente serão consideradas incompatíveis com as finalidades da coleta, salvo se houver autorização legal e desde que essas leis possuam certas salvaguardas aos titulares de dados, como o *opt-out*. Algumas leis locais proíbem

expressamente essa comercialização, como na França (onde é proibida a venda de registros eleitorais), na Bélgica (que proíbe o reuso de dados pessoais fins comerciais), ou na cidade de Berlim (que proíbe o uso de dados obtidos da FOIA - ou *Informationsfreiheitsgesetz*). Já em outros países, a prática é autorizada, porém condicionada à oferta de determinadas salvaguardas, como é o caso da Suécia, em relação aos registros populacionais para fins de *marketing* desde que assegurado o *opt-out*, e da Holanda, para práticas de *score* de crédito.

Em função disso, a WP 29 defendeu a necessidade de realizar **avaliação no caso concreto**, considerando as variáveis mencionadas e, eventualmente, observadas certas restrições de acesso (de certos dados, a certas pessoas, para certas finalidades etc.). Finalmente, também ressalta que certas bases de dados poderão ser divulgadas sem que para tanto seja necessária a divulgação de dados pessoais (e.g., em formato agregado).

União Européia, Nova Diretiva sobre Informações do Setor Público e Dados Abertos

Posteriormente, em 2011, a Comissão Europeia adotou uma proposta para emendar a Diretiva 2003/98/EC (Diretiva PSI)[262], com o objetivo de estimular países-membros a adotarem práticas de dados abertos (após aprovada, foi numerada Diretiva 2013/37/EU).[263]-[264] Entre as mudanças propostas estava a presunção de que qualquer dado público não protegido por exceções legais deverá ser divulgado pelo governo e ser reutilizado para finalidades comerciais e não comerciais. A proposta reconhecia também que não basta divulgar dados, sendo necessário adotar formatos que permitam seu posterior processamento por máquina.

A reação à iniciativa foi realizada pelo **European Data Protection Supervisor** ("EDPS"), autoridade destinada a supervisionar e assegurar que autoridades europeias observem as normas sobre proteção de dados pessoais.[265] Embora reconhecesse os efeitos benéficos dessa proposta normativa, o EDPS demonstrou preocupação com o uso tais dados para finalidades ilegítimas, na medida em que os dados estariam ainda mais acessíveis a qualquer interessado e estariam preferencialmente em formato sistematizado, legível por máquina e disponíveis sem custos. Por isso, argumentou que, exceto se salvaguardas forem

[262] Sobre as propostas de mudanças em Diretivas sobre o reuso de dados público, vide: https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information. Acesso em 05.03.2021.

[263] Disponível em: https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32013L0037. Acesso em 16.10.2022.

[264] A Diretiva PSI foi emendada mais uma vez, pela Diretiva 2019/1024, disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX:32019L1024. Acesso em 05.03.2021.

[265] Disponível em: https://edps.europa.eu/sites/default/files/publication/12-04-18_open_data_en.pdf. Acesso em 05.03.2021.

implementadas, os dados divulgados não poderão ser usados para finalidades distintas das informadas ao titular.

Em seguida, aponta que um dos maiores desafios na implementação de políticas de dados abertos está em compatibilizar os diversos usos atribuídos aos dados com o **princípio da finalidade**, que busca assegurar ao indivíduo certo controle sobre o uso de seus dados. Outro desafio apontado está em alinhar o **princípio da proporcionalidade** enquanto se assegura maior flexibilidade nas formas de disponibilizar os dados pessoais. Para tanto, destaca a necessidade de serem avaliados os riscos da disponibilização e de informar os titulares de dados sobre a possibilidade de exercer os seus direitos.

Conforme consta na diretiva, dados pessoais podem ser disponibilizados conforme o regime legal próprio de cada país. De todo modo, quando da divulgação, é necessário realizar análise de risco (que determine se o dado pode ser divulgado) e adotar salvaguardas (e.g., restringir as finalidades de reuso), que avalie: **(i)** se há base legal para a divulgação e reuso dos dados; **(ii)** verificação das finalidades de reuso compatíveis com a finalidade da coleta do dado, **(iii)** se os solicitantes cumprem com as exigências das leis de proteção de dados pessoais; **(iv)** possibilidade de anonimização de dados, caso em que é necessário verificar a possibilidade de re-identificar o titular dos dados - se a técnica adotada não for suficiente para uma anonimização efetiva, que é cada vez mais difícil de se atingir, os dados seguirão afetados por normas de proteção de dados pessoais.

Além disso, recomenda que, a depender do risco associado à divulgação, solicitantes de acesso a informações mantidas pelo poder público sejam exigidos a cumprir com obrigações adicionais de governança de dados, como a elaboração de relatório de impacto e a adoção de salvaguardas adicionais - caso contrário, poderão ter rejeitado seu pedido de acesso aos dados.[266] O EDPS também recomendou que: **(a)** a autorização de reuso fosse condicionada à verificação da finalidade que será atribuída aos dados; **(b)** que o poder público possa cobrar pelos custos decorrentes da anonimização de dados pessoais, de forma a garantir que essa atividade seja realizada devidamente; **(c)** o governo elabore templates com boas

[266] Em abril de 2018 a Comissão Europeia adotou nova proposta de modificação da Directiva PSI (após aprovada, foi numerada Diretiva EU 2019/1024), com o objetivo de aumentar a quantidade de dados que são divulgados para reuso. Reagindo à proposta, o EDPS publicou a **Opinião nº 05/2018**. Em geral, o documento apresenta sugestões de modificação de redação para a proposta apresentada e reforça recomendações apresentadas em opiniões anteriores, como a observância aos princípios da minimização e transparência, o estímulo à participação social na definição sobre interesse público no reuso de dados, a elaboração de relatório de impacto e a adoção de salvaguardas para proteger direitos de titulares de dados. Disponível em: https://edps.europa.eu/sites/edp/files/publication/18-07-11_psi_directive_opinion_en.pdf. Acesso em 05.03.2021.

práticas de anonimização e de cláusulas de licença de uso de dados, de forma a garantir mais consistência nessas práticas entre os distintos órgãos de governo.

9.2 Guias sobre publicação de dados

União Européia, Publicação de dados para Transparência e Accountability

A WP 29 elaborou a **Opinião nº 05/2001**,[267] que debate a tensão entre proteção de dados pessoais, *accountability* e transparência da administração pública. Esse documento buscou apresentar considerações sobre a recomendação apresentada pelo Ombudsman do Parlamento Europeu para a Comissão Europeia diante de recurso apresentado por um cidadão contra negativa de acesso a documentos públicos que continham dados pessoais (i.e. documentos sobre quais atores apresentaram recomendações ou participaram de reuniões na Comissão).[268] Em síntese, como condição para apresentar documentos governamentais com dados pessoais em resposta a pedido de acesso à informação, a Comissão Europeia deveria ter solicitado o consentimento prévio aos indivíduos mencionados nesses documentos. No entanto, como o consentimento não foi provido, o Ombudsman recomendou à Comissão enviar os documentos solicitados mesmo sem o consentimento dos titulares de dados.

Diante desse cenário, o WP 29 argumentou que a publicação de dados para as finalidades de transparência e *accountability*, ainda que considerada lícita e legítima *a priori*, nem sempre seria compatível com o **princípio da finalidade**. Segundo argumentou, não seria possível pressupor que a publicação de dados será sempre considerada compatível com a finalidade da coleta, e que a decisão de publicação deveria ser avaliada conforme o contexto e tendo como base as seguintes variáveis: **(i)** se a oferta do dado pelo cidadão foi compulsória; **(ii)** o tipo de dado pessoal; e **(iii)** a situação do titular de dados e as consequências que a disponibilização poderá causar.

Levando isto em conta, argumentou que a disponibilização de dados deverá observar alguma das **bases legais**, realizando ressalvas específicas em relação às bases legais de cumprimento de obrigação legal ou regulatória e de exercício de competências legais e observado o interesse público. Como na publicação de dados há conflito entre obrigações legais (transparência e proteção de dados), a utilização dessas bases legais exige avaliar no caso concreto qual direito prevalece. Ainda, ressaltou que certos países europeus apresentam a

[267] Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp44_en.pdf. Acesso em 04.03.2021.
[268] Vide: https://www.ombudsman.europa.eu/en/recommendation/en/426. Acesso em 04.03.2021.

proteção de dados como exceção à obrigação de transparência governamental, mas também preveem a possibilidade de disponibilizar dados somente a certos sujeitos que demonstrem possuir legitimidade para tanto, ou apenas quando envolver certos tipos de dados ou categorias de titulares de dados envolvidos.

União Europeia, Publicação de salários de servidores públicos

Após isso, em paralelo à aprovação da GDPR, a WP 29 editou a **Opinião nº 02/2016** sobre a publicação de dados pessoais para fins de transparência no setor público.[269] O documento possui como objetivo a ponderação entre os princípios da transparência e da proteção de dados pessoais quando da divulgação de dados de funcionários públicos.

A Opinião nº 02/2016 se inicia argumentando que o tratamento dos dados disponibilizados deverá observar os princípios e bases legais previstos na legislação de dados pessoais. Como bases legais, aponta a possibilidade de a atividade ser fundamentada na necessidade do tratamento para o cumprimento de uma obrigação legal, que deverá ser legítima e proporcional às finalidades almejadas e não deverá ser demasiadamente ampla, ou para a execução de atividade em benefício do interesse público, caso em que deverão ser divulgados apenas os dados necessários ao alcance dessas finalidades.

Em relação aos princípios, destaca que a análise sobre a sua aplicação à situação concreta exige clareza sobre a **finalidade** almejada, que consiste na divulgação de informações e conhecimento sobre as atividades governamentais. Ressalta que, no que diz respeito ao princípio da **proporcionalidade**, a Corte de Justiça Europeia determinou[270] ser necessário às Cortes nacionais avaliar se a divulgação dos nomes e salários, na forma tal como instrumentalizada pelo governo local, seria proporcional e adequada às finalidades almejadas pela divulgação. Segundo argumenta, a aplicação desse princípio requer a

[269] Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp239_en.pdf. Acesso em 05.03.2021.

[270] Nos casos C-465/00, C-138/01, C-92/09, C-92/03 e 139/01, julgados conjuntamente, a Corte de Justiça da União Europeia analisou a compatibilidade da divulgação de dados sobre os rendimentos de funcionários de entidades sujeitas à auditoria do Tribunal de contas austríaco com a Diretiva 95/46/CE, que regulava a proteção de dados pessoais à época. O tribunal decidiu pela necessidade de se "ponderar o interesse da República da Áustria em garantir uma utilização óptima dos fundos públicos e, em especial, a manutenção dos salários em limites razoáveis com a gravidade da violação ao direito das pessoas em causa a respeito da sua vida privada" (tradução livre). Nesse sentido, o tribunal entendeu que os órgãos jurisdicionais deveriam avaliar se há, na lei que trata sobre a divulgação dos dados dos funcionários públicos, previsibilidade sobre a divulgação dos dados, inclusive do nome das pessoas em causa em relação com os rendimentos que auferem, e se a divulgação ocorre por tempo necessário e adequado ao objetivo geral perseguido. Ainda, a corte fixou entendimento que a Diretiva em questão era aplicável, mas leis nacionais poderiam regular a publicação de dados pessoais para fins de fiscalização, e que de forma alguma a lei local poderia ser interpretada no sentido de legitimar uma violação ao direito à vida privada (CJUE, 2003).

realização de relatório de impacto à privacidade dos titulares de dados, que deverá avaliar quais dados serão divulgados e se há outras formas de fazê-lo sem que isso afronte a privacidade de servidores e outros indivíduos. Essa avaliação deverá considerar os diferentes grupos de indivíduos (ex.: detentores de cargos políticos, servidores ou outros indivíduos), casos e finalidades da publicação de dados pessoais.

Já o princípio da **minimização** requer que seja realizada avaliação sobre a necessidade e proporcionalidade da atividade de tratamento de dados pessoais em curso (a quantidade de dados tratada deve ser relevante, necessária e não excessiva para o alcance das finalidades almejadas). Em algumas situações, não é necessário fornecer grande detalhamento de dados pessoais, sendo suficiente a publicação de relatórios contendo dados agregados, indicadores de performance (e.g.,: seria necessário divulgar dados pessoais sobre familiares de servidores públicos?). Por sua vez, o princípio da finalidade exige que dados sejam tratados observando as finalidades para as quais foram coletados ou para **finalidades compatíveis**, sendo legítimo o tratamento subsequente para o alcance do interesse público, para pesquisas históricas ou para fins estatísticos.

Em seguida, a WP 29 observa que cuidados adicionais devem ser empregados no tratamento de **dados pessoais sensíveis**. Isso significa que cuidados adicionais devem ser empregados no tratamento de bases de dados como aquelas que possuem dados relacionados a procedimentos investigatórios, processos penais e medidas de segurança (sua publicação deve ser excepcional e/ou considerar a ponderação entre direitos). Argumenta também que dados devem ser tratados somente pelo período em que forem necessários para o alcance de sua finalidade, o que levaria à existência de **períodos de retenção** diferentes para o tratamento do dado pelo órgão público e para sua divulgação em portais de transparência. Além disso, os dados devem estar corretos e serem **constantemente atualizados**, reforçando a necessidade de órgãos públicos permitirem aos cidadãos o direito de correção de dados pessoais.

Finalmente, a WP determina que devem ser adotadas medidas de segurança que impeçam o acesso não autorizado ou o uso inadequado aos dados pessoais, bem como assegurem mecanismos para o exercício dos direitos de titulares. Em especial, destaca o direito de informação, que poderá ser decorrente de legislação determinando a divulgação de dados.[271]

[271] De forma similar, em 2007, anteriormente à edição da GDPR, *Autoriteit Persoonsgevens* elaborou relatório relativo à licitude da publicação de dados pessoais na internet através, por exemplo, de sites, fóruns de discussão, revistas *on-line*, ou redes sociais, frente à regulação de proteção de dados. Segundo a autoridade,

Estados Unidos, Política de abertura de dados da cidade de Seattle

Em 2016, a cidade de Seattle nos Estados Unidos divulgou política de dados abertos na qual se comprometeu a manter dados abertos por pressuposto, salvo quando isso significar em afronta à privacidade dos munícipes.[272] Para tanto, a cidade se comprometeu a elaborar análises de risco anuais e solicitou ao *Future of Privacy Forum* ("FPF"), além de ter contado com o apoio de institutos de pesquisa, como o *Berkman Klein Center for Internet and Society* da Universidade de Harvard, a elaboração de metodologia para a realização dessa atividade.

Como se verá, esse relatório possui enfoque distinto das manifestações de autoridades europeias com competências relacionadas à proteção de dados pessoais. Isso porque, enquanto esse relatório aborda aspectos técnicos, operacionais e organizacionais para auxiliar o gestor público na abertura responsável de dados, as manifestações das autoridades europeias focam na interpretação ou elaboração de normas que possam conduzir essa abertura de dados com a preocupação com a proteção de dados pessoais de cidadãos.

Para tanto, o relatório argumenta que o primeiro passo seria realizar uma análise que pondere os **riscos e os benefícios** relacionados à abertura de bases de dados. Para tanto, deverá seguir os seguintes passos: **(a)** avaliar as informações constantes da base de dados, que envolve verificar se há identificadores, dados sensíveis, o contexto da coleta dos dados, e a

---

seria necessário àqueles tratam e publicam dados na internet agir com cuidado e transparência perante os titulares de dados, além de atuarem em acordo com limitação de finalidade, justificação, qualidade e proporcionalidade, garantia de direitos de informação, segurança e restrição de transferência para países fora da União Europeia. Antes mesmo da publicação do dado na internet, o controlador deverá adotar uma série de medidas para assegurar sua adequação às leis vigentes, inclusive a de proteção de dados. Nesse sentido, cabe ao controlador de dados: **(a)** determinar se a publicação tem um propósito legítimo e se esse propósito é compatível com a finalidade para o qual os dados foram originalmente coletados; **(b)** solicitar o consentimento dos sujeitos dos dados, ou então ser capaz de comprovar que a publicação é permitida com base em uma das outras regras legais sobre a necessidade da publicação; e **(c)** tratar os dados por tempo limitado, de forma adequada, relevante e não excessiva, incluindo a adoção de medidas de segurança. Após a publicação, o agente de tratamento deverá oferecer informações sobre o propósito e a estrutura da publicação, sem esperar requerimento do titular, e seguir responsável pela remoção de dados incorretos ou desatualizados, e da gestão do consentimento dos titulares. Em relação ao tratamento posterior à coleta, o responsável deve determinar se a publicação é compatível com a finalidade originária. A lei em vigor na época exigia um equilíbrio entre a finalidade primária e o tratamento posterior. Para isso, cinco critérios deveriam ser considerados: **(i)** a relação entre a finalidade do tratamento previsto e a finalidade para a qual os dados foram obtidos; **(ii)** a natureza dos dados em questão; **(iii)** as conseqüências do tratamento previsto para a pessoa em questão; **(iv)** a forma como os dados foram obtidos; e **(v)** a medida em que são fornecidas garantias adequadas para a pessoa em questão. A licitude do tratamento posterior estaria condicionada à satisfação desses requisitos para que, assim, o processamento fosse considerado legítimo e em acordo com a lei de proteção de dados. Além disso, a autoridade destacou que para órgãos e entidades governamentais: **(a)** a lei de dados explicitamente conclamou a aplicação de tecnologias de proteção à privacidade; e **(b)** a minimização de dados pessoais assume particular importância na medida em que cidadãos têm menos oportunidades ou confiança de se oporem a uma publicação específica. Disponível em: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf. Acesso em 24.09.2022.

[272] Vide: https://privacytools.seas.harvard.edu/files/privacytools/files/fpf.pdf. Acesso em 14.03.2021.

chance de reidentificação dos dados; **(b)** avaliar os benefícios reais ou potenciais atrelados à divulgação da base de dados; **(c)** avaliar os riscos reais e potenciais associados à divulgação da base de dados; **(d)** ponderar os benefícios em relação aos riscos, e **(e)** avaliar se há elementos que justifiquem a publicação de dados a despeito dos riscos à privacidade.

Em relação aos riscos, o relatório os qualifica como sendo relacionados à: **(i)** reidentificação de cidadãos; **(ii)** qualidade e legitimidade dos dados; e **(iii)** confiança social. Em relação ao primeiro risco apontado, argumenta que bases de dados divulgadas poderão conter identificadores ou permitir a posterior identificação de indivíduos, o que pode resultar na ocorrência de danos para os indivíduos (e.g., divulgação de registros com nomes de mulheres vítima de violência sexual ou de alunos de escolas públicas que se consultam com analistas) e até mesmo ao governo (e.g., perda de confiança e pagamento de indenizações). Além disso, ressalta que esses riscos são de difícil remediação, em vista da dificuldade de posteriormente remover dados divulgados na internet.

Para o segundo risco (qualidade e legitimidade dos dados), destaca que dados mantidos por governos possuem o pressuposto de veracidade e acurácia, motivo pelo qual a divulgação de dados inverídicos, ou desatualizados, poderá gerar riscos como a tomada de decisão incorreta, ineficiente ou ilícita, que poderá afetar o titular de dados ou terceiros (eg., a inclusão errada de nome em bases de dados criminais poderá afetar a empregabilidade ou *score* de crédito do indivíduo ou a decisão automatizada que reforça preconceitos raciais). Aponta também que dados divulgados sem a devida precaução poderá, dada a dificuldade de realizar controle sobre como os dados são posteriormente utilizados, facilitar práticas criminosas ou abusivas, como o roubo de identidade ou a consulta da vida pessoal por parte de familiares, empregadores ou vizinhos.

No que diz respeito ao terceiro risco (confiança social), o relatório aponta que a divulgação de dados pessoais sem a devida cautela poderá resultar em perda de credibilidade da política de dados abertos, do governo enquanto gestor de bases de dados e, consequentemente, reduzir a motivação para que haja participação social ou até mesmo motivar indivíduos a fornecerem informações falsas para proteger seus direitos (e.g., não atualizar endereço para que não fique disponível em *websites* de órgãos públicos). Para tanto, o relatório ressalta a necessidade de adotar medidas que protejam a privacidade de indivíduos durante todo o ciclo de vida dos dados (ou seja, desde sua coleta até a divulgação pelo órgão público), com destaque para as práticas de transparência.

Em seguida, o relatório argumenta pela necessidade de adotar uma estrutura de governança com capacidade de avaliar a adequação das práticas de dados abertos em relação às normas de privacidade. Para tanto, seria necessário adotar práticas como: nomear funcionário para ser responsável pela garantia da privacidade no programa, estabelecer princípios que guiarão o desenvolvimento do programa, conduzir treinamentos com todos os funcionários, adaptar procedimentos e políticas aos princípios de privacidade, prever reavaliações periódicas sobre as análises previamente realizadas, adotar mecanismos para obter *feedback* sobre as medidas adotadas, e registrar as medidas adotadas durante todo o ciclo de vida dos dados, incluindo o processo de avaliação de risco e benefício de cada uma das bases de dados divulgadas.

O relatório também defende a necessidade de implementar práticas capazes de avaliar: **(i)** a chance de reidentificação dos dados em vista da tecnologia possuída pelo órgão público,[273] **(ii)** a qualidade dos dados constantes da base de dados, como a constante atualização e reavaliação das bases de dados e a garantia de meio para que os titulares possam exercer seus direitos, e **(iii)** se a divulgação preserva direitos de titulares de dados em situação de maior vulnerabilidade social. Nesse último caso, será necessário: **(a)** avaliar a representatividade dos dados publicados para evitar a publicação de mais dados sobre determinados grupos sociais ou de dados que possam reforçar preconceitos existentes contra determinados grupos sociais;[274] e **(b)** assegurar a devida transparência sobre as práticas de

[273] "Para amadurecer completamente sua caixa de ferramentas de desidentificação e estratégias de mitigação, a Cidade de Seattle deve, conforme apropriado: Desenvolver políticas e procedimentos para conduzir uma triagem adicional de conjuntos de dados e elevar a revisão de conjuntos de dados de risco ou sensíveis a especialistas em controle de divulgação ou um conselho de revisão de divulgação, quando apropriado; Desenvolver ou obter ferramentas apropriadas para desidentificar tipos de dados não estruturados ou dinâmicos; Consultar especialistas em controle de divulgação estatística e investir em ferramentas programáticas para avaliar o risco de reidentificação entre conjuntos de dados (incluindo King County, Washington State, dados federais abertos e bancos de dados comerciais); Consultar especialistas em controle de divulgação estatística sobre e investir em privacidade diferencial ou soluções de computação multipartidária segura para liberar dados que representem um risco à privacidade, para fornecer a mais forte proteção conhecida contra ataques de reidentificação atualmente; Desenvolver políticas e procedimentos para lidar com dados legados sobre dados. 179eattle. Gov e para remover ou modificar conjuntos de dados existentes que representem um risco inadequado de reidentificação; Investigar opções para um esquema de acesso limitado ou controlado para conjuntos de dados mais sensíveis (como um enclave de dados, salvaguardas contratuais, ou modelo de acesso por níveis); Criar uma comissão de análise interna ou externa que seja responsável e transparente, com representação diversificada e capacidade interdisciplinar para avaliar conjuntos de dados que exijam análise avançada (como conjuntos de dados envolvendo dados sensíveis, onde os funcionários municipais são sujeitos de dados, ou dados que possam representar preocupações de justiça social); Adotar contratos de fornecedores (como com fornecedores de plataformas de dados abertas) que apoiam o desenvolvimento e a implantação de ferramentas de dados abertos, diferentes e privados." (tradução nossa) Vide: https://privacytools.seas.harvard.edu/files/privacytools/files/fpf.pdf. Acesso em 14.03.2021.

[274] Nas palavras da autoridade: "Além disso, uma distribuição injusta dos benefícios e riscos dos dados em uma comunidade pode reforçar os preconceitos sociais, disfarçar a tomada de decisões preconceituosas e bloquear

tratamento de dados (em políticas de privacidade e nos demais momentos de contato com o cidadão), educar cidadãos sobre privacidade e disponibilizar mecanismos para que possam exercer seus direitos. Além disso, o relatório sugere a priorização na divulgação de bases de dados que sejam consideradas de interesse público, que será avaliado tendo em vista quem são os titulares de dados, os possíveis interessados em consumir essas informações e a frequência em que são acessados ou solicitados.

O relatório entende que o programa de dados abertos deverá desenvolver políticas e procedimentos para que os cidadãos possuam razoável poder de escolha sobre a coleta de dados ou, ao menos, a publicação desses dados no programa, em observância às ferramentas disponíveis para garantia da justiça e equidade também no uso dos dados. Quando o consentimento dos cidadãos para a coleta de dados não for obtido, mas ainda for justificável o tratamento dos dados dessas pessoas, cabe ao município desenvolver controles de privacidade adicionais para assegurar que os dados pessoais sejam usados de forma leal e justa com o cidadãos, como a não publicação dos dados no programa, ou a restrição do seu uso a uma faixa mais restrita de finalidades.

Como forma de endereçar esses riscos, o relatório elaborou um modelo de análise sobre os riscos e benefícios associados aos dados abertos. Esse modelo avalia os tipos de dados contidos no conjunto de dados abertos, os benefícios potenciais, e riscos concomitantes, da divulgação pública desses dados, e as estratégias para uma desidentificação eficaz e mitigação de riscos. Esta avaliação sistemática, dividida em cinco passos, orienta os funcionários da cidade para determinar se o conjunto de dados deve ser publicado em um ambiente de acesso aberto ou limitado, ou se ele não deve ser publicado.

O primeiro passo é a avaliação das informações contidas no banco de dados que será aberto para verificar a existência de identificadores diretos ou indiretos, atributos sensíveis ou

---

a igualdade de oportunidades para as populações marginalizadas ou vulneráveis. Alguns interessados em dados abertos levantaram preocupações de que, particularmente quando comercializados, os dados públicos municipais podem ser usados para "baixar os valores de propriedade, seguro de linha vermelha, etc., em bairros com altas taxas de criminalidade, em vez de abordar essas questões". Se os dados representados no programa de dados abertos forem coletados desproporcionalmente de certas populações sobre outras, ou forem usados contra certas populações sobre outras, ou se os dados expuserem populações vulneráveis a maiores riscos de privacidade ou a uma taxa mais alta do que outras, eles podem ser injustos. Por exemplo, dado que as populações minoritárias e vulneráveis, incluindo as comunidades imigrantes, tendem a ser superprotegidas em comparação com as populações majoritárias, particularmente no contexto da aplicação da lei e dos serviços sociais, elas podem estar desproporcionalmente representadas em conjuntos de dados abertos, criando motivos férteis para imprecisões e enviesamentos na tomada de decisões ou até mesmo apenas na comunicação de dados. Os governos devem esforçar-se constantemente para servir a todos os seus cidadãos de forma justa e eqüitativa, por mais difícil que seja atingir o equilíbrio das ações." (tradução nossa) Vide: https://privacytools.seas.harvard.edu/files/privacytools/files/fpf.pdf. Acesso em 14.03.2021.

informações que são de fácil identificação, além da possibilidade de relacionar o banco de dados aberto com outros dados disponíveis publicamente. O segundo e terceiro passos são a identificação dos benefícios e riscos associados à abertura dos dados e a probabilidade que eles ocorram. A próxima etapa é a combinação e balanceamento das etapas anteriores para determinar o método apropriado de abrir os dados, como limitação de acesso ao ambiente de liberação dos dados ou a vedação de publicar dados atuais em um determinado período de tempo. O quinto passo é a avaliação e documentação dos fatores compensatórios que justificam a abertura dos dados diante, por exemplo, de um interesse público naquela informação.

Para que a abertura dos dados no caso concreto seja segura, o relatório aplicou os cinco passos do modelo em seis domínios diferentes, quais sejam: (i) liderança em privacidade e gestão de programas, (ii) avaliação de risco-benefício, (iii) ferramentas e estratégias de desidentificação, (iv) qualidade dos dados; (v) equidade e justiça, e (vi) transparência e engajamento público. Esses filtros foram aplicados para percepção do impacto do uso de dados abertos na privacidade dos cidadãos e na utilidade daquelas informações para governantes e agentes privados, principalmente na implementação de políticas públicas e no desenvolvimento de soluções efetivas para os desafios da cidade, além do custo operacional dessa ferramenta de dados abertos.

Com o programa de dados abertos, a cidade de Seattle, ao mesmo tempo que desenvolve estudos úteis para autoridades formuladoras de políticas públicas, empresas e órgãos de pesquisa e é transparente quanto à forma de tratamento de dados pessoais aos seus cidadãos, também garante os direitos de privacidade e intimidade. Nesse sentido, o incentivo ao engajamento público na definição de prioridades e organização de políticas baseadas em dados se mostra uma medida benéfica na concretização da transparência e prestação de contas na relação entre o cidadão e o Estado, como um agente relevante na coleta e uso de dados pessoais. A tomada de decisão sobre o tratamento de dados e sua publicação, em programas de dados abertos, também devem incorporar as contribuições dos cidadãos, já que são os sujeitos a sofrerem o maior impacto dessa atividade, seja na implementação de políticas públicas direcionadas, seja no uso indevido de dados (GREEN, 2017).

9.3 Guias sobre compartilhamento de dados

União Europeia, Estratégia de Dados

Em fevereiro de 2020, a Comissão Europeia publicou a **Estratégia de Dados**,[275] na qual reconhece haver potencial de crescimento e inovação na disponibilidade e fluxo ágil de dados entre diferentes agentes e em múltiplos setores, motivo pelo qual propõe a criação de um espaço comum de dados para a Europa. Entre as medidas prioritárias da estratégia estão a criação de estrutura de governança capaz de apoiar decisões sobre quais dados podem ser utilizados em quais situações, e a avaliação de mudanças legais para viabilizar e/ou agilizar práticas de compartilhamento responsável de dados.

Diante disso, a Comissão propôs, em 25 de novembro de 2020, uma regulação de governança de dados para a região[276] que busca aumentar a confiança em agentes intermediários na cadeia de utilização de dados e fortalecer mecanismos de compartilhamento de dados entre países-membros.[277] No entanto, antes da publicação da proposta de regulação e diante da proposta divulgada em fevereiro de 2020, em junho daquele ano o EDPS publicou a **Opinião nº 03/2020**, com o objetivo de contribuir com o encaminhamento do debate público no tema.

Para tanto, o EDPS destaca a necessidade de o tratamento de dados realizados em benefício do interesse público ser realizado em observância aos princípios e demais regras da GDPR. Para tanto, ressalta a importância dos princípios da finalidade, transparência, *accountability*, necessidade e proporcionalidade para garantir que dados pessoais serão tratados dentro das expectativas dos titulares de dados. No mesmo sentido, recomenda o estabelecimento de regras para **(a)** que o tratamento subsequente de dados ocorra em observância às regras de proteção de dados pessoais, em especial o *privacy by design* e o *privacy by default*, que exigem ao agente de tratamento observar regras de privacidade como pressuposto e em todas as etapas do ciclo de vida dos dados; e **(b)** lidar com o aumento na quantidade e magnitude dos riscos de segurança da informação.

O EDPS também elogiou propostas que: **(i)** forneçam meios para que indivíduos exerçam alguma forma de controle sobre o uso de seus dados, que devem ser associados com

[275] Disponível em: https://ec.europa.eu/digital-single-market/en/european-strategy-data. Acesso em 05.03.2021.
[276] Disponível em: https://ec.europa.eu/digital-single-market/en/european-data-governance. Acesso em 05.03.2021.
[277] Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767. Acesso em 05.03.2021.

o recebimento de informações claras e legíveis por máquina sobre como seus dados poderão ser utilizados - eg., com a adoção de *Personal information management systems* (PIMS); e **(ii)** reconheçam a importância na adoção de tecnologias que apoiam a privacidade no uso de dados (conhecidas como PET ou *privacy preserving technologies*).

Em seguida, recomenda: **(a)** que o tratamento de dados dentro do contexto da estratégia europeia de dados, por envolver o tratamento de grande quantidade de dados e de finalidades, requer a elaboração e a divulgação de relatórios de impacto; **(b)** a organização de estrutura de governança que conte com o envolvimento da sociedade, de modo a construir confiança por parte dos diferentes interessados;[278] e **(c)** que o uso de dados compartilhados com terceiros para finalidade de alcance de interesse público (e.g., melhoria de transporte público ou para medidas de saúde pública) para atividades subsequentes com fins comerciais (e.g., pelo mercado de seguros ou de *marketing*) deve ser evitada.

Também reconhece a relevância de avaliação de legislação setorial na criação de determinados grupos de dados (*data spaces*), em especial em setores nos quais a natureza dos dados impõe maiores riscos (e.g., setor de saúde) ou quando a análise de dados poderá ser benéfica ao interesse público (e.g., setor de pesquisa). A depender do caso, devem ser impostas limitações ao reuso de dados, como para o uso de dados genéticos pelo setor de seguros.

Finalmente, em relação aos agentes envolvidos no arranjo de *data spaces*, sugere: **(i)** a criação de controles capazes de filtrar as organizações que terão acesso aos dados; **(ii)** a adoção de parâmetros para a prática de entidades envolvidas na coleta e/ou compartilhamento de dados; e **(iii)** o incentivo a práticas de educação de cidadãos sobre o exercício de direitos sobre seus dados pessoais, especialmente em cenário no qual se incentiva o indivíduo a atuar de forma altruísta e fornecer seus dados para determinadas finalidades.

[278] "23. Neste contexto, a EDPS observa que os dados, em particular as informações do setor público, poderiam desempenhar um papel fundamental no Mercado Único Digital. Além disso, a utilização inteligente dos dados, incluindo seu processamento via Inteligência Artificial, pode ter um efeito transformador em vários setores da economia. Ao mesmo tempo, a EDPS assinala que o compartilhamento de dados para necessidades sociais e outras necessidades comuns deve estar sujeito às salvaguardas adequadas de proteção de dados, de acordo com os princípios da necessidade e proporcionalidade." (tradução nossa).

União Europeia, Data Governance Act

Em março de 2021, o EDPS e a EDPB editaram opinião conjunta[279] a respeito da proposta de regulação do Parlamento Europeu e do Conselho Europeu sobre Governança de Dados Europeia, também chamada de Lei de Governança de Dados (Data Governance Act ou "DGD"), e que é fruto das medidas destinadas a efetivar a Estratégia Europeia de Dados.[280] A DGD (Regulação EU 2022/868, aprovada em Maio de 2022) faz parte de uma estratégia europeia de dados e parte do pressuposto de que o aumento na confiança em intermediários de dados e o fortalecimento de mecanismos de compartilhamento de dados na Europa poderá fomentar a disponibilização de dados que, por sua vez, é essencial para o treinamento de sistemas de inteligência artificial.

Assim, a DGD busca solucionar uma tensão essencial ao compartilhamento de dados mantido pelo poder público, consistente em facilitar o amplo fluxo de dados governamentais e, ao mesmo tempo, respeitar princípios de proteção de dados pessoais que impedem o compartilhamento de dados pessoais por padrão (*by default*).

Para tanto, as autoridades primeiro demonstraram preocupação em não ser editada norma que modifique ou possua disposições conflitantes com a GDPR, especialmente quando isso signifique desamparar direitos de titulares de dados. Para tanto, apresentam algumas críticas e sugestões à proposta de texto legal. Nesse sentido, destacaram que determinados conceitos apresentados pela proposta de Data Governance Act devem ser adequados à GDPR, como os exemplos de detentor ou usuário de dados. Segundo a EDPS e a EDPB, os conceitos apresentados asseguram direitos de acesso, compartilhamento ou uso dos dados, mas deveriam se focar nas condições nas quais o tratamento de dados poderá ocorrer de forma legítima. Além disso, aponta a **dificuldade em diferenciar na prática**, especialmente em cenário de aumento no fluxo de dados e geração de *big data*, **os conceitos dados pessoais e dados não pessoais** (quando eles se referem a comportamentos humanos de sujeitos não identificados). Isso ocorre porque, quanto maior a disponibilidade de dados, aumentam as chances de eles serem combinados entre si e re-identificados.

Outra preocupação demonstrada está relacionada à proposta de Estados membros da União Europeia instituírem autoridades (chamadas de "competent bodies") para auxiliar os

[279] Disponível em: https://edpb.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf. Acesso em 28.04.2021.
[280] Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767. Acesso em 28.04.2021.

órgãos públicos que disponibilizam dados para reuso, por meio da orientação em relação a atividades como a concessão de acesso aos dados e gestão de consentimento. Segundo o EDPB e o EDPS, as atribuições dessas autoridades seriam similares às atualmente exercidas pelas autoridades de proteção de dados pessoais e essa **confusão de competências** poderia atribuir complexidade e inconsistência nas regras aplicáveis à reutilização de dados.

As autoridades também apontam que o reuso de dados pessoais deve estar fundamentado em uma das **bases legais previstas na GDPR**, de tal modo que as disposições do Data Governance Act não podem ser interpretadas como uma ampliação das bases legais já previstas na legislação europeia. Inclusive, refletem sobre como será viabilizada a disposição da proposta (art. 5(6)) que requer ao poder público a auxiliar os consumidores de dados a obter o consentimento dos titulares de dados, especialmente considerando a necessidade de haver uma base legal prévia que justifique o contato com o titular de dados para obter seu consentimento para as novas finalidades para as quais os dados serão utilizados.

Além disso, destacam a necessidade de observar os princípios de proteção de dados pessoais, com especial destaque aos **princípios da transparência e da finalidade**, que asseguram confiança aos titulares de dados sobre os limites dentro dos quais seus dados poderão ser utilizados (e.g., quais dados, para quais finalidades e por quem serão utilizados). Por isso, em relação ao princípio da finalidade, **(i)** ressaltam a necessidade de **evitar finalidades comerciais** no uso subsequente de dados coletados para entes públicos exercerem suas atribuições legais; e **(ii)** argumentam que o reuso de dados pessoais mantidos pelo poder público somente poderá ocorrer quando estiver fundamentado em lei que estabeleça de forma clara as finalidades consideradas compatíveis ou que constituam medidas necessárias e proporcionais para alcançar finalidades como a segurança nacional ou o interesse público. Em relação ao princípio da transparência criticam a ausência de referência, na proposta de Data Governance Act, de obrigações ao poder público de informar os titulares de dados ou de os envolver na tomada de decisão sobre como seus dados serão reutilizados.

Para assegurar observância às bases legais, princípios e direitos dos titulares de dados, bem como para avaliar quais salvaguardas adotar para minimizar os riscos relacionados ao reuso de dados, a EDPB e a EDPS recomendam que a proposta normativa preveja a necessidade de órgãos ou entidades públicas elaborarem, antes da divulgação dos dados, um **relatório de impacto** à proteção de dados pessoais. Sugerem também que entes públicos podem condicionar o acesso a dados, anonimizados ou não, mediante a **prévia assinatura de**

termo de confidencialidade que proíba o receptor dos dados a divulgá-los, reidentificá-los ou utilizá-los de maneira a colocar em risco direitos de titulares.[281]

Em relação à ideia de *marketplace* de dados abertos, com a participação de intermediários, argumentam que seria contrário aos princípios de proteção de dados pessoais caso não seja fornecido aos titulares de dados **informação e escolha sobre quem e para quais finalidades** seus dados são utilizados. Sobre esse respeito, ressaltam que os intermediários **(i)** não devem atuar como provedores de serviços de compartilhamento de dados, e sim como **facilitadores do exercício de direitos** de titulares de dados (por exemplo, pela oferta de sistemas de gestão de informações pessoais); e **(ii)** especialmente os especializados em *data pooling* ou no compartilhamento de dados, devem adotar **mecanismos para evidenciar** que o uso de dados é realizado **segundo as normas** de proteção de dados pessoais, aderir a determinados padrões de mercado e serem submetidos à supervisão de autoridade de proteção de dados pessoais.

Em seguida, abordam o conceito de altruísmo de dados, consistente em pessoas naturais ou jurídicas voluntariamente disponibilizando dados, sem compensação, para reuso para finalidades de interesse geral. Para a EDPB e EDPS, não resta claro qual a diferença prática desse conceito em relação à já existente possibilidade de titulares consentirem com o

[281] Com preocupações similares, em julho de 2021 a Autoridade de Proteção de Dados Holandesa (*Autoriteit Persoonsgevens*) produziu relatório investigativo sobre o impacto das aplicações de cidades inteligentes na proteção de dados pessoais em espaços públicos.# A preocupação levantada pela autoridade tem como origem o uso, em larga escala e em conjunto,# de dispositivos de rastreamento Wi-Fi ou Bluetooth, câmeras de vigilância ou até sensores que coletam dados de tráfego, temperatura ou som dos espaços públicos dos municípios. De imediato, a autoridade ressalta a necessidade de desenvolver modelos de governança e fomentar a conscientização da população a respeito do uso de dados gerados por dispositivos de smart cities em observância aos direitos e liberdades dos cidadãos. Para tanto, o relatório aponta ser primeiro necessário aos municípios identificar se a coleta de dados em áreas públicas estaria ocorrendo em observância à legislação aplicável, e registrar e atualizar informações sobre as condições do processamento de dados pessoais em aplicações de cidades inteligentes através, por exemplo, da elaboração de Relatório de Impacto à Proteção de Dados (RIPD). Após a verificação da legalidade do tratamento, seria recomendável se considerar também as questões éticas relacionadas à aplicação. Em vista do elevado risco de violação do direito à proteção de dados, a autoridade entende que deve ser conduzido um RIPD sempre que houver processamento em grande escala ou monitoramento sistemático de dados pessoais: (i) gerados por dispositivos conectados à internet que podem transmitir ou trocar dados via Internet, como dispositivos associados à Internet das Coisas; (ii) em espaços acessíveis ao público com, por exemplo, câmeras ou drones; (iii) de localização de pessoas físicas; ou (iv) capturados por câmeras de vigilância, como câmeras corporais. Também seria necessário elaborar RIPD no compartilhamento de dados pessoais através de parcerias nas quais os municípios ou outras autoridades trocam dados pessoais de natureza sensível com outras partes públicas ou privadas. Além disso, a autoridade recomenda a utilização por municípios de aplicações desenvolvidas com garantia da privacidade desde a concepção, e aponta conselhos municipais como sendo espaços adequados para discussão e conhecimento dos efeitos da tecnologia nos espaços públicos. Para a autoridade, o diagnóstico e mitigação de riscos decorrentes da adoção dessas tecnologias deve contar com conhecimento de cidadãos sobre os espaços públicos, enquanto usuários cotidianos daqueles ambientes. Disponível em: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/investigation_report_development_of_dutch_smart_cities.pdf. Acesso em 04.08.2022.

uso de seus dados para finalidades legítimas específicas. Como **não seria possível aos titulares de dados renunciarem a seus direitos** de proteção de dados pessoais, o consentimento nos casos de altruísmo ser protegido pelas mesmas salvaguardas previstas na GDPR, como a garantia de escolha livre e informada sobre **quais finalidades de reuso** deseja consentir, **revogar o consentimento** e obter a **deleção** de seus dados. Não seria, portanto, possível consentir para finalidades amplas como "atividades de interesse geral" e deve estar claro para o titular de dados que ele poderá revogar seu consentimento a qualquer momento.

Ainda, as autoridades: **(a)** recomendam que a nova norma preveja mais claramente os **requisitos e procedimentos para que entidades possam ser autorizadas a atuar** como receptoras de dados oriundos de altruísmo; **(b)** discordam da qualificação dessas entidades como operadoras; **(c)** desconfiam sobre as formas de **financiamento** dessas entidades e dos estímulos negativos que isso pode oferecer para a proteção dos dados que gerenciam; e **(d)** recomendam que o **termo de consentimento** para altruísmo de dados seja melhor estruturado e institucionalizado, passando pela aprovação de autoridades competentes. Finalmente, destacam que, nos casos em que houver compartilhamento de dados pessoais ou altruísmo de dados, autoridades de proteção de dados pessoais devem ser as responsáveis por conduzir atividades como as de orientação e fiscalização.

Em maio e novembro desse mesmo ano, o *European Data Protection Board* editou o **Comunicado 05/2021** para tratar sobre o desenvolvimento dos debates legislativos em torno do DGA[282] e o **Comunicado sobre o Pacote de Serviços Digitais e Estratégia de Dados.**[283] Para tanto, a autoridade reforçou o entendimento exarado na Opinião Conjunta que elaborou com o EDPS de que, embora a proposta normativa de DGA seja uma iniciativa relevante, ela precisa melhor dialogar com a legislação existente sobre (mas não somente) proteção de dados pessoais de forma a não impor grave risco a direitos de cidadãos e minar a confiança social na economia de dados. Em especial, reitera, (i) a competência das Autoridades de Proteção de Dados pessoais para regular e viabilizar o livre fluxo de dados pessoais; (ii) que direitos relacionados a dados pessoais não podem ser dispostos, de modo que são inválidas as regras que permitem ao cidadão prestar autorizações amplas para o uso de seus dados; (iii) a necessidade respeitar regimes de confidencialidade estatística para não prejudicar a confiança social em relação a essas atividades; (iv) que devem ser assegurados mecanismos efetivos

[282] Disponível em: https://edpb.europa.eu/system/files/2021-05/edpb_statementondga_19052021_en_0.pdf. Acesso em 16.10.2022.

[283] Disponível em: https://edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf. Acesso em 16.10.2022.

para que usuários possam exercer seus direitos; (v) nos casos em que aplicável, o dever de controladores realizarem relatórios de impacto; (vi) a necessidade de definir o conceito de finalidades de interesse geral que autoriza práticas de altruísmo de dados.

9.4 Aprendizados com a experiência estrangeira

A análise da experiência internacional permite a identificação de medidas que poderão ser observadas quando da decisão a respeito da divulgação de dados pessoais mantidos pelo poder público. Essas etapas em muito se assemelham para as atividades de compartilhamento e publicação dos dados, se diferenciando essencialmente em relação: **(i)** ao objetivo da divulgação dos dados, **(ii)** ao receptor dos dados, e **(iii)** à capacidade de controle por aquele que irá divulgar documentos ou bases de dados sobre como os dados serão utilizados após a publicação ou o compartilhamento.

Enquanto o compartilhamento de dados tem como destinatários sujeitos específicos (agentes públicos ou privados) para finalidade determinada (como o cumprimento de obrigação legal ou colaborar com a prestação de serviços privados), a publicação de dados tem como destinatários uma quantidade indeterminada de sujeitos (o público em geral) e busca preferencialmente promover transparência e *accountability* governamental. Disso decorre que no compartilhamento de dados o órgão público geralmente possui maior clareza sobre quais serão as finalidades que serão atribuídas aos dados pelos seus receptores. Já na publicação de dados, por mais que seja possível ao órgão ou entidade públicos impor controles e licenças ao uso subsequente dos dados, há menos controle sobre quais serão esses usos subsequentes - o que é razoavelmente esperado, na medida em que a publicação de dados pelo governo tem por objetivo fornecer à sociedade informações para que possam ser utilizadas para o desenvolvimento de atividades em prol do interesse público.

A despeito das diferenças, há consideráveis semelhanças nas preocupações apresentadas tanto para a avaliação e implementação, no caso concreto, do compartilhamento e da publicação de dados (e, em alguns casos, como na Diretiva PSI, a legislação acaba por abranger igualmente essas duas modalidades de tratamento de dados) em observância à privacidade. Entre as semelhanças identificadas estão a necessidade (e a dificuldade) de assegurar os princípios da finalidade, necessidade e transparência, a fundamentação da atividade em uma base legal (com preferência ao cumprimento de obrigação legal ou à execução de políticas públicas), a elaboração de relatório de impacto, garantia de mecanismos

para o exercício de direitos pelos titulares de dados, e a adoção de licenças e salvaguardas técnicas (inclusive com a remoção de dados pessoais, sempre que possível e desde que não prejudique o interesse público).

A seguir há quadro-resumo das soluções apontadas pelas autoridades da União Europeia e no estudo publicado pela Cidade de Seattle, nos Estados Unidos, sobre cuidados com a privacidade na publicação e o compartilhamento de dados pessoais:

Quadro 6: Comparativo das soluções apontadas pelas autoridades sobre privacidade na publicação e o compartilhamento de dados pessoais

<table>
<tr><th>Publicação</th><th>Compartilhamento</th></tr>
<tr><td colspan="2">Opinião nº 03/1999 da WP 29
(PSI - Dados publicados ou compartilhados para finalidades diversas)[284]
● Base legal;
● Princípio da finalidade (tratamento subsequente para finalidades compatíveis);
● Transparência;
● Obter consentimento e/ou oferecer meio para opt-out;
● Adoção de salvaguardas técnicas.</td></tr>
<tr><td>Opinião nº 05/2001 da WP 29
(Transparência)
● Compatibilidade deve considerar:
○ se a coleta foi compulsória;
○ tipo de dado pessoal;
○ situação do titular;
○ consequências do tratamento.
● Bases legais;
● Avaliação do interesse público</td><td>N/A</td></tr>
<tr><td colspan="2">Opinião nº 07/2003 da WP 29
(PSI - Dados publicados ou compartilhados para finalidades diversas)[285]</td></tr>
</table>

[284] Considera-se que que essa Diretiva se aplica à publicação e ao compartilhamento, como se verifica por esse excerto do Considerando (31) da Diretiva PSI vigente (Directive (EU) 2019/1024): “Public sector bodies are increasingly making their documents available for re-use in a proactive manner, by ensuring online discoverability and actual availability of documents and associated metadata in em open format that ca189em achinene-readable and that ensure interoperability, re-use and accessibility. Documents should also be made available for re-use following a request lodged by a re-user. In those cases, the time limit for replying to requests for re-use should be reasonable and in accordance with the equivalent time for requests to access the document under the relevant access regime”."

[285] Considera-se que que essa Diretiva se aplica à publicação e ao compartilhamento, como se verifica por esse excerto do Considerando (31) da Diretiva PSI vigente (Directive (EU) 2019/1024)“ "Public sector bodies are

● Base legal; ● Remoção dos dados pessoais, sempre que possível; ● Adoção de salvaguardas técnicas; ● Observância aos princípios de qualidade, minimização e finalidade; ● Compatibilidade deve considerar: ○ expectativas razoáveis dos indivíduos, ○ se a coleta foi compulsória; as circunstâncias do tratamento de dados, como a natureza do dado, a forma de coleta e as salvaguardas oferecidas ao titular de dados ● Para poder público, a finalidade deve estar restrita às suas competências legais; ● Reuso para finalidades comerciais deve ponderar direitos do titular de dados e interesses comerciais, com preferência ao primeiro critério.	
Opinião do EDPS sobre reuso de dados **(PSI - Dados publicados ou compartilhados para finalidades diversas)** ● Preocupação com a publicação: ○ possíveis usos finalidades ilegítimas, na medida em que os dados estariam acessíveis a qualquer interessado e em formato aberto; ○ Dificuldade de assegurar observância ao princípio da finalidade; ● Transparência sobre o tratamento e direitos; ● Adotar salvaguardas: ○ base legal; ○ limites ao reuso; ○ assegurar que solicitante pode cumprir com normas de proteção de dados; ○ sempre que possível, anonimizar dados. ● Para atividades de maior risco, condicionar acesso à elaboração de Relatórios de Impacto e possíveis medidas adicionai; ● Templates de boas práticas de cláusulas de licença de uso e anonimização.	
Opinião nº 02/2016 da WP 29 **(Transparência)** ● Princípios (finalidade, minimização, proporcionalidade); ● Bases legais; ○ cumprimento de obrigação legal ou regulatória; ○ execução de atividade para o	N/A

increasingly making their documents available for re-use in a proactive manner, by ensuring online discoverability and actual availability of documents and associated metadata in an open format that can be machine-readable and that ensure interoperability, re-use and accessibility. Documents should also be made available for re-use following a request lodged by a re-user. In those cases, the time limit for replying to requests for re-use should be reasonable and in accordance with the equivalent time for requests to access the document under the relevant access regime”."

interesse público. ● Relatório de Impacto; ● Cuidado com dados sensíveis; ● Cuidado com períodos de retenção; ● Atualização dos dados; ● Direitos dos titulares; ● Adoção de salvaguardas técnicas.	
N/A	**Opinião nº 03/2020 da EDPS** **(Estratégia de dados)** ● Busca do interesse público; ● Princípios (finalidade, transparência, necessidade, proporcionalidade e *accountability*); ● Mecanismos para que titulares exerçam controle sobre dados; ● Adoção de salvaguardas técnicas; ● Grande quantidade de dados requer: ○ relatório de impacto; ○ estrutura de governança. ● Evitar uso de dados para fins comerciais; ● Regulação setorial sobre reuso; ● Intermediários de dados devem: ○ filtrar quem acessa os dados; ○ incentivar educação cidadã; ○ criar parâmetros para coleta e acesso aos dados.
Opinião Conjunta EDPB e EDPS sobre o Data Governance Act ● Quanto mais dados, maiores chances de reidentificação; ● Base legal para reuso; ● Princípios (finalidade, transparência); ● Compatibilidade deve: ○ evitar fins comerciais; ○ estar baseado em lei ou necessárias e proporcionais ao interesse público. ● Transparência sobre o tratamento e direitos; ● Relatório de impacto; ● Direitos dos titulares; ● Possibilidade de condicionar acesso a dados e limitação de outros reusos. ● Intermediários de dados: ○ não devem atuar como intermediários de compartilhamento de dados, mas como	

facilitadores de exercícios de direitos; ○ adotar melhores práticas de proteção de dados. ● Altruísmo de dados deve assegurar consentimento nos termos da GDPR (ie.: finalidades específicas e revogável); ○ Templates de boas práticas de consentimento em altruísmo de dados; ○ Estabelecer requisitos e procedimentos para entidades intermediárias.	
Relatório FPF Seattle ● Quanto mais dados, maiores chances de reidentificação; ● Ponderação de riscos e benefícios deve considerar: ○ tipos de dados; ○ benefícios reais ou potenciais ○ riscos reais ou potenciais ● Riscos da publicação relacionados a: ○ reidentificação; ○ qualidade e legitimidade dos dados; ○ confiança social. ● Estrutura de governança com: ○ encarregado; ○ princípios, procedimentos e mecanismos de privacidade; ○ *accountability* e reavaliação periódica; ○ meios de feedback; ● Transparência sobre o tratamento e direitos.	N/A

Também é possível identificar importantes semelhanças entre as soluções apresentadas nos documentos de autoridades dos Estados Unidos e da Europa, embora tenham matrizes interpretativas distintas sobre privacidade e proteção de dados pessoais. Essa semelhança pode ser explicada tanto pelo fato de normas sobre privacidade serem guiadas pelos *Fair Information Principles*, ainda que com diferenças, como pela existência de redes globais cujas trocas influenciam na interpretação das normas sobre privacidade de forma a viabilizar o fluxo internacional de dados (SCHWARTZ, 2012).

Em relação aos pontos em comum, os documentos elaborados por autoridades da Europa e o relatório dos Estados Unidos se assemelham nos seguintes pontos: (i) estabelecer com precisão os objetivos da divulgação; (ii) avaliar o interesse público na divulgação; (iii)

estabelecer uma estrutura de governança; (iv) elaborar relatório de impacto; e (v) adotar salvaguardas técnicas e jurídicas. Já os pontos de divergência estão relacionados ao regime jurídico de proteção de dados pessoais em cada local: (a) nos documentos de autoridades Europeias a avaliação de interesse público exige a observância das legítimas expectativas dos titulares de dados sobre o tratamento, e no relatório dos Estados Unidos essa avaliação contou com maior preocupação na avaliação dos riscos e benefícios do tratamento; e (b) nos documentos de autoridades da Europa exigiam fundamentação em base legal e a observância aos princípios de proteção de dados, o que não se observou no relatório de Seattle.

Em seguida, um aspecto que chama a atenção diz respeito à evolução no entendimento das autoridades europeias sobre o papel do consentimento no compartilhamento e na publicação de dados por governos. Nos primeiros documentos elaborados, antes da vigência da GDPR, se apontou a necessidade de obtenção de consentimento dos titulares de dados (Opinião WP 29 nº 05/2001). No entanto, nas próximas opiniões o consentimento foi substituído por outras bases legais (desde que o órgão ou entidade pública esteja atuando dentro de sua competência), ainda que por vezes tenha se apontado ser necessário oferecer *opt-out* para certas finalidades (Opinião WP 29 nº 07/2003) e/ou mecanismos para que usuários possam exercer alguma forma de controle sobre o uso de seus dados.

Outro aspecto dos guias publicados pelas autoridades europeias que merece destaque consiste no reconhecimento de que o princípio da finalidade é um dos principais desafios à publicação e ao compartilhamento de dados pelo poder público, na medida em que o dado é coletado por força de uma obrigação legal ou como condição para que o cidadão possa usufruir de direitos ou de serviços públicos. Assim, para estarem de acordo com o princípio da finalidade, novos usos atribuídos aos dados deveriam, em tese, estar atrelados a essa finalidade legal original (que justificou a coleta). No entanto, considerando a relevância do reuso de dados pessoais mantidos por governos, os guias de autoridades europeias estabeleceram que a avaliação de reuso deve considerar a competência legal do órgão ou entidade que publicou ou compartilhou os dados, assim como as expectativas razoáveis dos titulares de dados, a natureza dos dados divulgados, as circunstâncias em que os dados foram coletados, quem são os receptores dos dados, e os possíveis riscos aos titulares de dados decorrentes da publicação. Essa avaliação contextual permite atribuir alguma flexibilidade ao princípio da finalidade, especialmente considerando que: **(i)** na publicação de dados em portais de transparência e dados abertos ou no compartilhamento de dados em respostas a pedidos de acesso à informação, não será possível condicionar o fornecimento da informação

à comunicação da finalidade do reuso; e **(ii)** há interesse público no reuso de dados pessoais para finalidades não estritamente atreladas à finalidade que justificou a coleta dos dados (como o exemplo da realização de pesquisas históricas ou para fins estatísticos).

Embora os guias sugiram evitar que dados divulgados para o alcance do interesse público sejam reutilizados para fins comerciais ou de *marketing*, os últimos documentos publicados sugerem alternativas que possam viabilizar esses e outros possíveis reusos a dados pessoais mantidos pelo poder público, como o fornecimento de mecanismos para que os titulares de dados possam exercer escolha livre e informada sobre quais as finalidades de reuso que desejam autorizar. Essa solução ainda é incipiente e está sendo debatida na europa, em vista de fatores como a viabilidade prática dessas propostas (se os usuários efetivamente acessarão essas ferramentas e exercerão essa escolha) e sobre os incentivos existentes para as entidades responsáveis por disponibilizar essas ferramentas de escolha (por exemplo, as autoridades temem que determinadas instituições poderão atuar mais como marketplace de informação e não como promotores de direitos de titulares de dados).

Em relação ao relatório da Cidade de Seattle, destaca-se o procedimento sugerido para a identificação dos riscos reais e específicos a cada iniciativa de publicação de dados, a exemplo da: **(i)** avaliação sobre a probabilidade de a divulgação de determinada base de dados desidentificada resultar na posterior identificação dos indivíduos quando associados a outras bases de dados divulgadas online; e da **(ii)** garantia sobre a qualidade e legitimidade dos dados publicados, na medida em que informações divulgadas por governos geralmente possuem maior presunção de veracidade e que o tratamento de dados inverídicos ou imprecisos poderá resultar em decisões equivocadas e que impactam direitos de cidadãos.

As soluções apontadas possuem respaldo no disposto na legislação vigente no Brasil, mas apresentam soluções interpretativas para questões ainda não resolvidas no país. Por exemplo, a legislação brasileira exige que o poder público estabeleça claramente os objetivos do ato administrativo de publicação ou compartilhamento de dados pessoais mantidos por governos, que deverá ser necessário ao alcance do interesse público. Além disso, será preciso que essas atividades sejam estejam respaldadas em uma base legal e que o gestor público assegure mecanismos para que titulares de dados exerçam seus direitos e implementem salvaguardas técnicas e jurídicas para proteger a privacidade de cidadãos.

10 PARÂMETROS PARA A DECISÃO SOBRE COMPARTILHAR E PUBLICAR DADOS PESSOAIS

Tendo em vista os parâmetros estabelecidos pela legislação e jurisprudência nacionais, e tendo em vista sua similaridade com a experiência estrangeira abordada, a seguir será apresentado procedimento para a decisão sobre o compartilhamento e a publicação de dados pessoais pelo poder público em observância à privacidade, assim como indicadas interpretações possíveis das normas da LGPD à luz das atividades do poder público. A decisão sobre a divulgação de dados pessoais exige ao menos duas principais etapas: (i) delimitar o escopo da publicação ou do compartilhamento de dados; e (ii) avaliar se há interesse público nessa atividade.

A avaliação sobre a identificação do interesse público será abordada no próximo capítulo e, caso ela resulte em recomendação da divulgação de dados pessoais, o capítulo subsequente abordará cuidados adicionais que deverão ser adotados para sua realização em observância à privacidade e proteção de dados pessoais. Neste momento, serão estabelecidos parâmetros para auxiliar na delimitação do escopo da divulgação de dados pessoais mantidos pelo poder público, que é essencial para a realização de análise sobre a presença de interesse público.

Para tanto, o primeiro passo do processo decisório consiste em identificar se os arquivos ou bases de dados que se deseja publicar ou compartilhar contêm dados pessoais. Em seguida, deve-se compreender a finalidade da divulgação, a necessidade desses dados para o alcance da finalidade pretendida, e quem são os possíveis interessados em acessar esses dados.

10.1 Verificação sobre a presença de dados pessoais

Entre as primeiras etapas para estabelecer se dados mantidos pelo poder público devem ser divulgados está a identificação da presença de dados pessoais nos arquivos e bases de dados que se deseja divulgar. Para tanto, o gestor público deverá identificar se os arquivos ou base de dados que serão compartilhados ou publicados possuem identificadores diretos ou indiretos, ou a chance de dados anonimizados ou pseudonimizados serem re-identificados. A seguir serão apresentados os conceitos de dados pessoais, dados anonimizados ou pseudonimizados que devem guiar o administrador público nessa avaliação.

Dados identificados ou identificáveis

Essa atividade possui alguma complexidade em função da amplitude de alcance do conceito de dados pessoais tal qual adotado pela legislação brasileira. Segundo a LGPD, são dados pessoais as informações que identificam ou permitem a identificação de uma pessoa natural (LGPD, art. 5º, I, Decreto nº 7.724/2012,[286] art. 3º, V e Decreto nº 8.771/2016,[287] art. 14, I). Além disso, não será considerado dado pessoal aquele "relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (art. 5º, III e IX e art. 12). Com isso, a legislação estabelece que serão dados pessoais aqueles que identificam ou, pela utilização de meios técnicos razoáveis e disponíveis, permitem identificar uma pessoa natural.

Esse conceito de dado pessoal possui respaldo em normas anteriores, aplicáveis ao poder público, como a LAI e o *Habeas data*, ainda que de forma menos específica que o Decreto regulamentador do MCI e a LGPD, conforme se verifica no quadro que segue:

Quadro 7: comparativo de conceituação legal de dado pessoal

Habeas Data (Lei n° 9.507/1997)	**LAI (Lei n° 12.527/2011)**	**Regulação do MCI (D n° 8.771/2016)**	**LGPD (Lei n° 13.709/2018)**
Não conceitua, mas protege informações relativas à pessoa do impetrante, em registro ou banco de dados de entidades governamentais ou de caráter público (art. 7°, I)	Informação pessoal: relacionada à pessoa natural identificada ou identificável (art. 4°, IV)	Dado Pessoal: relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa (art. 14, I)	Dado Pessoal: relacionada a pessoa natural identificada ou identificável (art. 5°, I).

Esse conceito de dado pessoal espelha o conceito estabelecido na Europa,[288] em que o

[286] Decreto que regula a LAI no âmbito da administração pública federal.

[287] Decreto que regula o Marco Civil.

[288] Como explicam Schwartz & Solove (2011), nos Estados Unidos o conceito de dado pessoal é historicamente bastante mais restrito do que aquele adotado pela Europa“ "(...) uma que evita tanto a visão reducionista dos Estados Unidos sobre o PII, quanto a visão expansionista da União Europeia. Na visão redutora, a tendência é considerar o PII como apenas aqueles dados pessoais que foram especificamente associados a uma pessoa específica. Esse modelo protege apenas os dados identificados e, portanto, deixa demasiadas informações pessoais sem proteção legal. Na visão expansionista, é irrelevante se as informações já foram vinculadas a uma determinada pessoa, ou podem ser vinculadas no futuro; esta visão trata os dados identificados e identificáveis como equivalente”." (tradução nossa).

dado pessoal será qualquer dado, independente de seu conteúdo ou forma,[289] que seja relacionado a uma pessoa física identificada ou identificável.[290] Por sua vez, a pessoa identificável será aquela que pode ser identificada, direta ou indiretamente, especialmente em conexão com um identificador como os exemplos de nome, dados de localização ou aspectos físicos da pessoa.

A determinação sobre a presença de um dado identificável passa por avaliar os meios que poderão ser razoavelmente utilizados para identificar uma pessoa, conforme é estabelecido pelo Considerando 26 da GDPR. A avaliação do que seriam razoáveis chances de meios serem utilizados para identificar uma pessoa, devem se considerar fatores objetivos como o custo e o tempo para alcançar a identificação e a tecnologia disponível pelo controlador ou por terceiros[291] no momento do tratamento.[292] Por sua vez, o Working Party 29 (2007), ao analisar o conceito, pontuou que outros fatores também deverão ser avaliados,

---

[289] No julgamento do caso Nowak pela Corte Europeia de Justiça“ "O uso da expressã“ "qualquer informaç”o" na definição do conceito d“ "dados pessoa”s", dentro do artigo 2(a) da Diretiva 95/46, reflete o objetivo do legislador demUE de atribuir um amplo escopo a esse conceito, que não se restringe a informações sensíveis ou privadas, mas potencialmente abrange todo tipo de informação, não apenas objetiva, mas também subjetiva, sob a forma de opiniões e avaliações, desde “ue "se relac”one" com o titular dos da”os." (tradução nossa). Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=612765. Acesso em 18.07.2022.

[290] No primeiro julgamento a respeito de dados pessoais (caso C-101/01 Bodil Lindqvist [2003] ECR I-12992.), a Corte de Justiça da União Europeia determinou o seguinte: "o ato de se referir, em uma página da Internet, a várias pessoas e identificá-las pelo nome ou por outros meios, por exemplo, dando seu número de telefone ou informações sobre suas condições de trabalho e hobbies, constitui "o tratamento de dados pessoais por meios total ou parcialmente automáticos" na acepção do artigo 3(1) da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados." (tradução nossa). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN. Acesso em 17.07.2022.

[291] Nesse sentido se posicionou a Corte de Justiça da União Europeia no caso Patrick Breyer v Bundesrepublik Deutschland (2016): “(...)fica claro, pela redação do artigo 2(a) da Diretiva 95/46, que uma pessoa identificável é aquela que pode ser identificada, direta ou indiretamente. O uso pela legislatura da em da palavr“ "indiretamen”e" sugere que, para tratar informações como dados pessoais, não é necessário que essas informações, por si só, permitam a identificação do sujeito dos dados. Além disso, o considerando 26 da Diretiva 95/46 afirma que, para determinar se uma pessoa é identificável, devem ser levados em conta todos os meios que possam ser razoavelmente utilizados pelo responsável pelo tratamento ou por qualquer outra pessoa para identificar a referida pessoa. Na medida em que esse considerando se refere aos meios susceptíveis de serem razoavelmente utilizados tanto pelo responsável pelo tratamento como po“ "qualquer outra pess”a", sua redação sugere que, para que as informações sejam tratadas com“ "dados pessoa”s" na acepção do artigo 2(a) dessa diretiva, não é necessário que todas as informações que permitam a identificação da pessoa em questão estejam nas mãos de uma única pesso”." (tradução nossa). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582. Acesso em 17.07.2022.

[292] Excerto do Considerando 26 da GDPR: “Para determinar se uma pessoa física é identificável, devem ser levados em conta todos os meios razoavelmente prováveis de serem utilizados, tais como singling out, seja pelo controlador ou por outra pessoa para identificar a pessoa física direta ou indiretamente. Para determinar se os meios são razoavelmente prováveis de serem utilizados para identificar a pessoa física, devem ser levados em conta todos os fatores objetivos, tais como os custos e o tempo necessário para a identificação, levando em consideração a tecnologia disponível no momento do processamento e do desenvolvimento tecnológico.” (tradução nossa). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 17.06.2022.

como os riscos de exposição dos dados em incidentes de segurança da informação, a forma como o tratamento é estruturado e as medidas adotadas para evitar a identificação.

De forma similar, a legislação do Canadá determina que dados pessoais serão aqueles relacionados a uma pessoa identificável, sendo necessário para tanto haver uma expectativa razoável de que os dados tratados permitam a identificação do indivíduo. Por exemplo, a Suprema Corte do Canadá, no caso *Ministry of Community Safety and Correctional Services v Information and Privacy Commissioner,*[293] determinou a divulgação a jornalista de lista com os primeiros dígitos do código postal da residência de pessoas julgadas pelo cometimento de crimes sexuais, sob o entendimento de que não haveria expectativa razoável de que os dados divulgados permitissem a identificação aos indivíduos sobre quem os dados se referem, motivo pelo qual não deveriam ser tratados como dados pessoais.[294]

Em outro caso (*Ontario Attorney General v. Pascoe*), o *Information and Privacy Commissioner* de Ontário (IPC), Autoridade de Proteção de Dados da Província, entendeu que a divulgação a jornalista de documento contendo lista e descritivo dos 10 maiores gastos realizados entre 1998 e 1999 pelo Plano de Saúde de Ontário, não resultaria em razoável expectativa de identificação. A Justificativa para tanto foi que o Ministério da Saúde não demonstrou: **(i)** a existência de poucos médicos na província que exercem as atividades descritas no relatório solicitado; ou **(ii)** de que forma a combinação desses dados a outras informações permite a identificação das pessoas sobre quem os dados se referem.[295]

---

[293] https://scc-csc.lexum.com/scc-csc/scc-csc/en/13613/1/document.do. Acesso em 09.06.2022.

[294] Após ter acesso aos dados, o jornalista divulgou mapa com uma representação visual de onde se encontram pessoas acusadas de cometimento de crimes sexuais (Conroy & Scassa, 2015)

[295] O IPC destaca outros casos em que o teste de expectativa razoável de identificação: "Conforme delineado nas representações do Ministério, na Ordem P-230, o ex-comissário Tom Wright declarou: "Se existe uma expectativa razoável de que o indivíduo possa ser identificado a partir das informações, então tais informações se qualificam na subseção 2(1) como informações pessoais". Concordo com esta abordagem e a adoto para o propósito deste recurso. Na Ordem P-644, a ex-Adjudicadora Anita Fineberg considerou a política do Ministério que tratava da "contagem de pequenas células". Nessa ordem, a informação em questão era a classificação dos médicos que exerciam certas especialidades e que também realizavam eletrólise. A este respeito, o Ministério fez as seguintes apresentações: "Os médicos encaminham seus pacientes a especialistas e o fato de que certos especialistas [sic] também realizavam eletrólise era amplamente conhecido. Além disso, esta informação seria do conhecimento dos pacientes que o especialista tratou. Portanto, estes especialistas podem ser identificados no domínio público. O fato de que há tão poucos em cada especialidade realizando eletrólise revelaria ou inferiria informações financeiras sobre os especialistas individuais e deve ser cortado sob a seção 21 da Lei". O ex-adjunto Fineberg considerou os comentários feitos pelo ex-comissário Wright na Ordem P-230 e aplicou essa abordagem na Ordem P-644. Ela concluiu que, dado o pequeno número de indivíduos e a natureza das informações em questão, havia uma expectativa razoável de que a divulgação das informações divulgaria informações sobre indivíduos identificáveis. Em outro recurso (Ordem P-1137), entretanto, que mais uma vez tratou da política de "contagem de pequenas células" do Ministério, ela adotou uma abordagem diferente para a questão. Ela declarou:" Na Ordem P-230, o Comissário Tom Wright declarou: Se existe uma expectativa razoável de que o indivíduo possa ser identificado a partir das informações, então tais informações se qualificam na subseção

Interessante notar que no Canadá, conforme se verifica pelos casos citados, o parâmetro para avaliar qual dado seria identificável perpassa por uma avaliação subjetiva das possibilidades de identificação, cabendo ao custodiante dos dados apresentar elementos que demonstrem a chance real de identificação. Embora na Europa a análise também envolva algum nível de subjetividade, autoridades europeias apontam para alguns elementos objetivos que auxiliam nessa determinação, como o custo da identificação e a tecnologia disponível no momento.

De todo modo, na Europa, Canadá e Brasil, a determinação sobre a presença de tais dados será contextual (SCHWARTZ; SOLOVE, 2011), ou seja, ela será avaliada com base nas particularidades do caso concreto e no momento em que o tratamento será realizado, de modo que um dado considerado como não pessoal no momento de sua coleta poderá posteriormente ser qualificado como dado pessoal em função de novas circunstâncias do tratamento, a exemplo da evolução da tecnologia. No entanto, diferente da Europa e Canadá, ainda não há no Brasil jurisprudência ou orientação da ANPD sobre como avaliar no caso concreto o que seriam dados identificáveis. Inclusive, em casos de rejeição a pedido de acesso à informação com base na privacidade de indivíduos, tanto a Controladoria-Geral da União como o Supremo Tribunal Federal partem do pressuposto de que o dado é pessoal e passam a avaliar se há interesse público na sua divulgação.[296]

2(1) como informações pessoais". Com base nas apresentações do Ministério e adotando o teste estabelecido acima, concluí na Ordem P-644 que, dado o pequeno número de indivíduos e a natureza das informações em questão, havia uma expectativa razoável de que a divulgação das informações divulgaria informações sobre indivíduos identificáveis. Assim, concluí que as informações em questão eram informações pessoais. Neste recurso, o Ministério argumenta que os números constituem informações pessoais somente com base no fato de que estão em grupos de menos de cinco pessoas. Ao contrário das informações fornecidas na Ordem P-644, o Ministério não indicou como a divulgação do fato de que havia um hemofílico em uma determinada província que contraiu o HIV e que fez uma reclamação poderia possivelmente resultar na identificação desse indivíduo. Por exemplo, para uma das províncias, o número de indivíduos hemofílicos infectados pelo HIV é o mesmo que o número de tais indivíduos que apresentaram uma reclamação contra a província. Este número foi revelado porque é maior do que cinco. Na minha opinião, a divulgação das informações do Registro 135 não poderia levar a uma expectativa razoável de que os indivíduos poderiam ser identificados. Por conseguinte, considero que este documento não contém as informações pessoais de nenhum indivíduo identificável. Portanto, a seção 21 não tem aplicação. O Registro 135 deve ser divulgado ao apelante em sua totalidade." (tradução nossa). Disponível em: https://decisions.ipc.on.ca/ipc-cipvp/orders/en/item/131197/index.do .Acesso em 17.07.2022.

296 A título de exemplo, a CGU decidiu, no processo de referência 60502.001286/2014-25, sobre a divulgação de documentos relacionados à promoção funcional de professores do Instituto Tecnológico de Aeronáutica. O requerente solicitou acesso a diversos documentos que continham dados pessoais para que pudesse realizar controle social por meio de investigação própria sobre eventual fraude no processo de promoção dentro da instituição. Durante a tramitação do processo nas instâncias inferiores, o requerente afirmou que o parecer solicitado por ele não continha dados que exponham a intimidade do docente avaliado, já que as informações tradicionalmente informadas neste tipo de documento são a respeito de aspectos funcionais e profissionais do docente. A autoridade requerida negou acesso aos documentos sob argumento de tutela da privacidade e intimidade por serem informações reveladoras de aspectos pessoais. Para a CGU, não havia, a priori, informações sensíveis nos documentos objeto do pedido e que elas estariam, em regra, disponíveis

Quando da divulgação de dados mantidos pelo poder público, é possível que dados constantes dos documentos ou bases de dados identifiquem diretamente uma pessoa (e.g., nome e CPF), permitam razoavelmente a identificação de pessoas (e.g., o CEP associado a outros dados permite identificar titulares de dados) ou não permitem a fácil identificação de uma pessoa (e.g., dados sobre precipitação de chuva na cidade). No entanto, a determinação pelo gestor público de quais dados deverão ser divulgados em observância às normas de proteção de dados oferece alguma complexidade porque os dados divulgados poderão ser posteriormente combinados com outros dados detidos pelo novo controlador ou por terceiros e resultar na identificação de seus titulares. Assim, um dado que originalmente era desidentificado ou incapaz de levar à identificação de alguém poderá assumir a qualidade de dado pessoal quando, diante de sua associação a outros dados ou até mesmo em função do avanço da tecnologia, permitir identificar, qualificar ou realizar inferências sobre uma pessoa natural.[297]

Na verdade, a complexidade na determinação sobre a presença de dados pessoais em documentos ou bases de dados não é uma particularidade da divulgação de dados pessoais pelo poder público. É por isso que a abrangência do conceito de dado pessoal vem sendo objeto de críticas e reflexões também em outros países. Como argumenta Purtova (2018), a evolução da tecnologia e o aumento do uso de informações, incluindo dados que geralmente não seriam associados a uma pessoa, como informações sobre o meio ambiente, para influenciar o cotidiano de pessoas, faz com que leis como a GDPR, que possuem um amplo conceito de dado pessoal, terão sua abrangência ampliada (se tornando "the law about everything"), na medida em que quase qualquer coisa pode ser associada a um indivíduo e, portanto, ser considerada dado pessoal.[298]

Diante dessa constatação, Solove e Schwartz (2014) propõem que princípios de proteção de dados pessoais (as já mencionadas FIPPs) devem se aplicar integralmente

---

publicamente pela plataforma Lattes, mas que seriam dados pessoais. Logo, a CGU determinou acesso aos documentos solicitados, tendo em vista que, segundo a Controladoria-Geral, a divulgação não afronta o direito de privacidade dos envolvidos, em que pese a opinião contrária existente em precedentes da CGU sobre matéria semelhante. Para mais informações, acesse: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/60502001286201425_CGU.pdf#search=%22privacidade%22. Acesso em 26.11.2022.

297 Além disso, é possível que a análise de bases de dados mistas (com dados pessoais e dados que, a princípio, não identificam uma pessoa natural) ou compostas de informações aparentemente não pessoais permita a extração de inferências sobre pessoas naturais. Por exemplo, bases de dados sobre mobilidade urbana, que possuem dados sobre a condição física das vias e sobre a circulação de automóveis na malha urbana, podem fornecer substratos para análises a respeito de rotinas de moradores de determinada região.

298 A autora argumenta que o conceito não deverá ser interpretado de forma mais restritiva, mas que a intensidade da regulação sobre os dados deve variar de acordo com as chances de os dados serem associados a um indivíduo.

somente quando os dados forem identificados ou quando houver risco significativo de que os dados sejam posteriormente identificados. Para verificar se um dado tem risco significativo de ser posteriormente identificado, o controlador deverá ponderar aspectos como o tempo em que a informação será mantida, as chances de futuro desenvolvimento da tecnologia, os incentivos que possui para identificar uma pessoa, e as medidas que adota para evitar que os dados sejam associados a um indivíduo. No caso de dados meramente identificáveis, os autores sugerem que apenas os FIPPs sobre segurança, transparência e qualidade dos dados deveriam se aplicar. Já os princípios relacionados a acesso, correção e deleção de dados não seriam aplicáveis na medida em que assegurá-los exige do controlador a manutenção de formas de associar os dados. Também não seriam aplicáveis os princípios relacionados à limitação de uso e minimização de dados, na medida em que garanti-los para dados meramente identificáveis exigiria esforço desproporcional ao risco que causam aos titulares de dados. Por sua vez, os autores recomendam que, quando houver reduzidas chances de identificação dos indivíduos sobre a que os dados se referem, os FIPPs não deverão se aplicar. Com isso, Solove e Schwartz buscam evitar a imposição de ônus excessivo ao uso de dados cujas chances de associação a uma pessoa natural são reduzidas.

De forma similar, sob a preocupação de que o amplo escopo da legislação sobre proteção de dados pessoais poderá prejudicar o mercado Europeu, o Parlamento Europeu editou a Regulação 2018/1807,[299] que regula o uso de dados não-pessoais. Esse Regulamento seria uma dentre as medidas da estratégia do Mercado Único Digital, anunciada pela Comissão Europeia para assegurar a livre circulação de bens, pessoas, serviços e capitais na região.[300] Conforme estabelece o Regulamento, suas normas se aplicam somente quando o tratamento de dados não envolver dados pessoais. No entanto, a norma não apresenta conceito objetivo para dado não-pessoal, apenas informando que serão dados pessoais aqueles não qualificados como dados pessoais. Por isso, o European Data Protection Supervisor pondera que tal definição será de difícil implementação prática, na medida em que a definição de dado pessoal é contextual e intencionalmente ampla (EDPS, 2018).[301]

---

[299] Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1807. Acesso em 17.07.2022.

[300] Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192. Acesso em 17.07.2022.

[301] No mesmo sentido se posicionaram Inge Graef, Raphael Gellert e Martin Husovec (2018): "a noção de dados não pessoais como ponto de partida para novas políticas de inovação de dados é contraproducente por três razões fundamentais: (1) os conjuntos de dados são freqüentemente mistos e os limites dos dados pessoais são muito fluidos para agir como âncora reguladora; (2) dois regimes separados aplicáveis a conjuntos de dados opacos podem levar a um comportamento estratégico de empresas explorando a rivalidade regulatória; (3) os dados têm valor econômico independentemente de sua classificação legal, e não há evidência de que

Como se verifica, a amplitude conceitual de dados pessoais poderá oferecer desafios práticos ao controlador, na medida em que todos (ou quase todos) os dados contidos em documentos ou bases de dados poderão ser qualificados como dados pessoais. Com isso, e considerando que governos mantêm grandes quantidades de dados, seria necessário adotar medidas de adequação à LGPD a quase toda atividade de tratamento de dados. Essa conclusão é ainda mais latente quando se trata de disponibilização de dados por governos, na medida em que, os receptores de dados poderão associá-los a um sem-número de outras bases de dados e acabar por identificar as pessoas sobre quem os dados se referem. Por isso, é recomendável à ANPD estabelecer critérios objetivos para auxiliar o gestor público na avaliação sobre a presença de dados pessoais nas bases de dados que gerencia, de forma a lhes promover segurança no desenvolvimento atividades de tratamento de dados pessoais e também para não impor ônus excessivo ao poder público no exercício de suas atribuições legais.

Por exemplo, as experiências internacionais e literatura apresentam parâmetros objetivos que podem ser aproveitados para a experiência nacional, como a avaliação, no caso concreto, de fatores como o custo da identificação, os riscos de exposição dos dados em incidentes de segurança da informação, a tecnologia no momento do tratamento e as medidas adotadas para evitar a identificação, e os estímulos que o controlador possui na identificação da pessoa.

Dados confidenciais, públicos ou tornados públicos não deixam de ser dados pessoais

O caráter confidencial ou público do dado não é relevante para sua categorização como dado pessoal. Ou seja, o fato de o dado ser enviado pelo titular de dados ao governo, ser divulgado com terceiros ou ser protegido por norma de sigilo (ou confidencialidade) não remove sua característica de dado pessoal.

Em relação à confidencialidade e sigilo de dados, ela poderá incidir sobre dados pessoais e dados não pessoais (por exemplo, alcançando dados de pessoas jurídicas), e resultará na restrição do tratamento de dados que resulte em sua revelação a terceiros não autorizados em legislação específica. A confidencialidade poderá assumir contornos distintos,

---

uma zona elusiva de dados não pessoais seja mais essencial como entrada de inovação. Argumentamos que uma abordagem holística dos "dados" como tais, que a priori incorpora considerações de proteção de dados em sua concepção, tem mais probabilidade de proporcionar uma política de inovação bem-sucedida." (tradução nossa).

a exemplo do sigilo de comunicações,[302] médico, financeiro, ou sobre informações que imponham risco à segurança da sociedade e do Estado,[303] e seu descumprimento poderá resultar em sanções administrativas (como a perda de licença de atuação profissional) ou criminais (a exemplo da quebra de sigilo bancário, tal qual previsto na Lei Complementar 105).

As regras de sigilo têm fundamentos distintos. Por exemplo, o sigilo de comunicações e o sigilo bancário buscam proteger cidadãos contra práticas como a vigilância estatal, e o sigilo regulamentado pela LAI busca evitar que a divulgação de certas informações mantidas pelo poder público ofereça risco à segurança da sociedade e do Estado. A despeito de regularem a circulação de dados, impondo requisitos adicionais ao tratamento de dados consistente em divulgar dados a terceiros, não removem do dado a qualidade de dados pessoais. Também não atribuem a dados não pessoais as proteções oferecidas pela legislação, especialmente pela LGPD, a informações relacionadas a uma pessoa física. Como mencionado, as normas de sigilo apenas limitam a circulação de determinados dados e informações.

A legislação brasileira de proteção de dados também determina que o dado pessoal poderá ser qualificado como "dado cujo acesso é público" ou "dado tornado público pelo titular". Na primeira situação (dado cujo acesso é público), o dado será divulgado ao público por alguma obrigação legal ou regulatória (e.g., dados pessoais contidos em documentos processuais, obrigações legais de publicidade em sociedades anônimas etc.).[304] Para Giovanna Milanez (2021), o conceito de dado de acesso público é abrangente, estando presente sempre que observados os seguintes critérios "(i) a publicidade ampla do dado, ou seja, seu livre

---

[302] O sigilo de comunicações (Constituição Federal, art. 5º, XII) foi interpretado pelo Supremo Tribunal Federal de tal forma a não se referir ao conteúdo das informações comunicadas por telefone (estando excluídas comunicações por telegramas e cartas) ou aos metadados a elas relacionados (eg., tempo de duração e circunstâncias da comunicação), mas à sua comunicação

[303] A legislação reconhece sigilo nos casos em que a informação solicitada por cidadão em pedido acesso à informação é imprescindível à segurança da sociedade e do Estado (art. 5º, XXXIII, da CF), caso em que é classificada como ultrassecreta, secreta ou reservada. O art. 23 da LAI explicita casos que estariam subsumidos a esta previsão de sigilo, como em situações nas quais a informação possa: (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; ou (iii) pôr em risco a vida, a segurança ou a saúde da população.

[304] Nesse sentido se posicionou Juliana Ruiz no artigo "o que são dados públicos?", divulgado pelo centro de pesquisas InternetLab: "entende-se que dados de acesso público são dados cuja divulgação pública é obrigatória por lei – o fato de alguém ser proprietário de um imóvel, ou sócio de uma empresa, por exemplo, ou os dados acerca das atividades de órgãos públicos, nos termos da Lei de Acesso a Informações." Disponível em: https://internetlab.org.br/pt/opiniao/o-que-sao-dados-publicos/#:~:text=Seja%20como%20for%2C%20entende%2Dse,Lei%20de%20Acesso%20a%20Informa%C3%A7%C3%B5es. Acesso em 12.10.2022.

acesso pelo público geral; e (ii) a divulgação do dado por terceiros que não o próprio titular", o que envolve o "divulgado publicamente por terceiros com livre acesso pelo público em geral (publicidade e acessibilidade amplas)." Para esta tese, esse conceito mais abrangente exige que a divulgação seja realizada dentro das legítimas expectativas do titular de dados. Caso contrário, a divulgação será indevida e os dados somente poderão ser legitimamente reutilizados com ciência e anuência do titular de dados, de modo a buscar superar a ausência dos requisitos de validade do ato da divulgação.

Em seguida, é interessante a diferenciação apontada pela mesma autora (MILANEZ, 2021) de que dados públicos seriam tal como o conceito de dado acessível ao público no art. 2º, II, do Decreto nº 8.777/2016, que são "aqueles gerados ou que se encontram sob a guarda do Governo Federal e que não estejam sob sigilo ou restrição de acesso" e que dados disponíveis publicamente seriam tal como o conceito de dados abertos previsto no art. 2º, III, do Decreto nº 8.777/2016: "referem-se basicamente a dados que são acessíveis ao público no geral." Embora esta tese prefira o termo "dados mantidos pelo poder público" ao termo "dados públicos", e reconheça que nem todo dado disponível publicamente observará os requisitos para que um dado seja qualificado como dado aberto, a distinção realizada entre dados públicos e dados disponíveis publicamente reconhece que há dados mantidos pelo poder público que possuem o potencial de serem divulgados (na medida em que não são protegidos por normas de sigilo ou restrição de acesso), mas que ainda não o são.[305]

Na segunda situação (dado tornado público pelo titular), o titular de dados voluntariamente publica suas informações a uma coletividade (ex.: informação sobre profissão tornada pública na rede social do titular). Neste ponto, concorda-se com Giovanna Milanez (2021) quando argumenta ser necessário estar clara pretensão e expectativa do indivíduo de que seus dados serão divulgados ao público e poderão ser posteriormente reutilizados por terceiros, assim como que o controlador deverá assegurar que essa decisão foi alcançada de maneira informada e não acidental ou involuntária.

De todo modo, tanto no caso de dados cujo acesso é público e de dados tornados públicos pelo titular de dados, os dados divulgados permanecem na qualidade de dados pessoais enquanto identificarem ou permitirem a identificação de um titular de uma pessoa

[305] Ainda que com divergências sobre o conceito de dado aberto, esta tese concorda com Giovanna Milanez (2021)) quando afirma que "é possível evidenciar que todo dado público tem vocação para ser um dado disponível publicamente, bastando que este esteja à disposição de qualquer cidadão. Quando isso acontece, o dado público torna-se um dado aberto e, caso possua o qualificador pessoal, ou seja, esteja relacionado a uma pessoa natural identificada ou identificável, torna-se, em verdade, um dado pessoal de acesso público, conforme ilustrado na imagem abaixo."

física.[306] A divulgação de um dado não remove a sua qualidade de dado pessoal (ou de se tornar dado pessoal quando associado a outros dados) e tampouco afasta o dever de serem observados cuidados específicos quando do seu reuso. Conforme será abordado em mais detalhes adiante, para esses dados a LGPD apresentou regulação própria, reconhecendo a relevância do seu uso (para o dado cujo acesso é público) ou a autorização prévia fornecida pelo titular de dados (para o dado tornado manifestamente público pelo titular de dados), de modo a flexibilizar exigências, mas seguir exigindo, que eles sejam tratados conforme as boas práticas estabelecidas na legislação.

No entanto, é importante ressalvar que esses conceitos não alcançam qualquer dado que esteja disponível na internet, mas somente aqueles que forem divulgados por determinação legal ou por manifestação expressa do titular de dados. Assim, dados divulgados de outras maneiras, especialmente por razão de incidentes de segurança da informação, como phishing e ataques hacker, não serão abrangidos pela regulação do art 7º, §§ 3º e 4º da LGPD.

Posicionamento similar pode ser encontrado em manifestação da *Working Party 29* (a extinta autoridade europeia com competência interpretativa sobre a legislação de proteção de dados pessoais) na Opinião nº 03/1999. Segundo o WP 29, o termo "dados disponíveis publicamente", utilizado nos casos em que dados mantidos por governos são publicados em portais oficiais, deveria ser evitado por criar a impressão de que poderiam ser utilizadas para quaisquer finalidades. Isso porque, mesmo que disponibilizados para acesso por uma maior quantidade de interessados, dados que permitam a identificação de uma pessoa natural não perderão sua qualificação como pessoais e seu tratamento estará abrangido por normas específicas (WP 29, 1999).

No mesmo sentido se manifestou o Tribunal de Justiça da União Europeia (TJUE) no caso C-73/2007 (conhecido como *Satakunnan & Satamedia*), no qual se discutiu se a coleta de dados fiscais de cidadãos disponibilizados por órgão público, bem como sua posterior publicação em jornal e divulgação por CD ou SMS seriam consideradas atividades de tratamento de dados pessoais. Na oportunidade, o Tribunal entendeu que a Diretiva 95/46/EC

[306] Novamente concordamos com o posicionamento de Juliana Ruiz no artigo "o que são dados públicos?", divulgado pelo centro de pesquisas InternetLab de que: "se, por um lado, o requisito do consentimento parece não ser necessário para o tratamento de dados públicos, por outro, todas as demais normas relativas à proteção de dados são aplicáveis, inclusive os princípios da finalidade, adequação, não discriminação, entre outros. ." Disponível em: https://internetlab.org.br/pt/opiniao/o-que-sao-dados-publicos/#:~:text=Seja%20como%20for%2C%20entende%2Dse,Lei%20de%20Acesso%20a%20Informa%C3%A7%C3%B5es. Acesso em 12.10.2022.

(norma europeia de proteção de dados pessoais que precedeu a GDPR) deveria ser aplicada mesmo quando os dados em questão fossem públicos.[307] Portanto, o mero fato de os dados em questão serem do setor público não justificaria um direito das empresas em utilizá-los para quaisquer propósitos ou não cumprir com as determinações legais preexistentes. Vale ressaltar que a decisão foi posteriormente confirmada pela Corte Europeia de Direitos Humanos em 2017[308], o que reforça a plausibilidade dos seus argumentos.

Similar entendimento é adotado em outros países da América Latina, como o México. Segundo a autoridade de proteção de dados pessoais Mexicana (INAI, *Instituto Nacional de Transparência, Accesso à la Información y Proteção de Datos Personales*), embora os dados disponíveis em uma fonte de acesso público não possam ser considerados como informação confidencial, sua acessibilidade ao público não afasta o princípio da finalidade, que deverá orientar todo o tratamento de dados pessoais.[309] Da mesma forma, embora a lei Mexicana afaste a necessidade de obter consentimento (no México, o consentimento é a única base legal

---

[307] "Importa assinalar que os dados objecto desta questão, que respeitam ao apelido e ao nome de determinadas pessoas singulares cujos rendimentos excedem determinados limites, bem como, nomeadamente, avaliado com uma margem de erro de 100 euros, ao montante dos respectivos rendimentos do trabalho e do capital, constituem dados pessoais, na acepção do artigo 2.°, alínea a), da directiva, uma vez que se trata de «informação relativa a uma pessoa singular identificada ou identificável» (v., igualmente, acórdão de 20 de Maio de 2003, Österreichischer Rundfunk e o., C‑ 465/00, C‑ 138/01 e C‑ 139/01, Colect., p. I‑ 4989, n.° 64). Basta referir, em seguida, que resulta claramente da própria leitura da definição contida no artigo 2.°, alínea b), da directiva que a actividade objecto desta questão é abrangida pela definição de «tratamento de dados pessoais», na acepção dessa disposição da directiva.Por conseguinte, há que responder à primeira questão que o artigo 3.°, n.° 1, da directiva deve ser interpretado no sentido de que o facto de os dados de pessoas singulares relativos aos seus rendimentos do trabalho e do capital e ao seu património: - serem recolhidos com base em documentos públicos da Administração Fiscal e tratados para efeitos de publicação; - serem publicados por categoria de rendimentos e por ordem alfabética, sob a forma de listas elaboradas em cada município; - serem cedidos em CD‑ ROM para efeitos de tratamento com objectivos comerciais; - serem utilizados no âmbito de um serviço de SMS que permite aos utilizadores de telefones móveis, após enviarem para um número determinado uma mensagem curta com o nome e o domicílio de uma pessoa, receber os dados sobre os rendimentos do trabalho e do capital dessa pessoa, bem como sobre o seu património; deve ser considerado «tratamento de dados pessoais», na acepção dessa disposição." Decisão disponível em: https://curia.europa.eu/juris/document/document.jsf;jsessionid=7C8116ACA27A0C978056F6AD2B06A816?text=&docid=76075&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=818229. Acesso em 21.04.2021

[308] Matéria sobre o caso: https://medium.com/golden-data/satakunnan-and-satamedia-freedom-of-expression-v-data-protection-in-the-eu-e0b95b3cffd7. Acesso em 21.04.2021

[309] Segundo Mejia (2020): "Na prática do Órgão de Transparência, esta tipologia é inexistente e estranha. É, em seu quadro de referência, uma exceção ou uma anomalia; um oximoro, uma contradição típica em termos de termos. O fato de as informações pessoais terem sido objeto de publicidade, por estarem em um registro público ou em uma fonte publicamente acessível, não as torna públicas informações pessoais per se" e "Diante da possível antinomia entre o último parágrafo do artigo 18 (não confidencialidade das informações pessoais encontradas em registros públicos ou em fontes publicamente acessíveis), e o artigo 20, seção II (dados pessoais só podem ser processados para a finalidade para a qual foram obtidos), o IFAI, em seu critério 013 de 2009, afirmou que o princípio da finalidade tinha prioridade"(tradução nossa).

aplicável)[310] para o tratamento de dados obtidos de fontes de acesso público, seu manuseio deverá ocorrer em observância às regras de proteção de dados pessoais (art. 42).

Interessante notar que a Lei define como fontes de acesso público às bases de dados, os documentos ou os arquivos que, por força de lei, podem ser consultados por qualquer pessoa e não contenham informações obtidas de forma ilícita, a exemplo das (i) páginas da Internet projetadas para fornecer informações ao público e estejam abertas à consulta geral; (ii) listas telefônicas nos termos da regulamentação específica; (iii) jornais, periódicos e diários oficiais, de acordo com seus regulamentos; (iv) meios de comunicação social (art. 5). Com isso, o legislador restringe o alcance do conceito de dados obtidos de fontes públicas, que resulta na dispensa de consentimento, para informações tornadas públicas por força de lei, acessíveis a todo o público e que não tenham restrição legal de acesso.

No Canadá, a *Privacy Act*,[311] legislação que o tratamento de dados pelo poder público, que será mais detidamente abordada adiante, não apresenta conceito para dados publicamente acessíveis, mas assim como ocorre no México, afasta a necessidade de obter consentimento para o tratamento de tais dados (o Canadá também só possui consentimento como base legal). Além disso, como aponta a OPC, autoridade Canadense de proteção de dados pessoais, o conceito não deverá ser tão amplo para afastar qualquer proteção à privacidade dos indivíduos, de forma que somente serão considerados publicamente acessíveis os dados que estejam razoavelmente acessíveis a qualquer pessoa.[312]

Em 2020 o governo Canadense iniciou consulta pública destinada a modernizar o *Privacy Act*[313] e, entre os temas objeto de discussão, estão a regulação sobre o conceito e cuidados que devem ser adotados no tratamento de dados acessíveis publicamente. Segundo a proposta de governo, que está em geral alinhada com os conceitos da LGPD, serão considerados como de acesso público aqueles dados **(i)** tornados manifestamente públicos pelo indivíduo a que se refere, **(ii)** disponíveis de forma ampla e contínua para todos os membros do público e o indivíduo não tem expectativa razoável de privacidade das informações; e **(iii)** disponíveis ao público por força de legislação. A OPC se manifestou sobre essa proposta, reforçando que a habilidade de acessar dados pessoais online não remove

---

310 Disponível em: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf. Acesso em 18.07.2022.
311 Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html. Acesso em 18.07.2022.
312 Disponível em https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_r/pa_reform_060605/. Acesso em 19.07.2022.
313 Vide: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html. Acesso em 19.06.2022.

sua qualidade de dados pessoais e que seu tratamento deverá ocorrer de acordo com o estabelecido em legislação.[314]

Conforme se verifica, não somente a legislação brasileira, mas também de países de diversas regiões no mundo, reconhecem que a qualidade de dado pessoal não é determinada pela confidencialidade ou publicidade do dado, mas pela sua capacidade de identificar um indivíduo. Além disso, verifica-se que, embora a legislação brasileira e estrangeira flexibilize determinadas regras para o tratamento desses dados (e.g., dispensa de consentimento para o tratamento de dados tornados manifestamente públicos pelo titular de dados), exige que seja realizado em observância às demais normas da lei de proteção de dados pessoais.

Dados anonimizados ou pseudonimizados

Por outro lado, a LGPD estabelece que não será considerado dado pessoal o dado anonimizado, isto é, o dado que não possibilite a identificação de um titular, sendo impossível a sua associação direta ou indireta a um indivíduo por meio da utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (LGPD, art. 5°, III e XI). Importante notar que o dado anonimizado poderá ser reconsiderado como dado pessoal se o processo de anonimização ao qual os dados foram submetidos for revertido mediante a utilização exclusiva de meios próprios[315] ou pelo emprego de esforços razoáveis e disponíveis no momento do tratamento (LGPD, arts. 6º, XI e 12).[316] Assim, se for possível re-identificar o dado de alguma forma, este não será considerado anonimizado e será submetido às regras da LGPD. Por sua vez, quando o dado apenas perde a possibilidade de associação momentânea a um indivíduo, trata-se de pseudonimização (LGPD, art. 13, § 4º). Exemplo desse caso consiste na re-identificação de um indivíduo pelo uso de informação adicional, como uma chave mantida separadamente em ambiente controlado e seguro.

---

[314] Mais informações em https://priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_jus_pa_2103/. Acesso em 19.06.2022.

[315] Uma vez que o controlador desidentifica os dados e disponibiliza-os para outras partes sem as chaves ou qualquer outra engenharia de reversão que possam os re-identificar, para esses terceiros, esses dados estarão anonimizados. Isso porque a chave não faria parte dos meios próprios do terceiro para reverter o processo de anonimização. No entanto, da perspectiva do controlador e para seu tratamento interno, esses dados seriam sempre pessoais, pois o controlador possui um meio próprio (chave) para re-identificá-los. Nestes casos, estaríamos diante de tratamento de dados pseudononimizados.

[316] A qualificação do conceito de **razoabilidade** deverá levar em consideração fatores objetivos (tempo para a reversão ou processo de anonimização) e deverá ser esclarecida pela Autoridade Nacional de Proteção de Dados ("ANPD"). Assim, se para a correlação entre um dado e uma pessoa demanda-se um esforço fora do razoável, o dado será considerado anonimizado e, portanto, não-pessoal.

A LGPD não traz definições e critérios técnicos objetivos para que se considere que algum dado está suficientemente anonimizado. De fato, a lei não explica o conceito de esforços razoáveis para reversão do processo de anonimização (central para identificar se o dado será pessoal ou anonimizado), mas estabelece quais parâmetros que deverão ser observados nessa análise, como o custo e o tempo necessários para reverter o processo de anonimização e a tecnologia disponível no momento do tratamento (BIONI, 2020).

O mesmo é aplicável quando se observa a legislação europeia, que estabelece conceito similar de anonimização (utilização de meios técnicos razoáveis e disponíveis na ocasião que não implique na re-identificação dos dados) e também não traz critérios objetivos para definir dado anonimizado. Não obstante isso, autoridades europeias se manifestaram sobre o tema, a exemplo da WP 29, reconhecendo a dificuldade de alcançar a anonimização absoluta, motivo pelo qual estabelecem a necessidade de avaliá-la no contexto em que aconteceu e exigem que o agente responsável pelo tratamento não consiga realizar posterior re-identificação dos dados. Para a avaliação do contexto, a WP 29 recomenda que sejam verificados fatores como custos e recursos exigidos para a reidentificação, além da probabilidade de reidentificação quando são removidos apenas identificadores ou quando o agente de tratamento de dados ainda possui acesso à base de dados não anonimizada. Assim, quanto mais alto for o gasto e a quantidade de recursos empregados, menor a chance de outros agentes terem sucesso na re-identificação.

Assim, o conceito de anonimização é demasiadamente abstrato (visto que a legislação e as autoridades não apresentam com clareza quais parâmetros técnicos podem ser considerados como aptos a anonimizar dados) e possui restrições práticas relevantes, especialmente considerando que dados desidentificados poderão ser reidentificados quando associados a outros conjuntos de dados. Em outras palavras, em vista da variedade e da quantidade de dados divulgados, bem como dos avanços tecnológicos que permitem a combinação de dados de formas antes não previstas, é possível que a divulgação de bases de dados públicas permita a identificação de indivíduos, mesmo quando são adotadas técnicas de anonimização ou pseudonimização às bases de dados (GREEN *et al.*, 2017; Altman *et al.*, 2018).[317]

[317] Nesse sentido se posicionaram o EDPS e EDPB em opinião conjunta elaborada sobre proposta de Data Governance Act: "A este respeito, a EDPB e a EDPS sublinham que a distinção entre categorias de dados pessoais e não pessoais é difícil de ser aplicada na prática. De fato, na prática, a partir de uma combinação de dados não pessoais é possível inferir ou gerar dados pessoais, ou seja, dados relativos a uma pessoa identificada ou identificável, especialmente quando os dados não pessoais são o resultado da anonimização

Por essa razão, é possível afirmar que há considerável limitação à viabilidade concreta de divulgar dados mantidos pelo poder público sem que haja a possibilidade de sua posterior identificação. Desse modo, é importante ter em mente que governos poderão escolher compartilhar ou publicar dados pessoais e dados não identificados, mas que poderão ser posteriormente associados a uma pessoa física.[318] Não somente poderá ocorrer a divulgação voluntária de dados pessoais em vista do seu interesse público, como poderá ocorrer a re-identificação de dados publicados de forma pseudonimizada ou anonimizada. Essa re-identificação de dados pode ocorrer, especialmente quando: **(a)** não são removidos (ou não são suficientemente extraídos) dados que permitem a identificação direta ou indireta do indivíduo; **(b)** são adotadas técnicas de engenharia reversa à base de dados; ou **(c)** os dados mantidos são associados a dados constantes de outras bases de dados, privadas ou públicas.

10.2 Definição da finalidade da publicação e do compartilhamento

Em seguida, será necessário identificar as finalidades da divulgação[319] e quais dados são necessários para alcançar as finalidades pretendidas. De fato, como já mencionado, a divulgação de dados em políticas de transparência e dados abertos possui como objetivo geral o fomento à transparência e *accountability*, podendo também buscar promover outras finalidades, como a inovação e benefício econômico. Já o compartilhamento de dados busca a promoção da eficiência e o aprimoramento na prestação de serviços públicos, mas poderá também promover outras finalidades como as já mencionadas inovação e benefício econômico.[320] No entanto, é necessário identificar no caso concreto qual ou quais finalidades

---

de dados pessoais e, portanto, informações originalmente relacionadas a pessoas físicas. Além disso, nos cenários previstos pela proposta de maior disponibilidade, reutilização e compartilhamento de informações, com o objetivo de "permitir a detecção de padrões de '*Big Data*'" ou aprendizagem de máquinas ", quanto mais dados não pessoais forem combinados com outras informações disponíveis, mais difícil será assegurar a anonimização, devido ao maior risco de reidentificação dos sujeitos dos dados." (tradução nossa). Disponível em: https://edpb.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf. Acesso em 28.04.2021.

[318] Nas palavras de Miriam Wimmer (2020): "Também é possível que os direitos de anonimização, de bloqueio ou de eliminação de dados desnecessários ou excessivos encontrem, na prática, limitações quanto à sua aplicação no âmbito do poder público. Isso pode se dar em razão do eventual confronto não apenas com princípios gerais do direito administrativo, como o da formalidade dos atos processuais, mas também em decorrência do conflito com normas concretas que disciplinam a forma e os prazos para guarda e arquivamento de registros e de documentos oficiais."

[319] Por exemplo, caso o objetivo da publicação seja evitar desvios de recursos públicos, a divulgação deverá ter como foco os documentos ou bases de dados como as que possuem informações sobre entradas de recursos, valores auferidos por servidores públicos, e contratos com prestadores de serviços. Por outro lado, se a finalidade for permitir a realização de pesquisas sobre padrões decisórios dos Tribunais, a divulgação deverá focar nas diferentes modalidades de decisões proferidas no curso de processos judiciais.

[320] Por exemplo, a publicação de documentos de Tribunais por vezes tem entre suas finalidades viabilizar *accountability* do Judiciário, a realização de estudos acadêmicos, ou assegurar subsídios para a prevenção de

específicas se deseja alcançar com o compartilhamento ou com a publicação de dados mantidos pelo poder público. Com essa identificação é possível determinar com mais clareza quais dados serão efetivamente necessários e por quanto tempo.

Finalidade legítima, explícita, informada e em observância ao interesse público

A definição da finalidade é essencial não somente para que se possa delimitar quais arquivos e bases de dados serão divulgados e em quais condições, mas é exigência legal, conforme o princípio da finalidade, que possui contornos próprios na legislação de proteção de dados pessoais e nas normas aplicáveis à administração pública.

Em relação à proteção de dados pessoais, o princípio da finalidade foi primeiro previsto no Marco Civil da Internet, ao determinar que **(i)** usuários da internet teriam o direito de tratamento de seus dados pessoais somente para finalidades que justifiquem sua coleta, não sejam vedadas pela legislação e estejam especificadas em contratos de prestação de serviços ou em termos de uso de aplicações de internet (art. 7º, VIII); e **(ii)** provedores de aplicação não estão autorizados a guardar dados pessoais excessivos à finalidade consentida pelo seu titular (art. 16, II). Isso significa que, segundo o MCI, não somente é necessária a observância de finalidades compatíveis com aquelas informadas previamente ao titular de dados - o que resulta em restrição de forma e de tempo de uso dos dados -, mas a finalidade deverá ser lícita e estar informada em instrumentos contratuais específicos.

Mais recentemente, a LGPD estabeleceu que o tratamento de dados pessoais deve ser realizado para finalidades legítimas, lícitas e estarem pautadas na boa-fé objetiva, o que significa que o tratamento não poderá possuir vedação específica em legislação vigente e estar de acordo com as legítimas expectativas dos titulares de dados. Em relação à boa-fé, essa exigência tem respaldo também no CDC, que determina que a harmonização de interesses nas relações de consumo seja pautada pela boa-fé e equilíbrio (art. 4º, III), e no princípio constitucional da boa-fé (arts. 15, V, 37, § 4º e 85, V da Constituição), segundo o qual o poder público deverá atuar de forma leal e honesta (DI PIETRO, 2015).[321] Conjuntamente, essas

---

fraudes ou o desenvolvimento de novos negócios. Outro exemplo consiste no compartilhamento de dados por Tribunais Eleitorais para finalidades como a fiscalização de candidatos e a desburocratização do cadastro eleitoral. Por sua vez, informações sobre servidores públicos e beneficiários de programas sociais são publicados ou compartilhados para fins como o controle social sobre gastos públicos e a execução de políticas sociais. Já a publicação ou compartilhamento de dados sobre vacinação pode se dar para controle social e para permitir o desenvolvimento de pesquisas em saúde pública.

[321] Nas palavras de Maria Sylvia Zanella Di Pietro (2015): "Na Constituição, o princípio não está previsto expressamente, porém pode ser extraído implicitamente de outros princípios, especialmente do princípio da moralidade administrativa e da própria exigência de probidade administrativa que decorre de vários

disposições exigem que o tratamento de dados pessoais pelo poder público busque preservar a confiança entre governo e cidadão.[322] Para tanto, e considerando o princípio constitucional da legalidade, a atuação em observância à boa-fé exige ao poder público atuar de acordo com a lei e com o direito, se alinhando também à exigência de que dados pessoais sejam tratados para finalidades legítimas e lícitas.

A LGPD também previu expressamente o princípio da finalidade (art. 6º, I), que estabelece a necessidade de se delimitar previamente os objetivos do tratamento, que devem almejar propósitos legítimos, serem específicos e explícitos, e informados aos titulares de dados anteriormente à coleta dos dados, não sendo autorizadas atividades posteriores e incompatíveis com as finalidades informadas ao titular no momento da coleta de sus dados. Com isso, o princípio auxilia na definição dos contornos do tratamento de dados pessoais que será realizado, como quais dados são necessários ou por quanto tempo serão utilizados.

O requisito da especificação da finalidade exige que os objetivos e justificativa do tratamento sejam bem delimitados, sendo "ilegítimo o tratamento realizado com base em finalidades amplas ou genéricas" (MENDES, 2014).[323] O propósito dessa exigência é assegurar que o titular compreenderá com clareza os objetivos da utilização de seus dados e que o controlador conseguirá delimitar com precisão quais salvaguardas serão necessárias. Sobre isso, o Supremo Tribunal Federal declarou, no julgamento da ADI nº 6389 (sobre o envio de dados de serviços de telefonia para o IBGE), que não basta à legislação indicar genericamente as finalidades para as quais dados pessoais serão tratados pelo poder público,

---

dispositivos constitucionais (arts. 15, V 37, § 4º, 85, V). A Lei no 8.429, de 2-6-92 (Lei de Improbidade Administrativa), considera como ato de improbidade que atenta contra os princípios da administração pública "qualquer ação ou omissão que viole os deveres de honestidade, imparcialidade, legalidade e Lealdade às instituições" (art. 11). O princípio da boa-fé abrange um aspecto objetivo, que diz respeito à conduta leal, honesta, e um aspecto subjetivo, que diz respeito à crença do sujeito de que está agindo corretamente. Se a pessoa sabe que a atuação é ilegal, ela está agindo de má-fé. Há quem identifique o princípio da boa-fé e o da proteção à confiança. É o caso de Jesús González Perez, em sua obra sobre *El principio general de la buena fe en eI derecho administrativo*. Na realidade, embora em muitos casos, possam ser confundidos, não existe uma identidade absoluta. Pode-se dizer que o princípio da boa-fé, deve estar presente do lado da Administração e do lado do administrado. Ambos devem agir com lealdade, com correção. O princípio da proteção à confiança protege a boa-fé do administrado; por outras palavras, a confiança que se protege aquela que o particular deposita na administração pública. O particular confia em que a conduta da Administração esteja correta, de acordo com a lei e com o direito. É o que ocorre, por exemplo, quando se mantêm atos ilegais ou se regulam os efeitos pretéritos de atos inválidos."

322 É por isso que Laura Schertel Mendes (2018) argumenta que as finalidades informadas ao titular de dados devem observar a "boa-fé objetiva, as expectativas legítimas do consumidor, bem como os impactos e os riscos do tratamento de dados pessoais para o consumidor" (Mendes, 2018).

323 "As Diretrizes da OCDE enfatizam a flexibilidade e mencionam especificamente que "a especificação dos objetivos pode ser feita de várias formas alternativas ou complementares, por exemplo, por meio de declarações públicas, informações aos sujeitos dos dados, legislação, decretos administrativos e licenças fornecidas pelos órgãos de supervisão". O que importa é a qualidade e a consistência das informações fornecidas." (tradução nossa). Vide: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em 09.08.2020.

sendo necessário haver "justificação minudente e exaustiva das finalidades atribuídas ao tratamento de dados".[324] No caso, o Tribunal entendeu que a norma impugnada limitou-se a enunciar que os dados serão utilizados para a proteção de estatística oficial, não delimitando "o objeto da estatística a ser produzida, nem a finalidade específica, tampouco sua amplitude." De forma similar, no julgamento da ADPF nº 695 (sobre o envio de dados do Denatran à Abin, por forma do Decreto nº 10.046/2019), o Ministro Gilmar Mendes esclarece que o afastamento da autodeterminação do titular de dados deverá ocorrer de forma excepcional e justificada pela "identificação da finalidade e no estabelecimento de limites ao tratamento de dados em padrão suficientemente específico, preciso e claro para cada área."[325] Assim, o controle das finalidades de tratamento de dados pessoais passa a ser o elemento central da proteção constitucional, e não mais o conteúdo dos dados. Por isso, considerou que a autorização ampla concedida no Termo de Autorização nº 07/2020 e pelas normas que regulam o Sistema Brasileiro de Inteligência (SISBN) não atendem o requisito de especificação da finalidade.

Portanto, não basta ao atendimento do requisito da especificação da finalidade a existência de uma norma geral autorizando de forma ampla a realização de certas atividades de tratamento de dados pessoais ou que estabeleça as atribuições legais de determinado órgão ou entidade público. Será necessário haver especificação da finalidade do tratamento de dados, o que não precisará ser realizado por lei em sentido estrito (bastando que essa especificação seja realizada por meio de ato administrativo válido editado por autoridade competente).[326]

---

[324] No caso em exame, o art. 2º, § 1º, da MP, ao dispor sobre a finalidade e o modo de tratamento dos dados, cinge-se a prever que estes serão utilizados "direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares". O art. 3º da MP dispõe ainda que os dados terão caráter sigiloso, não serão utilizados como objeto de certidão ou meio de prova em processo administrativo, fiscal ou judicial e serão usados exclusivamente para a finalidade prevista no § 1º do art. 2º. Como destacado acima, a doutrina e a própria legislação aplicável impõem que a autodeterminação só possa ser afastada por um dever de justificação minudente e exaustivo das finalidades atribuídas ao tratamento de dados. No caso em tela, há uma enorme dificuldade de se extrair do texto normativo um contorno mínimo de segurança sobre a finalidade do tratamento de dados que é simplesmente referenciado com o objetivo de "produção estatística oficial". (Supremo Tribunal Federal. Ação Declaratória de Inconstitucionalidade nº 6389. Relatora Ministra Rosa Weber. Voto Min Gilmar Mendes. Julgado em 07.05.2020. Disponível em:https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358482. Acesso em 19.10.2022.

[325] Disponível em: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADPF%20695%22&base=decisoes&pesquisa_inteiro_teor=false&sinonimo=true&plural=true&radicais=false&buscaExata=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em 12.10.2022.

[326] Sobre a forma de especificar a finalidade, a Working Party 29 esclarece na Opinião nº 03/2013 sobre o princípio da finalidade que: "as Diretrizes da OCDE enfatizam a flexibilidade e mencionam especificamente

Por sua vez, a exigência de que a finalidade seja informada e explícita estabelece que não basta ao controlador definir e registrar em procedimentos internos a finalidade específica das atividades que realiza, sendo necessário informar ao titular de dados previamente e de forma clara e inteligível sobre o tratamento, de forma que possa exercer escolhas conscientes sobre a entrega dos dados e, caso queira, possa exercer seus direitos. Em outras palavras, além de a informação ser fornecida antes do tratamento, ela deverá estar disponível em local de fácil acesso e evitando a utilização de linguagem vaga ou ambígua. No julgamento do Mandado de Segurança nº 36.150 o Ministro Luís Roberto Barroso reforça que a prestação de informações prévias e precisas compõem a validade da autorização fornecida pelo titular de dados:

> No caso, no entanto, as informações que se quer acessar foram prestadas para uma finalidade declarada no ato da coleta dos dados e sob a garantia de sigilo do Inep quanto às informações pessoais. Nesse aspecto, a transmissão a outro órgão do Estado dessas informações e para uma finalidade diversa daquela inicialmente declarada subverte a autorização daqueles que forneceram seus dados pessoais, em aparente violação do dever de sigilo e da garantia de inviolabilidade da intimidade.

Por sua vez, será legítima quando estiver fundamentada em alguma base legal, observar os demais princípios de proteção de dados pessoais, cumprir com as demais normas do ordenamento jurídico,[327] e contemplar as legítimas expectativas do titular de dados.[328]

---

que "a especificação dos objetivos pode ser feita de várias formas alternativas ou complementares, por exemplo, por meio de declarações públicas, informações aos sujeitos dos dados, legislação, decretos administrativos e licenças fornecidas pelos órgãos de supervisão". Em termos de responsabilidade, a especificação da finalidade por escrito e a produção de documentação adequada ajudarão a demonstrar que o controlador cumpriu com a exigência do Artigo 6(1)(b). Também permitirá que os sujeitos dos dados exerçam seus direitos de forma mais eficaz – por exemplo, fornecerá prova da finalidade original e permitirá a comparação com finalidades de processamento subseqüentes. A especificação da finalidade por escrito pode ser útil, ou mesmo necessária, em muitas circunstâncias. Em particular, hoje em dia, muitas atividades de processamento de dados acontecem em um contexto complexo, opaco e ambíguo, especificamente na Internet. Nessas situações, é necessário um cuidado especial para especificar sem ambigüidade os propósitos. Dito isto, às vezes, o contexto e o costume podem tornar suficientemente claro para todos os envolvidos, incluindo aqueles que processam os dados, bem como os sujeitos dos dados, como os dados pessoais serão utilizados. Se isto for possível sem correr o risco de incerteza e ambigüidade, o artigo 6(1)(b) mau às vezes é satisfeito expressando apenas os elementos essenciais." (tradução nossa). Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em 12.10.2022.

[327] Segundo a WP 29: "A exigência de legitimidade significa que os objetivos devem estar "de acordo com a lei" no sentido mais amplo. Isto inclui todas as formas de direito escrito e comum, legislação primária e secundária, decretos municipais, precedentes judiciais, princípios constitucionais, direitos fundamentais, outros princípios legais, assim como jurisprudência, pois tal "lei" seria interpretada e levada em consideração pelo tribunal competente." (tradução nossa). Vide: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf .Acesso em 13.09.2020.

[328] Para o poder público a ANPD (2022) argumenta que: "deve estar sempre associado a uma finalidade pública, que seja: (i) legítima, isto é, lícita e compatível com o ordenamento jurídico, além de amparada em uma base legal, que autorize o tratamento; (ii) específica, de maneira que a partir da finalidade seja possível delimitar o escopo do tratamento e estabelecer as garantias necessárias para a proteção dos dados pessoais; (iii) explícita, isto é, expressa de uma maneira clara e precisa; e (iv) informada, isto é, disponibilizada em linguagem simples e de fácil compreensão e acesso ao titular dos dados. Tratamento de dados pessoais pelo Poder

Para o tratamento de dados pelo poder público, essa exigência é reforçada pelo art. 23 da LGPD, que exige que o tratamento seja realizado para o "atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar suas competências legais ou cumprir as atribuições legais do serviço público" e desde que sejam prestadas informações sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas (art. 23, I). Com isso, o princípio da finalidade no caso de tratamento de dados pessoais pelo poder público deverá também observar: **(i)** a finalidade pública do órgão e/ou entidade em questão; **(ii)** o interesse público; e **(iii)** o alcance dos objetivos de executar competências legais ou cumprir atribuições legais do serviço público - que deverão estar respaldados em previsão legal específica. Assim, o princípio da finalidade da LGPD dialoga com os princípios constitucionais da legalidade e da finalidade, aplicáveis à atuação do poder público, na medida em que exige da administração pública atuar para o alcance de objetivos legalmente estabelecidos que, em última análise, correspondem ao alcance do interesse público. Nesse mesmo sentido se manifestou o Ministro Gilmar Mendes no julgamento da ADPF nº 695:

> [...] a LGPD parece ter limitado o tratamento de dados pelo Poder Público às atividades principais e acessórias de provisão de serviços públicos. Uma interpretação dessa lei alinhada ao princípio constitucional da legalidade impõe ainda que essas finalidades conexas à prestação de serviços públicos estejam, ao máximo possível, amparadas em previsões legais específicas.

No direito administrativo, o princípio da finalidade é inerente ao princípio da legalidade, na medida em que, nas palavras de Celso Antônio Bandeira de Mello (2014) ele "corresponde à aplicação da lei tal qual ela é, ou seja, na conformidade de sua razão de ser, do objetivo em vista do qual foi editada". Por isso, o princípio da finalidade permeia e consiste em elemento central de todos os atos realizados pelo agente público, que deve se pautar pelo disposto no ordenamento jurídico e, por consequência, buscar o alcance do interesse público (MEIRELLES, 2015; MOREIRA NETO, 2015).

Isso decorre da própria natureza do Estado Republicano e Democrático de Direito, que legitima a atuação do Estado a partir de um poder detido por aqueles que ele representa. Por isso, a atividade pública somente será válida se exercida por um agente investido na função pública e atuando dentro de suas competências legalmente atribuídas (SUNDFELD, 2013). Assim, não apenas a finalidade é um princípio da administração pública, como um elemento

---

Público. Versão 1.0., publicado em janeiro de 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico___defeso_eleitoral.pdf. Acesso em 12.10.2022.

em si do ato administrativo. Em outras palavras, o ato administrativo tão somente se legitima quando associado à finalidade estabelecida em lei.

Essa ideia se assenta em uma tradicional formulação de que o administrador público atua sempre no estrito cumprimento de seu dever legal. Segundo explica Floriano Marques Neto (2002), essa tradicional formulação decorre da própria construção do direito administrativo, com base na clássica ideia da sujeição da administração pública à *rule of Law*, à *legalité* ou ao *Rechtsstaatlickeit*. Nesse contexto, se o agente público agir em desconsideração a esse fim - pela busca de finalidade alheia ao interesse público, ou quando pretende finalidade de interesse público diversa da categoria do ato praticado - estará incorrendo em desvio de poder ou finalidade (MEIRELLES, 2015, ZANELLA DI PIETRO, 2015, BANDEIRA DE MELLO 2015). Já para o moderno direito administrativo, embora o ato praticado esteja adstrito a uma finalidade prevista no ordenamento jurídico, ele é também resultado de um juízo subjetivo, em menor ou maior grau, daquele agente público (Binenbojm, 2014). Com isso, o direito sempre forneceria os elementos para identificação, ainda que por via negativa, da finalidade do ato administrativo, valendo-se de ideias como razoabilidade, moralidade, boa-fé, para identificar as finalidades legítimas dos atos (SUNDFELD, 2013).

Além disso, o princípio da finalidade também está relacionado aos princípios da moralidade e da indisponibilidade do interesse público (MOREIRA NETO, 2015). Quanto ao princípio da moralidade, trata-se de um mandamento segundo o qual há determinado padrão ético a ser observado pelos gestores públicos, em consideração aos valores morais albergados na lei (SUNDFELD, 2015). Ao buscar alcançar aquilo que efetivamente (e não hipoteticamente) foi disposto na legislação, sem dela desviar, o gestor público estaria agindo em consonância com os padrões éticos dele esperado, e, portanto, em linha com o princípio da moralidade. Assim, moralidade é, senão, um reforço do princípio da legalidade (BANDEIRA DE MELLO, 2015), que, como citado acima, representa a própria ideia de função administrativa e da vinculação da atuação do gestor público aos fins dispostos na lei. Já a proximidade do princípio da finalidade com o princípio da indisponibilidade do interesse público se revela na ideia de que o poder público não é o titular do interesse público, mas apenas seu guardião, de tal modo que é um dever do gestor agir de acordo e nos termos da lei (GARCIA CABRAL, 2020). Ou seja, o princípio da finalidade abarca um sentido de dever público do gestor para atender aos fins previstos em lei, e, nesse aspecto, converge ao

princípio da indisponibilidade do interesse público, pois se escora na ideia de que a administração pública atua sempre no contexto de uma função, em benefício da coletividade.

Por isso, não somente deverá o compartilhamento e a publicação de dados pelo poder público buscar atender um objetivo específico informado ao titular de dados, mas a finalidade almejada deverá estar contemplada no ordenamento jurídico (reforçando a exigência de finalidade legítima, exigida pela LGPD) e almejar o alcance do interesse público. Como se verá em maiores detalhes a seguir, esse interesse público é atualmente compreendido como o resultado da mediação entre interesses heterogêneos presentes na sociedade, tarefa esta que poderá ser realizada previamente pelo legislador ou pela administração pública no exercício e dentro dos limites da discricionariedade que lhe é permitida pelo ordenamento jurídico.

Finalmente, a depender da finalidade do tratamento de dados, é possível que a divulgação de dados pessoais resulte em exceção à aplicação da LGPD, a exemplo do uso de dados para fins de atividades de jornalismo, pesquisa acadêmica ou para práticas de segurança pública, a LGPD será excetuada ou se aplicará apenas parcialmente. Por exemplo, o art. 4º da LGPD determina que seus dispositivos são excetuados para atividades realizadas para finalidades particulares e não econômicas (inciso I), jornalísticas (inciso II, a), acadêmicas (inciso II, b), ou de segurança pública, defesa nacional, segurança do Estado ou medidas de investigação e repressão de infrações penais (inciso III). Às exceções previstas no inciso III do art. 4º aplicam-se o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD (art. 4º, §1º), e à exceção do inciso II, b do art. 4º, exige-se a adequação da atividade a uma das bases legais previstas nos arts. 7º e 11 da LGPD.[329]-[330]

[329] Em relação à exceção relacionada às atividades de pesquisa acadêmica (art. 4º, II, b), que pode beneficiar atividades de instituições públicas de ensino, a ANPD esclareceu (2022.4) que a exceção deve ser interpretada restritivamente, aplicando-se somente a atividades estritamente vinculadas ao exercício da liberdade acadêmica, como as atividades realizadas "em salas de aula, congressos e seminários científicos". De todo modo, a LGPD requer que atividades acadêmicas devem ser fundamentadas nas bases legais previstas nos arts 7º e 11 da LGPD e respaldadas nos demais dispositivos da lei que estabelecem os contornos e obrigações relacionados a essas bases legais. Por exemplo, caso o legítimo interesse seja a base legal utilizada para fundamentar determinada atividade de pesquisa, deverão ser observados os critérios estabelecidos no art. 10 para avaliar se estão estabelecidas as condições necessárias para a qualificação do interesse legítimo do controlador no tratamento almejado.

[330] Segundo a autoridade (ANPD, 2022.4), o objetivo desse dispositivo da LGPD seria reconhecer que a proteção de dados pessoais não deverá se sobrepor ao disposto no art. 206, incisos II e III da Constituição Federal, que assegura a "liberdade de aprender, ensinar, pesquisar e divulgar o pensamento, a arte e o saber" e o "pluralismo de ideias e de concepções pedagógicas". Em vista desse intuito da norma, a ANPD determina que não estariam contempladas na exceção do art. 4º da LGPD atividades como procedimentos administrativos realizados por instituições de ensino ou a contratação por instituição privada de instituto de pesquisa para o desenvolvimento de atividades comerciais. No entanto, nem sempre será tão simples definir se determinada atividade se enquadra na exceção, em vista da complexidade dos arranjos existentes entre agentes como universidades, governos, e empresas no financiamento e desenvolvimento de pesquisas.

Finalidade compatível com aquela que justificou a coleta dos dados

Outro elemento importante do princípio da finalidade consiste na determinação de que dados pessoais devem ser tratados nos limites do informado aos seus titulares, sendo vedados usos posteriores para finalidades incompatíveis com aquelas informadas. Segundo Mário Viola e Danilo Doneda (2009), o princípio da necessidade "pode ser tomado como corolário de um pressuposto segundo o qual a informação pessoal, como expressão direta da personalidade de seu titular, nunca perde seu vínculo com este" e constitui "mecanismo que evit[a] a chamada utilização secundária da informação pessoal à revelia do seu titular".

Assim, o princípio restringe a utilização posterior do dado para outras finalidades, salvo se compatíveis com aquelas informadas no momento da sua coleta. Dito de forma distinta, esse princípio assegura flexibilidade para o exercício de novas finalidades distintas das informadas ao titular quando da coleta de seus dados, mas desde que essas novas finalidades sejam compatíveis com as finalidades que justificaram sua coleta.[331] Com isso, assegura-se ao titular de dados previsibilidade sobre como seu dado será utilizado, ao mesmo tempo em que assegura mais flexibilidade no tratamento desses dados (WP 29, 2013).

A legislação nacional não especifica como deverá ser a avaliação de compatibilidade entre finalidades de tratamento. Para autoridades europeias - a exemplo da WP 29 e da EDPB - a avaliação deverá considerar alguns elementos.[332] *Primeiro*, deverá ser avaliada a **relação entre as novas finalidades e aquelas para as quais o dado foi coletado**, caso em que a nova finalidade pode estar implícita na finalidade informada ao titular quando da coleta dos dados ou consistir em uma nova finalidade. *Segundo*, a compatibilidade também é avaliada com base no **contexto de coleta dos dados e as legítimas expectativas do titular** em relação aos seus posteriores usos. Isso significa que, quanto menos previsível for a nova finalidade ou quanto maior for a disparidade de poder entre titular de dados e o controlador, menor a chance de ser considerado compatível. *Terceiro*, a análise de compatibilidade deve observar a **natureza do dado pessoal e o impacto do novo tratamento sobre o titular**, de modo que

[331] Nas palavras de Mário Viola e Danilo Doneda (2009): "O vínculo entre a informação e a sua finalidade não é, no entanto, absoluto. Como ressaltamos, a relação entre a utilização dos dados e a finalidade para a qual foram coletados não deve ser interpretada de forma restritiva, mas sim como uma relação de compatibilidade entre os fins e a modalidade da coleta. Há de existir, em suma, uma relação de proporcionalidade entre a finalidade do tratamento e os interesses em questão e o motivo da coleta."

[332] Como indica a WP 29, há duas técnicas possíveis de realizar essa avaliação sobre a compatibilidade de usos: (i) método objetivo, que simplesmente compara a finalidade informada ao titular de dados com a desejada nova finalidade; (ii) método subjetivo, que além dos elementos considerados no método objetivo, avalia também o contexto das duas finalidades – é nesse método que se enquadram os elementos apontados nos itens (ii) a (iv). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em 09.08.2020.

será mais difícil argumentar a compatibilidade quando o tratamento envolver dados pessoais sensíveis, for realizado por outro controlador em diferente contexto, ou for realizada análise de *big data*. Finalmente, possíveis salvaguardas adotadas podem atuar como uma forma de compensação pela mudança de finalidade, a exemplos da pseudonimização ou da ampliação de medidas destinadas a garantir transparência sobre o tratamento (WP 29, 2013).

Mário Viola e Danilo Doneda (2009) se posicionaram de forma alinhada às mencionadas autoridades europeias, antes mesmo da edição da LGPD, esclarecendo que a compatibilidade pode ser avaliada levando em consideração vários critérios, como os seguintes exemplos "[...] o fato de o titular dos dados poder antecipar que seus dados seriam utilizados para aquela finalidade [...], quando os dados a serem tratados forem indispensáveis para a realização da atividade pretendida, ou quando a finalidade apresentar um interesse público relevante.".

Assim, considerando que a LGPD busca assegurar, em última análise, que titulares de dados tenham razoáveis e legítimas expectativas sobre o tratamento de dados realizados e os riscos dele decorrentes,[333] é possível adotar no Brasil, respeitadas as particularidades locais, similares critérios aos sugeridos por autoridades europeias para o teste de compatibilidade da nova finalidade de tratamento (i.e., relação entre a finalidade original e a nova finalidade, contexto da coleta de dados, legítimas expectativas do titular, natureza do dado pessoal e os riscos que o tratamento oferece ao titular de dados). Esse entendimento está alinhado com o exposto pelo Ministro Gilmar Mendes no julgamento da ADI nº 695 a respeito dos requisitos do princípio da finalidade: "A incidência do princípio da finalidade nessas relações [...] deve levar em consideração também elementos como (i) as expectativas razoáveis do titular, (ii) a natureza dos dados processados e (iii) os possíveis prejuízos a serem suportados pelo titular."

Para o tratamento de dados pessoais mantidos pelo poder público haverá desafio particular em comprovar que a nova finalidade é compatível com aquela que justificou a coleta do dado, na medida em que: **(a)** coleta de dados normalmente decorre de alguma obrigação legal (e.g., para poder votar no Brasil, o cidadão deverá fornecer seus dados biométricos) ou enquanto condição para usufruir de determinado serviço público (e.g., recebimento de valores pelo Programa Bolsa Família ou a utilização de meios de transporte

[333] Vide, por exemplo, o disposto no art. 44 da LGPD: "O tratamento de dados pessoais será irregular quando deixar de **observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar**, consideradas as circunstâncias relevantes, entre as quais: I – o modo pelo qual é realizado; II – **o resultado e os riscos que razoavelmente dele se esperam**; III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado."

público); e **(b)** geralmente haverá disparidade de poder entre cidadão e Estado, visto que muitas vezes o fornecimento do dado será uma condição ao exercício de direitos, à utilização de serviços públicos, ou ao recebimento de benefício social. Diante disso, os titulares de dados **(i)** nem sempre possuem a expectativa de que seus dados serão utilizados para finalidades distintas; e **(ii)** não terão meios eficazes de impedir que seus dados sejam utilizados para finalidades distintas, em função da disparidade de poder que possui em relação ao Estado.

Por outro lado, como demonstrado nesta tese, o reuso de dados mantidos pelo poder público, mesmo que para finalidades não estritamente compatíveis com aquelas que justificaram sua coleta, muitas vezes será de interesse público. Tendo isso em vista (e como sugerido pela experiência estrangeira), a avaliação sobre a compatibilidade do compartilhamento e da publicação pretendida deverá considerar as particularidades desse tratamento e o interesse público. Com base no disposto no art. 23 da LGPD, e segundo os princípios da legalidade e finalidade administrativa, esse tratamento deverá observar os mesmos fatores observados em qualquer modalidade de reuso de dados pessoais, mas considerando as atribuições legais dos órgãos e entidades públicos envolvidos na divulgação e o interesse público da atividade. Em outras palavras, os requisitos de compatibilidade de "relação entre a finalidade original e a nova finalidade" e "contexto da coleta de dados" devem levar em consideração as atribuições legais dos sujeitos envolvidos no tratamento. Além disso, para assegurar que a divulgação esteja nas legítimas expectativas dos cidadãos, o poder público deverá oferecer ativamente informações a respeito das novas finalidades de uso que serão atribuídas aos dados.

Assim, nessa leitura do teste de compatibilidade, observa-se o conceito de "separação informacional dos poderes", cunhado pelo Tribunal Alemão no julgamento de 1980 sobre a constitucionalidade do censo populacional, segundo o qual o Estado não deve ser considerado uma entidade única para fins de coleta e utilização de dados pessoais (MENDES, 2020). Para tanto, determinado órgão ou entidade pública deverá tratar dados nos estritos limites de suas atribuições legais, não podendo coletar dados para finalidades não informadas aos cidadãos ou para o cumprimento de obrigações de outro ente público. Isso não significa que órgãos ou entidades públicos não podem atuar em parceria ou em substituição a outros entes públicos, mas evita que dados de cidadãos sejam coletados pelo governo e posteriormente utilizados para quaisquer finalidades que porventura algum órgão ou ente público possa precisar.

De todo modo, a realização do teste de compatibilidade nesse formato (ou seja, considerando também as atribuições legais dos entes públicos e o interesse público na divulgação) permite atribuir alguma maleabilidade ao princípio da finalidade para o compartilhamento e a publicação de dados pelo poder público, especialmente considerando os benefícios sociais em certos reusos de dados pessoais realizados para finalidades não estritamente atreladas à finalidade que justificou a coleta dos dados. Isso não significa, no entanto, que o princípio da finalidade deverá ser relaxado para o poder público, especialmente em vista dos possíveis riscos da inadequada divulgação e publicação de dados pessoais por governos.[334]

Por exemplo, uma realidade que impõe dificuldade à observância do princípio da finalidade consiste na promoção de interoperabilidade de sistemas e a criação de bases de dados centralizadas. Embora a legislação vigente reconheça a importância da interoperabilidade para a melhoria das atividades desenvolvidas pelo poder público e estimula que governos armazenem dados em formato interoperável,[335]-[336] ela pode permitir ampliação no uso dos dados para finalidades distintas daquelas que justificaram sua coleta, e sem a devida transparência. Além disso, como as propostas de interoperabilidade estão geralmente associadas à criação de base de dados centralizada, a escala de dados tratados aumenta os riscos de uso incompatível com a finalidade original. Com isso, as finalidades atingidas com essa prática poderão ou não estar nas legítimas expectativas dos titulares de dados e impactá-los nas formas mais diversas.[337]-[338]

---

[334] Em relação à limitação de controle de usos posteriores, ela será mais detidamente abordada no capítulo sobre salvaguardas à publicação e ao compartilhamento.

[335] De fato, no julgamento da ADI nº 6649, o Ministro Gilmar Mendes ressalta o reconhecimento da legislação infralegal sobre relevância da interoperabilidade entre sistemas governamentais para promover a eficiência na gestão da coisa pública: "Nossa legislação federal, portanto, contempla um plexo de disposições normativas que impõem à Administração Pública a difícil tarefa de implementar bancos de dados de natureza interoperável, desenvolvidos para permitir o compartilhamento eletrônico de informações entre órgãos governamentais, sem prejuízo da irrestrita observância dos princípios gerais e mecanismos de proteção elencados na Lei Geral de Proteção de Dados Pessoais."

[336] Como mencionado nesta tese, a promoção da interoperabilidade necessária para a promoção de serviços integrados não somente é esperada como desejável. Por exemplo, é benéfico ao titular de dados o compartilhamento de dados entre entes públicos para a prestação do Programa Bolsa Família (PBF). Sobre esse respeito, pesquisa elaborada pelo InternetLab (FRAGOSO *et al.*, 2021) explica que esse programa "tem sua existência condicionada ao compartilhamento e tratamento de dados em diferentes níveis da administração pública" e que "os dados coletados no âmbito do PBF podem ser utilizados para analisar o perfil das famílias beneficiárias, verificar o impacto do programa, atender a outras políticas públicas e desenvolver iniciativas de combate à pobreza".

[337] De fato, quando do julgamento da ADI nº 6649, que avaliou a constitucionalidade do Decreto nº 10.046/2019, o Ministro Gilmar Mendes argumentou que previsões legais de interoperabilidade entre sistemas governamentais com previsão de amplo e irrestrito compartilhamento de dados serão incompatíveis com a constituição federal: "Qualquer interpretação [...] no sentido de possibilitar ampla, irrestrita e irresponsável difusão dos dados pessoais custodiados pelo Estado, conflita não apenas com diversas

Por isso, o compartilhamento de dados por órgãos e entidades públicas, além de buscar o interesse público, deve também ser acompanhado de salvaguardas que assegurem controles sobre as novas finalidades de uso,[339] como: **(a)** a demonstração das finalidades específicas para as quais os dados serão utilizados, que deverão ser pautadas pelo interesse público e às competências legais do órgão ou entidade pública que compartilha o dado; **(b)** concessão de acesso apenas àqueles que comprovarem possuir autorização legal ou interesse legítimo no tratamento; **(c)** conceder acesso apenas aos dados necessários para o alcance da finalidade informada e por período determinado.

Por sua vez, quanto à publicação de dados, em portais de transparência e dados abertos, embora geralmente seja realizada para finalidades legítimas, como transparência e *accountability*, nem sempre alcançará o requisito da compatibilidade.[340] Entre os maiores desafios para tanto estão: **(a)** a identificação da legítima expectativa do cidadão de que seus dados poderão ser divulgados ao público; e **(b)** a limitada capacidade de entes públicos controlarem os usos secundários que serão atribuídos aos dados por aqueles que os acessam.

Em relação à verificação da compatibilidade, o cidadão em regra poderá prever que determinados dados fornecidos ao poder público serão publicados por força das obrigações de transparência às quais o poder público é submetido, na medida em que prevalece na administração pública a publicidade sobre informações que custodiam. Por exemplo, por força da determinação constitucional de transparência de processos judiciais (art. 5º, LX) cidadãos

---

previsões expressas do próprio decreto presidencial, mas principalmente com preceitos sensíveis que compõem a espinha dorsal da Constituição da República e da Lei Geral de Proteção de Dados Pessoais, como os direitos à privacidade e à autodeterminação informativa. [...] Embora seja permitida e até mesmo necessária a instituição de instrumentos de interoperabilidade aptos a simplificar o fluxo de dados entre órgãos públicos, as inúmeras alusões feitas pelo decreto ao regime protetivo instituído pela LGPD impõem a necessidade de estabelecimento de ferramentas rigorosas de controle de acesso ao Cadastro Base do Cidadão."

338 Por exemplo, a interoperabilidade que permite o Ministério Público a livremente acessar dados de registros públicos de forma a buscar subsídios para o início de ações penais não será igualmente esperada pelos cidadãos e poderá inclusive resultar em desconfiança do cidadão em relação a esse serviço público. Sobre tema relacionado, vide o artigo Modernização do registro eletrônico de imóveis no Brasil, elaborado Por Ronaldo Lemos, Natalia Langenegger, Flávia Cano e Leonardo Chaim, disponível em: https://www.irib.org.br/noticias/detalhes/artigo-jota-info-modernizacao-do-registro-eletronico-de-imoveis-no-brasil-por-ronaldo-lemos-flavia-cano-leonardo-chaim-e-natalia-langenegger. Acesso em 12.10.2022.

339 Nesse sentido: https://edps.europa.eu/sites/edp/files/publication/19_03_13_formal_comments_2_proposals_conditions_for_accessing_information_systems_for_etias_purposes_en.pdf., Acesso em 13.03.2021.

340 Nesse sentido se manifestou a Working Party 29 na Opinião 05/2001. A WP 29 argumentou não ser possível pressupor que similar publicação de dados será sempre considerada compatível com a finalidade para a qual o dado foi coletado, o que deverá ser avaliado conforme o contexto e tendo como base as seguintes variáveis: (i) se a oferta do dado pelo cidadão foi compulsória; (ii) o tipo de dado pessoal; e (iii) a situação do titular de dados e as consequências que a disponibilização poderá causar.

esperam que determinados dados pessoais estejam disponíveis dentro de documentos divulgados no site dos Tribunais.[341]

No entanto, há casos em que a legislação prevê a limitação da publicidade ou em que não há uma legítima expectativa de publicação. Por exemplo, a Constituição Federal estabelece que determinadas ações serão protegidas pelo segredo de justiça (CF, art. 5º, LX) e há situações em que o Conselho Nacional de Justiça estabeleceu restrição de acesso por diagnosticar que sua divulgação deverá ser restringida para evitar prejuízos às partes (CNJ, Resolução nº 121/2010),[342] como no caso de processos criminais transitados em julgado. Outro exemplo consiste na divulgação de dados protegidos por sigilo fiscal, em que a própria legislação estabelece restrição de acesso a terceiros (Lei nº 5.172/1966).

Diante de uma ausência de presunção de que cidadãos terão a legítima expectativa de que seus dados serão disponibilizados ao público, a avaliação da compatibilidade na publicação de dados em políticas de transparência e dados abertos deve **(i)** verificar a presença de uma obrigação legal específica, **(ii)** avaliar as circunstâncias do tratamento de dados, como a natureza do dado, a forma de coleta e as salvaguardas oferecidas ao titular de dados; e **(iii)** considerar os impactos negativos gerados sobre cidadãos em função da divulgação. Além disso, entes públicos devem adotar formas eficientes de comunicar que seus dados serão divulgados, a finalidade específica dessa divulgação, mecanismos disponíveis para exercer seus direitos e salvaguardas adotadas para mitigar riscos existentes.

Necessidade e adequação dos dados para a finalidade pretendida

Com a definição da finalidade do tratamento e dados pessoais, é possível verificar se o pretendido reuso de dados pessoais observa o princípio da necessidade.[343] Esse princípio requer ao controlador limitar a coleta de dados pessoais e o tratamento subsequente ao estritamente relevante e necessário para alcançar a finalidade[344] informada aos titulares de

---

[341] O mesmo ocorre também com dados oferecidos por professores e pesquisadores que registram suas informações no sistema *lattes*, na medida em que o sistema é amplamente conhecido no ambiente acadêmico e informa aos usuários as condições segundo as quais os dados serão divulgados na internet.

[342] Disponível em: https://atos.cnj.jus.br/atos/detalhar/atos-normativos?documento=92. Acesso em 10.12.2022.

[343] Chamado de princípio da minimização na Europa (nessa região o princípio da necessidade, em conjunto com o princípio da proporcionalidade, consiste em procedimento que deve ser observado em casos de limitação de direitos).

[344] Além disso, como se verifica, esse princípio está intimamente ligado ao princípio da finalidade, na medida em que somente após a definição do objetivo do tratamento será possível delimitar quais são são necessários e o período dentro do qual seu tratamento será considerado legítimo. Isso foi, inclusive, ressaltado pela Autoridade de Proteção de Dados Pessoais da Espanha (AEPD). Vide:

dados. Isso envolve: **(i)** avaliar a possibilidade de alcançar a finalidade com outros ou menos dados, ou mediante outra atividade de tratamento;[345]-[346] **(ii)** limitar quais dados e qual quantidade de dados é efetivamente necessário tratar; e **(iii)** realizar o tratamento pelo período necessário para alcançar os objetivos anunciados aos titulares de dados. Nesse sentido se posicionou a Corte Administrativa Federal Austríaca (BVwG), de que o referido princípio

> [...] limita a profundidade da intervenção e, portanto, o tipo de dados, a natureza pessoal dos dados, a quantidade de dados, o nível de detalhe dos dados, o período de armazenamento dos dados, o número de usos e o círculo de pessoas autorizadas a acessar os dados. Minimizar a quantidade de dados significa minimizar o número de titulares de dados e minimizar a quantidade de dados por titular de dados. [...] significa, em particular, verificar se a finalidade do tratamento também pode ser alcançada com dados pseudonimizados, agregados ou anonimizados. Mesmo a mera exibição de dados em vez de sua reprodução é uma forma de minimização de dados se isso for suficiente para atingir o objetivo" (tradução livre).[347]

Além disso, o princípio deverá ser observado em todas as etapas do tratamento de dados pessoais, não bastando observá-lo apenas no momento da coleta de dados, mas também quando da análise ou da definição do período de armazenamento desses dados. Para tanto, atrelado ao princípio da minimização há regras sobre deleção ou anonimização de dados, pois essas atividades de tratamento deverão ser desenvolvidas sempre que encerrada a finalidade que justificou a coleta ou tratamento subsequente informado aos titulares de dados.

---

https://gdprhub.eu/index.php?title=AEPD_-_PS/00240/2019#On_the_data_minimization_principle. Acesso em 13.10.2022.

345 Nesse sentido se posicionou a Autoridade de Proteção de Dados Pessoais da Noruega (Datatilsysnet): "O princípio da minimização de dados no Artigo 5 (1) (c) implica que os dados pessoais devem ser adequados, relevantes e limitados ao necessário para os fins para os quais são processados. De acordo com o princípio da minimização de dados, não é suficiente que seja prático ou desejável processar dados pessoais; o tratamento deve ser necessário para que o propósito seja alcançado. O controlador de dados deve fazer avaliações específicas de quais dados pessoais são necessários para processar em relação a cada finalidade individu"l." (tradução nossa). Disponível em: https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_20/01626. Acesso em 13.10.2022.

346 Por outro lado, Bygrave (2014) esclarece que "As disposições que incorporam um critério de "necessidade" também incorporam uma exigência de proporcionalidade: "com relação à necessidade de que um registro centralizado como o AZR esteja disponível para atender às exigências das autoridades responsáveis pela aplicação da legislação relativa ao direito de residência, mesmo que se suponha que os registros descentralizados, como os registros distritais de população, contenham todos os dados relevantes para fins de permitir que as autoridades assumam suas funções, a centralização desses dados pode ser necessária, na acepção do artigo 7(e) da Diretiva 95/46, se contribuir para a aplicação mais eficaz dessa legislação no que diz respeito ao direito de residência dos cidadãos da União que desejam residir num Estado-Membro do qual não são nacionais". Esta leitura de "necessário" está em conformidade com a jurisprudência do TEDH, nos termos do artigo 8(2) da CEDH. 27 A mesma interpretação deve provavelmente ser aplicada às outras cláusulas do artigo 7. Ao mesmo tempo, o Tribunal considerou como outro requisito para satisfazer o critério da necessidade que o AZR "contém apenas os dados necessários para a aplicação por essas autoridades dessa legislação". 28 Além disso, sustentou que o armazenamento e processamento de dados não anonimizados no AZR para fins estatísticos "não pode, em nenhuma base" satisfazer o critério de necessidade do artigo 7(e). 29a " (tradução nossa).

347 Disponível em: https://gdprhub.eu/index.php?title=BVwG_-_W211_2210458-1/10. Acesso em 13.10.2022.

Mais que isso, o tratamento de dados será ilícito sempre que ele não for necessário (Bygrave, 2014). Isso porque as bases legais, que serão abordadas mais adiante, apenas são aplicáveis quando a atividade de tratamento de dados for necessária para o alcance da finalidade que justificaria a sua aplicação. Por exemplo, não seria possível aplicar a base legal de obrigação legal ou regulatória à manutenção de dados por tempo superior ao exigido pela legislação aplicável (e.g., manter dados de acesso à aplicação por mais de 6 meses, salvo quando houver solicitação de extensão do prazo por autoridade competente, tendo como fundamento a base legal de cumprimento de obrigação legal).

No Brasil, o princípio da necessidade encontrou respaldo jurídico no Marco Civil e em seu Decreto regulamentador (Decreto nº 8.771/2016). Em relação ao MCI, o referido princípio pode ser extraído da exigência de: **(i)** somente realizar o tratamento de dados para finalidades que justifiquem sua coleta; e **(ii)** excluir dados pessoais, mediante solicitação, após o término da relação entre as partes. Ainda que indiretamente, essas obrigações resultam no princípio da necessidade, na medida em que delimitam as possibilidades de tratamento de dados pessoais ao necessário e enquanto existentes as finalidades que justificaram sua coleta.

Já o Decreto nº 8.771/2016, embora não fale expressamente em princípio da necessidade, o regula de forma mais direta. Isso porque determina aos provedores de internet o dever de reter a menor quantidade possível de dados, comunicações privadas e registros de conexão e acesso a aplicações, que deverão ser excluídos assim que atingida a finalidade de seu uso ou se encerrado o prazo determinado por obrigação legal (art. 13, § 2º). Em outras palavras, agentes de tratamento deverão restringir o uso de dados pessoais e prever política que exija a exclusão de dados tão logo encerrada a finalidade que justificou a sua coleta e utilização.

Sobre esse respeito, interessante mencionar as decisões proferidas pelo Tribunal de Justiça do Rio Grande do Sul ("TJRS")[348] e pelo Tribunal de Justiça de Rondônia ("TJRO")[349] que, com base no Marco Civil, rejeitaram a validade de leis municipais que determinavam a empresas privadas prestadoras de serviços de transporte privado o compartilhamento de dados com municípios. Entre os argumentos apresentados estava justamente a falta de clareza sobre

[348] TJRS, ADI 70075503433 RS, Des.Rel. Marilene Bonzanini, Julgado em 24.09.2012. Disponível em: https://tj-rs.jusbrasil.com.br/jurisprudencia/759485066/direta-de-inconstitucionalidade-adi-70075503433-rs/inteiro-teor-759485067. Acesso em 13.09.2020.

[349] TJRO, ADI 0802559-78.2018.822.0000 RO 0802559-78.2018.822.0000, Des.Rel. Eurico Montenegro, Julgado em 01.04.2019. Disponível em: https://tj-ro.jusbrasil.com.br/jurisprudencia/699366137/direta-de-inconstitucionalidade-adi-8025597820188220000-ro-0802559-7820188220000/inteiro-teor-699366139. Acesso em 13.09.2020.

a necessidade de, para as finalidades de fiscalização e desenvolvimento de políticas públicas, serem enviados todos os dados previstos nas respectivas leis. Segundo argumentado pelos Tribunais, não seria permitida a apresentação de exigências amplas como realizado pelas normas impugnadas nos referidos casos.

Mais recentemente, a LGPD previu expressamente o princípio da necessidade (LGPD, art. 6º, III), que exige o uso de tratamento de dados pessoais de forma restrita ao mínimo necessário para a realização das finalidades legítimas estabelecidas pelo controlador, o que envolve a utilização apenas de dados pertinentes, proporcionais e não excessivos. Assim, a LGPD exige ao agente de tratamento identificar quais dados e quais usos são efetivamente necessários para o alcance da finalidade almejada. Por exemplo, no julgamento da ADI nº 6389, dentre os argumentos apresentados pela Ministra Rosa Weber para conceder liminar para suspender os efeitos da Medida Provisória nº 954/2020, que determinava o envio de dados de consumidores de serviços de telefonia para o IBGE, foi justamente a falta de justificativa sobre a necessidade do compartilhamento para alcançar a finalidade almejada.[350]

Além disso, o princípio impede que dados sejam coletados ou mantidos com a justificativa de possível utilidade futura ainda desconhecida. A título de exemplo, pesquisa elaborada por Bruno Bioni e Jorge Machado (2016) argumenta que o tratamento de dados pessoais realizado pelo programa Nota Fiscal Paulista violava os princípios da necessidade e da adequação porque coletava mais dados do que o necessário para a operação do programa. Como apontado pelos autores, o programa coleta dados como CNPJ do estabelecimento, o CPF do cidadão, o valor total pago e a data, quantidade e marca da mercadoria e hora da transação, o que "vai muito além do necessário para que programa em questão opere. A rigor, o estado precisaria, tão somente, do CPF do cidadão, do CNPJ do fornecedor e/ou prestador do serviço ou produto e, por fim, do valor do bem de consumo." Além disso, a Secretaria receptora dos dados, que era a Secretaria da Fazenda, não teria política de restrição ao período de armazenamento, resultando em tratamento dos dados pelo período superior ao necessário para a execução das atividades necessárias à operação da política.

[350] Nas palavras da Ministra Rosa Weber: "Observo que o único dispositivo da MP n. 954/2020 a dispor sobre a finalidade e o modo de utilização dos dados objeto da norma é o § 1º do seu art. 2º. E esse limita-se a enunciar que os dados em questão serão utilizados exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. Não delimita o objeto da estatística a ser produzida, nem a finalidade específica, tampouco a amplitude. **Igualmente não esclarece a necessidade de disponibilização dos dados nem como serão efetivamente utilizados**."

Nesse ponto, o princípio da necessidade impõe desafios para práticas de criação de bases de dados centralizadas e publicação de dados em portais de transparência e dados abertos. Para observar o princípio, será necessário aos detentores das bases de dados identificar previamente a relevância de cada um dos dados para alcançar a finalidade pretendida (e se essa finalidade poderia ser alcançada de outra forma, sem a divulgação desses dados), além de identificar prazos para a ocorrência da divulgação.

No caso de bases de dados centralizadas, o órgão ou entidade pública gestora deverá ter clareza sobre a justificativa legal para a manutenção dos dados e estabelecer procedimento rígido de acesso aos dados por terceiros, nos quais se exige a avaliação prévia sobre objetivos do acesso, quais dados são necessários para o alcance dessa finalidade e por quanto tempo. Autorizado o acesso aos dados, o gestor da base de dados e o terceiro podem formalizar as condições e período do compartilhamento (a exemplo do determinado na Portaria Denatran nº 15/2016, que regula o acesso por terceiros aos seus sistemas e subsistemas).[351] De forma a evitar a burocratização desse acesso a dados, é possível a elaboração de procedimentos simplificados para casos recorrentes e/ou em que o acesso aos dados impõe menores riscos aos direitos e liberdades de cidadãos. No entanto, tal como determinado no julgamento sobre a constitucionalidade do Decreto nº 10.046/2019, determinações de compartilhamento amplo de dados pessoais são incompatíveis com o texto constitucional, por afrontarem os direitos fundamentais à privacidade e à proteção de dados pessoais.

Por sua vez, na publicação de dados em portais de transparência e dados abertos, o gestor dos arquivos ou base de dados que se deseja publicar deverá realizar cuidadosa análise sobre os objetivos da publicação para identificar quais dados são necessários para alcançá-los. Essa análise deverá ser reavaliada periodicamente com o objetivo de identificar a permanência do interesse público na divulgação desses dados, levando em consideração aspectos como as outras bases de dados disponíveis aos público (por exemplo, para identificar duplicidade na publicação de certos dados ou as chances de os dados serem combinados com outros tornados acessíveis ao público) e os pedidos de acesso à informação recebidos (para compreender quais dados poderiam ser proativamente divulgados).

---

[351] Os possíveis interessados devem justificar o interesse e a necessidade do acesso integral ou parcial de acesso (além de especificar os meios que serão utilizados para esse acesso). Caso concedido esse acesso, o interessado deverá assinar Termo de Comprometimento no qual são detalhadas suas condições de acesso e limitados os usos posteriores aos dados.

10.3 Identificação de receptores da informação que se deseja publicar ou compartilhar

Em seguida, será necessário identificar quem são os agentes envolvidos nessa divulgação, na medida em que permite estabelecer com maior clareza a forma, condições e responsabilidade relacionados à divulgação.

Agentes do ecossistema de uso de dados mantidos pelo poder público

A identificação de quem serão os receptores de dados mantidos pelo poder público deverá considerar **(ii)** quem detém a base de dados - detentores ou custodiante das bases de dados; **(iii)** os interessados em acessar as bases de dados - consumidores de dados; e **(iv)** aqueles que atuam na promoção do relacionamento entre detentores e interessados no acesso às bases de dados - intermediários.

Primeiramente, existem os **detentores das bases de dados** (ou custodiante de dados, nos termos do Decreto nº 10.046/2019), que são aqueles que realizam a coleta e armazenam informações para o alcance de finalidades específicas. No caso de bases de dados mantidas por órgão ou entidade pública, os dados poderão ser coletados dos titulares de dados diretamente pela administração pública, serem transferidos ao governo por particulares ou compartilhados entre órgãos e entidades públicas.

Por exemplo, no caso de órgãos de trânsito brasileiros, os dados são oriundos de fontes diversas, como **(i)** obtidos diretamente do titular de dados quando da elaboração ou renovação da CNH; **(ii)** recebidos de outros órgãos públicos, a exemplo da divulgação de dados realizada em função de parceria estabelecida entre certos Detrans e órgãos eleitorais; ou **(iii)** obtidos por intermédio de prestadoras de serviços de trânsito e transporte, como os dados de bilhetagem em transporte público.

As entidades detentoras das bases de dados assumem responsabilidade em relação à devida utilização dos dados, na medida em que deverão assegurar que os dados foram devidamente coletados, prestar informações e assegurar os direitos dos indivíduos em relação aos seus dados, manter a segurança das informações e instituir regras para o adequado acesso aos dados por possíveis interessados (BHATTACHARJEE; CHEN; DASGUPTA, 2020).[352]

[352] Sobre esse respeito, destaca-se manifestação constante da opinião conjunta do EDPS e EDPB a respeito do Data Governance Act, que será mais detidamente abordado no Capítulo 5: A definição de "detentor de dados" prevista no artigo 2(5) da Proposta: A definição de "detentor de dados" prevista no artigo 2(5) da Proposta: "a pessoa jurídica ou o titular dos dados que, de acordo com a legislação da União ou nacional aplicável, tem o direito de conceder acesso ou de compartilhar certos dados pessoais ou não pessoais sob seu

Isso não significa, todavia, conforme se verá adiante, que os demais agentes da cadeia de utilização de dados não assumem responsabilidade sobre o uso dos dados.

Finalmente, o detentor da base de dados poderá atribuir a terceiros (ou gestor de dados, nos termos do Decreto nº 10.046/2019), público ou privado, a gestão da base de dados e o relacionamento com interessados e titulares de dados, como o exemplo da contratação do Serpro pelo Denatran. Tanto o detentor das bases de dados como esse terceiro poderão possuir equipe (*data stewards*) destinada a iniciar e facilitar a utilização dos dados para fins destinados ao alcance do interesse público (VERHULST *et al*., 2020). São esses os indivíduos que serão capacitados para conduzir a promoção de colaboração e pelos cuidados relacionados ao uso responsável de dados pessoais.

Outros agentes da cadeia de utilização de bases de dados são os **intermediários de dados**,[353]-[354] que atuam em etapas diversas do ciclo de vida dos dados na intermediação entre o detentor da base de dados e os possíveis interessados em acessar esses insumos. Eles eram originalmente entendidos como simples conectores (*building bridges*) entre os detentores de bases de dados e seus possíveis interessados, especialmente considerando as dificuldades de acesso e de capacidade técnica para o consumo das informações. No entanto, esses atores passaram a assumir outras funções, como a agregação de dados; a coleta e combinação de bases de dados; a correção de dados inadequados, incompletos ou datados; a interpretação de

---

controle" não está de acordo com os princípios gerais da GDPR, bem como com a letra da GDPR. A este respeito, a EDPB e a EDPS observam que podem surgir incertezas jurídicas pelo fato de a GDPR não mencionar o direito da pessoa em questão de conceder acesso ou de compartilhar seus dados pessoais com terceiros e muito menos um direito equivalente para a pessoa jurídica, que parece ser possível extrapolar a partir da definição de "titular dos dados". Ao contrário, a GDPR garante a cada indivíduo o direito à proteção dos dados pessoais que lhe dizem respeito, o que se refere a um conjunto abrangente de regras para o processamento de dados pessoais que são vinculativas para cada entidade que processa os dados (controlador de dados/controlador conjunto) ou que processa os dados em nome do controlador de dados (operador)" (tradução nossa). Disponível em: https://edpb.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf. Acesso em 28.04.2021.

353 Esse conceito é utilizado pela proposta de Data Governance Act, conforme se verifica pelo Considerando 22: "Espera-se que os prestadores de serviços de compartilhamento de dados (intermediários de dados) desempenhem um papel fundamental na economia de dados, como uma ferramenta para facilitar a agregação e o intercâmbio de quantidades substanciais de dados relevantes. Os intermediários de dados que oferecem serviços que conectam os diferentes atores têm o potencial de contribuir para o agrupamento eficiente de dados, bem como para a facilitação do compartilhamento bilateral de dados. Os intermediários de dados especializados que são independentes tanto dos detentores de dados quanto dos usuários de dados podem ter um papel facilitador no surgimento de novos ecossistemas orientados por dados, independentes de qualquer ator com um grau significativo de poder de mercado." (tradução nossa). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767. Acesso em 28.04.2021.

354 No entanto, a EDPS e a EDPB ressaltam que: "lembramos que o serviço de compartilhamento de dados como plataforma "intermediando entre um número indefinido de titulares e usuários de dados", excluindo o uso por um grupo fechado de usuários de dados, na medida em que a intermediação diga respeito a dados pessoais, deve estar em conformidade com o princípio de proteção de dados por projeto e por padrão sob o artigo 25 da GDPR" (tradução nossa). Disponível em: https://edpb.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf. Acesso em 28.04.2021.

informações; a representação de dados em diferentes formatos, como mapas e infográficos; a disseminação de dados em formas mais acessíveis; a expansão de dados por meio da identificação de limitações e criação de dados; e a conexão e apoio nas interações entre cidadão e governo (DUMPAWAR, 2015).[355]

Assim, essas entidades localizam bases de dados, conectam e estruturam as informações localizadas, produzem valor e complementam as bases de dados, bem como oferecem-na em formato estruturado para interessados diversos. Com isso, os intermediários de dados podem auxiliar na circulação de informações, na medida em que removem obstáculos e facilitam o acesso e uso de informações por terceiros (VAN SCHALKWYK *et al*., 2015).

Entre os formatos assumidos pelos intermediários de dados, que podem ser entidades públicas ou privadas, estão *data brokers*, os fiduciários ou cooperativas de dados *(data trusts and cooperatives*),[356]-[357] entre outros (EDPS, 2020). Eles poderão utilizar os dados para produção de valor ao interesse público, mas também para o empoderamento de titulares de dados (por meio do fornecimento de suporte e mecanismos para que possam gerenciar seus dados), ou para a criação de inovação e valor comercial.

Por exemplo, os *data brokers* são entidades que coletam, gerenciam e vendem dados customizados. São empresas cujo principal negócio é coletar informações pessoais de uma variedade de fontes e agregar, analisar e compartilhar essas informações. Esses *players* não realizam contato direto com os consumidores finais e, no entanto, podem coletar dados de usuários no mundo todo. Tais empresas prestam serviços de análise de mercado para diferentes setores e com diferentes finalidades, como *marketing* personalizado, preços personalizados, customização de produtos, entre outros. Por isso, *data brokers* são enunciados como centros para acesso abrangente a dados para definições de público-alvo em qualquer fase do funil de venda, de modo a ser utilizado por outra empresa em qualquer mercado, em vista da vastidão de informações que essas empresas tratam.

---

[355] Nos termos do Decreto nº 10.046/2019 esses intermediários poderão assumir o papel de plataforma de interoperabilidade, recebedor ou solicitante de dados.

[356] Sobre essas modalidades de intermediários ainda há pouca pesquisa, como ressaltou a EDPS (2020): "a EDPS considera que os intermediários que visam capacitar os sujeitos dos dados através de ferramentas técnicas e outras para gerenciar o uso de seus dados merecem consideração, mais pesquisa e apoio efetivo, pois contribuem para uma utilização sustentável e ética dos dados, de acordo com os princípios da GDPR" (tradução nossa). Vide: https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf. Acesso em 30.08.20202.

[357] Esse é o caso do projeto Decode, que busca desenvolver soluções práticas para que cidadãos possam gerenciar o uso de seus dados. Vide: https://decodeproject.eu/. Acesso em 06.09.2020.

Já os *data trusts* (em português, fiduciários de dados) têm assumido relevância no debate sobre tratamento de dados mantidos pelo poder público, na medida em que, por serem organizações independentes e destinadas a alcançar o interesse público, mantém, controlam e negociam como os dados serão utilizados pelos seus potenciais interessados. A ideia possui paralelo com o movimento de códigos abertos (*open source*), que atribuem a certas organizações (como a Fundação Mozilla ou Apache) o controle sobre seus códigos. [358]

No governo federal brasileiro, é possível afirmar que o Serpro atua enquanto intermediário de dados quando fornece serviços de validação de dados. Isso porque utiliza de bases de dados de outros órgãos públicos (e.g., Denatran e Receita Federal) para auxiliar terceiros a verificar a autenticidade de documentação fornecida por titulares de dados, a exemplo do uso do Datavalid para parceria realizada com Uber na verificação da autenticidade da CNH fornecida por potenciais motoristas.

Há também os **consumidores de dados**,[359] que são os destinatários finais da cadeia de utilização de dados. Esses atores poderão utilizar dados de forma independente, sem envolvimento direto do detentor da base de dados; cooperativa, caso no qual o detentor e o consumidor das bases de dados decidem conjuntamente sobre os usos que serão atribuídos aos dados; direcionada, caso em que o detentor do dado procura estabelecer parceria para assegurar a reutilização dos dados para determinada finalidade (VERHULST *et al*., 2019.2).[360]

A utilização independente de dados poderá ocorrer em duas situações principais: viabilizada pela publicação de bases de dados ou pela utilização de tecnologias para extrair ou baixar conteúdo disponível em *websites* ou plataformas. No caso da utilização de dados

---

[358] https://www.alliancemagazine.org/blog/data-21st-century-oil-foundations-right-owners/. Acesso em 09.10.2020.

[359] Sobre esse respeito, destaca-se manifestação constante da opinião conjunta do EDPS e EDPB a respeito do Data Governance Act, que será mais detidamente abordado no Capítulo 5: "a interação entre a noção de usuário de dados como "pessoa física ou jurídica [autorizada a usar dados para fins comerciais e não comerciais]" e as noções de controlador, controlador conjunto ou processador sob a GDPR também não é clara. Além disso, a Proposta refere-se a uma possível qualificação como controlador ou processador e suas obrigações sob a GDPR para os prestadores de serviços de compartilhamento de dados, mas não para o usuário dos dados ou para as organizações de altruísmo de dados (apesar do fato de que este último também pode ser controlador, co-controlador ou processador sob a GDPR). Mais em geral, a EDPB e a EDPS sublinham que a proposta deve definir os papéis no que diz respeito à lei de proteção de dados pessoais (controlador de dados, processador ou co-controlador) de cada tipo de "ator" (prestador de serviços de compartilhamento de dados, organização de altruísmo de dados, usuário de dados) não apenas para evitar ambigüidade sobre as obrigações aplicáveis da GDPR, mas também para melhorar a legibilidade do texto legal." (grifo meu) (tradução nossa). Disponível em: https://edpb.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf. Acesso em 28.04.2021.

[360] Nos termos do Decreto nº 10.046/2019 os consumidores de dados poderão assumir o papel recebedor ou solicitante de dados.

publicados, o detentor das bases de dados escolhe por tornar a informação acessível ao público - o que deverá ocorrer após a avaliação sobre os riscos dessa atividade aos titulares de dados. Já nas práticas de *scrapping*, a coleta de dados ocorre independentemente de uma ação do detentor das bases de dados, por meio da busca e extração proativa de dados pelo seu consumidor (o que poderá ser viabilizado por intermediários, como visto).

Em relação ao consumo cooperativo ou direcionado dos dados, as decisões pela divulgação e quanto às formas de reuso dos dados contam com a participação tanto do detentor das bases de dados quanto dos intermediários e/ou dos consumidores de dados. Nessas duas modalidades de uso de dados, a sua divulgação será restrita a uma menor quantidade de atores e deverá observar as regras do acordo de compartilhamento de dados.

Tal como em relação aos detentores e intermediários de dados, os consumidores de dados poderão ser entidades públicas ou privadas. Como mencionado anteriormente, as bases de dados da administração pública poderão ser compostas de dados obtidos por intermédio de terceiros. Assim, é possível que órgãos públicos desempenhem *scrapping* de dados em *websites* ou realizem parcerias para recebê-los de terceiros.

Outra forma de categorizar os agentes de tratamento de dados está relacionada com as finalidades de compartilhar e/ou conduzir análise conjunta de dados, ou para fornecer *insights* e *expertise* com vistas à produção de valor público (VERHULST; SANGOKOYA, 2015). Quando diferentes agentes da cadeia de utilização de dados realizam parcerias para promover o uso de dados em prol do interesse público, fala-se em ***data collaboratives***, termo cunhado pelo instituto *the Governance Lab*, da Universidade de Nova York, que compreende parcerias estabelecidas entre entidades públicas e privadas (e.g., empresas, sociedade civil e academia).

Esse conceito considera a forma de atuação dos agentes de tratamento e busca compreender práticas destinadas a reduzir a disparidade entre oferta e demanda por dados (VERHULST; YOUNG, 2018) - visto que os consumidores de dados por vezes não sabem onde encontrá-los ou como analisá-los, e os detentores de bases de dados podem enfrentar desafios em atender as demandas por dados - e fomentar a utilização responsável e inovadora de dados (DE MONTJOYE; GAMS; BLONDEL, *et al*., 2018).

Assim, dentre as iniciativas de *data collaboration* mapeadas estão a: **(a)** a combinação de bases de dados - chamada de *data pooling*; **(b)** a disponibilização de bases de dados para desenvolvedores que irão concorrer a prêmios pela criação de novas aplicações; **(c)** a condução de pesquisas por universidades, acadêmicos ou outros pesquisadores; **(d)** a geração

de novos produtos destinados a apoiar interesses sociais ou humanitários, **(e)** a disponibilização de *Application Programming Interfaces* (APIs), que oferecem acesso direto a bases de dados atualizada em tempo real; e **(f)** intervenção qualitativa de intermediários - os *trusted intermediaries*.[361]

Por exemplo, no caso de *data pooling*, bases de dados públicas e privadas são mescladas e divulgadas para o acesso público, com a finalidade de prover subsídios para usos de interesse público. O *Global Forest Watch* é experiência interessante dessa prática, pois reúne dados fornecidos por governos, universidade e indústria para viabilizar o monitoramento de situações de degradação ambiental no mundo (VERHULST *et al*., 2019.2).

Já as ***trusted intermediaries*** são os intermediários que apoiam o uso responsável de dados, visto que auxiliam na localização e utilização de bases de dados enquanto realizam controles restritos de acesso aos dados (VERHULST *et al*., 2019.2). Há, inclusive, *data brokers* que colaboram para o interesse público como o *Consumer Data Research Center* (CDRD), que realiza ponte entre dados sobre consumidores mantidos por empresas e pesquisadores de Universidades da Inglaterra, ou o projeto *Yale University Open Data Access* (YODA) que facilita o compartilhamento de dados entre detentores de dados clínicos e pesquisadores diversos (VERHULST *et al.*, 2019.2).

Conforme será abordado nesta tese, essas diferentes motivações no acesso de dados devem ser reguladas de formas distintas. Especial cuidado deve ser observado aos *data brokers*, que coletam quantidades enormes de bases de dados, em sua maioria oriundas de fontes públicas ou extraídas de redes sociais, com objetivos diversos e por vezes em desacordo com a legislação aplicável e as legítimas expectativas dos titulares de dados (EDPS, 2020).

Como a lei regula os agentes de tratamento de dados mantidos pelo poder público?

Os conceitos apresentados acima foram extraídos da literatura sobre dados abertos e governo eletrônico e deverão ser compatibilizados com as qualificações apresentadas na legislação. Como mencionado anteriormente, a LGPD possui capítulo específico destinado a regular o tratamento de dados pelo poder público. No art. 24 desse capítulo da LGPD, que

[361] Vide https://hbr.org/2018/01/how-the-data-that-internet-companies-collect-can-be-used-for-the-public-good#:~:text=Shared%20(often%20aggregated)%20corporate%20data,support%20public%20or%20humanitarian%20objectives. e https://link.springer.com/content/pdf/10.1007%2F978-3-030-13895-0_92-1.pdf. Acesso em 05.09.2020.

será mais detidamente abordado no próximo capítulo desta tese, consta que as normas específicas para o poder público são aplicáveis **(i)** aos órgãos públicos da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, Judiciário e Ministério Público; **(ii)** às autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios; e **(iii)** aos serviços notariais e de registro.

Em relação às empresas públicas e às sociedades de economia mista (pessoas jurídicas de direito privado), o capítulo de tratamento de dados pelo poder público será aplicável quando suas atividades estiverem relacionadas à operacionalização de políticas públicas. Nas demais hipóteses em que estiverem atuando em regime de concorrência, se submeterão às mesmas regras aplicáveis às pessoas jurídicas de direito privado (LGPD, art. 24).[362]

A redação desses dispositivos sobre o alcance das normas do Capítulo IV da LGPD permite divergência de interpretação. Segundo consta no art. 23, as regras sobre tratamento de dados pelo poder público seriam aplicáveis às pessoas jurídicas de direito público previstas no parágrafo único do art. 1º da Lei nº 12.527/2011 (Lei de Acesso à Informação). Uma interpretação estrita da norma permite a conclusão de que estariam excluídas do alcance desse Capítulo as entidades como autarquias e fundações públicas constituídas como pessoas jurídicas de direito privado (ADAMI; LANGENEGGER, 2020).[363] No entanto, como aponta Fabrício da Mota Alves (2020), essa seria mais uma dentre as imprecisões normativas das regras sobre o tratamento de dados pelo poder público, de modo que o Capítulo IV poderá eventualmente se aplicar também a determinadas pessoas jurídicas de direito privado.

---

[362] Esse entendimento literal foi reforçado pelo Guia da ANPD, em que autoridade evidencia a extensão do Poder Público às empresas públicas e sociedades de economia mista, desde que (i) não estejam atuando em regime de concorrência; ou (ii) operacionalizem políticas públicas, no âmbito da execução destas (ANPD, 2022.3, p. 5).

[363] Segundo Mateus Piva Adami e Natalia Langenegger (2020), a redação restrita da LGPD leva a interpretações restritivas sobre o alcance das regras constantes do capítulo da LGPD sobre tratamento de dados públicos, conforme se verifica: "A LGPD prevê regramento específico para as atividades de tratamento de dados pelo Poder Público (Capítulo IV). Para tanto, estabelece que estarão abrangidos no escopo dessas normas as pessoas jurídicas de direito público (art. 23, LGPD) referidas no parágrafo único do art. 1º da Lei nº 12.527/2011 (Lei de Acesso à Informação ou "LAI"). Referido dispositivo da LAI trata de dois grupos de pessoas jurídica, que são: **(i)** os órgãos públicos da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, Judiciário e Ministério Público; e **(ii)** as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios. Além disso, a LGPD também estabelece que serviços notariais e de registro deverão observar às mesmas regras. No entanto, tendo em vista que o art. 23 da LGPD se refere exclusivamente às pessoas jurídicas de direito público, estarão abrangidos pelas regras do capítulo de tratamento de dados pelo poder público somente **(a)** os órgãos da administração pública, direta ou indireta, de qualquer dos Poderes de Estado (executivo, legislativo e judiciário) e das instâncias federativas (união, estados, distrito federal e municípios).; e **(b)** as autarquias e as fundações públicas constituídas como pessoas jurídicas de direito público (ou seja, que possuem personalidade jurídica pública)."

Além disso, a LGPD estabelece que os **agentes de tratamento** de dados são aqueles que utilizam os dados pessoais, que podem atuar no papel de controlador ou operador (LGPD, art. 5º, IX).[364] As entidades e órgãos públicos são agentes de tratamento de dados pessoais (art. 5º, IX) geralmente qualificadas como controladoras de dados pessoais. Isso se dá porque, segundo a LGPD, os controladores são aqueles agentes a quem cabem as decisões sobre as atividades que serão realizadas com os dados pessoais e que fornecem instruções aos operadores sobre o modo que estes devem atuar (art. 5º, VI). Os operadores, por sua veze, são aqueles que atuam no tratamento de dados pessoais segundo as orientações do controlador (art. 5º, VII). São sobre esses agentes que recaem as obrigações da lei e que resultam na busca pela devida proteção a dados pessoais.

Disso decorre que somente o controlador poderá determinar os propósitos do tratamento de dados pessoais e os meios essenciais de tratamento de dados pessoais, como os tipos de dados a serem tratados, seu período de retenção, de quais titulares determinados os dados serão coletados e quem terá acesso a eles. Quando mais de um agente está envolvido na definição de finalidades de uso dos dados pessoais, poderá haver mais de um controlador.

Já os meios não essenciais de tratamento de dados podem ser definidos pelos operadores. Ainda que a legislação brasileira não faça essa distinção, é esperado que seja autorizado ao operador determinar alguns dos meios essenciais do tratamento. Na verdade, é comum que o operador tenha alguma liberdade para definir questões como quais *software* e *hardware* serão utilizados na prestação dos serviços, sem que por isso assuma o papel de controlador.

Entes públicos geralmente são, em função de suas atribuições legais, os agentes responsáveis por estabelecer como os dados serão utilizados. Embora a legislação brasileira não estabeleça isso expressamente, a entidade que realizar tratamento de dados pessoais exclusivamente para cumprir com finalidades estabelecidas por legislação será considerada controladora. Essa conclusão, que é extraída de orientações de autoridades europeias,[365] pode ser também aplicável à LGPD porque, do contrário, não haveria controlador de dados pessoais para atividades realizadas em função de determinação legal. Como se verá adiante, como a responsabilidade sobre o devido tratamento de dados pessoais recai essencialmente sobre o

[364] Não somente é possível, como é comum que uma mesma entidade se situe nas diferentes posições da cadeia de uso dados (ou seja, detentores, intermediários ou consumidores).

[365] Nesse sentido, vide o posicionamento do Information Commissioner's Office (ICO) da Inglaterra: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf ou da Working Party 29: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. Acesso em10.04.2021.

controlador, é essencial que qualquer atividade de tratamento possua pelo menos um controlador - o mesmo não se aplica a operadores, que poderão não estar presentes.

Assim, por exemplo, o Denatran é controlador dos dados pessoais que coleta ou recebe em função do exercício de suas atribuições legais, ainda que atribua ao Serpro a gestão desses dados. Nesse sentido se manifestou o Comitê Central de Governança de Dados, instituído pelo Decreto nº 10.046/2019, em Guia de Boas Práticas, publicado em abril de 2020. Em suas palavras, "[n]o âmbito da administração pública, o Controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de tais dados." O CCGD dá um passo adiante e afirma que o controlador, a entidade dotada de capacidade de representação jurídica, será representado pelo órgão com competência para a tomada de decisão sobre a atividade em questão.[366]

De forma similar, a ANPD esclarece que, na administração pública, o papel de controlador recai sobre a entidade detentora de personalidade jurídica, mas que os órgãos e outros entes despersonalizados devem observar as obrigações do controlador, por mais que não possamos ser diretamente responsabilizados pelas atividades de tratamento, na medida em que não são centros de imputação de normas jurídicas. Nas palavras da Autoridade, as atribuições de controlador "são exercidas pelos órgãos públicos que desempenham funções em nome da pessoa jurídica da qual fazem parte" (ANPD, 2022.1). Isso importa para definição de obrigações dos órgãos públicos, enquanto parte de agentes controladores de dados, na medida em que os órgãos públicos passam a ter de nomear encarregados de dados (art. 23, III, LGPD), cumprir com deveres de transparência (art. 23, I, LGPD), observar parâmetros específicos para compartilhamento de dados (art. 26, LGPD) e sofrer sanções administrativas (art. 52, §3º, LGPD).

De fato, essa lógica não se aplica diretamente a qualquer entidade ou órgão público que realize o tratamento de dados pessoais. Por exemplo, há determinadas entidades cujas funções institucionais consistem na prestação de serviços de processamento de dados pessoais para outros entes públicos, a exemplo do Serpro, do DataPrev, da Companhia de Processamento de Dados do Estado de São Paulo ("Prodesp"), da Companhia de Processamento de Dados do Estado da Bahia ("Prodeb"), da Companhia de Tecnologia da Informação do Estado de Minas Gerais ("Prodemge"), entre outras. No entanto, essas instituições poderão atuar como controladoras de dados pessoais, como em relação ao

[366] Disponível em: https://www.in.gov.br/web/dou/-/resolucao-n-4-de-14-de-abril-de-2020-253999748. Acesso em 11.04.2021.

tratamento de dados de seus servidores e/ou funcionários, quando sua ingerência sobre o tratamento de dados excede à definição de meios não essenciais ou quando fornecem serviços próprios com os dados que gerenciam.

Por exemplo, uma empresa de processamento de dados não atua somente como operadora de dados pessoais quando se utiliza de *data lake*, com dados obtidos de diversos entes públicos, para extrair análises próprias capazes de auxiliar nas atividades de outros órgãos ou entidades públicas. No entanto, caso essa empresa apenas disponibilize os meios técnicos para que as entidades detentoras das bases de dados forneçam seus dados para compor *data lake* e para que as entidades consumidoras possam solicitar ou extrair análises de seu interesse, ela será considerada como operadora dos dados.

Também há casos em que os controladores de dados pessoais poderão atuar, pontualmente, como operadores de dados pessoais. Na verdade, a qualificação dos agentes de tratamento de dados pessoais enquanto operadores ou controladores é contextual, ou seja, está relacionada com o papel que exercem em determinada atividade de tratamento de dados pessoais (WP 29, 2010). Isso significa que uma entidade poderá facilmente atuar como operadora e controladora ao mesmo tempo para atividades distintas de tratamento de dados pessoais.

Essa definição é importante para a distribuição de obrigações e responsabilidades entre as partes para determinada atividade de tratamento de dados pessoais.[367] Como o controlador é quem toma as decisões sobre o tratamento de dados pessoais, a ele recaem mais deveres e maior responsabilidade. É o controlador que deverá receber e responder a solicitações enviadas pelos titulares dos dados pessoais quando relacionadas ao acesso, correção e portabilidade de seus dados (LGPD, art. 18), por exemplo.

Também é do controlador a responsabilidade solidária de indenizar titulares de dados em casos de danos provocados a eles, salvo quando conseguir demonstrar que a atividade foi realizada em observância às determinações legais, que não realizou a atividade de tratamento ou que o fato foi provocado por culpa exclusiva do titular de dados ou de terceiros (LGPD, art. 43). Já o operador, como age segundo as instruções do controlador, desde que se atente às instruções recebidas do controlador e não pratique ele mesmo alguma ilegalidade, possui

[367] Algumas normativas editadas por autoridades públicas previam que o controlador de dados era a pessoa do presidente da Corte ou do Procurador-Geral e os operadores eram os demais servidores, funcionários e estagiários, a exemplo da Portaria Conselho da Justiça Federal n. 64/2021 e do Provimento da Procuradoria-Geral de Justiça do Estado do Rio Grande do Sul n. 68/2020, além da Resolução do Tribunal de Justiça do Distrito Federal e Territórios n. 9/2020. No entanto, esse entendimento não deve prosperar.

menores responsabilidades relacionadas ao tratamento de dados. Apenas diante do descumprimento de instruções diretas, ou prática de ilícitos, o operador equipara-se ao controlador.

Como se verifica, sob o olhar da legislação, os diversos agentes da cadeia de utilização dos dados poderão atuar, conjuntamente ou não, como controladores de dados pessoais, na medida em que estabelecem as finalidades para as quais os dados serão tratados. Por exemplo, intermediários e consumidores de dados poderão utilizar bases de dados públicas (ou seja, detidas e divulgadas pelo poder público) para finalidades que venham a determinar de forma autônoma. Nesses casos, serão solidariamente responsáveis pelo tratamento dos dados, ainda que eventualmente possa recair sobre o detentor das bases de dados a obrigação de realizar a interface mais imediata com os titulares de dados pessoais (e.g., obtenção de autorização legal para o compartilhamento de dados).

11 CONCLUSÃO PARCIAL: NECESSIDADE DE DELIMITAR COM PRECISÃO O ESCOPO DA PUBLICAÇÃO E DO COMPARTILHAMENTO DE DADOS PELO PODER PÚBLICO

Diante da apontada ausência de clareza das normas vigentes no Brasil sobre os cuidados que devem ser observados para decidir e implementar a divulgação de dados pelo poder público, neste capítulo foram apresentados entendimentos constantes de guias sobre o tema elaborados por autoridades de proteção de dados da Europa e relatório elaborado por municipalidade dos Estados Unidos. A escolha por estudar esses guias e relatórios está relacionada à influência que a legislação e práticas europeias de proteção de dados pessoais na prática brasileira do tema, assim como pelo pioneirismo acadêmico do relatório elaborado para o programa de dados abertos da cidade estadunidense de Seattle.

Como se pôde observar, há considerável similaridade nas soluções apresentadas pelos guias analisados para viabilizar a publicação e o compartilhamento de dados pelo poder público em observância à privacidade e proteção de dados pessoais de cidadãos. Essa semelhança se dá em dois principais eixos: **(i)** semelhança entre soluções apontadas na Europa e nos Estados Unidos; e **(ii)** semelhança nas soluções identificadas tanto para o compartilhamento como para a publicação. Em relação às diferenças entre soluções apresentadas entre países/regiões estão que, enquanto na Europa há exigência de observação de bases legais, princípios e direitos de titulares de dados, no relatório de Seattle essas exigências não estão presentes e há maior foco na análise dos riscos e benefícios da divulgação de dados. Quanto às diferenças entre soluções apresentadas para o compartilhamento e para a publicação, elas estão mais relacionadas às condições em que essa divulgação ocorre (e.g, objetivo da divulgação, quem é o receptor dos dados e capacidade de controle sobre usos secundários) do que em relação à qualificação da atividade como compartilhamento ou publicação.

Em relação à similaridade entre os documentos elaborados por autoridades europeias e o relatório dos Estados Unidos, destacam-se a necessidade de observar alguns procedimentos mínimos durante e após a publicação e o compartilhamento dos dados, como a identificação dos objetivos da divulgação, a avaliação do interesse público na divulgação, a instituição de estrutura de governança, elaborar relatório de impacto, e adoção de salvaguardas.

Em vista do aprendizado com a prática estrangeira e tendo em vista o disposto na legislação nacional, esta Parte da tese propôs alguns cuidados que deverão ser adotados pelo poder público na definição sobre a publicação ou o compartilhamento de dados pessoais. Primeiro, o agente público deverá identificar se a divulgação **envolve dados pessoais identificados** ou as chances reais de a divulgação de dados permitir a posterior identificação dos titulares de dados. Isso se dá porque dados constantes dos documentos ou bases de dados que se pretende divulgar podem identificar diretamente uma pessoa, permitir razoavelmente a identificação de pessoas ou não permitir a fácil identificação de uma pessoa. Essa atividade apresenta complexidade em vista da constante evolução tecnológica e da amplitude de alcance do conceito de dados pessoais, tal qual adotado pela legislação brasileira (que considera o dado pessoal como aquele que permite identificar uma pessoa natural).

Considerando que os governos possuem grandes quantidades de dados e que os receptores de dados poderão posteriormente associá-los a outras bases de dados (de forma a facilitar a possibilidade de identificar as pessoas sobre quem eles se referem), muitos dos dados divulgados pelo poder público poderão ser qualificados como dados pessoais. De todo modo, entre os critérios que podem ser considerados para a avaliação sobre a presença de dados pessoais na divulgação de dados desidentificados estão o custo da identificação, os riscos da ocorrência de incidentes de segurança da informação, a tecnologia disponível no momento do tratamento, e os estímulos que o controlador possui na identificação da pessoa.

Além disso, deve-se destacar que a divulgação ou a incidência de sigilo ou confidencialidade sobre o dado não removem a sua caracterização como dado pessoal. Em outras palavras, o fato de o dado ser controlado pelo governo, ser divulgado com terceiros ou ser protegido por norma de sigilo ou cláusula de confidencialidade não remove sua proteção enquanto dado pessoal. De fato, a legislação de proteção de dados pessoais reconhece que esse dado poderá ser de acesso público, por força de obrigação legal ou regulatória, ou tornado manifestamente público pelo titular, sem que deixem de receber proteção legal própria de dados pessoais, ainda que possuam regras específicas aplicáveis ao seu tratamento. Do mesmo modo, eventual divulgação de dados protegidos por norma de sigilo ou confidencialidade deverá ser realizada segundo autorização legal ou judicial e/ou mediante o consentimento livre, expresso e informado do titular de dados.

Em seguida, é necessário ter clareza sobre **quais os objetivos almejados com a divulgação**. Com isso, é possível determinar quais bases de dados ou documentos devem ser publicados ou compartilhados e quais medidas devem ser observadas para que esses usos

sejam realizados em observância ao determinado pela legislação. Essa definição também é essencial para a observância do princípio da finalidade, tal como previsto na legislação de proteção de dados pessoais e nas normas aplicáveis à administração pública. Na perspectiva da proteção de dados pessoais, o princípio da finalidade exige que o objetivo do tratamento busque propósitos legítimos, específicos, explícitos, e previamente informados aos titulares de dados, não sendo autorizadas atividades posteriores e incompatíveis. Com isso, assegura-se ao titular de dados mais elementos para que possa exercer sua autodeterminação em relação a como seus dados pessoais serão utilizados por terceiros. Por sua vez, na perspectiva do direito administrativo, o princípio da finalidade corresponde à aplicação da legislação da forma como idealizada pelo legislador, para o alcance do interesse público e segundo as atribuições legais do agente público. Nesse sentido, pela leitura conjunta do princípio da finalidade, segundo a lei de proteção de dados pessoais e a teoria administrativista, não somente deverá o compartilhamento e a publicação de dados pelo poder público buscar atender um objetivo específico informado ao titular de dados, mas a finalidade pretendida deverá estar prevista no ordenamento jurídico, ser realizada conforme as atribuições legais do órgão ou entidade pública, e almejar o alcance do interesse público.

Outro aspecto do princípio da finalidade consiste na exigência de que dados pessoais sejam tratados nos limites do informado aos seus titulares, sendo vedados usos posteriores para finalidades incompatíveis com aquelas informadas. A avaliação sobre a compatibilidade do tratamento envolve identificar a relação entre as novas finalidades e aquelas para as quais o dado foi coletado, o contexto de coleta dos dados, as legítimas expectativas do titular, a natureza do dado pessoal, e o impacto do novo tratamento sobre o titular. Para o tratamento de dados pelo poder público, haverá desafio particular em comprovar a compatibilidade do novo tratamento, visto que a coleta de dados normalmente decorre de alguma obrigação legal ou regulatória e haverá disparidade de poder entre cidadão e Estado. Por isso, cidadãos nem sempre terão a expectativa de que seus dados serão utilizados para finalidades distintas e nem sempre terão meios de impedir que seus dados sejam utilizados para tais finalidades distintas.

Isso se agrava em relação ao compartilhamento e à publicação, que ampliam as possibilidades de reuso de dados pessoais por terceiros, inclusive para finalidades não compatíveis com aquelas que justificaram a sua coleta. Por isso, para casos de divulgação de dados pelo poder público, a avaliação da compatibilidade deve ser realizada considerando a competência do ente público que divulga ou que recebe os dados, e também verificar a presença de uma obrigação legal específica, as circunstâncias do tratamento de dados, como a

natureza do dado, a forma de coleta e as salvaguardas oferecidas ao titular de dados, e os impactos negativos que poderão ser gerados sobre cidadãos em função da publicação.

Nesse momento, o agente público deverá identificar também se a divulgação e o pretendido reuso do dado observa o **princípio da necessidade**, o que importa em limitar o tratamento ao estritamente relevante e necessário para alcançar a finalidade informada aos titulares de dados. Esse esforço requer identificar se a finalidade pode ser alcançada por outro meio menos lesivo a direitos e liberdades de indivíduos, ou pelo tratamento de outros ou menos dados. Além disso, envolve assegurar que o tratamento será realizado pelo período estritamente necessário para alcançar as finalidades informadas aos titulares de dados.

A observância do princípio da necessidade na divulgação de dados pelo poder público enfrenta desafios, na medida em que exige do agente público ter clareza sobre justificativa legal para a manutenção dos dados e estabelecer procedimento rígido de acesso aos dados por terceiros, que deverá ser revisto com alguma periodicidade.

Outra etapa necessária à determinação sobre a divulgação de determinada base de dados ou documento, é identificar **quem são os agentes envolvidos** nessa divulgação, de forma a melhor distribuir responsabilidades relacionadas à divulgação. Em novas modalidades de governo, como governos eletrônicos ou abertos, há um complexo arranjo de agentes na circulação de dados. Conhecer quem são esses agentes permite melhor distribuir obrigações e responsabilidades para o uso adequado de dados pessoais de cidadãos. Naturalmente, os detentores das bases de dados objeto do compartilhamento ou da publicação de dados pessoais estudados nesta tese são órgãos ou entidades públicas (ou particulares atuando em nome do Estado), independente do fato de os dados terem sido coletados diretamente dos titulares de dados ou recebidos de terceiros, agentes públicos ou privados, ou de a gestão dos dados ser atribuída a outra entidade com expertise nessa atividade. Sobre esses agentes recai a responsabilidade de assegurar a devida utilização dos dados.

Outros agentes importantes na divulgação de dados pelo poder público são os intermediários de dados, que atuam na intermediação entre os detentores das bases de dados e os possíveis interessados em acessar esses dados. Esses agentes assumem particular relevância em vista da multiplicidade de canais e formatos em que dados são divulgados pelo poder público, o que pode dificultar seu conhecimento e acesso por terceiros. Os serviços que oferecem são de diversos formatos, podendo consistir na localização, conexão ou estruturação de informações, assim como a produção de valor e complementação de bases de dados. A

responsabilidade desses agentes dependerá de seu modelo de atuação, dependendo da sua ingerência decisória sobre como os dados serão tratados.

Na literatura há bastante foco e crítica a intermediários como data *brokers*, que realizam varredura e venda customizada de dados. De fato, não há dúvida sobre o potencial malicioso de atividades realizadas por intermediários dessa natureza. No entanto, não é desejável rejeitar de princípio modelos de negócios, sendo necessário refletir detidamente sobre os limites éticos de sua atuação e assegurar que observam regulação específica (incluindo a legislação sobre proteção de dados pessoais). Inclusive, como se verifica na literatura estrangeira, há novos modelos de intermediários que atuam na promoção do interesse público ou na facilitação do exercício de direitos por parte dos titulares de dados.

Outro agente da cadeia de divulgação de dados são os consumidores de dados, que são os destinatários finais dos dados e poderão ser agentes públicos ou privados. Sua utilização dos dados poderá ser independente do detentor ou do intermediário de dados, ou poderá ser de forma cooperativa. Esse agente, assim como o detentor dos dados (e, em determinadas situações, o intermediário), será responsável pelo devido tratamento dos dados pessoais. Para além de observar as normas de proteção de dados pessoais, terão que observar também regras e limitações ao reuso de dados impostas pelo detentor das bases de dados ou pela legislação (a exemplo da limitação imposta pelo princípio da finalidade, que restringe o reuso de dados para finalidades não compatíveis com as informações prestadas ao titular de dados).

Esses conceitos extraídos da literatura de publicação e compartilhamento de dados não têm equivalência na LGPD, mas dialogam com ela na medida em que permitem melhor definir a participação de cada agente na atividade de tratamento de dados pessoais. Conforme a LGPD, os sujeitos envolvidos no uso de dados pessoais são qualificados como agentes de tratamento de dados e podem assumir o papel de controlador ou de operador. A responsabilidade sobre o tratamento recai essencialmente sobre os controladores, na medida em que estabelecem as finalidades e condições do tratamento. Os operadores serão responsabilizados em situações específicas, quando atuarem de forma ilícita ou fora das orientações do controlador. No caso de tratamento de dados pelo poder público, em regra, órgãos e entidades públicas atuarão como controladores, em vista de suas atribuições legais, motivo pelo qual serão responsáveis por garantir que dados pessoais sejam tratados em conformidade com a legislação.

Finalmente, nos casos em que a base de dados possuir dados identificados ou identificáveis, e sempre que a divulgação desses dados for essencial ao alcance de finalidades almejadas, será necessário **avaliar se há interesse público** na divulgação, conforme será mais detidamente abordado no capítulo que segue. Essa avaliação pode já ter sido concretizada em norma anterior que restringe ou determina a divulgação em questão (caso em que ao gestor público caberá apenas ponderar as condições da divulgação determinadas em lei) ou deverá ser realizada pelo gestor público no caso concreto.

PARTE IV IDENTIFICAÇÃO DO INTERESSE PÚBLICO NO COMPARTILHAMENTO E NA PUBLICAÇÃO DE DADOS PELO PODER PÚBLICO

12 MÉTODO PARA A IDENTIFICAÇÃO DE INTERESSE PÚBLICO

Caso a base de dados ou documentos que se deseja divulgar possua dados pessoais, identificados ou que possam ser posteriormente associados a uma pessoa natural, será necessário avaliar se há interesse público na divulgação desses dados.

Como mencionado anteriormente, tanto a legislação que regula a divulgação de dados por órgãos públicos como a LGPD estabelecem o interesse público enquanto baliza para a tomada de decisão sobre a publicação ou o compartilhamento de dados pessoais mantidos pelo poder público. De um lado, a LAI estabelece que dados pessoais poderão ser transferidos mediante consentimento ou em situações como o alcance do interesse público (LAI, art. 31, §3˚, I a V). Além disso, os atos administrativos devem ser pautados pelos princípios da legalidade e da finalidade, que exigem que a atuação do agente público seja pautada pelo interesse público no cumprimento de suas atribuições legais. De outro lado, o capítulo da LGPD sobre tratamento de dados pelo poder público estabelece que as atividades de tratamento de dados pessoais pelo poder público deverão ser orientadas ao atendimento de suas finalidades públicas, na persecução do interesse público e tendo como objetivo a execução de competências ou atribuições legais do serviço público (art. 23). Para além disso, por ser a proteção de dados pessoais um direito constitucional, sua flexibilização deverá ocorrer para o alcance de "finalidades de interesse público legitimamente protegidas pelo ordenamento jurídico".[368]

Assim, para a determinação por entes públicos sobre o compartilhamento e a publicação de dados pessoais, identificados ou identificáveis, será necessário avaliar se há interesse público nessa divulgação. No entanto, o conceito de interesse público nem sempre é claramente estabelecido em lei, de forma que recai ao administrador público ou a magistrados identificar, dentro de parâmetros constitucionais e legais, quando o interesse público impõe determinado nível de flexibilização à privacidade e à proteção de proteção de dados pessoais

[368] Vide: voto do Ministro Gilmar Mendes, na Medida Cautelar na ADPF 6.390-DF, julgada em 07.05.2020. Disponível em https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358567. Acesso em 05.09.2022.

de cidadãos. Para tanto, é necessário compreender os contornos de como aplicar esse conceito quando da divulgação de dados mantidos pelo poder público.

Como demonstrado anteriormente, essa ausência de parâmetros claros tem permitido a tomada de decisões arbitrárias e incoerentes na avaliação do interesse público (que muitas vezes sequer é feita) atrelado a determinada divulgação de dados, como apontado por esta tese. De um lado, há ausência de harmonia na publicação de dados pessoais por força da Lei de Acesso à Informação. Por exemplo, enquanto, no meio de uma pandemia, se determinou o sigilo da carteira de vacinação do Presidente da República, pessoa cujo alcance da privacidade é restringido em vista da relevância do cargo que ocupa, dados identificadores de cidadãos beneficiários de programas sociais foram publicados no portal da transparência. Por outro lado, há também incoerência decisória em casos de pedidos de acesso à informação e de compartilhamento de dados pelo poder público. Por exemplo, enquanto a LGPD tem sido frequentemente utilizada para rejeitar pedidos de acesso aos registros de quem entra no Palácio do Planalto, dados da carteira nacional de habilitação de cidadãos são cada vez mais compartilhados com terceiros, como a Abin e o Tribunal Superior Eleitoral.

Essa mesma preocupação - sobre a falta de parâmetros claros para determinar quando o interesse público resultar na divulgação de dados pessoais mantidos pelo poder público - foi demonstrada também pela Autoridade de Proteção de Dados do Canadá (OPC, 2021), como se verifica:

> Critérios claros e específicos em uma nova lei [...] ajudariam a orientar os tomadores de decisão ao considerar fazer divulgações de interesse público e forneceria salvaguardas importantes contra a divulgação injustificada de informações pessoais. Isso é particularmente importante devido à ausência de definições legais a serem extraídas do estatuto, de outra legislação ou da jurisprudência do Canadá interpretando o conceito. O 'interesse público' é obviamente um conceito muito amplo que pode ser difícil de definir, particularmente quando deixado à opinião ou discrição individual. (tradução livre).

Assim, a indefinição sobre o conceito de interesse público não é uma particularidade do Brasil (ou do Canadá). Como mencionado por Feintuck (2004), o conceito de interesse público é tão frequentemente utilizado e historicamente persistente, que é mobilizado sem muita reflexão a respeito do seu significado. No entanto, trata-se de conceito importante na medida em que exige que decisões tomadas no âmbito do poder público avaliem aspectos essenciais ao bem-estar dos membros da comunidade (PATERSON; MCDONAGH, 2017).

Diante da relatada ausência de coerência na determinação do interesse público, neste momento se buscará identificar como as doutrinas de direito administrativo e de direito

constitucional nacional, assim como a prática estrangeira, conceituam o interesse público. O objetivo desse esforço não será alcançar uma definição única para o conceito de interesse público, mas tão somente compreender seus contornos, de modo a estabelecer parâmetros para auxiliar agentes públicos na tomada de decisão em casos concretos de compartilhamento ou publicação de dados pessoais.

12.1 Interesse público segundo a teoria administrativista

Em relação ao conceito de interesse público no direito administrativo, será realizada breve apresentação sobre as duas principais teses em torno do conceito e realizada análise da mais recente e majoritária corrente. A despeito da divergência existente entre essas correntes, conforme se verá em seguida, a mais recente doutrina administrativa (aqui representada especialmente por Floriano Marques Neto, Gustavo Binenbojm e Juliana Palma) no tema melhor se relaciona com a regulação e doutrina sobre proteção de dados pessoais, que entendem superada a dicotomia entre o público e o privado.

Em sua versão mais tradicional, o interesse público é considerado a dimensão pública ou a soma dos interesses individuais que formam um coletivo que,[369]-[370] por sua vez, deverá prevalecer aos interesses individuais (BANDEIRA DE MELLO, 2015). Assim, o interesse público não seria contraposto aos interesses dos indivíduos, mesmo que sejam diferentes em seus objetivos gerais, visto que o primeiro seria o resultado da agregação dos últimos dentro de uma sociedade.

Para tanto, a determinação do conteúdo do interesse público seria realizada previamente pelo legislador, por meio da Constituição e legislação ordinária. Isso significa que, para essa corrente, o interesse público está relacionado ao princípio da legalidade, na

---

[369] "[...] os interesses dos cidadãos expressam-se mediante duas dimensões: (i) uma particular, que corresponde às conveniências exclusivamente pessoais do indivíduo, singularmente considerado (v.g., interesse de não ter o seu imóvel expropriado); (ii) uma pública, representada pelo interesse do indivíduo considerado como membro da coleti- vidade maior na qual está inserido (v.g., interesse do mesmo indivíduo de que exista o instituto da desapropriação, e de que ele seja utilizado quando necessário).18 A primeira delas traduz o interesse privado; a segunda, o público." HACHEM, D. W. A dupla noção jurídica de interesse público em Direito Administrativo. **A&C - Revista de Direito Administrativo & Constitucional**, v. 11, n. 44, p. 59, 16 abr. 2011.

[370] Em rigor, o necessário é aclarar-se o que está contido na afirmação de que interesse público é o interesse do todo, do próprio corpo social, para precatar-se contra o erro de atribuir-lhe o *status* de algo que existe por si mesmo, dotado de consistência autônoma, ou seja, como realidade independente e estranha a qualquer interesse das partes. O indispensável, em suma, é prevenir-se contra o erro de, consciente ou inconscientemente, promover uma separação absoluta entre ambos, ao invés de acentuar, como se deveria, que o interesse público, ou seja, o interesse do todo, é "junção" qualificada dos interesses das partes, um aspecto, uma forma específica, de sua manifestação. (BANDEIRA DE MELLO, 2015).

medida em que seu conteúdo seria uma representação daquilo que está previsto em lei. Ao gestor público caberão alguns restritos espaços de discricionariedade na execução do ato administrativo (ou seja, momentos em que o administrador pratica atos com certa margem de liberdade), o que poderá se dar em relação ao momento da prática do ato, à forma do ato, ao motivo do ato, à finalidade do ato ou ao conteúdo do ato (DE MELLO, 2014). Tendo em vista atender ao princípio da legalidade, o grau de liberdade do administrador poderá ser maior para as primeiras variáveis indicadas e menor para as últimas. Ou seja, essa gradação na intensidade da discricionariedade administrativa ocorre porque o gestor deverá sempre observar critérios previamente estabelecidos pela legislação, contemplando ao menos a competência e a finalidade do ato praticado (esta última será sempre um interesse público).

Mais recentemente, a doutrina argumenta pela inexistência de um interesse público definido *ex ante* e que deverá prevalecer ao interesse de particulares (MARQUES NETO, 2002; BINENBOJ, 2014; PALMA, 2015). Isso se daria, entre outros, pelo reconhecimento de que existe uma pluralidade (e até mesmo fragmentação) de interesses dentro da sociedade que impossibilita essa concepção prévia e unitária do que seria o resumo dos interesses de indivíduos em uma determinada sociedade (MARQUES NETO, 2002). Assim, o conceito deve ser entendido como indeterminado e o preenchimento de seu significado depende de processo administrativo que pondere os diferentes interesses existentes na sociedade e seja resolvido por decisão pública motivada (BINENBOJM, 2014).

Considerando que esses direitos possuem estrutura maleável, seria inadequado realizar uma avaliação estanque e *a priori* que sempre priorize os interesses da coletividade em detrimento de direitos individuais (BINENBOJM, 2014). Mais que isso, não seria mais possível falar nessa dicotomia entre o público e o privado (MEDAUAR, 2017). A ponderação entre interesses será geralmente realizada pelo legislador, mas sempre caberá ao gestor público alguma margem de decisão no caso concreto. Com isso, o alcance do interesse público seria resultado de controle interno pelo órgão público com o apoio de participação social (MARQUES NETO, 2002), realizado em esforço de ponderação entre direitos fundamentais destinado a buscar a maximização de sua consecução mútua (MARRARA, 2012; BINENBOJM, 2014).

Assim, o poder público passaria a assumir o resultado de uma mediação entre diferentes interesses sociais (MARQUES NETO, 2002), resultando em um interesse público heterogêneo (que se contrapõe à anterior compreensão de que seria o resultado de uma agregação de interesses individuais quase homogêneos). Por isso, o devido processo decisório

assume grande relevância, sendo necessário prever mecanismos capazes de assegurar escuta dos interesses envolvidos, que resultará em decisão de alcance transindividual e que deverá ser motivada e pública (PALMA, 2015).[371] Mais que isso, quando não houver real conflito entre interesses privados e coletivos, o procedimento do qual se extrai o interesse público poderá ser dotado de consensualidade (PALMA, 2015).

Como se verifica, segundo a mais atual teoria do direito administrativo, a compreensão do conteúdo desse interesse público que será responsável por balizar o devido tratamento de dados pessoais por órgãos e entidades públicas envolve a condução de processo participativo que resultará em decisão maximizadora dos diferentes interesses sociais envolvidos e do princípio da legalidade. Em outras palavras, sob essa perspectiva, as atividades com dados pessoais realizadas pelo governo deverão ser amplamente publicizadas e documentadas (em observância aos princípios da transparência e *accountability*), além de serem formalizadas em processos que contem com participação social e realizem a ponderação entre os interesses contrapostos.

12.2 Identificação do interesse público com apoio do teste de proporcionalidade

Considerando o exposto acima, a definição do interesse público perpassa pelo reconhecimento de que existe uma pluralidade de interesses da sociedade que deverão ser ponderados em uma decisão pública motivada (BINENBOJM, 2014). Quando se trata da divulgação de dados pessoais, por meio do compartilhamento ou da publicação, os interesses que porventura se encontram em conflito são o direito fundamental à proteção de dados pessoais (que, como mencionado anteriormente nesta tese, possui respaldo nos direitos da dignidade da pessoa humana e da privacidade) e os princípios da eficiência, impessoalidade e transparência governamentais, além da liberdade de expressão, sempre que a publicação de conteúdo pelo governo seja relevante para a formulação de um debate público livre. Seguindo a doutrina constitucional alemã e amplamente adotada nas Cortes brasileiras, esses valores jurídicos são princípios, que possuem alcance abstrato e estão em constante tensão entre si.

---

[371] Nas palavras de Floriano Azevedo de Marques Neto (2002): "O princípio da supremacia do interesse público, parece-nos deve ser aprofundado de modo a adquirir a feição da prevalência dos interesses públicos e desdobrando-se em três subprincípios balizadores da função administrativa: (i) a interdição do atendimento de interesses particularisticos (v.g., aqueles desprovidos de amplitude coletiva, transindividual); (ii) a obrigatoriedade de ponderação de todos os interesses públicos enredados no caso específico; e (iii) a imprescindibilidade de explicitação das razões de atendimento de um interesse público em detrimento dos demais."

Trata-se, portanto, de conflito entre princípios constitucionais, cuja delimitação de escopo ocorre no caso concreto quando do sopesamento de princípios que estejam em conflito. Como um mandamento de otimização, segundo a teoria predominante adotada em solo nacional, sua eventual limitação em função de outro princípio constitucional deverá ser precedida da avaliação sobre a proporcionalidade da medida pretendida. Para tanto, deverá ser aplicado teste específico, cujo objetivo, nas palavras do Ministro Gilmar Mendes, "é fazer com que nenhuma restrição a direitos fundamentais tome dimensões desproporcionais".[372]

Como aponta Virgílio Afonso da Silva (2002), a avaliação sobre a proporcionalidade da medida concreta que resulta na limitação de princípios constitucionais exige o percurso de três etapas fundamentais, consistentes na identificação se a medida é adequada, necessária e proporcional em sentido estrito (ainda que a jurisprudência do STF não realize ou não torne claro seu esforço em observar essas três etapas da regra da proporcionalidade).

A etapa da **adequação** consiste em identificar se os meios escolhidos são aptos a alcançar ou fomentar o resultado almejado. Em outras palavras, a limitação proposta a determinado princípio fundamental será inadequada se deixar de contribuir para que o resultado desejado seja ao menos fomentado. Já a etapa da **necessidade** determina que o objetivo almejado não poderá ser promovido com a mesma intensidade caso sejam adotadas medidas alternativas que limitem em menor intensidade o princípio fundamental em questão. Nessa etapa, a avaliação pressupõe a comparação entre a medida adotada com relação a outras medidas que poderiam ser menos ofensivas ao direito fundamental. Por sua vez, o exame de **proporcionalidade em sentido estrito** que exige o sopesamento entre a intensidade de prejuízo da restrição a um direito fundamental com o benefício da garantia do direito fundamental colidente. Assim, uma medida não será proporcional em sentido estrito se o peso dos motivos que a fundamentam não for suficiente para justificar a restrição ao outro direito.

Segundo a teoria alemã, à qual Virgílio Afonso da Silva se filia, a aplicação dessas três etapas inerentes ao teste de proporcionalidade deverá observar uma ordem específica, iniciando pela avaliação da adequação da medida, passando pela identificação da sua necessidade e finalizando com a ponderação sobre sua proporcionalidade em sentido estrito. Além disso, é possível que o teste de proporcionalidade se encerre com a avaliação da adequação sem que seja necessário identificar a presença da necessidade e da proporcionalidade em sentido estrito. Isso significa que, se não comprovada a adequação da

[372] Excerto extraído do julgamento da ADI 6398. Disponível em: https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf. Acesso em 02.11.2022.

medida, sequer deverá ser realizado o teste sobre sua necessidade ou da proporcionalidade em sentido estrito.[373]

De todo modo, há na doutrina e na prática ao menos duas outras tendências em relação à aplicação de teste de proporcionalidade. Como aponta Virgílio (2002), há autores que no teste de proporcionalidade apenas empregam as etapas da adequação e da necessidade, sem passar pela proporcionalidade em sentido estrito, e autores que estudam a Corte Europeia de Direitos Humanos identificam elemento adicional antes da análise de adequação, necessidade e proporcionalidade em sentido estrito, consistente na análise de legitimidade dos fins que a medida questionada pode atingir. Além disso, o autor aponta que, no Brasil, o Supremo Tribunal Federal adota a regra da proporcionalidade, mas a utiliza de forma eventualmente imprecisa[374] ou sem justificar o cumprimento das três etapas do teste.[375]

No entanto, há doutrina que aponta preocupação com a utilização arbitrária do balanceamento entre interesses constitucionais, que porventura impõe risco a direitos humanos.[376] Por exemplo, Stavros Tsakyrakis (2009) critica a utilização da regra da proporcionalidade para a solução de conflito de interesses sob o argumento de que, em sua busca por objetividade e neutralidade, afasta considerações em torno de argumentos morais. Com isso, não se questiona mais o que seria certo ou errado em casos de direitos humanos,

---

[373] Essa observância da ordem no teste de proporcionalidade é explicada por Virgílio Afonso da Silva (2002): "A análise da adequação precede a da necessidade, que, por sua vez, precede a da proporcionalidade em sentido estrito. A real importância dessa ordem fica patente quando se tem em mente que a aplicação da regra da proporcionalidade nem sempre implica a análise de todas as suas três sub-regras. Pode-se dizer que tais sub-regras relacionam-se de forma subsidiária entre si. Essa é uma importante característica, para a qual não se tem dado a devida atenção. A impressão que muitas vezes se tem, quando se mencionam as três sub-regras da proporcionalidade, é que o juiz deve sempre proceder à análise de todas elas, quando do controle do ato considerado abusivo. Não é correto, contudo, esse pensamento. É justamente na relação de subsidiariedade acima mencionada que reside a razão de ser da divisão em sub-regras. Assim, a aplicação da regra da proporcionalidade pode esgotar-se, em alguns casos, com o simples exame da adequação do ato estatal para a promoção dos objetivos pretendidos. Em outros casos, pode ser indispensável a análise acerca de sua necessidade." Disponível em: https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf. Acesso em 02.11.2022.

[374] Nas palavras do autor: "a regra da proporcionalidade na jurisprudência do STF pouco ou nada acrescenta à discussão e apenas solidifica a idéia de que o chamado princípio da razoabilidade e a regra da proporcionalidade seriam sinônimos. A invocação da proporcionalidade é, não raramente, um mero recurso a um topos, com caráter meramente retórico, e não sistemático. Em inúmeras decisões, sempre que se queira afastar alguma conduta considerada abusiva, recorre-se à fórmula "à luz do princípio da proporcionalidade ou da razoabilidade, o ato deve ser considerado inconstitucional".

[375] Nas palavras do autor: "Apesar de salientar a importância da proporcionalidade "para o deslinde constitucional da colisão de direitos fundamentais", o Tribunal não parece disposto a aplicá-la de forma estruturada, limitando-se a citá-la. [...] nem sempre o recurso à regra da proporcionalidade é justificado nas decisões do Supremo Tribunal Federal. Muitas vezes é a fundamentação simplesmente pressuposta, como se se tratasse da utilização de um princípio constitucional de larga tradição no direito brasileiro".

[376] De fato, na obra *Proportionality and the Rule of Law*, autores diversos debateram a adequação dos métodos de ponderação à defesa dos direitos fundamentais e do princípio da legalidade. HUSCROFT, Grant; MILLER, Bradley W.; WEBBER, Grégoire, *et al*. Proportionality and the Rule of Law – Rights, Justification, Reasoning, Cambridge University Press, New York, 2014.

mas busca-se avaliar se algo é apropriado, adequado e se ocorre na intensidade correta. Por não serem quantificáveis, aos argumentos morais não seria atribuída a relevância devida na avaliação da proporcionalidade, permitindo que direitos humanos se tornem fortes candidatos a sofrer distorções. Por isso, o autor argumenta que juízes, quando diante de conflitos entre interesses, não tenham receio de entrar em embates morais (que estão naturalmente sempre presentes, a despeito da tentativa do teste de proporcionalidade de encontrar neutralidade e objetividade) e reconheçam e abertamente enfrentem os conflitos morais presentes no caso.

De forma similar, Grégoire Webber (2014) argumenta que uma abordagem recepcionada dos direitos humanos (identificada como aquela pautada pela proporcionalidade), permitiria a equiparação entre direitos e interesses, com a conclusão de que não há óbice para seu balanceamento. E isto, em sua visão, reduz os direitos a interesses derrotáveis, desrespeitando a noção essencial da prioridade moral dos direitos sobre interesses. Nesta "abordagem recepcionada", um aplicador do direito seria convocado a deliberar sobre a juridicidade de determinada situação em um processo de duas fases: **(i)** o juiz atribuiria uma formulação dos direitos envolvidos no caso, que geralmente corresponderia à sua versão mais amplamente concebida; e **(ii)** após isso, o juiz deveria analisar em que medida esses direitos amplamente concebidos devem ser legitimamente limitados. Assim, essa abordagem tomaria uma alegação inicial de direito que poderá ser violado, contanto que de forma justificada. Webber denuncia a abordagem recepcionada sob o argumento de que ela leva a um divórcio entre a determinação do *escopo* ou *conteúdo* de um direito e a análise sobre o que uma *alegação de direito* efetivamente significaria na prática, sendo que a consequência de definir prematuramente os direitos é admitir que eles sejam frequentemente violados. Por isso, defende que direitos serão *absolutos* e *inderrotáveis*, de modo que a confirmação da existência de um direito deverá ser seguida da consideração moral dos direitos envolvidos.

Por sua vez, Francisco Urbina (2012) concorda com Grégoire Webber e Stavros Tsakyrakis (além de autores como John Finnis e John Alder) de que o teste de proporcionalidade, em uma tentativa de atribuir objetividade a decisões, busca estabelecer comparações que fogem da racionalidade porque direitos não seriam comparáveis entre si ou, ainda que existam elementos comparáveis entre os direitos em conflito, a proporcionalidade acaba por recorrer a elementos incomensuráveis. Mais que isso, argumenta que a proporcionalidade por vezes permitirá a limitação de direitos em função de interesses ilegítimos. Em seguida, discorda de autores como Mattias Kumm, que sugerem a inclusão às

etapas do teste de proporcionalidade o raciocínio não condicionado, na medida em que isso significaria remover a objetividade que é central à utilização deste método de adjudicação de direitos, o que traria graves problemas (como a ausência de coerência jurisprudencial). É necessário que o direito e a doutrina jurídica apresentem parâmetros para auxiliar a decisão do magistrado e outros agentes competentes para a adjudicação de direitos. Em função disso, Urbina argumenta que um método apropriado para decidir casos envolvendo a limitação de direitos humanos deveria ser capaz de responder a raciocínios morais por meio de categorias legais que guiam a atuação judicial a soluções racionais, o que a proporcionalidade não seria capaz de alcançar.

A despeito dessas críticas, como apontam Jud Mathews e Alex Sweet (2010), a estrutura relativamente sistemática e transparente do teste de proporcionalidade atribui maior objetividade analítica e evita patologias (a exemplo da experiência da Suprema Corte dos Estados Unidos, que, ao adotar meio menos sistemático de adjudicação de direitos, abriu espaço para incoerências jurisprudenciais e fragilização de direitos humanos no país). Segundo os autores, a proporcionalidade oferece procedimento, baseado em uma série de teses, que exige ao decisor justificar eventual limitação a um direito fundamental (MATHEWS; SWEET, 2019). Além disso, eventuais decisões contrárias a direitos humanos poderão ser evitadas, ainda que com imperfeições, tanto na etapa da avaliação da legitimidade quanto no momento do balanceamento de interesses.

Mais que isso, a proporcionalidade consiste no método mais adotado pela literatura e jurisprudência nacional e internacional,[377] de países de *common law* ou de *civil law*, para mediar princípios. Jud Mathews e Alex Sweet (2019) demonstram essa tendência em estudo comparado sobre a utilização a proporcionalidade, momento no qual argumentam: "[h]oje, a proporcionalidade está cada vez mais consagrada nos textos constitucionais e foi totalmente constitucionalizado em toda a Europa, em partes da América Latina e Ásia, e em sistemas de direito consuetudinário tão diversos quanto Canadá, África do Sul, Israel e o Reino Unido".

---

[377] Nesse sentido se posiciona a *European Data Protection Supervisor* (EDPS): "Qualquer proposta de limitação do direito à proteção de dados pessoais deve estar em conformidade com a legislação da em. Isto significa garantir que esta limitação seja ao mesmo tempo necessária e proporcional. Nossas Diretrizes de Proporcionalidade, combinadas com o Kit de Ferramentas de Necessidade que publicamos em 2017, visam tornar a avaliação da necessidade e proporcionalidade mais rápida e fácil para os formuladores de políticas, ajudando-os a garantir que todas as novas propostas da UE respeitem o direito fundamental à proteção de dados pessoais." (tradução nossa). Disponível em: https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2019-14-proportionality_guidelines_en.pdf. Acesso em 02.11.2022.

Por isso, de forma a dialogar com a doutrina adotada majoritariamente na prática brasileira, e também na experiência internacional, esta tese entende que a análise de proporcionalidade consiste em um meio eficaz de atribuir objetividade na identificação do interesse público na publicação ou no compartilhamento de dados pessoais mantidos pelo poder público. De forma similar - ou seja, reconhecendo o papel central da proporcionalidade como método mais adequado para a construção do significado e alcance da privacidade e proteção de dados pessoais quando em conflito com outros bens jurídicos constitucionalmente assegurados - se manifestou o Ministro Gilmar Mendes no julgamento da ADI 6389:

> Desde a concepção do direito à privacidade como manifestação do direito à autodeterminação informacional pela Corte Constitucional alemã, já se reconhece que o princípio da proporcionalidade desempenha relevante papel de aferição da constitucionalidade das interferências à proteção jurídica da autodeterminação informacional. O teste da proporcionalidade, a propósito, foi central na construção realizada pelo BVerfG a partir do julgamento da Lei do Censo de 1983.[378]

De todo modo, em razão da utilização do teste de proporcionalidade para determinar se o interesse público no caso concreto consiste na publicação ou no compartilhamento de dados pessoais, seus contornos no caso concreto poderão variar. Em certas ocasiões, o interesse público resultará na divulgação de dados e, em outras, poderá resultar na preponderância de direitos de privacidade e proteção de dados pessoais sobre a divulgação. Para identificar elementos que conduzam a decisão para um outro outro sentido (ie.: privilegiar a divulgação ou a privacidade e proteção de dados pessoais), mais adiante (após análise sobre a experiência internacional) serão observados exemplos de decisões em que o STF e o CGU solucionam conflitos entre transparência e/ou eficiência em relação à privacidade e proteção de dados pessoais.

12.3 Exemplos estrangeiros de identificação do interesse público

Neste momento se buscará identificar, em outras jurisdições que também utilizam o conceito de interesse público para determinar quando poderão ser divulgados dados pessoais mantidos pelo poder público, parâmetros para identificar no caso concreto situações em que o interesse público está presente. Para tanto, serão apresentadas de forma exemplificativa as experiências da União Europeia, Reino Unido e Canadá.

A escolha de observar a prática europeia reside essencialmente na já apresentada influência que exerce na prática de privacidade e proteção de dados pessoais brasileira,

[378] Vide voto disponível em: https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf. Acesso em 02.11.2022.

inclusive ao prever o interesse público como fundamento para atividades de tratamento de dados pessoais realizada por governos. Em relação ao Reino Unido, além de sua regulação de proteção de dados pessoais estar originalmente (anteriormente ao Brexit) atrelada à GDPR, sua Autoridade de Proteção de Dados Pessoais (*Information Commissioner's Office* ou ICO) também reúne competências atreladas ao direito de transparência e acesso à informação. Já a experiência do Canadá foi observada porque o país possui lei específica para o tratamento de dados pessoais realizado pelo poder público e que conta com disposições sobre interesse público na publicação e compartilhamento de dados.

Para tanto, buscou-se identificar a regulação do conceito de interesse público em legislação sobre proteção de dados pessoais e sobre divulgação de dados pessoais mantidos pelo poder público, e também em decisões ou orientações de autoridades locais. Assim, o foco adotado nesse momento foi identificar normas e manifestações de autoridades que abordam a divulgação pelo poder público de informações pessoais mantidas em seus arquivos e bases de dados. Essa pesquisa não se pretendeu exaustiva, e a seleção do material analisado foi realizada com apoio de artigos acadêmicos.

Na União Europeia, o termo interesse público aparece na legislação de proteção de dados pessoais, a GDPR, em dois principais cenários: **(a)** como um dos requisitos das bases legais previstas nos arts. 6(1)(e)[379] e 9(2)(i); e **(b)** para qualificar determinadas atividades, como atividades de interesse público na área de saúde pública ou o arquivamento de informações para o interesse público. No entanto, a despeito de ser uma condição para a caracterização das situações elencadas acima (e.g., o interesse público é requisito para a utilização das bases legais previstas nos arts. 6(1)(e) e 9(2)(i)), não há na GDPR conceito de interesse público, que deverá ser estabelecido por regulação nacional dos Estados membros.[380] Esse fundamento jurídico poderá prever disposições específicas, como os tipos de dados objeto de tratamento, os titulares dos dados, as entidades a que os dados pessoais poderão ser comunicados e para que efeitos, os limites da finalidade de tratamento ou os prazos de conservação.

Para tanto, a **Lei que regulava a GDPR no Reino Unido** (o *Data Protection Act* 2018 ou DPA 2018), em seu art. 8 do Capítulo 2, Parte 2 d, regulava o art. 6(1)(e) da GDPR,

[379] O artigo dispõe que "O tratamento será legal somente se e na medida em que pelo menos uma das seguintes condições se aplique: [...] (e) tratamento necessário para a performance de uma tarefa realizada no interesse público ou no exercício de uma autoridade oficial investida no poder de controlador".

[380] Por exemplo, o artigo 6(3) estabelece que o fundamento legal para essa base legal deve ser previsto em lei da União Europeia ou do Estado membro ao qual o controlador esteja sujeito.

estabelecia exemplos de situações nas quais poderá será ser utilizada a base legal de exercício de função para o alcance do interesse público, entre as quais estão os tratamentos necessários para (i) administração da justiça e funções parlamentares; (ii) funções estatutárias e propósitos governamentais e (iii) atividades que apoiam ou promovem o engajamento democrático.[381] Essas hipóteses não são taxativas, de modo que outras situações poderão ser incluídas desde que o fundamento para a função seja específica, clara e previsível.

Para o tratamento de dados sensíveis, os arts. 6 a 29, Parte 2, Seção 1 do DPA 2018 regulam o que seria interesse público substancial para fins do art. 9(2)(g) da GDPR. Para tanto, o estabelece as condições para a qualificação, no caso concreto, dessa modalidade interesse público, que são: (i) Objetivos estatutários e governamentais; (ii) Administração da justiça e fins parlamentares; (iii) Igualdade de oportunidade ou tratamento; (iv) Diversidade racial e étnica em níveis superiores; (iv) Prevenir ou detectar atos ilícitos; (vi) Proteger o público; (vii) Requisitos regulamentares; (viii) Jornalismo, academia, arte e literatura; (ix) Prevenção de fraudes; (x) Suspeita de financiamento ao terrorismo ou lavagem de dinheiro; (xi) Apoio a indivíduos com uma deficiência ou condição médica específica; (xii) Aconselhamento; (xiii) Salvaguarda de crianças e indivíduos em risco; (xiv) Salvaguarda do bem-estar econômico de certos indivíduos; (xv) Seguro; (xvi) Pensões profissionais; (xvii) Partidos políticos; (xviii) Representantes eleitos respondendo a solicitações; (xix) Divulgação aos representantes eleitos; (xx) Informar os representantes eleitos sobre os presos; (xxi) Publicação de sentenças judiciais; (xxii) *Antidoping* no esporte; e (xxiii) Padrões de comportamento no esporte.

Essas condições exigem a adoção de uma série de medidas, como a elaboração de documentação apropriada.[382] O interesse substancial poderá ser inerente em determinadas condições (e.g., administração da justiça, igualdade de oportunidade ou tratamento, prevenção de fraudes e partidos políticos), mas em outras será necessário demonstrar sua presença no caso concreto (e.g., prevenir ou detectar atos ilícitos, Proteger o público, Salvaguarda de crianças e indivíduos em risco e Seguro). Como esclarece a ICO, em vista dos riscos inerentes ao tratamento de sensíveis, a qualificação do interesse público substancial deverá ser real e material. Em outras palavras, o interesse não deve ser vago ou genérico, sendo necessário

[381] Vide: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf. Acesso em 26.06.2022.

[382] "Um documento de política apropriado é um documento curto que descreve suas medidas de conformidade e políticas de retenção para dados de categoria especial. O DPA 2018 diz que você deve ter um em vigor para quase todas as condições substanciais de interesse público (e também para a condição de emprego, previdência social e proteção social), como medida específica de responsabilidade e documentação." https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-substantial-public-interest-conditions/. Acesso em 26.06.2022.

especificar os argumentos sobre os benefícios concretos do tratamento em questão (ICO, 2020.1). Além disso, para a qualificação de algumas condições, o controlador deverá apresentar a razão que torna inviável obter consentimento do indivíduo para o tratamento de seus dados (e.g., diversidade racial e étnica em níveis superiores, e representantes eleitos respondendo a solicitações). Essa regra se justifica pelo fato de que, na ausência da base legal de interesse público substancial, o consentimento seria a base legal aplicável (especialmente por não ser possível fundamentar o tratamento de dados sensíveis no legítimo interesse).

Em relação à regulação sobre divulgação de dados pelo poder público, na União Europeia a atividade é reconhecida no art. 42 da Declaração Europeia de Direitos Fundamentais e pela Corte Europeia de Direitos Humanos, com base em uma interpretação do direito de liberdade de expressão previsto no art. 10 da Convenção Europeia de Direitos Humanos, e regulada por legislação de Acesso à Informação editada pelos Estados-membros. Assim como a privacidade, enquanto um direito humano, sua limitação, deverá ocorrer por meio do teste de balanceamento que, segundo a Corte Europeia de Direitos Humanos, contará com uma etapa adicional, consistente na avaliação sobre a legitimidade da medida (ou seja, a limitação não poderá ser ilegal ou promover prejuízos sociais).[383]-[384]

[383] Caso interessante que mostra esse teste de balanceamento sendo realizado por Tribunais Europeus é o caso C-27 que, embora avalie o conflito entre privacidade e liberdade de expressão (e não envolve a transparência ou eficiência governamental), demonstra a preocupação com a publicação de documentos com dados fiscais de cidadãos finlandeses. O caso, envolve o *Ombudsman* de proteção de dados da Finlândia (Tietosuojavaltuutettu), e as empresas Satakunnan Markkinapörssi Oy ("Markkinapörssi") e Satamedia Oy ("Satamedia"), que realizavam o processamento de dados fiscais divulgados na internet. As empresas coletaram e divulgaram informações sobre os rendimentos e o patrimônio líquido tributável de 1.2 milhão de pessoas na Finlândia, primeiro por meio de um jornal e depois através de um serviço de mensagens de texto no qual as pessoas enviavam o nome de uma pessoa e recebiam as informações fiscais dessa pessoa. Essa prática foi questionada administrativa e judicialmente pelo *Ombudsman* de proteção de dados. No julgamento pelo Tribunal de Justiça da União Europeia, em 2008, o Tribunal entendeu que as atividades das duas empresas constituíam tratamento de dados no escopo de incidência da então vigente Diretiva de Proteção de Dados e que a publicação de dados de acordo com a legislação nacional poderia ser classificada como atividade jornalística se o seu único objetivo fosse a divulgação ao público de informações, opiniões ou ideias. Já no julgamento pela Corte Europeia de Direitos Humanos (ECHR), em 2017, a Corte entendeu não haver violação do direito à liberdade de expressão quando os Tribunais e Autoridades finlandesas proibiram as duas empresas de processar dados fiscais pessoais da maneira em que o fizeram. Para a Corte, a publicação em massa de dados pessoais não contribui para o interesse público e, com isso, deveria haver distinção entre a acessibilidade garantida aos dados e a extensão ilimitada em que eles eram publicados pelas empresas, uma vez que tornavam os dados acessíveis de uma forma e em medida não pretendida pelo legislador. Além disso, a corte concluiu não estar convencida de que a publicação de dados fiscais na forma e na medida feita pelas empresas contribuísse para um debate de interesse público interesse ou que seu objetivo principal era fazê-lo, mas poderia contribuir para a satisfação da curiosidade de um leitor sobre a vida privada do titular dos dados financeiros. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62007CJ0073. e https://globalfreedomofexpression.columbia.edu/cases/case-satakunnan-markkinaporssi-oy-satamedia-oy-v-finland/. Acesso em: 06.11.2022.

[384] Em outro caso, a corte de Munique julgou sobre a possibilidade de divulgação dos resultados de auditorias regulatórias, inclusive de dados pessoais contidos nessas auditorias, realizadas por uma autoridade pública responsável pelo controle de qualidade dos alimentos de Munique. O tribunal determinou que a lei de

No **Reino Unido** o acesso a informações mantidas pelo poder público está regulado está na *Freedom of Information Act* 2000 (FOI). A Lei estabelece que registros mantidos pelo governo serão, por pressuposto, disponibilizados para acesso ao público, salvo quando presentes exceções estabelecidas em lei, à exemplo da proteção à privacidade de indivíduos (ICO, 2017). Nesse caso, será necessário ao gestor público realizar o teste de interesse público para definir se os registros deverão ser publicados ou mantidos em sigilo. Segundo a seção 40 do FOI, não será possível publicar dados pessoais em desconformidade com os princípios estabelecidos no DPA 2018. Por outro lado, a Seção 40(2) estabelece que registros poderão ser divulgados quando o interesse público for igual ou superior ao risco gerado à privacidade de indivíduos, e desde que: **(i)** observados os princípios de proteção de dados pessoais, e **(ii)** não haja objeção ao tratamento; ou **(iii)** os dados integrem as exceções ao direito de acesso (ICO, 2020.2). Em relação à objeção feita pelo indivíduo, a Seção 40(3) autoriza o controlador a rejeitá-la, caso em que será cabível recurso judicial para questionar essa rejeição (Seção 40(4)).

O *Information Commissioner 's Office* (ICO, 2020.1), em guia divulgado em 2016, esclarece que o conceito de interesse público engloba uma série de valores e princípios relacionados ao bem público ou que busquem os melhores interesses da sociedade.[385] Esclarece também que o interesse público pode assumir diversas formas, como a promoção da transparência e *accountability*, a garantir de informação ao público, a proteção do processo democrático, a tomada qualificada de decisão por órgãos públicos, a garantia do melhor uso de dinheiro público (ICO, 2022). Aponta, no entanto, que essas situações nem sempre levam à conclusão de que a informação deverá ser divulgada, sendo necessário ao gestor público realizar balanceamento dos interesses em jogo.[386] O ICO também esclarece que não devem ser considerados na avaliação sobre interesse público: (i) a informação de interesse para o

---

informação do consumidor alemã está de acordo com o regulamento de proteção de dados europeu diante dos interesses do consumidor, que se beneficiaria com a divulgação das auditorias, considerado mais relevante que os interesses da empresa em manter informações sobre a auditoria confidenciais. VGH Munchen. 5 CS 19.2087. Julgado em: 15.04.2020. Disponível em: https://gdprhub.eu/index.php?title=VGH_M%C3%BCnchen_%E2%80%93_5_CS_19.2087. Acesso em 14.12.2022.

[385] Por isso, interesses próprios, como interesses privados ou comerciais, não podem sozinhos qualificar o interesse público. Para que haja interesse público, interesses privados devem estar acompanhados de interesses da comunidade.

[386] Por exemplo, veja-se o **Caso Standard de curso de farmácia**, citado por Carter & Bouris (2006). O solicitante de acesso à informação buscou acesso a todos os documentos relacionados a investigações realizadas a respeito de standards de cursos de farmácia de determinada universidade. Entre os argumentos apresentados para rejeitar o acesso a determinados documentos esteve a proteção à privacidade de pessoas. Ao avaliar o recurso apresentado, *o Information Commissioner* do Reino Unido determinou que a divulgação da informação sem o nome de professores e alunos, que poderiam ser tarjados, era suficiente para alcançar a finalidade pretendida pelo solicitante de acesso a dados.

público;[387] e (ii) interesses privados, visto que o interesse público é aquele que beneficia a sociedade como um todo e não apenas uma única pessoa.[388]

Em seguida, o ICO aponta que, após a identificação do interesse público no caso concreto, será necessário avaliar se ele deverá prevalecer em relação à privacidade do indivíduo. Para tanto, devem ser considerados fatores como: (a) as chances de a divulgação gerar prejuízos aos titulares de dados (e.g.,: irá acontecer ou poderá acontecer); (b) a gravidade do prejuízo decorrente da divulgação da informação (significativo ou não significativo); (c) o tempo decorrido desde que a informação foi produzida, na medida em que o passar do tempo em geral reduz a necessidade de a exceção à publicidade ser mantida; (d) a intensidade em que a divulgação da informação irá beneficiar o interesse público; (e) se a informação já está em domínio público, caso em que sua divulgação irá contribuir pouco para o interesse público. Realizada a avaliação de todos esses fatores, as autoridades públicas devem ponderar se o interesse público deverá preponderar em relação à exceção legal ao dever de publicidade.

No **Canadá** há legislação específica a respeito do tratamento e divulgação de dados pessoais mantidos pelo poder público, o *Privacy Act* (1983).[389] A lei prevê (art. 8(2)) que entes públicos podem divulgar informações pessoais mediante o consentimento do titular de dados ou em situações como: (i) alcançar as finalidades para as quais os dados foram obtidos ou para finalidades correlatas; (ii) quando autorizado por lei ou regulamento aplicável; (iii) contribuir com procedimentos legais e investigativos ou cumprir com determinação judicial; (iv) compor acervos e bibliotecas nacionais; (v) para pesquisas ou propósitos estatísticos, desde que demonstrado que o envio de dados pessoais identificados é essencial para alcançar

---

[387] Como exemplo, o ICO cita: "No Guardian Newspapers Ltd e Heather Brooke v o Comissário de Informação e a British Broadcasting Corporation (EA/2006/0011 e 0013, 8 de janeiro de 2007) o Tribunal de Informação disse no parágrafo 34: "O Sr. Wells também exibiu em sua declaração uma longa lista de artigos de imprensa relacionados com o caso. Lord Wilberforce disse em British Steel Corp v Granada Television Ltd [1981] AC 1096 em 1168: "Há uma grande diferença entre o que é interessante para o público e o que é do interesse público dar a conhecer". (tradução nossa).

[388] Como exemplo, o ICO menciona: "o caso Grace Szucs contra o Comissário de Informação (EA/2011/0072, 16 de agosto de 2011) dizia respeito a um pedido da Sra. Szucs ao Escritório de Propriedade Intelectual (IPO) para o aconselhamento jurídico que haviam recebido sobre como lidar com um pedido anterior que o marido da Sra. Szucs havia apresentado. O Sr. Szucs estava envolvido em uma disputa com o IPO sobre como ele havia tratado uma reclamação dele. Em resposta ao pedido da Sra. Szucs, o IPO reteve a assessoria jurídica sob a seção 42(1) da FOIA. Ao realizar o teste de interesse público, o Tribunal de Primeira Instância distinguiu entre os interesses privados e o que é de interesse público. Eles disseram no parágrafo 54: "A divulgação das informações contestadas não é necessária para que o público obtenha informações sobre a OPI". O fato do conselho jurídico que a IPO recebeu em relação ao pedido de informações feito pelo Sr. Szucs em 2005 pode ser de interesse para a Sra. Szucs, seu marido, seus associados e talvez uma seção um pouco mais ampla do público, mas não segue a divulgação é de interesse público." (tradução nossa).

[389] Vide: https://laws-lois.justice.gc.ca/eng/acts/p-21/fulltext.html. Acesso em 19.06.2022.

a finalidade almejada e desde que nova divulgação não ocorra de forma a expor dados pessoais; ou (vi) para qualquer finalidade em que o interesse público na divulgação claramente supere os riscos à privacidade resultantes da divulgação, ou em que a divulgação claramente beneficia o indivíduo a quem as informações se referem (art. 8(2)(m)).

Além disso, para a divulgação de dados pessoais realizada com base no interesse público preponderante ou no benefício ao titular de dados, o ente público que realizar a divulgação deverá notificar o Autoridade de Proteção de Dados Pessoais Federal (*Office of the Privacy Commissioner*, chamado de "OPC") anteriormente à divulgação, sempre que razoavelmente possível. Por sua vez, a autoridade poderá notificar o titular de dados caso julgue apropriado.

Como se verifica, o consentimento, única base legal aplicável segundo o *Privacy Act*, será dispensado para a divulgação de dados mantidos pelo poder público quando houver interesse público que claramente supere os riscos à privacidade ("*clearly outweighs*") ou nos casos em que fique claro benefício ao titular de dados ("*clearly benefit*"). São exemplos desse tipo de situação casos em que a saúde ou a segurança de uma ou diversas pessoas podem estar em risco, como da notificação a autoridades de saúde sobre a exposição de certos indivíduos a doenças contagiantes ou da localização de indivíduos feridos ou falecidos (OPC, 2022).

Outro exemplo em que o interesse público dispensa o consentimento para a divulgação de informações pessoais está relacionada ao *Access to Information Act* (*AI Act* ou Lei de Acesso à Informação do Canadá). A referida lei proíbe a divulgação de registros que contenham dados pessoais (art. 19(1)), salvo se diante da hipótese prevista no art. 8(2)(m) do *Privacy Act*, que permite a divulgação desses dados quando houver interesse público que claramente supera os riscos à privacidade do titular de dados (art. 19(2)).

De todo modo, para a avaliar se a divulgação claramente supera os riscos à privacidade, o agente público deverá aplicar o teste de "invasão à privacidade", que exige a avaliação dos seguintes fatores de risco, em conjunto com as características específicas do caso concreto: (i) sensibilidade da informação; (ii) expectativa do indivíduo; e (iii) grau e probabilidade do dano. Em relação à sensibilidade da informação, deve se avaliar se há informações detalhadas (e.g., nome e endereço) ou altamente pessoais (e.g., dados de saúde), e a sensibilidade do contexto em que a informação foi obtida (e.g., a coleta de dados para identificar pessoas com uma doença específica). Para avaliar a expectativa do indivíduo, será necessário identificar o contexto em que os dados foram coletados, quais expectativas de

confidencialidade geradas no indivíduo no momento da coleta, e as expectativas razoáveis do indivíduo em relação ao uso desses dados (que deve considerar as circunstâncias da coleta, como o local e contexto em que ocorreu). Já a probabilidade ou grau do dano que a divulgação poderá provocar deve ser considerada em comparação com os benefícios da divulgação e também considerar os potenciais riscos de posterior divulgação inadequada (OPC, 2022).

Na prática, a regra que exige a clara prevalência do interesse público ao risco oferecido à privacidade de cidadãos acaba por priorizar a privacidade sobre a transparência.

O Canadá aplica um teste de interesse público para decidir sobre a divulgação de dados pessoais, em acordo com o *Access to Information Act*, de 1982, e o *Privacy Act*,[390] do mesmo ano. Quando o direito de acesso à informação esbarrar em dados pessoais, a seção 19 do *Access to Information Act* determina que as informações pessoais podem ser divulgadas se a divulgação estiver de acordo com o *Privacy Act*. Esta lei determina que os dados pessoais podem ser divulgados para qualquer finalidade onde, na opinião do chefe da instituição que os controla, o interesse público na divulgação superar claramente qualquer invasão de privacidade que possa resultar da divulgação. Nesse sentido, o tomador de decisões sobre a divulgação ou não de dados pessoais provavelmente teria que estar confortavelmente satisfeito com o fato de que o saldo do teste é a favor da divulgação, porém não há definição clara do que seria considerado interesse público e quando ele seria aplicado para derrogar o acesso à informação.

Um estudo conduzido pela *University College London* indica que o *Office of the Information Commissioner*, autoridade responsável pela aplicação do *Access to Information Act*, teve de considerar o teste do interesse público em onze decisões entre o período de 1994 e 2005 (CARTER; BOURIS, 2006), sendo que apenas residualmente o interesse público na divulgação pesava claramente mais do que a invasão de privacidade ou danos a terceiros. Assim, o interesse público geralmente não resultou na divulgação de dados pessoais.

Por exemplo, o *Commissioner* analisou recurso oferecido por jornalista em face de decisão proferida pela autoridade de transportes canadense *(Transport Canada)* que rejeitou pedido de acesso a registros relacionados a violações por pilotos comerciais da Lei e Regulamentos da Aeronáutica, sob a justificativa de que atender à solicitação afrontaria a

[390] Vide: Disponível em: https://laws-lois.justice.gc.ca/eng/acts/p-21/fulltext.html. Acesso em: 06.11.2022.

proteção à privacidade dos pilotos.[391] Em outro caso, a Diretoria de Serviços Jurídicos canadense solicitou ao Departamento de Cidadania e Imigração que rotineiramente disponibilizasse detalhes sobre os refugiados detidos para fins de melhor organizar uma representação legal para esses refugiados. Na análise do caso, o *Commissioner* concluiu que a invasão de privacidade não se justifica por haver outras formas de lidar com as preocupações da Diretoria. Para o Comissário, o fato de o Conselho querer uma divulgação rotineira de informações sinalizou que as partes deveriam trabalhar em conjunto para além da lei para encontrar outras soluções.

Por sua vez, entre as decisões em que o *Commissioner* considerou haver interesse público na divulgação de informações, destaca-se pedido formulado por funcionário público de acesso a documentos relacionados a uma investigação de irregularidades na contratação de serviços em órgão de Obras Públicas e Serviços Governamentais do Canadá, que foi recusado para assegurar a privacidade dos envolvidos no procedimento. No entanto, ao avaliar recurso oferecido contra a referida decisão, o *Commissioner* considerou haver interesse público na exposição de casos de apropriação indevida de fundos públicos que claramente compensam a invasão de privacidade dos investigados (CARTER; BOURIS, 2006).

Resumidamente, como mencionado por Carter e Bouris (2006), no Canadá se privilegia a divulgação de dados em relação à privacidade quando o acesso à informação for necessário para promover *accountability* política e burocrática, viabilizar a participação social em processos políticos, ou evitar prejuízos para áreas sociais, como a saúde e a segurança pública. Por outro lado, essas autoridades protegem a privacidade em relação à divulgação de informações em casos nos quais o propósito da divulgação poderia ser alcançado por outros meios, se a divulgação resultasse em prejuízo financeiro ou contratual ao poder público ou quando as informações já estavam disponíveis publicamente.

De todo modo, em 2020 o governo Canadense iniciou consulta pública destinada a modernizar o *Privacy Act*.[392]-[393] Entre os temas objeto de modernização estão a divulgação de informações mantidas por órgãos públicos em caso de claro interesse público preponderante ("*clearly outweighs*"), na medida em que a interpretação corrente sobre legislação vigente

[391] Em outro caso, o *Commissioner* discutiu o equilíbrio entre manter material estatístico disponível para pesquisa e assegurar o sigilo dos registros do censo, a fim de incentivar a participação dos cidadãos nos censos. Segundo o entendimento da autoridade, o sigilo seria necessário, mas diminuiu progressivamente ao longo do tempo (dependendo da jurisdição, desaparecendo por completo em 92 anos).

[392] Vide: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html. Acesso em 19.06.2022.

[393] Vide: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/index.html. Acesso em 19.06.2022.

impede o desenvolvimento de práticas destinadas a mudar o paradigma de governo desconectado, que opera com silos de informações.

Segundo a proposta do governo, o poder público poderá divulgar dados sem a necessidade de consentimento sempre que a divulgação for razoavelmente necessária ("*reasonably required*") para o alcance do interesse público (em oposição ao critério anterior de o interesse público claramente superar o risco à privacidade do cidadão). Para determinar se a divulgação seria razoavelmente necessária, seria necessário considerar os seguintes fatores: (i) a finalidade específica da divulgação dos dados; (ii) os mecanismos ou meios utilizados para divulgar a informação; (iii) se há forma menos intrusiva de alcançar a mesma finalidade com similares benefícios ao interesse público e a um custo similar; (iv) a intensidade da intrusão que a divulgação comparada com o benefício público almejado.

Nessa oportunidade, a OPC se manifestou sobre a proposta de atualizar a regulação (OPC, 2021). Embora considere que os parâmetros legais vigentes resultem em balanço adequado entre interesses (caso em que a presunção tem sido em favor da não divulgação de dados pessoais), a nova proposta seria benéfica desde que da avaliação sobre qual divulgação seria "razoavelmente necessária" requeira a observância das quatro etapas estabelecidas pelo governo e da identificação de que a afronta à privacidade é proporcional ao interesse público almejado. Para tanto, o OPC sugere que a identificação da finalidade da divulgação deverá ser realizada com precisão, estar fundamentada em uma base legal e que sua relevância para o alcance do interesse público deverá estar embasada em evidências. Além disso, sugere que a avaliação sobre a existência de meios menos intrusivos à privacidade deverá eventualmente permitir a adoção de soluções mais caras e mais protetivas. Embora o custo necessário para adoção de soluções de meios menos intrusivos seja relevante, ele não deverá ser o principal fator para justificar a adoção de meios mais intrusivos.

A despeito da relevância dos debates em torno da modernização das regras a respeito da divulgação de registros que contenham dados pessoais, o governo ainda não apresentou Projeto de Lei para debate pelo Poder Legislativo. Nesse sentido, segue vigente no Canadá a regra de que o interesse público deverá claramente prevalecer ao risco à privacidade.

Assim, tal como demonstrado em pesquisa realizada por Carter e Bouris (2006), a análise sobre o interesse público em países de *common law*, tal como o Canadá e Reino Unido, deverá avaliar, no caso concreto, o conteúdo que se deseja divulgar, o contexto em que

a informação foi produzida e a finalidade da divulgação.[394] Interessante que, em consonância com o verificado nos julgados da Europa e Canadá ora apresentados, a pesquisa identificou situações em que o interesse público poderia justificar o afastamento das exceções legais à publicidade governamental, incluindo a privacidade de cidadãos, entre as quais estão o auxílio à compreensão pela população de: (i) tema que é objeto de debate público no país; (ii) sobre como são realizados gastos públicos; (iii) o funcionamento e decisões tomadas pelo Poder Judiciário; (iv) fatos e análises relacionadas ao desenvolvimento de políticas públicas e prestação de serviços públicos; (v) venda de bens de propriedade do governo; (vi) licitações e contratos firmados por órgãos públicos; (vii) salários de servidores públicos; e (viii) saúde pública. Além disso, a pesquisa aponta que nesses países não se pode utilizar como motivo para deixar de publicar informações a possibilidade de a informação ser mal interpretada, demasiadamente técnica ou resultar na redução de confiança da população no governo.

[394] A pesquisa aponta que, no caso de pedidos de acesso à informação, embora o solicitante não tenha a obrigação de apresentar uma justificativa para o acesso aos dados, essa informação poderá auxiliar o gestor público a avaliar se há interesse público que justifique a divulgação de dados a priori sigilosos.

13 SITUAÇÕES CONCRETAS DE IDENTIFICAÇÃO DE INTERESSE PÚBLICO NA RELAÇÃO DO COMPARTILHAMENTO E DA PUBLICAÇÃO DE DADOS COM A PRIVACIDADE

Nesse momento será realizada análise exemplificativa de como é solucionado, em casos concretos, o conflito entre os preceitos da transparência e eficiência governamental com os da privacidade e proteção de dados pessoais. Para tanto, serão abordadas decisões do Supremo Tribunal Federal e da Controladoria-Geral da União que enfrentam esses conflitos, de forma a identificar parâmetros que permitam identificar quando haverá interesse público no compartilhamento, na publicação ou na restrição de acesso aos dados.

A escolha por realizar análise de decisões do STF e da CGU se deve por sua competência institucional, seja para o enfrentamento de conflitos entre princípios constitucionais ou para avaliar recursos denegatórios a pedidos de acesso à informação formulados em face de órgãos ou entidades da administração pública Federal. Além disso, a seleção dos julgados foi realizada de forma não exaustiva, de tal modo que a análise realizada não pretende apresentar tendências jurisprudenciais, mas tão somente identificar critérios para a mediação, no caso concreto, desses interesses constitucionalmente protegidos.

Os julgados foram selecionados tendo como fundamentos utilização de critérios como: (a) garantia de representatividade de situações de conflito abordadas nesta tese - naturalmente, como a CGU possui competência para apreciar pedidos de acesso à informação, foram encontrados mais casos de conflito entre privacidade e transparência governamental; (b) condições em que as informações divulgadas foram obtidas - por exemplo, dados sobre o exercício de função pública, gastos públicos ou coletados por força de obrigação legal; e (c) repercussão e relevância do julgamento, como as paradigmáticas decisões sobre a constitucionalidade da divulgação de salários de servidores públicos ou que reconheceram a proteção constitucional à proteção de dados pessoais.

13.1 Decisões sobre proteção à privacidade na publicação de dados

Nesse momento serão abordadas decisões do STF e da CGU que abordam o conflito entre os princípios de eficiência e transparência governamental privacidade e os direitos de proteção de dados pessoais em casos de publicação de dados pessoais pelo poder público.

13.1.1. Dados sobre servidores públicos

Salário e benefícios auferidos por servidores públicos

O Supremo Tribunal Federal foi convocado a se manifestar em casos nos quais sindicatos e demais organizações representantes de servidores públicos de diversas jurisdições (do Distrito Federal e de Estados como São Paulo, Rio de Janeiro e Minas Gerais)[395] questionaram a constitucionalidade de leis que determinaram a publicação, no *website* do órgão público competente, de salários e informações relacionadas aos servidores.

Segundo os requerentes, a divulgação de dados individualizados (como nome completo, remuneração, cargos e funções por eles titularizados, órgãos de formal lotação, endereço completo, CPF e jornada de trabalho) resultaria em afronta à privacidade, a dignidade da pessoa humana e fragilizaria a segurança física dos servidores e de sua família.

No julgamento dessas causas, o STF entendeu que a divulgação de dados sobre remuneração de servidores públicos seria, primeiramente, essencial para concretizar a República enquanto forma de governo, na medida em que fornece aos cidadãos informações sobre como são geridos os gastos públicos e lhes municia para exercer com maior eficácia o controle social sobre a administração pública. Além disso, os Ministros argumentaram que, diferentemente do que ocorre com outros cidadãos, que não exercem função pública, a divulgação de salário de servidores públicos é instrumento para a concretização dos princípios da moralidade e da publicidade, e do direito à informação, previstos nos art. 37 e art. 5°, XIV da Constituição.

Inclusive, o Ministro Gilmar Mendes argumentou em alguns casos sobre a importância na granularidade das informações divulgadas. Isso porque, para o controle social efetivo, é importante que se tenham elementos que permitam ao cidadão compreender a composição e/ou evolução salarial do servidor. Por exemplo, dados sobre cargos que ocupa ou quantidade de filhos que possui podem explicar certos acréscimos ao montante pago a determinado servidor.

---

[395] STF, SS 3902 AgR-segundo 3902 - Segundo Agravo Regimental na Suspensão de Segurança. Relator Ministro Ayres Britto. Julgado em 09/06/2011; STF, RG ARE 652.777 - Repercussão Geral com Agravo em Recurso Extraordinário. Relator Ministro Ayres Britto. Julgado em 29/09/2011; STF, SS 3902 SL 623 - Suspensão de liminar. Relator Ministro Ayres Britto. Julgado em 10/07/2012; STF, AO 1823/ MG. Relator Ministro Luiz Fux. Julgado em 14/10/2013. STF, RE 766390 AgR/DF. Relator Ministro Ricardo Lewandowski. Julgado em 24/06/2014; STF, ARE 652.777. Relator Ministro Teori Zavascki. Julgado em 23/04/2015; STF AO 2367/DF Relator Ministro Roberto Barroso. Julgado em 13/03/2017.

Por isso, as informações divulgadas seriam de interesse público e aceitar o pedido feito pelos requerentes resultaria em grave lesão à ordem pública. Todavia, os Ministros argumentaram ser possível construir saídas para reduzir os possíveis riscos à privacidade de servidores sem, todavia, prejudicar a concretização da transparência governamental. Por exemplo, seria possível remover certos dados como o endereço residencial ou o número completo do CPF do servidor público, ou substituir o nome do servidor pela sua matrícula funcional.

Nesse sentido, para os Ministros, haveria apenas aparente conflito de princípios, já que a publicidade administrativa determina o dever estatal de divulgação dos atos públicos para garantir transparência na gestão da coisa pública. Ao mesmo tempo, a divulgação de salários não violaria a esfera de intimidade e privacidade, já que versa sobre a atuação dos agentes públicos enquanto agentes públicos e não pessoas individualmente consideradas, sendo um encargo àqueles que optaram pela carreira pública em um Estado republicano.

Diante de diversos precedentes, o tribunal formulou a seguinte tese de repercussão geral: "é legítima a publicação, inclusive em sítio eletrônico mantido pela administração pública, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias".[396]

Lista de membros de bancas examinadoras em concursos públicos

A Controladoria Geral da União foi recorrentemente solicitada a apreciar recursos em face de decisões denegatórias a pedidos de acesso a lista de elaboradores de questões de provas e integrantes das bancas examinadoras de concursos públicos, como o exemplo do processo nº 23480.027986/2013-38 (CGU, 2014). Nesse caso, a justificativa apresentada pelo solicitante para acessar a informação reside em assegurar a lisura de processos seletivos para a ocupação de cargos públicos e na inexistência de situação que justifique o sigilo capaz de restringir o princípio da publicidade. Por sua vez, o órgão demandado justificou a rejeição do pedido em termos e cláusulas de sigilo assinadas entre a banca examinadora e o órgão que realiza concurso público, além da necessidade de preservar a privacidade dos membros da banca em vista de riscos de retaliações e ameaças por sua participação no certame.

[396] A posição do STF não é unânime entre a doutrina. Há quem defenda que "tem--se a sensação de que as garantias individuais são relativizadas, afastando--se deles a condição primeira de cidadãos para revesti-los exclusivamente da posição de funcioná- rios cumpridores de deveres legais, desprovidos de direitos" (Limberger & Ritter, 2017). Essa posição está relacionada à falta de delimitação dos casos em que informações devem ser publicizadas por serem consideradas informações relevantes publicamente, o que permite a violação dos direitos de privacidade e intimidade dos servidores públicos.

A CGU rejeitou o recurso sob o argumento de que a não divulgação de informações sobre a banca examinadora consistiria em exceção legal à transparência governamental, uma vez que "a divulgação sujeitaria esses membros a pressões exacerbadas, interferindo na vida privada daqueles que produzem questões de concursos públicos e contrariando o disposto no art. 31 da Lei de Acesso à Informação". Além disso, informações prestadas aos avaliadores no momento de sua contratação reforçariam a sua expectativa de privacidade, na medida da relevância da imparcialidade dos criadores de questões e de examinadores, e do afastamento dessa informação do conhecimento público. Isso porque a confidencialidade em relação aos membros da banca é uma das ferramentas utilizadas para garantir a imparcialidade dos avaliadores e evitar que sejam submetidos a constrangimentos.

Assim, embora tenha reconhecido que a divulgação dos nomes de membros da banca pode ser medida destinada ao aprimoramento da imparcialidade e qualidade técnica da banca, essa não seria a forma mais eficaz de fazê-lo. Com isso, não estaria configurada também a possibilidade de restringir o direito fundamental à privacidade. Além disso, a CGU entendeu ser necessário observar a legítima expectativa de privacidade por parte dos membros da banca, tendo em vista aos Contratos e Termo de Compromisso que assinaram quando da sua contratação pelo órgão público promotor do concurso público.

Informações sobre promoção funcional

No processo nº 60502.001286/2014-25 (CGU, 2015.1), o cidadão formulou pedido de acesso à informação ao Comando da Aeronáutica (COMAER) do Ministério da Defesa para obter documentação relativa aos processos de progressão/promoção funcional de três professores do Instituto Tecnológico de Aeronáutica (ITA), além do seu próprio. O pedido incluía os seguintes documentos, que poderiam conter dados pessoais: (i) relatórios de avaliação de desempenho elaborados pela Chefia Imediata, ouvido o Conselho Departamental ou Comissão especialmente designada para avaliação de desempenho; (ii) parecer do Conselho da Divisão Acadêmica do professor; (iii) avaliação do desempenho acadêmico do docente, realizada pelo relator do processo; e (iv) parecer final das comissões envolvidas, incluindo justificativas das pontuações atribuídas ao candidato nos casos de processos de progressão ou de promoção não aprovados.

O ente recorrido rejeitou o pedido formulado sob o argumento de que o nível de detalhes solicitado resultaria em violação à privacidade de outros servidores públicos, sujeitos à disponibilização de informação. No entanto, o recorrido entende que a avaliação da chefia

imediata, o parecer do Conselho da Divisão e a avaliação realizada pelo relator do processo, em regra, não contêm informações que exponham a intimidade, vida privada, honra e imagem do docente avaliado. Por outro lado, a CGU julgou procedente o recurso e determinou a divulgação das avaliações de desempenho individuais dos professores, das avaliações quantitativas e dos pareceres Divisionais/Departamentais aplicáveis.

Nessa oportunidade, a CGU reconheceu que a privacidade poderá sofrer limitações quando em conflito com outros direitos, como recorrentemente ocorre com a publicação de salários de servidores públicos, que também se aplicaria a informações sobre avaliação de desempenho, na medida em "tratam da conduta interna de servidor no âmbito de suas atividades funcionais". Para corroborar esse entendimento, a CGU citou decisão da Corte Interamericana de Direitos Humanos que reconhece a limitação do alcance da privacidade de ocupantes de cargos públicos, na medida em que "influenciam questões de interesse público, se expuseram voluntariamente a um escrutínio público mais exigente e, consequentemente, nesse âmbito, estão submetidos a um maior risco de críticas, já que suas atividades saem do domínio da esfera privada para inserir-se na esfera do debate público".[397]

Conteúdo de e-mails de servidores públicos

No processo administrativo nº 99936.000114/2017-12 (CGU, 2018), foi apresentado recurso à CGU contra decisão da Empresa Brasil de Comunicação S.A. (EBC) negando acesso às correspondências digitais remetidas e recebidas no ano de 2017 no e-mail institucional do Presidente da entidade e do seu Chefe de Gabinete. Entre os argumentos apresentados pelo solicitante de acesso à informação esteve que a presença de informações pessoais não seria fundamento suficiente para a negativa de acesso aos e-mails funcionais, na medida em que não são o escopo do pedido e poderiam ser tarjadas pelo órgão solicitante, além da caixa de entrada solicitada ser ferramenta utilizada por servidor público no exercício de seu cargo.

Por outro lado, a EBC solicitou a rejeição do pedido com fundamento no seguintes argumentos: (i) o conteúdo de e-mails não se enquadra nas hipóteses de exceção compreendidas nos incisos do art. 7º da LAI; (ii) é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas; (iii) as informações

[397] O caso é evidenciado em ROJAS, Claudio Nash. Las relaciones entre el derecho de la vida privada y el derecho a la libertad de información en la jurisprudência de la Corte Interamericana de Derechos Humanos. Estudios Constitucionales, ano 6, nº 1, 2008, pp. 155-169. Disponível em: http://www.cdh.uchile.cl/media/publicaciones/pdf/28.pdf. Acesso em 04.01.2023.

solicitadas são pessoais, tanto em relação aos remetentes das mensagens enviadas à caixa institucional, quanto ao destinatário delas; e (iv) o pedido do requerente é desproporcional e desarrazoado, dado o lapso de tempo exigido de um ano.

Quando do julgamento do caso, a CGU determinou que o sigilo das comunicações não alcança mensagens enviadas pelo poder público, "já que a garantia fundamental protege o cidadão do Estado, e não o contrário"[398] e que "mensagens trocadas por agentes públicos em caixas de e-mail institucionais não podem ser automaticamente consideradas informações pessoais".[399] Ao mesmo tempo, a CGU entende ser possível que informações pessoais sensíveis estejam presentes nessas comunicações solicitadas, o que torna necessário a análise de todas as mensagens trocadas pelo remetente requerido, a fim de se verificar a existência de informações pessoais ou sujeitas a outras hipóteses legais de sigilo.

No entanto, em vista da abrangência do pedido, que exigiria analisar todas as mensagens enviadas e recebidas pelo Presidente da EBC e por seu Chefe de Gabinete durante período de um ano, para verificar a existência de informações pessoais ou protegidas por outras hipóteses de sigilo, um volume relevante, a CGU considerou que o atendimento ao pedido de acesso à informação criaria um trabalho desproporcional para a EBC. Por esse motivo, o recurso foi desprovido e o acesso à informação não foi garantido.

13.1.2 Despesas relacionadas ao desempenho de função pública

Outra hipótese de ponderação entre interesse público e privacidade enfrentada pelo Supremo Tribunal Federal consiste na divulgação de relatório de despesas realizadas por ocupantes de cargos políticos. Dentre os casos encontrados, três são Mandados de Segurança impetrados pela empresa jornalística Folha da Manhã em face de atos da Câmara dos Deputados e do Senado Federal, julgados pelo STF entre 2003 e 2015, e outro é o Recurso Extraordinário 586.424/RJ ajuizado pela Assembleia Legislativa do Estado do Rio de Janeiro contra decisão que determinou a divulgação de informações de viagens realizadas por deputados estaduais com dinheiro público.

O Mandado de Segurança nº 24.725-DF foi impetrado em novembro de 2003 contra ato do presidente da Câmara do Deputados para obter acesso aos documentos comprobatórios das despesas custeadas pela Verba Indenizatória do Exercício Parlamentar. Em julgamento

[398] Esse entendimento foi fixado no processo 00077.000615/2016-18.
[399] Esse entendimento foi fixado no processo 71200.000472/2013-87.

liminar, o relator Ministro Celso de Mello entendeu pela existência de um direito de acesso a documentos públicos relativos aos gastos com a verba em questão, na medida em que existe um interesse coletivo no teor dos documentos para fins de controle de fiscalização dos atos dos agentes públicos. Segundo o relator, os princípios da publicidade, moralidade e responsabilidade determinam que a utilização e comprovação dos gastos de recursos públicos não devem estar sob regime jurídico do sigilo e que a limitação no acesso dessas informações só poderá ser feito dentro das limitações fixadas no art. 5º, XIV e XXXIII, da Constituição.[400]

Os Mandados de Segurança nº 28.177-DF nº 28.178-DF foram impetrados contra atos da Câmara dos Deputados e do Senado Federal que indeferiram pedido de acesso aos comprovantes apresentados pelos parlamentares para recebimento de verba indenizatória entre setembro e dezembro de 2008. Na justificativa apresentada pelas Casas Legislativas para a recusa em fornecer a informação solicitada estavam a garantia de segurança, o resguardo ao sigilo de fontes e a proteção à vida privada e à intimidade dos parlamentares.

Ao deferir a liminar no Mandado de Segurança nº 28.177-4-DF,[401] determinando o acesso aos documentos solicitados pela empresa jornalística, o Ministro Relator Marco Aurélio ressaltou o direito público subjetivo à informação por parte dos veículos de comunicação, especialmente quando trazem ao escrutínio social a adequação de despesas públicas aos princípios da impessoalidade, legalidade, moralidade, publicidade e eficiência. Além disso, ressalta não ser possível limitar a publicidade governamental e o direito à informação com base no argumento de existência de dificuldades burocráticas. Sobre isso, ressalta o Ministro que os princípios da publicidade e eficiência governamental previstos no art. 37 da constituição são unidos pelo conectivo "e", de forma a demonstrar que a eficiência pressupõe a publicidade, quando possível. Por isso, os documentos comprobatórios de despesas públicas deveriam estar espontaneamente estampados na internet.

Também no Mandado de Segurança nº 28.178-DF o STF concedeu a ordem para determinar que o Senado Federal divulgasse à impetrante os documentos solicitados.[402] No caso, o site da Casa legislativa divulgava informações sobre as verbas indenizatórias auferidas

---

[400] Vide: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2184937. Acesso em 24.09.2022.

[401] O caso não foi apreciado pelo plenário em face da desistência do pedido pela impetrante por conta da entrega dos dados solicitados por parte da impetrada. Disponível em: https://www.conjur.com.br/dl/ms-28177.pdf. Acesso em 03.07.2022.

[402] O caso não foi apreciado pelo plenário em face da desistência do pedido pela impetrante por conta da entrega dos dados solicitados por parte da impetrada. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=8399320. Acesso em 03.07.2022.

por cada Senador desde 2008, mas não divulgava os documentos que instruíam os pedidos de ressarcimento e não especificava o nome, CPF ou CNPJ dos fornecedores.

Em seu voto, o Ministro Relator Luís Roberto Barroso esclarece que a prestação de contas públicas possui como pressuposto a publicidade, por força do direito de acesso à informação (art. 5º, XXXIII), ao princípio da publicidade (art. 37, *caput* e §3º, II) e ao princípio republicano (art. 1º). Especifica também que a ressalva à publicidade poderá ocorrer em casos limitados - quando o sigilo for imprescindível à segurança da sociedade e do Estado (art. 5º, XXXIII) ou para proteger a privacidade (art. 5º, X e art. 37, §3º, II) - e desde que comprovada a necessidade do afastamento dessa regra geral de publicidade.

Em relação à exceção atrelada ao direito de privacidade, o Ministro Luís Roberto Barroso argumentou que ela não poderá ser utilizada de forma abstrata. Conforme argumenta, se o parlamentar pode repassar à sociedade custos relacionados ao exercício de suas atividades, especialmente quando se trata de aquisição de material de expediente para escritório, transporte, alimentação e hospedagem, há um direito público à fiscalização desses gastos. Nesses casos não há divulgação de dados sobre a vida privada do agente público. No mesmo sentido, a Ministra Cármen Lúcia demonstrou estranhamento no uso do direito à privacidade para justificar o sigilo aos documentos, na medida em que informações sobre gastos públicos não dizem respeito à vida privada do ocupante de cargo público, mas sim de como são utilizadas as verbas que cidadãos entregaram aos servidores públicos. Por isso, sequer haveria a essas informações a proteção constitucional da privacidade.

Por sua vez, em julgamento do Recurso Extraordinário 586.424/RJ, interposto pela Assembleia Legislativa do Estado do Rio de Janeiro em face de decisão que determinou a divulgação de informações de viagens realizadas por deputados estaduais com dinheiro público. O relator, Ministro Gilmar Mendes, manteve o entendimento das instâncias de superposição e determinou a ampla divulgação das informações solicitadas, na medida em que não seriam protegidas por qualquer norma de sigilo e não violariam o direito à privacidade dos deputados. Para o Ministro, no voto do Recurso Extraordinário 586.424, "torna-se incabível limitar o acesso a dados públicos com base em uma apreciação discricionária da administração pública acerca da adequação e conveniência do exame de informações públicas",[403] de forma que a divulgação de informações está de acordo com a liberdade de imprensa e democracia, além do acesso às informações públicas de natureza financeira para

[403] Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=293883709&ext=.pdf. Acesso em 16.09.2022.

controle social (arts. 5º, XXXIII e 37, Constituição Federal). Com isso, o STF reafirmou seu posicionamento sobre a existência de interesse público e sobre o dever de publicidade de informações sobre a gestão da coisa pública, ainda que possam revelar aspectos da intimidade de agentes públicos.

13.1.3 Dados de particulares em relação a verbas e funções públicas

Registro de acesso a prédios públicos

A Controladoria-Geral da União foi recorrentemente solicitada a apreciar recursos em face de decisões denegatórias a pedidos de acesso a registros de pessoas que visitam determinados órgãos públicos, como o Palácio do Planalto, em um período de tempo específico. Os pedidos geralmente solicitam o detalhamento do nome do visitante, a data e hora de entrada e saída, nome do funcionário que autorizou a entrada e o órgão visitado.[404]

Tais pedidos de acesso têm sido negados pelo órgão solicitado, especialmente o Gabinete de Segurança Institucional da Presidência da República (GSI), com fundamento na proteção de dados pessoais assegurada pela LGPD e na competência da GSI em zelar pela segurança pessoal do presidente da República, delimitada na Lei nº 13.844/19. Quanto à proteção de dados, a preocupação demonstrada pelos órgãos solicitados é que o tratamento dos dados pessoais coletados (nome e data de entrada de visitantes) cumpriria apenas a finalidade específica de segurança do presidente. Assim, o GSI não concedeu acesso aos dados solicitados com fundamento no princípio da finalidade, previsto na LGPD, na medida em que o tratamento dos dados pessoais pretendido pelo solicitante estaria em desconformidade com a finalidade informada ao titular de dados quando o dado foi originalmente coletado, qual seja, a segurança do Presidente da República.[405] Diante disso, o órgão não estaria juridicamente permitido a compartilhar essas informações para propósitos

---

[404] Dentre eles, citamos os processos administrativos apreciados pela CGU nº 00137.003633/2021-67 (julgado em: 07/05/2021, disponível em: https://static.poder360.com.br/2022/04/parecer-CGU.pdf). 00137.006543/2021-28 (julgado em: 30/06/2021, disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/00137006543202128_CGU.pdf) 00137.022808/2020-54 (julgado: 23/03/2021, disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/00137022808202054_CGU.pdf), 00137.008313/2021-01 (julgado em: 07/07/2021, disponivel em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/00137008313202101_CGU.pdf). Acesso em 16.09.2022.

[405] A título exemplificativo, no processo 00137.022808/2020-54, o GSI destacou que "o tratamento dos dados pessoais coletados (nome e data de entrada) de visitantes cumpre finalidade específica de segurança da mais alta autoridade do Poder Executivo do país". Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/00137022808202054_CGU.pdf. Acesso em 16.09.2022.

distintos que não estariam alinhados às legítimas expectativas do titular de dados. Em recurso, os requerentes argumentaram que o atendimento ao pedido de acesso à informação em questão não exigiria o tratamento de dados pessoais, na medida em que as informações solicitadas envolvem somente registros de acesso a prédios públicos para reuniões com autoridades públicas.[406]

Ao apreciar o recurso contra a negativa de acesso às informações, a CGU entendeu não serem procedentes os argumentos apresentados pelo GSI e determinou a disponibilização dos registros de acesso a prédio público com informações de horário de entrada e saída, além do destino que recebeu o visitante. No entendimento da Controladoria, há interesse público nas informações de registro de acesso a prédios públicos, visto que elas permitem a identificação de possíveis irregularidades e conflitos de interesse no exercício da função pública, que poderiam comprometer os interesses coletivos de maneira imprópria. Essa divulgação, inclusive, encontra respaldo na LAI e na Lei nº 12.813/2012, que dispõe sobre conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal.

Além disso, a CGU argumentou que "[...] o tratamento de dados pelo Poder Público [...] tem como pressuposto o atendimento a uma finalidade pública, à persecução do interesse público e à execução pelo ente público de suas competências legais ou cumprimento de suas atribuições". Por isso, e conforme dispõe a LGPD, o Poder Público estaria autorizado a processar dados pessoais para a execução de políticas públicas ou para cumprimento da lei, de forma a assegurar o interesse da coletividade. Para tanto, esclarece que os dados devem ser tratados tendo em vista os princípios da LGPD e que usos secundários devem observar a finalidade, boa-fé e o interesse público (LGPD, art. 7º, §3º).

Finalmente, argumenta ser necessário assegurar uma interpretação harmônica da LGPD e LAI, a fim de se garantir os direitos fundamentais de acesso à informação e devida proteção aos dados pessoais. Para tanto, o órgão público deverá ponderar o interesse público na divulgação dos dados com o risco que a divulgação pode impor aos direitos e liberdades dos titulares de dados. Nesse momento, será importante considerar a natureza da relação estabelecida entre Estado e indivíduo, de forma a adequadamente ponderar os interesses.

Dados de beneficiários de programa social

[406] Como exemplo, no processo 00137.006543/2021-28, a CGU descreve que o recorrente "não concordou com a alegação de que as informações são dados pessoais" e, posteriormente, alegou novamente que o pedido não trata de dados pessoais. Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/00137006543202128_CGU.pdf. Acesso em: 16.09.2022.

No julgamento do Agravo Regimental no Recurso Extraordinário 631.104/SC,[407] a primeira turma do Supremo Tribunal Federal julgou que o acesso a informações relativas à relação dos beneficiários do Programa Luz para Todos seria de interesse público. O recurso foi interposto contra acórdão do Tribunal Regional Federal da 4ª Região em Mandado de Segurança que buscava a obtenção da relação de beneficiários do referido programa social no município de São José do Cedro em Santa Catarina, mas que não foram fornecidas, sob o argumento de falta de interesse do impetrante em acessar as informações solicitadas. Em seu voto, o Ministro Relator Luís Roberto Barroso determinou a divulgação das informações solicitadas, na medida em que a demonstração de interesse individual do solicitante não é requisito para acesso a documentos públicos e não pode limitar o princípio da publicidade na Administração pública. Para tanto, reiterou precedentes nos quais o STF determinou o dever de transparência a respeito de gastos de verbas públicas quando não presente uma das exceções constitucionais que justificam o sigilo da informação. A despeito de referenciar seus precedentes, o Ministro deixou de se aprofundar sobre a semelhança e diferença entre os casos, o que deveria ter sido realizado, tendo em vista que o precedente avalia a divulgação de informações sobre viagens realizadas por parlamentares, enquanto o caso em julgamento tratava da publicação de informações sobre beneficiários de programas sociais. O relator também não analisou a pertinência das categorias de dados divulgados para o alcance do interesse público.

De forma diferente se manifestou a CGU no ano de 2017, quando do julgamento do Recurso nº 46800.001705/2016-03,[408] movido contra decisão do Ministério do Trabalho e Emprego (MTE) de rejeição parcial a pedido de acesso para fornecer dados sobre a quantidade de trabalhadores que possuem direito ao abono salarial no ano de 2016, mas não ao número do PIS desses trabalhadores para quem foram concedidos direito a abono salarial no referido ano. A recusa realizada pelo MTE de acesso ao número do PIS dos trabalhadores foi justificada pelo fato de que as informações solicitadas seriam dados pessoais sensíveis, nos termos do artigo 32, §1º, I, da Lei nº 12.527/2011. Já o recorrente argumentou que as informações solicitadas: **(i)** estão relacionadas à utilização de recursos públicos, **(ii)** foram produzidas e acumuladas por órgãos públicos, de forma que devem ser disponibilizados ao

[407] https://portal.stf.jus.br/processos/downloadPeca.asp?id=310857467&ext=.pdf e https://portal.stf.jus.br/processos/downloadPeca.asp?id=311612174&ext=.pdf. Acesso em 09.07.2022.

[408] Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/46800001705201603_CGU.pdf#search=%22privacidade%22. Acesso em 01.10.2022.

público; e **(iii)** não afrontariam a privacidade dos trabalhadores porque não permite terceiros a encontrar dados pessoais do trabalhador ou acessar sistemas de consulta ao cidadão.

Em sua decisão, a CGU argumentou que o controle social viabilizado pelo acesso à informação possui limites, a exemplo da privacidade de cidadãos. Além disso, esclareceu que

> [...] deve-se realizar a ponderação entre os direitos conflitantes para se averiguar qual deve prevalecer" e que "nem todas as informações de caráter pessoal devem ser restringidas, mas somente as informações pessoais sensíveis, ou seja, aquelas que possam de algum [modo] devassar o direito do cidadão em ter a sua intimidade e a sua vida privada preservadas.

No entanto, a CGU entendeu que o número do PIS não seria dado sensível, motivo pelo qual os dados poderiam ser divulgados para fins de controle social, e que "a atividade de controle [...] não se exerce somente sobre o valor aplicado em determinado programa social, mas também sobre o sujeito ao qual se destina o erário, principalmente quando há determinação específica em lei." Por isso, a Controladoria entendeu que poderia haver a divulgação do número do PIS, em vista do interesse público em investigar e controlar os recursos públicos.

Alinhado a essa decisão, em julho de 2020, o Portal da Transparência do Governo Federal divulgou lista completa de beneficiários do Auxílio Emergencial, programa social instituído pela Lei nº 13.982/2020, concedido em virtude da pandemia por COVID-19, composto por dados de mais de 53 milhões de beneficiários. Os dados disponibilizados sobre cada beneficiário são nome completo, município de residência, valor recebido do governo e uma parcela do CPF (ex.: ***.441.691-**). É possível buscar beneficiários específicos por meio da inserção, em campos de busca próprios, com base no nome completo, número do CPF ou número de identificação social ("NIS").

Esse ato do governo federal enfrentou críticas pela divulgação de dados pessoais de grande quantidade de cidadãos em situação de risco social, que poderão sofrer ainda maior estigmatização em vista da divulgação de seu nome, cidade de residência e valores auferidos. No entanto, o julgamento do Tribunal de Contas da União na Representação nº 018.851/2020-7,[409] sobre possíveis irregularidades no pagamento do auxílio emergencial, determinou o prosseguimento da divulgação dessas informações. Essa representação foi formulada pela Secretaria de Controle Externo da Gestão Tributária, da Previdência e da Assistência Social

409 Vide: https://pesquisa.apps.tcu.gov.br/#/documento/processo/*/NUMEROSOMENTENUMEROS%253A1885120207/DTAUTUACAOORDENACAO%2520desc%252C%2520NUMEROCOMZEROS%2520desc/0/%2520. Acesso em: 5.10.2022.

do TCU para averiguar os indícios de irregularidade nos pagamentos do auxílio emergencial, a pessoas que estariam erroneamente incluídas como beneficiárias do auxílio emergencial (eg., militares, parentes de empresários e servidores).

Para identificação dessas inconsistências, os CPFs dos beneficiários do programa social foram cruzados com dados das bases da folha de pagamento do Poder Público, da Relação Anual de Informações Sociais e do Sistema Integrado de Administração de Pessoal (Siape). Após essa verificação, os Ministérios da Defesa e da Cidadania editaram Nota de Esclarecimento conjunta, na qual informaram sobre a existência de irregularidades no pagamento do auxílio emergencial. Foram identificados 73.242 CPFs de beneficiários do programa social na base de dados do Ministério da Defesa, empregados desse ministério, apesar de não respeitarem os critérios legais mínimos para auferir esses valores.

Assim, o TCU determinou cautelarmente a cessação da admissão de novos casos de militares como aptos a receberem o auxílio emergencial, bem como o cancelamento dos cadastros admitidos e obtenção do ressarcimento dos valores já pagos. Além disso, reforçou a relevância da publicação de dados pertinentes a programas sociais em portais de transparência para viabilizar o controle social de irregularidades.[410]

Como se verifica, a divulgação de dados de beneficiários de programas sociais (como NIS, nome e cidade de residência) é fundamentada pela possibilidade de particulares contribuírem com fiscalização estatal sobre a devida alocação de verbas públicas. Por outro lado, os titulares de dados terão restrito o seu direito à privacidade. Além disso, esses indivíduos são geralmente mulheres que enfrentam dificuldades no exercício de direitos básicos (como o acesso ao mercado formal de trabalho), além de esses dados serem recorrentemente utilizados de forma discriminatória ou para a prática de fraudes (FRAGOSO *et al*., 2021). Nesse caso, os riscos gerados à privacidade dos titulares de dados tendem a se sobrepor ao interesse público subjacente.[411]

---

[410] Mais informações em: https://pesquisa.apps.tcu.gov.br/#/documento/processo/*/NUMEROSOMENTENUMEROS%253A18851202 07/DTAUTUACAOORDENACAO%2520desc%252C%2520NUMEROCOMZEROS%2520desc/0/%2520. Acesso em 05.10.2022.

[411] Na Argentina houve julgamento paradigmático em que se determinou a existência de interesse público na divulgação de dados pessoais de beneficiários de auxílios sociais. Em março de 2014, a Corte Suprema de Justiça da Nação, na Argentina, determinou que o Estado publicasse informações requeridas pela organização CIPPEC sobre planos sociais de assistência à comunidade administrados pelo Ministério de Desenvolvimento Social (MDS), órgão que negou acesso a essas informações. Segundo a Corte, haveria interesse público na divulgação dos dados pessoais de beneficiários de auxílios sociais, mesmo que isso minimize o direito à intimidade e honra dessas pessoas. Nos motivos do recurso, o requerente havia argumentado não haver razões válidas para a recusa de acesso aos dados solicitados, pois não impactam a segurança, a privacidade

Dados sobre doadores para campanhas políticas

Em março de 2018, foi julgada a ADI nº 5394, na qual se questionava a constitucionalidade da do art. 28, §12 da Lei nº 9.504/97 (Lei das Eleições), incluído ao texto legal após a aprovação da Lei nº 13.877/2019, que determina que os valores oriundos de doações serão registrados nos relatórios de prestação de contas dos candidatos e partidos como sendo uma transferência dos partidos aos candidatos.[412] A ação foi movida pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), sob o argumento que passaria a ser possível a ocorrência de doações ocultas, na medida em que não mais seria possível identificar quem são os doadores pessoas físicas, de forma a dificultar o rastreamento das doações por eleitores e a favorecer a prática de relações pouco republicanas entre os políticos e os seus doadores.

Em julgamento da medida cautelar, o STF determinou a suspensão da eficácia da expressão "sem individualização dos doadores" constante do dispositivo impugnado, posteriormente declarada inconstitucional pela maioria do Tribunal, sob o argumento de que a divulgação de informações sobre os doadores de campanhas políticas é essencial para fortalecer o controle sobre "os diversos grupos de pressão, não autorizando o fortalecimento dos atores invisíveis de poder, que tenham condições econômicas de desequilibrar o resultado das eleições e da gestão governamental." Além disso, o pleno da Corte entendeu que o acesso a essa informação não deve ser limitado às instâncias estatais de fiscalização sobre a regularidade do processo eleitoral, devendo também ser autorizado aos eleitores para que possam se informar sobre a confiabilidade da campanha eleitoral promovida por candidatos e partidos.[413] Por isso, o STF considerou haver interesse público na divulgação de dados pessoais de indivíduos que realizam doações para candidatos ou partidos políticos.

---

ou a honra dos indivíduos. Da mesma forma, defendeu que referidas informações são de interesse público e sua divulgação daria efeito ao princípio da publicidade dos atos governamentais. Por outro lado, o MDS e outros intervenientes no processo afirmaram que a individualização dos beneficiários de subsídios pode envolver aspectos íntimos da pessoa que o cedente deve proteger, além de a divulgação de dados de beneficiários de planos sociais aprofundar as condições de desigualdade, constituindo assim um fator estigmatizante. Corte Suprema de Justicia de la Nación. CSJN, Fallos, C. 830. XLVI, 2014. § 25. Sentença de 26 de março de 2014. Buenos Aires, 2014. CIPPEC c/ EN - Mº Desarrollo Social - dto. 1172/03 s/amparo, lei 16.986. Disponível em: http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-cippec-desarrollo-social-dto-1172-03-amparo-ley-16986-fa14000040-2014-03-26/123456789-040-0004-1ots-eupmocsollaf. Acesso em 11.02,2022.

412 Disponível em https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADI%205394%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em 03.11.2022.

413 Segundo a ementa do acórdão referente ao julgamento da medida cautelar "o esclarecimento público da realidade do financiamento de campanhas (a) qualifica o exercício da cidadania, permitindo uma decisão de

Em seu voto, o Ministro Relator Teori Zavascki (no julgamento cautelar) argumentou que os dados de nome e identificação do doador devem ser divulgados não somente durante o período eleitoral, mas também antes desse período, de forma a viabilizar a formação de opção de voto por cidadãos. Nas palavras do Ministro, saber o nome dos doadores de cada candidato "ilumina conexões políticas facilmente subtraídas do público nos discursos de campanha, denunciando a maior ou menor propensão dos candidatos e partidos a abandonar suas convicções ideológicas em posturas de pragmatismo político questionáveis". Nesse sentido, o Ministro considerou que a publicação dessas informações deve ser realizada em observância ao direito fundamental à informação e à publicidade governamental, que são condições necessárias à realização da democracia.

O plenário, no julgamento da ADI 2.859, por maioria dos votos e nos termos do voto do novo Relator, Ministro Alexandre de Moraes, confirmou a decisão cautelar e declarou a inconstitucionalidade da expressão "sem individualização dos doadores", constante da parte final do § 12 do art. 28 da Lei 9.504/97, acrescentada pela Lei 13.165/2015.[414] O Ministro Relator destacou a necessidade de transparência para o cumprimento dos princípios republicanos em vista das formas de organização política que são afetadas pelo dispositivo impugnado, como os grupos de pressão política e participação de atores no processo decisório, que participam das decisões políticas sem "o delineamento de um marco regulatório apto a prescrever dessa seara práticas espúrias e prejudiciais à democracia brasileira". Por isso, entendeu não haver interesse público na manutenção do sigilo da identidade de doadores a candidatos nas eleições, que passam a influir diretamente nas escolhas políticas e no resultado das eleições.

As divergências foram apresentadas pelos Ministros Marco Aurélio e Edson Fachin, que argumentaram que a expressão "sem individualização dos doadores" não se refere ao repasse feito pelo partido ao candidato, mas exclusivamente à prestação de contas do partido, e que o §12 como um todo era inconstitucional, de forma a não considerar constitucional

---

voto melhor informada; (b) capacita a sociedade civil, inclusive os partidos e candidatos que concorrem entre si, a cooperar com as instâncias estatais na verificação da legitimidade do processo eleitoral, fortalecendo o controle social sobre a atividade político-partidária; e (c) propicia o aperfeiçoamento da própria política legislativa de combate à corrupção eleitoral, ajudando a denunciar as fragilidades do modelo e a inspirar propostas de correção futuras. Sem as informações necessárias, entre elas a identificação dos particulares que contribuíram originariamente para legendas e para candidatos, com a explicitação também destes, o processo de prestação de contas perde em efetividade, obstruindo o cumprimento, pela Justiça Eleitoral, da relevantíssima competência estabelecida no art. 17, III, da CF".

[414] Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15339527374&ext=.pdf. Aceso em: 06.11.2022.

também a prestação de contas dos candidatos como registro de transferência dos partidos e vice-versa.

13.1.4 Dados pessoais de particulares mantidos pelo governo

Dados coletados por serviço consular

Em 2021, a CGU julgou recurso apresentado no processo nº 09002.001842/2021-76,[415] no qual um cidadão solicitou acesso às comunicações trocadas entre o Ministério da Relações Exteriores (MRE) e a Embaixada do Brasil no Egito, referentes às tratativas para libertar brasileiro preso por assédio cometido naquele país. O pedido foi originalmente negado pelo MRE porque nos documentos solicitados haveria informações pessoais e o tarjamento de dados pessoais não bastaria para preservar a privacidade do indivíduo, visto que a imprensa amplamente divulgou o caso, e poderia impactar na confiança dos cidadãos em relação à inviolabilidade de suas informações que são mantidas pelo Estado.[416]

O MRE também apontou que o caso foi acompanhado pela Embaixada do Brasil no Cairo como uma prestação de serviço público ordinário, nos termos do art. 55 do Decreto nº 9.683/2019 (que define competências de repartições consulares), combinado com o art. 36 do Decreto nº 61.078/1967 (Convenção de Viena sobre Relações Consulares), e para o qual deve-se observar a proteção das informações pessoais ao usuário deste serviço nos termos do art. 6º, IV da Lei nº 13.460/2017 (Lei de Defesa do Usuário dos Serviços Públicos), que define a proteção das informações pessoais ao usuário deste serviço. Ademais, argumentou que não se evidenciou no caso concreto que o brasileiro detido no Cairo tivesse tido relação anterior com o Poder Executivo Federal, de modo que fosse considerado uma figura pública, sujeita ao escrutínio pelo interesse público.

Por sua vez, o recorrente argumentou que a solicitação de informação busca apurar irregularidades, nos termos do art. 58, I do Decreto nº 7.724/2012, que determina não ser

---

[415] Vide: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/09002001842202176_CGU.pdf#search=%22privacidade%22 Acesso em 02.10.2022.

[416] Nas palavras da GCU: "[o] recorrido advoga que o mero tarjamento das informações constantes nos documentos solicitados, assim consideradas as da pessoa identificada, como nome, endereço residencial, ou números de documentos pessoais, em atendimento ao disposto no art. 7º, §2º da LAI, seria insuficiente para anonimizar as informações pessoais constantes nos documentos solicitados, pois as demais informações que relatariam a evolução do caso, se tornariam da pessoa identificável, pos, como o caso foi "amplamente divulgado pela imprensa", estas seriam suficientes para identificar as pessoas envolvidas, o que poderiam lhes afetar a intimidade, a vida privada, a honra e a imagem, contrário ao disposto no caput do art. 31 da LAI."

possível ao órgão público negar acesso à informação, inclusive quando referente a dados pessoais, que possa prejudicar processo de apuração de irregularidades, conduzido pelo Poder Público, em que o titular das informações for parte ou interessado, como no caso do indivíduo preso. Dessa forma, o MRE não poderia se valer da restrição de acesso a dados pessoais, já que seriam utilizados para investigação de irregularidades.

No entanto, a CGU rejeitou o recurso apresentado pelo cidadão, de forma a não atender ao pedido de acesso à informação, na medida em que não estaria demonstrado o interesse público que justificaria a divulgação dos dados sem a necessidade de consentimento do titular de dados.[417] A Controladoria também acatou os argumentos apresentados pelo MRE de que o atendimento afrontaria a legítima expectativa de privacidade do indivíduo e prejudicaria a confiança social no Estado em proteger dados pessoais que custodiam. Segundo a CGU: "a expectativa de privacidade da sociedade quanto à prestação de um serviço público está normatizada no art. 6º, IV da Lei nº 13.460/2017, que impõe a proteção das informações pessoais do usuário dos serviços públicos nos termos do art. 31, § 1º da LAI. "

Dados mantidos em arquivos públicos

Em 2015, a CGU julgou recurso apresentado no processo nº 01590.000162/2015-01,[418] contra uma decisão negativa da Fundação Casa de Rui Barbosa (FCRB) a pedido formulado por pesquisador para ter acesso aos arquivos de Manuel Bandeira e Vinicius de Morais, inclusive folhas de diário de Francisco de Assis, que estavam reservadas até 2015 ao Arquivo Museu de Literatura Brasileira.

Entre os argumentos apresentados pela instituição demandada para recusar o acesso a esses arquivos estava que a divulgação dos documentos estaria condicionada à autorização dos respectivos herdeiros. Por outro lado, o solicitante de acesso à informação discordou da justificativa apresentada e recorreu sob o argumento que a documentação solicitada foi doada a uma instituição pública para posterior acesso por pesquisadores, estando reservada pelo período de 30 anos, que se encerrava no ano da solicitação. Decorrido esse prazo, caberia aos herdeiros decidir sobre a eventual publicação dos documentos e cobrança de direitos autorais,

[417] Nas palavras da CGU: "[a]bstraindo-se a notoriedade do caso, a qual suscita naturalmente o interesse "do" público ou a curiosidade pública, que é diferente do "interesse público" e aplicando-se o teste de "expectativa razoável de privacidade", adaptada ao ordenamento jurídico brasileiro, verifica-se que (...) não se caracterizou suficientemente o interesse público para se afastar o consentimento para se conceder o acesso às informações nos termos do art. 31, §3º, inciso IV da LAI".

[418] Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/01590000162201501_CGU.pdf#search=ALL%28%22carta%22%20%22vinicius%22%29. Acesso em 03.10.2022.

mas não sobre o acesso a esses documentos, "uma vez que a doação foi feita em caráter irrevogável e com a ciência de que o material estaria acessível à pesquisa”.

Nesse sentido, formou-se uma controvérsia sobre o acesso a tais documentos, em vista da negativa de acesso aos conteúdos referentes a Mário de Andrade e também da existência de dados pessoais no conteúdo das cartas e poemas. Em sua análise, a CGU reconhece que nas cartas há informações que revelam aspectos da intimidade de seus autores, mas que em casos envolvendo fatos históricos de maior relevância seria possível limitar o direito à privacidade em benefício do interesse público. Para tanto, argumenta ser de interesse público o acesso por pesquisadores de documentos que estejam em guarda do governo e que permitam a reconstrução de fatos históricos.

Nas palavras da Controladoria, o pesquisador solicitante de acesso à informação "deseja conhecer o teor de cartas, poemas inéditos e páginas de um diário, documentos produzidos entre as décadas de 1930 e 1950, recebidas por um arquivo público em razão de sua importância para a História e a Literatura" e "se os documentos dos escritores não servissem como fonte de pesquisa aos estudiosos da literatura e aos historiadores, seria difícil encontrar uma justificativa para a aplicação de recursos públicos na sua conservação e guarda". Assim, a Controladoria reconhece a relevância dos escritores para a história e cultura do país, e argumenta que a simples manutenção e preservação dos documentos pelo governo por si só demonstra o inerente interesse público nessas informações.

Diante disso e considerando o decurso do prazo contratual de sigilo sobre as cartas e poemas ao qual se solicita acesso, a CGU entendeu não haver justificativa legal para se privilegiar a privacidade dos escritores em relação ao interesse público de remontar fatos históricos. Além disso, relembrou que, na eventualidade de algum herdeiro dos autores se sentir lesionado pela divulgação dessas cartas e poemas, poderá acionar o poder judiciário para obter a reparação cabível. Essa avaliação deverá sempre ser posterior à divulgação, sob pena de configurar como situação de censura prévia.

13.2 Decisões sobre proteção à privacidade no compartilhamento de dados

Nesse momento serão abordadas decisões do STF e da CGU que abordam o conflito entre os princípios de eficiência e transparência governamental privacidade e os direitos de proteção de dados pessoais em casos de compartilhamento de dados pessoais pelo poder público.

13.2.1 Dados e microdados sobre sistema de ensino

A divulgação de dados do Inep é objeto de frequentes disputas mesmo antes da vigência da LGPD, mas que se intensificaram após a edição da lei. Ainda em 2018, o TCU proferiu o Acórdão 2609/2018, no Processo TC 032.908/2017-2,[419] para determinar que o Inep entregasse microdados dos estudantes vinculados ao Censo da Educação Básica e ao Enem, nos anos de 2013 a 2016, para auditoria do Programa Bolsa Família.

No entendimento apresentado pelo Tribunal de Contas, os dados seriam imprescindíveis para auditar a efetividade do programa Bolsa Família, na medida em que permitem apurar se jovens integrantes de famílias beneficiárias acessam o mercado formal de trabalho. Nesse sentido, o TCU entendeu que o Edital do ENEM de 2017 permitiria ao Tribunal acessar informações pessoais dos participantes, já que previa a disponibilização de notas e informações dos participantes no âmbito de programa governamental, o que incluiria o controle externo desses programas.[420] Porém, o Inep negou acesso à informação na extensão solicitada pelo TCU, uma vez que, para o Instituto, o compartilhamento de dados sem o consentimento do indivíduo só seria legal se não resultasse na identificação das pessoas.

Contra essa decisão, o Inep impetrou o Mandado de Segurança nº 36.150/DF perante o STF, fundamentado na proteção ao sigilo das informações estatísticas, conforme art. 5º, incisos XIV e XXXIII, da CF, além da garantia do sigilo dos dados, como previsto na LAI. O Instituto ainda argumentou que a requisição do TCU poderia abalar a confiança dos estudantes que fornecem seus dados, colocando em risco a capacidade de pesquisa e monitoramento das políticas públicas de educação do Inep, além de violar o próprio direito dos titulares de manter sigilo sobre suas informações.

Em decisão monocrática, o Ministro Barroso destacou que "as informações que se quer acessar foram prestadas para uma finalidade declarada no ato da coleta dos dados e sob a garantia de sigilo do Inep quanto às informações pessoais". Nesse sentido, segundo o Ministro, os estudantes não esperam que suas informações sejam compartilhadas com terceiros para outras finalidades, de forma que o envio de dados ao TCU violaria essa legítima expectativa e significaria uma quebra da confiança estabelecida entre estudantes e Inep.

---

[419] Vide: https://contas.tcu.gov.br/egestao/ObterDocumentoSisdoc?codPapelTramitavel=60225650. Acesso em 10.10.2022.

[420] Como fundamento legal, o TCU apontou a aplicabilidade do item 16.3 do Edital ENEM 2017, que assegura o uso da informação dos estudantes para programas governamentais, além das exceções previstas no art. 31, §1º da LAI, sobre o acesso restrito a informações pessoais aos agentes públicos legalmente autorizados ou diante de previsão legal.

Ainda, considerando que a negativa do pedido cautelar esvaziaria o objeto da demanda, o Ministro deferiu esse pedido para suspender a obrigação do Inep em compartilhar dados.[421]

Instada a se manifestar nos autos, a Procuradoria-Geral da República argumentou que a Lei de Acesso à Informação não limita o envio de dados pretendido porque: (i) ela não se aplica aos compartilhamento de dados entre órgãos públicos, mas apenas a pedidos formulados por particulares, como pesquisadores e entidades privadas; e (ii) caso ela fosse aplicável, o compartilhamento pretendido estaria autorizado pelo art. 87, III, da Lei Orgânica do Tribunal de Contas da União (Lei 8.443/1992).[422] A PGR também argumentou que a LGPD autoriza compartilhamento de dados pessoais pelo Poder Público para atender às finalidades atribuídas em lei, e que eventuais abusos devem ser fiscalizados na medida em que ocorrerem.[423]

Ao final, o Ministro Luís Roberto Barroso entendeu por julgar a ação procedente para suspender a obrigação imposta pelo TCU ao Inep de fornecimento de dados individualizados do censo escolar e Enem, reiterando os argumentos anteriormente formulados, ainda que tenha deixado de aplicar a LGPD porque a lei estaria em *vacatio legis* à época que praticado o ato coator.[424] Quanto ao dever de sigilo, o Ministro entendeu que "os dados individualizados requisitados pelo TCU cuidam de informação sobre a qual há dever de sigilo, uma vez que se demanda o acesso à informação relacionada à pessoa natural identificada ou identificável". Ainda, a finalidade da coleta de dados seria diferente da finalidade perseguida pelo TCU, o que subverteria a autorização dada pelo titular ao Inep e violaria o dever de sigilo. Contra essa decisão foi interposto Agravo Regimental pelo Advogado-Geral da União, que foi desprovido para confirmar a liminar e anular a determinação de entrega de dados ao Inep.

De forma similar se posicionou a CGU ao analisar o recurso nº 23480.013438/2016-73[425], que tratava de pedido contra decisão do Inep de negar ao solicitante acesso a lista com os CPFs de todas as pessoas inscritas no Enem desde 2011, assim como a indicação dos CPFs

---

421 https://jurisprudencia.stf.jus.br/pages/search/despacho937080/false. Acesso em 30.07.2022.

422 Art. 87. Ao servidor a que se refere o artigo anterior, quando credenciado pelo Presidente do Tribunal ou, por delegação deste, pelos dirigentes das unidades técnicas da secretaria do Tribunal, para desempenhar funções de auditoria, de inspeções e diligências expressamente determinadas pelo Tribunal ou por sua Presidência, são asseguradas as seguintes prerrogativas: (...) III – competência para requerer, nos termos do Regimento Interno, aos responsáveis pelos órgãos e entidades objeto de inspeções, auditorias e diligências, as informações e documentos necessários para instrução de processos e relatórios de cujo exame esteja expressamente encarregado por sua chefia imediata.

423 Vide: http://www.mpf.mp.br/pgr/documentos/MS_36150.pdf. Acesso em 28.05.2022.

424 https://portal.stf.jus.br/processos/downloadPeca.asp?id=15349322719&ext=.pdf. Acesso em 30 jul. 2022. https://www.conjur.com.br/dl/stf-garante-sigilo-informacoes.pdf. Acesso em 28.05.2022.

425 Disponível em: .http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/23480013438201673_CGU.pdf. Acesso em 18.10.2022

que fizeram a prova e dos que se ausentaram. Em sua justificativa, o Inep argumentou que os dados solicitados são informações pessoais e que já publica microdados ao público, inclusive com condições específicas a pesquisadores e professores. Em sua decisão, a CGU rejeitou o pedido por considerar haver risco na divulgação de informações pessoais de estudantes e que o Inep possui canais específicos para atender a pedidos de pesquisadores.

Após a edição da LGPD, o órgão passou a adotar medidas para adequar suas atividades às normas de proteção de dados pessoais. Por exemplo, o Inep editou a Portaria nº 592/2020 para instituir uma força-tarefa para diagnóstico dos impactos da LGPD às suas atividades.[426] Em 2021, e motivado por estudo realizado pela Universidade Federal de Minas Gerais que diagnosticou que as práticas de anonimização de dados adotadas pelo Inep seriam insuficientes para alcançar os patamares da LGPD, o instituto editou a Nota Técnica nº 14/2021 para determinar que, enquanto não finalizado estudo sobre a adequação de suas práticas de anonimização dados, deverá haver a simplificação dos modelos de divulgação de microdados do ENEM e a remoção ou substituição de dados que permitem a identificação de pessoas.[427] Já em 2022 a Procuradoria do Inep elaborou o parecer nº 18/2022, igualmente se manifestando no sentido de, até que seja adotada técnica de divulgação de dados pessoais em consonância com o disposto na LGPD, suspender a divulgação de novos microdados e remover os dados já publicados do censo escolar e do ENEM.[428]

Diante dessa determinação, não somente os dados referentes ao censo escolar e do ENEM 2021 não foram divulgados, como foram removidas as bases de dados anteriormente divulgadas (referentes às edições de 1998 a 2019). A despeito do objetivo do Inep em proteger dados pessoais, a remoção de bases de dados e a não publicação de novos dados foi alvo de duras críticas. Isso porque os dados divulgados pelo Inep e do ENEM são utilizados para elaboração de pesquisas e indicadores educacionais.

Diante da grande repercussão, a ANPD editou a Nota Técnica nº 46/2022 na qual declara que a proteção de dados pessoais não deve obstar a transparência governamental.[429] No entanto, a autoridade reconheceu a relevância da preocupação do Inep em assegurar que suas práticas de anonimização estão adequadas às exigências da legislação de proteção de dados, mas identificou que essa é apenas uma das salvaguardas existentes e exigidas para a

[426] Vide: https://download.inep.gov.br/acesso_a_informacao/tratamento_de_dados_pessoais/portaria_592-2020.pdf. Acesso em 28.05.2022.
[427] Vide: https://download.inep.gov.br/microdados/nota_tecnica_14-2021_daeb.pdf. Acesso em 28.05.2022.
[428] Vide: https://download.inep.gov.br/microdados/parecer_00018-2022_PFInep.pdf. Acesso em 28.05.2022.
[429] Vide: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000730_2022_53-nt-46.pdf. Acesso em 28.05.2022.

garantia da proteção de dados pessoais mantidos por órgãos e entidades públicas. Mais que isso, indicou a necessidade de o Instituto elaborar o RIPD, para avaliar os riscos que podem ser gerados aos titulares de dados em função da divulgação de dados, determinar quais dados deverão ser mantidos em sigilo, e assegurar transparência sobre as salvaguardas adotadas para garantir a segurança e integridade dos dados divulgados, assim como os direitos dos titulares.[430]-[431]

De todo modo, o Ministério Público Federal (MPF) ajuizou ação civil pública (nº 1027450-46.2022.4.01.3400) perante a Justiça Federal, em Brasília, para exigir ao Inep a retomada na divulgação de dados sobre o censo escolar e o ENEM.[432] Para o MPF, o Inep "utilizou a LGPD como um escudo argumentativo" para descumprir a LAI e restringir os direitos à publicidade e transparência. No entanto, a despeito da pesquisa conduzida pela UFMG, o MPF afirmou que os dados divulgados pelo Inep são anonimizados, de forma a não estarem no escopo da LGPD. Por isso, o MPF pediu, liminarmente, que o Inep adotasse as medidas administrativas necessárias para a divulgação dos microdados referentes ao Enem de 2020 e do Censo Escolar da Educação Básica de 2021, além dos exames que os sucederem, bem como para que sejam novamente disponibilizados os resultados históricos dos exames outrora realizados, sob pena de fixação de multa. A ação aguarda julgamento.

Como consequência desse caso, passou a tramitar no Senado Federal, após a aprovação da Câmara dos Deputados, o Projeto de Lei 454/2022[433] que visa alterar a LGPD para autorizar, expressamente, o compartilhamento dos dados e microdados brutos das crianças para fins associados ao Censo Escolar.

---

[430] A ANPD também passou a cooperar com a CGU para desenvolver políticas destinadas a oferecer a órgãos públicos orientações sobre como assegurar transparência em observância à proteção de dados pessoais, atuar em conjunto em reclamações relacionadas ao suposto embate entre LAI e LGPD, e assegurar a responsabilização prevista na LAI e na LGPD em casos de descumprimento dessas leis. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-cgu-estreitam-relacoes-para-aplicacao-da-lgpd-e-da-lai. Acesso em 27.05.2022.

[431] Embora esta tese concorde com a ANPD na conclusão de que órgãos públicos devem realizar RIPD e adotar salvaguardas à proteção de dados pessoais para além do emprego de técnicas de anonimização, é necessário cuidar para que a necessidade de adotar essas medidas não seja utilizada como justificativa para remover, atrasar ou simplesmente não publicar dados de interesse público.

[432] Vide: http://www.mpf.mp.br/df/sala-de-imprensa/docs/PRDFMANIFESTACAO147412022.pdf. Acesso em 27.05.2022.

[433] Vide: disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2317281. Acesso em 20.08.2022.

13.2.2 Envio de dados por entes privados para o governo

Em maio de 2020, o plenário do STF julgou as ADIs nº 6387, nº 6388, nº 6389, nº 6390 e nº 6393,[434] quando da análise da constitucionalidade da Medida Provisória nº 954/2020, que impunha às empresas de telefonia a obrigação de envio de dados de seus clientes (ie., nome, número de telefone e endereço) para o IBGE, a fim de que o Instituto realizasse pesquisa estatística oficial durante a situação de emergência de saúde pública do COVID-19.[435]

Em seu voto em apreciação cautelar, a Ministra Relatora Rosa Weber entendeu que a Medida Provisória estaria em desconformidade com a Constituição Federal, ao afrontar os direitos de privacidade e de livre desenvolvimento da personalidade (art. 5º, X e XII da Constituição), ao não oferecer salvaguardas técnicas e administrativas suficientes para o compartilhamento e subsequente tratamento aos dados pessoais de consumidores de empresas de telefonia. Neste momento, a Ministra também reconheceu a existência do direito fundamental de proteção de dados pessoais, como já abordado anteriormente nesta tese. O entendimento da Ministra Rosa Weber foi confirmado pela maioria do Tribunal, vencido o Ministro Marco Aurélio.

No julgamento plenário, a Ministra relatora argumentou que o compartilhamento de dados pessoais pretendido pela Medida Provisória nº 954/2020 é excessivo e desproporcional, em vista da grande quantidade de titulares afetados, falta de clareza sobre a finalidade e necessidade que se deseja alcançar com o compartilhamento, extensão indeterminada de tempo em que os dados poderiam ser utilizados pelo IBGE (trinta dias após o término do período da situação de emergência de saúde pública) e ausência de salvaguardas para a proteção da privacidade dos titulares de dados afetados.[436] Diante disso, e a despeito de reconhecer a seriedade do IBGE e das dificuldades em executar suas atividades em momento de pandemia, a Ministra entendeu não demonstrada a proporcionalidade e a razoabilidade da medida para a limitação à privacidade e proteção de dados pessoais de consumidores de serviços de telefonia. Por sua vez, os Ministros Luís Roberto Barroso e Luiz Fux, em adição

---

[434] O julgado foi anteriormente analisado nesta tese, mas sob a perspectiva do reconhecimento pelo STF do direito fundamental à proteção de dados pessoais.

[435] Vide: Medida Cautelar disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949382&ext=.pdf. Acesso em 20.11.2022.

[436] Nesse momento, a Ministra distinguiu o compartilhamento de dados pretendido em relação à antiga divulgação de listas telefônicas (que continham nome, telefone e endereço) em vista da existente tecnologia disponível na atualidade para o processamento, cruzamento e filtragem de dados em larga escala e para a formação de perfis do titular.

aos argumentos apresentados pela Ministra Relatora, entenderam que o compartilhamento de dados para fins de produção de estatísticas seria realizado em observância à privacidade apenas caso houvesse clara delimitação da finalidade do tratamento, restrição de acesso aos dados, adoção de procedimentos de segurança para para prevenir riscos de acesso desautorizado, vazamentos acidentais ou utilização indevida, e elaboração de relatório de impacto à proteção de dados pessoais antes do compartilhamento. Como a Medida Provisória não atendia a esses requisitos, os Ministros seguiram o entendimento da Ministra Relatora de que a Medida Provisória seria inconstitucional.

Também o Ministro Gilmar Mendes reforçou e aprofundou o argumento de ausência de salvaguardas mínimas para a garantia da privacidade de usuários de serviço de telefonia no Brasil. Para tanto, o Ministro argumenta que a finalidade apresentada pela Medida Provisória para justificar o compartilhamento seria demasiadamente ampla ("produção de estatística oficial"), de forma contrária ao exigido pelos princípios da finalidade e transparência, que são essenciais à consecução da autodeterminação informativa do titular de dados e ao exercício do teste de proporcionalidade, essencial à eventual limitação do direito à privacidade. Por isso, afirma que a Medida Provisória não apresenta "[...] interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia, consideradas a necessidade, a adequação e a proporcionalidade da medida.".

Finalmente, em voto vencido, o Ministro Marco Aurélio argumentou que a Medida Provisória buscou permitir a obtenção de informação para a realização de estatísticas necessárias à execução de políticas públicas. Essas atividades ficaram inviabilizadas pela necessidade de distanciamento social exigido pela pandemia do COVID-19, gerando prejuízo a toda a coletividade. Por isso, argumentou que o interesse no compartilhamento de dados pretendido deveria prevalecer sobre o direito individual de privacidade. Além disso, entendeu que a Medida Provisória teria definido balizas suficientes para a garantia da privacidade de cidadãos, a exemplo da definição de que a finalidade do tratamento seria a realização de pesquisas estatísticas oficiais e que os dados somente poderiam ser tratados até 30 dias após o término das restrições relacionadas ao enfrentamento da pandemia. Diante disso, entendeu que a Medida Provisória impugnada seria constitucional.

13.2.3 Compartilhamento de dados para fins de fiscalização

Informações do Departamento Nacional de Trânsito

A ADPF nº 695[437], que discute a constitucionalidade do Termo de Cooperação nº 07/2020, que autoriza o compartilhamento de dados entre a Agência Brasileira de Inteligência (Abin) e o Denatran por intermédio do Serpro, e a ADI 6649, que questiona a constitucionalidade do Decreto nº 10.046/2019, que regula o compartilhamento de dados entre órgãos e entidades da administração pública federal, foram julgadas pelo STF. O pedido liminar solicitado na ADPF nº 695 foi negado pelo Ministro Relator Gilmar Mendes, em função da revogação pelo Advogado-Geral da União do Termo de Cooperação nº 07/2020 (no dia em que estava pautado o julgamento da medida).

Em seu voto, o Ministro reforçou ser a proteção de dados pessoais um direito fundamental, em uma releitura do direito à privacidade como liberdade negativa e positiva, que possui caráter comunitário e assegura autodeterminação informativa aos cidadãos.[438] Por isso, avalia se os atos impugnados apresentam salvaguardas suficientes para a pretendida limitação a direitos fundamentais, consistentes na "existência de mecanismos adequados de controle das finalidades desse compartilhamento".

Além disso, destaca não ser possível simplesmente transladar as regras da LGPD aplicáveis ao setor privado para o poder público, visto que o uso de dados é uma condição para que o Estado desempenhe seu mandado constitucional e considerando que muitas vezes não será possível assegurar aos cidadãos os mesmos direitos que consumidores de serviços prestados por uma empresa possuem (como a deleção ou portabilidade de dados). Em função disso, seria necessário considerar a LGPD em conjunto com as normas e princípios aplicáveis à atuação do poder público, como a limitação do tratamento de dados pelo poder público às atividades principais e acessórias de provisão de serviços público e amparadas em legislação, decorrente da interpretação conjunta do art. 23 da LGPD e do princípio da legalidade.

Por isso, o Ministro avalia que as salvaguardas previstas no Decreto nº 10.046/2019 (que são essencialmente relacionadas à segurança da informação) não são suficientes e, inclusive, que suas disposições removem barreiras ao livre fluxo de dados pessoais entre órgãos e entidades públicos, e promovem a criação de base de dados centralizadas que poderá

[437] https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693. Acesso em 15.10.2022.
[438] Vide: voto disponível em: https://www.conjur.com.br/dl/gilmar-manda-plenario-analise.pdf. Acesso em 15.10.2022.

ser utilizada indistintamente pelo poder público. Em relação ao Termo de Cooperação, embora reconheça o interesse público na apuração de irregularidades que são do escopo de atuação da Abin, não restaria clara a necessidade, para a realização dessas atividades, do compartilhamento de dados pessoais que não integram o Sistema Brasileiro de Inteligência. Não obstante isso, avaliou que a pretendida limitação aos direitos à privacidade e proteção de dados pessoais não seriam proporcionais - na verdade, considerou que a ausência de parâmetros mínimos no Termo de Autorização nº 07/2020 sequer permitia a realização do teste.

No julgamento pelo pleno, realizado conjuntamente para a ADPF nº 695 e para a ADI 6649, a o Tribunal, por maioria, julgou parcialmente procedente os pedidos, conferindo interpretação conforme ao Decreto nº 10.046/2019 para determinar que o compartilhamento de dados entre o poder público pressupõe:[439] **(a)** a identificação de finalidades legítimas, específicas e explícitas para o tratamento de dados; **(b)** compatibilidade do tratamento com as finalidades informadas; **(c)** observância ao princípio da necessidade; **(d)** a observância integral dos requisitos, garantias e procedimentos estabelecidos na LGPD, no que cabível ao setor público; e **(e)** rigorosa observância do art. 23, I da LGPD, que exige a ampla publicidade sobre a previsão legal, finalidade e procedimentos adotados no tratamento de dados. O descumprimento doloso deste último requisito resultará, no entendimento da Corte, na responsabilização do agente público por improbidade administrativa. Para o compartilhamento de dados para finalidades de inteligência, o Tribunal deverá observar o disposto em legislação específica e os parâmetros estabelecidos no julgamento da ADI nº 6.529[440] pelo STF que, em adição aos estabelecidos para o compartilhamento de dados entre órgãos e entidades públicas, consistem na instauração de procedimento administrativo motivado que permita o controle de legalidade judicial.

---

[439] Extrato de julgamento disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693. Acesso em 15.10.2022

[440] Outra demanda relacionada ao tema foi a ADI 6529, de relatoria da Ministra Cármen Lúcia, que versou sobre a obrigatoriedade de motivação no ato administrativo de solicitação de dados de inteligência aos órgãos do Sistemas Brasileiro de Inteligência pela Agência Brasileira de Inteligência. O STF fixou entendimento no sentido da legitimidade do compartilhamento de conhecimentos específicos com a ABIN, desde que observados os requisitos legais de comprovação do interesse público da medida, afastada qualquer possibilidade de o fornecimento desses dados atender a interesses pessoais ou privados, e de motivação para eventual controle de legalidade pelo Poder Judiciário. Para tanto, a Ministra relatora destacou que "a natureza da atividade de inteligência, que eventualmente se desenvolve em regime de sigilo ou de restrição de publicidade, não afasta a obrigação de motivação dos atos administrativos, especialmente se considerado que esses atos podem importar em acesso a dados e informações sensíveis dos cidadãos, limitando os direitos fundamentais à privacidade e à intimidade". Supremo Tribunal Federal (STF). Ação Direta de Inconstitucionalidade 6.529 Distrito Federal. Requerente: Rede Sustentabilidade. Intimado: Presidente da República e Congresso Nacional. Relatora: Ministra Cármen Lúcia. Brasília, 11 de out. de 2022. Disponível em:https://portal.stf.jus.br/processos/downloadPeca.asp?id=15348384228&ext=.pdf. Acesso em 31.08.2022.

Em relação ao Cadastro Base do Cidadão, o STF determinou que o CCGD preveja, considerando os parâmetros aplicáveis a qualquer compartilhamento de dados pelo poder público: **(i)** mecanismos rigorosos de controle de acesso ao Cadastro Base, limitado a órgãos e entidades que comprovarem real necessidade de acesso aos dados pessoais nele reunidos; **(ii)** justificativa formal, prévia e minudentemente da necessidade de inclusão de novos dados pessoais na base integradora e a escolha das bases temáticas que comporão o Cadastro Base; **(iii)** instituir medidas de segurança que observem os princípios da LGPD, em especial a criação de sistema eletrônico de registro de acesso. Além disso, a Corte estabeleceu que o art. 20 do Decreto, que estabelece a composição do CCGD, seria inconstitucional. Com isso, a Presidência da República teria 60 dias a contar da data do julgamento para atribuir ao órgão perfil independente e plural, aberto à participação democrática, além de assegurar aos seus membros garantias mínimas contra influências indevidas.

Em seu voto, o Ministro Relator, Gilmar Mendes parte do pressuposto de que a declaração de inconstitucionalidade de todo o Decreto nº 10.046/2019 removeria do Poder Executivo as normas necessárias ao compartilhamento de dados para a eficiente e segura prestação de serviços públicos. Também considerou que a repristinação do Decreto nº 8.789/2016 seria ainda mais nocivo, na medida em que o texto era obsoleto e estabelecia o compartilhamento de dados entre órgãos públicos de forma preferencialmente automática. Diante disso, assim como do prejuízo à privacidade e à eficiência governamental que seria gerada por uma declaração de ampla inconstitucionalidade da norma, na medida em que o compartilhamento de dados é parte integrante da moderna prestação de serviços públicos, o Ministro adotou o método de interpretação conforme a Constituição.

Nesse sentido, determina que qualquer norma ou interpretação legal que resulte no irrestrito compartilhamento de dados pessoais entre órgãos da administração pública será contrário ao disposto na constituição, de forma que somente as informações gerais do Estado, como aquelas relativas ao funcionamento do aparato estatal (por exemplo, a gestão de pessoal e do patrimônio público, o uso de recursos orçamentários, e a formalização de atos e contratos administrativos) seriam alcançadas por similar determinação. Assim, desde que o Decreto impugnado seja interpretado em conjunto com as normas da LGPD, entende que a norma não autoriza o fluxo de dados pessoais de forma ampla e irrefletida ou a composição de base

integradora descomunal e suscetível a abusos. Qualquer entendimento contrário a essa lógica seria, portanto, eivado de inconstitucionalidade.[441]

Dados protegidos por sigilo bancário

Em 2015, a 1ª Turma do STF julgou o Mandado de Segurança 33.340/DF[442] impetrado pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e pelo BNDES Participações S.A. (BNDESPAR), contra decisão do TCU que os exigiu enviar documentos (e.g., saldo devedor das operações de crédito, a situação cadastral no BNDES do Grupo Friboi, dados sobre a situação de adimplência do Grupo) referentes às operações financeiras realizadas entre o BNDES e o Grupo JBS/Friboi. Segundo o BNDES e o BNDESPAR, o envio de informação ao TCU violaria a expectativa de sigilo do cidadão ao se relacionar com instituições financeiras. Por sua vez, o TCU defende que os documentos solicitados não seriam protegidos por sigilo bancário, vez que os contratos e operações às quais se referem foram custeados com recursos de origem pública.

Ao apreciar o caso, o STF avaliou a proporcionalidade do pedido de acesso a informações sobre gastos públicos diante da proteção à privacidade de cidadãos, tendo concluído pela proporcionalidade da solicitação feita pelo TCU, na medida em que não haveria expectativa de sigilo bancário sobre operações financeiras que envolvem recursos públicos e que a insuficiente limitação ao direito à privacidade seria lesiva ao interesse social de exigir transparência sobre atos da administração pública. Além disso, considerou que a questionada solicitação de dados pelo TCU está entre suas prerrogativas legais, visto que é o ente público responsável por controlar a legitimidade do emprego de recursos públicos, além de os dados solicitados serem adequados e necessários para o alcance da finalidade de controle financeiro. A adequação e necessidade residiria no fato de o TCU ter realizado

[441] Ainda em 2022 houve outro julgamento sobre a legalidade da obtenção, sistematização e compartilhamento, por parte do Sistema Brasileiroo de Inteligência, de dados sobre a orientação política de cidadãos. Especificamente, a Arguição de Descumprimento de Preceito Fundamental n. 722 movida pela Rede Sustentabilidade, questionou prática adotada pelo Ministério da Justiça e Segurança Pública (MJSP) consistente em investigar servidores públicos opositores ao governo sob a fundamentação de atividade de inteligência. No julgamento da ação, o pleno do STF deferiu a medida cautelar para suspender atos do MJSP consistentes em elaborar e compartilhar informações de servidores públicos, incluindo professores universitários, que exerçam licitamente seus direitos de expressão e associação. Em seu voto, a Ministra relatora, Cármen Lúcia, defendeu que a coleta e o compartilhamento de dados entre órgãos do SISBN seja desenvolvido em observância ao "interesse público, observância aos valores democráticos e respeito aos direitos e garantias fundamentais", de tal forma que sua realização para o interesse privado do órgão ou de agente público caracteriza desvio de finalidade e abuso de poder. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754179572. Acesso em 14.12.2022.

[442] Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur313576/false. Acesso em 16.10.2022

solicitação não genérica, que apontou interesse em acesso a informações específicas e relevantes à sua atuação, além de atuar de forma a gerar a menor quantidade de prejuízo aos destinatários do controle.

Embora este caso não aborde o tratamento de dados pessoais, tal como previsto na LGPD (na medida em que a privacidade protegida é de uma entidade jurídica), ele envolve a ponderação entre privacidade e norma de sigilo em casos de fiscalização sobre a utilização de recursos públicos. Como se pôde verificar, assim como nos julgados sobre transparência a respeito do gasto de verbas públicas, neste caso também se entendeu haver interesse público na limitação a garantias de privacidade oferecidas a cidadãos e até mesmo a empresas.

13.3 Análise sobre interesse público nos julgados analisados

Primeiramente, cumpre observar que esta análise não se pretende exaustiva, mas somente uma reflexão sobre fatores considerados pelo Supremo Tribunal Federal e pela Controladoria-Geral da União quando da avaliação do interesse público em situações de publicação e de compartilhamento de dados pessoais mantidos pelo poder público.

Primeiro, os julgados selecionados sobre interesse público na publicação de dados pessoais mantidos pelo poder público envolveram a divulgação de informações sobre (**i)** identificação e divulgação de informações sobre servidores públicos; **(ii)** como são realizados gastos públicos; **(iii)** fatos e análises relacionadas ao desenvolvimento de políticas públicas e prestação de serviços públicos; **(iv)** financiamento de campanhas e candidatos a cargos eletivos; **(v)** tema que é objeto de debate público no país; e **(vi)** fatos históricos constantes de documentos mantidos em arquivos públicos. Em relação às decisões analisadas sobre compartilhamento de dados pessoais por entes públicos, elas envolveram essencialmente a divulgação de dados considerados como necessários à prestação de serviços públicos, ao desenvolvimento de políticas públicas, e à fiscalização de atos da administração pública.

Em todas as situações analisadas sobre o compartilhamento e a publicação de informações para o **controle de gastos públicos**, o entendimento da CGU e do STF foi de que o interesse público resultaria na divulgação de dados pessoais. Em outras palavras, em casos envolvendo transparência sobre gastos públicos, será possível flexibilizar a privacidade e a proteção de dados pessoais em favor da divulgação de dados. Por exemplo, a jurisprudência do STF é pacífica sobre a existência de interesse público na publicação de informações sobre

salários e benefícios auferidos por servidores públicos, e de despesas de verbas públicas realizadas por ocupantes de cargos políticos.

No julgamento de processos envolvendo a divulgação de **salários e benefícios de servidores públicos** (ou de critérios utilizados para promoções funcionais), se considerou que a transparência sobre essas informações estaria atrelada ao princípio republicano que exige a viabilização da participação social na coisa pública. Já na apreciação de recursos relacionados às **despesas de ocupantes de cargos políticos**, os Ministros entenderam que a publicação de despesas realizadas com verbas públicas por ocupantes de cargos políticos não atenta contra a privacidade desses agentes públicos porque informações pertinentes a atividades realizadas no exercício de função pública não seriam dados pessoais. Embora esse entendimento não esteja plenamente adequado ao conceito de dados pessoais previsto na LGPD, o resultado do julgamento está alinhado à jurisprudência do STF que reconhece o interesse público na divulgação de informações que permitam a fiscalização social de gastos públicos.

De forma similar, o STF e a CGU estabeleceram haver interesse público na publicação e no compartilhamento de **dados pessoais de cidadãos (não ocupantes de cargos públicos) que recebem benefícios sociais, realizam doações para partidos ou candidatos políticos e acessam prédios públicos**. No caso de beneficiários de programas sociais, a divulgação de dados de cidadãos foi determinada para viabilizar meios para que a sociedade possa exercer controle sobre a higidez no gasto de verbas públicas. Já em relação às últimas duas situações (ie.: dados pessoais de doadores de campanha eleitoral e de cargos eletivos e lista de visitantes a prédios públicos), tanto o STF como a CGU entenderam que o interesse público estaria em permitir que a sociedade tenha conhecimento sobre influências externas exercidas sobre o processo eleitoral ou sobre a gestão da coisa pública.

Também em relação à divulgação de dados pessoais de cidadãos, tanto o STF como a CGU consideraram ser possível sua divulgação em casos de **importância histórica** e quando forem necessários para a **execução de políticas públicas e cumprimento de atribuições legais** do órgão ou entidade pública.[443] Em um caso, a CGU entendeu ser possível divulgar cartas e poemas de escritores brasileiros notáveis, após 30 anos de sua guarda por arquivos públicos, dada a sua relevância para a produção científica nacional. Por sua vez, em julgamentos mais recentes, o STF argumentou ser possível o compartilhamento de dados

[443] Note que, como mencionado, essas hipóteses são apenas exemplos de situações em que haverá interesse público na publicação ou no compartilhamento de dados pessoais. Por isso, as situações ora abordadas não são exaustivas, podendo haver outros casos em que essa divulgação é desejável.

quando necessários para a execução de políticas públicas e para o cumprimento de atribuições legais do agente público, desde que observados os procedimentos previstos na LGPD, a exemplo da indicação de finalidades legítimas e específicas, observância da transparência e necessidade, e a adoção de salvaguardas técnicas para evitar a ocorrência de incidentes de segurança.

Por outro lado, houve situações em que a não divulgação dos dados foi justificada pela presença de **norma ou determinações contratuais de confidencialidade**. Em caso de solicitação de acesso à lista de membros de banca examinadora de concurso público, a restrição de acesso foi justificada, entre outros, na existência de cláusula contratual com os membros da banca examinadora que determinava o sigilo sobre sua participação no certame e que geram no titular de dados uma expectativa de confidencialidade sobre essa informação. Já no caso de pedido de acesso a comunicações estabelecidas entre a embaixada do Brasil no Egito e o MRE, a recusa foi justificada em normas que estabelecem a confidencialidade de informações a respeito de cidadãos brasileiros atendidos por repartições consulares, cujo objetivo é assegurar confiança social no Estado em proteger informações pessoais que custodia. Por sua vez, no caso de acesso a documentos mantidos em arquivos públicos, embora a CGU tenha determinado a divulgação dos dados ao pesquisador solicitante, somente o fez após o término do prazo contratual de confidencialidade dos documentos, assinado pelo arquivo público com os herdeiros de escritores brasileiros notáveis.

Como se verifica, a presença no caso concreto de cláusula ou norma de confidencialidade esteve destinada a assegurar confiança dos titulares de dados sobre a privacidade de seus dados em relação a outros órgãos governamentais ou à sociedade, de tal forma que a sua inobservância afrontaria a legítima expectativa dos titulares de dados sobre como eles serão utilizados. Por isso, a avaliação do interesse público, sempre que o sigilo ou a cláusula de confidencialidade observar o disposto na legislação, tenderá a privilegiar a privacidade e a proteção de dados pessoais. No entanto, em casos nos quais as cláusulas de confidencialidade ou a determinação de sigilo forem abusivas, será possível ao órgão recursal competente afastar a sua aplicação e determinar a divulgação dos dados, a exemplo do realizado no julgamento avaliado sobre o compartilhamento de dados protegidos por sigilo bancário.

Verifica-se, portanto, que nos julgados analisados a CGU e o STF entenderam haver interesse público na publicação e no compartilhamento pelo poder público de dados pessoais de indivíduos não ocupantes de cargos ou funções públicas para fins de dar transparência

sobre gastos públicos e financiamento de campanhas eleitorais e candidatos a cargos eletivos, auxiliar com o desenvolvimento de políticas públicas e prestação de serviços públicos, e permitir acesso sobre fatos de importância histórica. Por outro lado, não são de interesse público informações que apenas saciam a curiosidade do público e dados protegidos por disposições legítimas de sigilo ou confidencialidade, especialmente porque a divulgação estaria fora das legítimas expectativas dos titulares de dados.

Em seguida, como a maioria das decisões avaliadas são anteriores à LGPD, foi possível identificar inconsistências no seu conteúdo em relação aos dispositivos da referida lei, especialmente quanto: **(i)** à avaliação sobre a presença de dados pessoais no caso concreto; **(ii)** à qualificação dos dados como sensíveis e possibilidade de sua divulgação; **(iii)** à pouca reflexão sobre a necessidade da divulgação de cada um dos dados e sobre formas de publicar ou compartilhar dados pessoais em observância à privacidade.

Em relação à avaliação sobre a **presença de dados pessoais no caso concreto**, foi possível identificar decisões em que dados pessoais não foram qualificados como tais ou em que foi possível a terceiros reidentificar dados publicados de forma agregada e desidentificada. Na primeira situação, Ministros do STF entenderam que a publicação de despesas realizadas com verbas públicas por ocupantes de cargos políticos não exporia informações pessoais. No entanto, informações que permitam a identificação de uma pessoa natural, ainda que ocupante de cargo público, serão pessoais e merecem os cuidados previstos na LGPD. Ressalte-se, isso não significa que os dados não devam ser divulgados, mas que são dados pessoais e que seu tratamento está contemplado no escopo da LGPD.

Na segunda situação, pesquisadores diagnosticaram ser possível reidentificar microdados publicados pelo Inep, motivo pelo qual a entidade optou por remover de seus sistemas públicos dados anteriormente publicados. No entendimento do Inep, a despeito da relevância da publicação desses dados para fins de pesquisas acadêmicas e jornalísticas, o interesse público resultaria na privacidade e proteção de dados pessoais de estudantes e professores, especialmente diante de garantias de confidencialidade oferecidas aos cidadãos no momento da coleta de dados. Para situações em que dados divulgados de forma desidentificada passam a ser reidentificados por terceiros, deverá ser feita avaliação sobre as chances reais de reidentificação e os riscos da divulgação de dados pessoais para seus titulares, mas também deverá ser considerada a adoção de salvaguardas para mitigar tais riscos.

Quanto à **avaliação da natureza dos dados pessoais**, foi possível notar a existência de decisões que justificaram a não divulgação de dados por serem qualificados como sensíveis e, como consequência, poderiam gerar maiores prejuízos aos titulares de dados (e.g., restrição à divulgação do PIS de beneficiários de programas sociais). No entanto, (i) os dados envolvidos nos casos nem sempre se tratavam do que hoje a legislação qualifica como sendo dados pessoais sensíveis (e.g., raça, religião e orientação sexual do indivíduo), e (ii) a legislação não impede a divulgação de dados pessoais sensíveis. Embora o tratamento de dados sensíveis tenha o potencial de gerar riscos mais elevados, nem todo tratamento desses dados será necessariamente de elevado risco. Por exemplo, a publicação na internet do número integral do CPF de uma pessoa poderá impor maiores riscos se comparado com a publicação de dados qualificados como sensíveis (especialmente se não forem tratados para a extração de inferências sensíveis), a exemplo da divulgação de determinados campos da carteira de vacinação de pessoas politicamente expostas.[444]-[445]

De todo modo, o risco do tratamento de dados qualificados como sensíveis varia segundo o contexto no caso concreto, por meio da avaliação de elementos como a identificação de quem são os titulares de dados (e.g., pessoa em situação de vulnerabilidade ou pessoa politicamente exposta), qual a finalidade do tratamento (e.g., para fins de saúde pública ou para criação de perfis de crédito), e as salvaguardas implementadas (e.g., divulgação de dados específicos, anonimização de dados e previsão de controles de acesso). Não se deve pressupor que os tratamentos realizados com dados pessoais sensíveis são sempre de elevado risco e, por consequência, não podem ser publicados ou compartilhados. Isso decorre especialmente do fato de que a divulgação de determinados dados sensíveis poderá ser de interesse público, a exemplo da publicação de filiados em partidos políticos ou do compartilhamento entre órgãos e entidades públicas de dados de saúde de cidadãos para fins de pesquisa, de promoção de medidas de saúde pública ou o desenvolvimento de políticas públicas. De todo modo, a análise sobre o interesse público na divulgação deverá ser mais rigorosa e os cuidados na divulgação serão mais rígidos.

---

[444] Isso pode ser ilustrado pela divulgação por Senador brasileiro de documento contendo o número de seu CPF, o que permitiu a terceiros cadastrarem-no em diversos serviços e filiarem-no em partido político. Vide: https://congressoemfoco.uol.com.br/area/governo/apos-vazamento-de-dados-internautas-tentam-filiar-bolsonaro-ao-pt/. Acesso em 29.12.2023. De todo modo, em casos de menor repercussão política nacional, são recorrentes os casos em que agentes maliciosos se utilizam do número de CPF de terceiros (muitas vezes disponíveis *online* em função de incidentes de segurança da informação) para o cometimento de crimes.

[445] Como reiterado pelo STF em decisões diversas, inclusive em demandas sobre direito ao esquecimento e elaboração de biografias não autorizadas, pessoas notórias e/ou ocupantes de cargos políticos possuem menor expectativa de privacidade pelo fato de ocupar cargos públicos.

Além disso, não se deve justificar a decisão de restrição de acesso a arquivos e documentos pela possibilidade abstrata de possuírem dados sensíveis, a exemplo do realizado no caso de solicitação de acesso a e-mail de servidores públicos. Nessa situação, caso constatada a presença de dados sensíveis entre os e-mails trocados, deveria ser realizada análise específica sobre o interesse público na divulgação e, na impossibilidade de realizar a divulgação, excluir as informações qualificadas como sensíveis e divulgar as demais informações (salvo se não houver outra justificativa para a restrição de acesso).

Em seguida, como as decisões referentes à publicação de dados são em sua maioria anteriores à edição da LGPD, foi possível notar pouca reflexão sobre a necessidade dos dados individualmente considerados para o alcance do interesse público e sobre a possibilidade de serem adotadas salvaguardas para assegurar a divulgação em observância à proteção de dados pessoais. Por exemplo, como argumentado anteriormente, para se determinar a presença de interesse público, é necessário avaliar se a divulgação almejada alcança a finalidade almejada (e.g., a publicação do salário dos servidores públicos é relevante para a finalidade de fiscalização de gastos públicos?) e se os dados divulgados são necessários para o alcance dessa finalidade (e.g., a publicação sobre a quantidade de filhos de um servidor público é relevante para o *accountability* de gastos públicos? E se o dado for relevante para identificar o motivo pelo qual o servidor aufere benefícios como auxílio creche?).

Além disso, como mencionado, na condução do teste de proporcionalidade para identificar a presença de interesse público na divulgação de dados pelo poder público, deverão ser avaliados os riscos da limitação proposta a direitos fundamentais. Esse esforço deve levar em consideração a eficiência das salvaguardas adotadas pelo controlador (e.g.: o tarjamento parcial do CPF mitiga devidamente os riscos à privacidade de servidores públicos? Se sim, o mesmo processo não deveria ser adotado com identificadores de beneficiários de programas sociais?), de forma a não indevidamente pender o resultado do teste em favor da divulgação ou da restrição de acesso a dados. Assim, deverá haver maior reflexão sobre o conteúdo e condições do compartilhamento ou da publicação de informações, de forma a considerar não somente os benefícios ou riscos da divulgação, a necessidade e adequação dos dados divulgados para o alcance da finalidade almejada, e a efetividade de possíveis salvaguardas.

14 PROPOSTA: INTERESSE PÚBLICO ENQUANTO PONDERAÇÃO ENTRE PRIVACIDADE E EFICIÊNCIA E/OU TRANSPARÊNCIA GOVERNAMENTAL

Caso a base de dados que se deseja divulgar possua dados pessoais (identificados ou razoavelmente identificáveis) efetivamente necessários para o alcance de determinada finalidade, será necessário avaliar se há interesse público na divulgação desses dados. Trata-se de exigência oriunda da legislação de proteção de dados pessoais (LGPD, art. 23), da Lei de Acesso à Informação (LAI, art. 31, §3˚, I a V) e dos princípios da legalidade e da finalidade, aplicáveis às atividades da administração pública.

No entanto, o conceito de interesse público é amplo, devendo ser estabelecido *ex ante* pela legislação ou pelo administrador, ou pelo magistrado em avaliação *ex post* do caso concreto. Segundo a teoria de direito administrativo, a identificação do interesse público primeiro requer o reconhecimento de que existe uma pluralidade de interesses dentro da sociedade e que o interesse público não necessariamente será oposto a interesses particulares. Para determinar os contornos do interesse público, os interesses envolvidos devem ser ponderados. Essa função é primariamente atribuída ao legislador, mas recai também à administração pública (no exercício da discricionariedade administrativa) ou ao judiciário (quando diante de conflitos cuja solução lhe foi solicitada). Todos esses poderes devem obedecer a suas regras e processos próprios, que envolvem a mediação de interesses sociais conflitantes.

No caso de compartilhamento ou publicação de dados, os interesses que podem conflitar são os direitos fundamentais à privacidade e proteção de dados pessoais em relação aos princípios da eficiência e transparência governamentais. Esses valores jurídicos, tal como sugerido pela doutrina e jurisprudência majoritária, são direitos e princípios constitucionais e sua eventual limitação deverá ser precedida da avaliação sobre a proporcionalidade da medida. Ainda que objeto de críticas teóricas, entre outros motivos, por considerar direitos fundamentais como sendo passíveis de serem limitados, até mesmo por interesses ilegítimos, o método mais recorrentemente utilizado pela jurisprudência nacional e internacional para mediar princípios no caso concreto consiste no teste de proporcionalidade.

Diante disso, a avaliação do interesse público no caso concreto deverá ponderar a eficiência e a transparência governamental em relação à privacidade e proteção de dados pessoais. Com isso, a depender das particularidades do caso concreto, o interesse público

poderá significar a divulgação ou a restrição de acesso aos dados. Assim, a determinação do interesse público envolve não somente a identificação dos benefícios sociais da divulgação de dados, mas também a análise sobre os riscos oferecidos à privacidade e à proteção de dados pessoais de cidadãos coletivamente considerados (BLACK; STEVENS, 2013; RAAB, 2012).[446] Em outras palavras, o interesse público não se definiria como os interesses da coletividade que limitam o direito à privacidade, como recorrentemente argumentado pela literatura,[447] mas, sim, como o resultado da mediação entre os princípios da publicidade e eficiência governamental (e do direito de acesso à informação) em relação ao direito à privacidade e proteção de dados pessoais (que, como defendido nesta tese, alcança a toda a coletividade, e não somente o indivíduo).

Para tanto, tendo em vista a finalidade que se deseja alcançar com a divulgação (que deverá ser legítima, específica e compatível com as finalidades informadas aos titulares de dados), o agente público deverá realizar o teste de proporcionalidade, que se inicia pela análise sobre a **adequação** da divulgação pretendida para alcançar ou fomentar esse objetivo almejado. Entre as possíveis reflexões que podem ser feitas nesse momento, destaca-se: os dados usados e o tratamento proposto podem resultar na finalidade almejada? Por exemplo, a publicação de decisões judiciais é medida apta a assegurar ou fomentar a transparência e *accountability* da atuação do Poder Judiciário? O compartilhamento de dados biométricos de cidadãos entre o Denatran e o TSE é medida apta a promover ou fomentar a desburocratização do processo eleitoral? Essa reflexão envolve avaliar a observância aos já abordados princípios da finalidade (art. 6º, I da LGPD) e da legalidade administrativa (art. 37, Constituição), segundo os quais a divulgação de dados pessoais por governos deve buscar finalidades legítimas, fundamentadas em lei e compatíveis com o informado ao titular.[448]

O próximo passo consiste em avaliar a **necessidade** da medida, ou seja, identificar se a finalidade almejada poderá ser promovida com a mesma intensidade caso sejam adotadas outras medidas menos gravosas à privacidade e proteção de dados pessoais de cidadãos. Entre as possíveis reflexões que podem ser levantadas nesta etapa do teste de proporcionalidade estão: a finalidade estabelecida pode ser alcançada ou fomentada de forma alternativa à

---

[446] Assim, concorda-se com Charles Raab (2012) quando destaca "o valor não individual e de interesse público da privacidade, a partir de uma visão de complexidade social, [ampliando] a própria ideia de "interesse público" para incluir mais claramente a proteção da privacidade individual, ao invés de oposição a ela."

[447] Charles Raab (2012) aponta essa tendência quando argumenta que "tornou-se lugar-comum construir a relação entre privacidade e interesse público como uma oposição de soma zero: um só pode aumentar às custas do outro."

[448] Segundo a concepção de Cortes Europeias sobre o teste de proporcionalidade, a legitimidade da medida é anterior às demais etapas do teste de proporcionalidade.

divulgação proposta? É possível divulgar os dados de forma anonimizada, com controles de acesso ou regras de sigilo sem prejuízo aos objetivos da publicação ou do compartilhamento? Por exemplo, é possível ao IBGE obter os dados necessários para a condução de suas pesquisas de forma alternativa ao recebimento de dados de todos os usuários de serviços de telefonia? Pesquisadores conseguem realizar análises qualificadas sobre o sistema de ensino caso recebam acesso a apenas dados agregados e não a dados individualizados? Essa reflexão envolve avaliar aspectos do mencionado princípio da necessidade (6º, III, LGPD), segundo o qual a divulgação de dados deve ser limitada ao necessário para o alcance de suas finalidades.

Por fim, a última etapa dessa análise consiste em avaliar a **proporcionalidade em sentido estrito**, que exige o sopesamento dos benefícios e dos riscos decorrentes da divulgação. Entre as possíveis reflexões que podem ser feitas nesse momento estão: a intensidade dos benefícios da divulgação dos dados supera a intensidade dos riscos que ela oferece à privacidade de cidadãos? Por exemplo, os benefícios do *accountability* de gastos públicos justifica os riscos impostos à privacidade em casos de publicação de salários de servidores ou de benefícios sociais auferidos por populações em situação de vulnerabilidade? Essa análise deverá ser realizada levando em consideração os riscos reais do tratamento de dados pessoais e as possíveis salvaguardas (e.g., anonimização de dados ou licenças de uso) que podem ser adotadas para mitigar os riscos identificados.

O balanceamento entre riscos à privacidade e benefícios da divulgação variam conforme as particularidades do caso concreto e do contexto no qual o tratamento se insere (e.g., cultura de transparência e/ou de privacidade no país e estado do desenvolvimento tecnológico).[449] Por exemplo, no Canadá, o teste de balanceamento penderá para a transparência ou para a eficiência governamental, caso os benefícios da divulgação claramente superem a invasão de privacidade que possa resultar do compartilhamento ou da publicação. Por sua vez, no Brasil, desde que superadas as duas primeiras etapas do teste de proporcionalidade (ie.: comprovar que a divulgação contribui para fomentar a transparência e eficiência governamental e que isso não seria razoavelmente viabilizado pela adoção de medidas alternativas) e demonstrada a adoção de salvaguardas suficientes para mitigar os riscos à privacidade e proteção de dados pessoais (ou seja, se a divulgação não resultar em riscos demasiadamente elevados à privacidade do cidadão e/ou as salvaguardas propostas

[449] Esse entendimento está em linha com o argumentado por Helen Nissenbaum (2004) segundo a qual "[...]as prescrições sobre privacidade, agora moldadas em grau significativo por fatores locais, podem variar de acordo com a cultura, período histórico, local, etc.."

forem satisfatórias para mitigá-los), o teste de balanceamento poderá pender em favor da divulgação dos dados.

De todo modo, a utilização do teste de proporcionalidade para determinar se há interesse público no caso concreto permite ao agente público determinado nível de subjetividade. Isso tem gerado (em conjunto com outros fatores que excedem ao escopo desta pesquisa) certa arbitrariedade na avaliação sobre o papel da privacidade e da proteção de dados pessoais na determinação sobre o compartilhamento ou publicação de dados por governos. Enquanto a LGPD tem sido utilizada para limitar certas práticas de transparência governamental, para medidas de eficiência governamental, por muitas vezes, não se observa o mesmo cuidado. Por isso, se faz necessário identificar parâmetros que permitam ao agente público maior objetividade na determinação do interesse público no caso concreto.

Para identificar elementos que auxiliem na realização do teste de proporcionalidade, esta tese realizou análise não exaustiva das experiências Europeia e Canadense na avaliação de interesse público na divulgação de dados pessoais mantidos por governos, além de decisões do STF e da CGU a respeito do conflito entre transparência e/ou eficiência governamental e os direitos de privacidade e proteção de dados pessoais.

Na Europa, a GDPR atribui ao Estado-membro regular o conteúdo de interesse público para fins de fundamentação de atividades de tratamento na base legal de exercício de função para o alcance de interesse público. No caso do Reino Unido, a lei que regulava a GDPR estabelecia exemplos de situações nas quais essa base legal pode ser utilizada, entre as quais estão os tratamentos necessários para **(i)** administração da justiça e funções parlamentares; **(ii)** funções estatutárias e propósitos governamentais e **(iii)** atividades que apoiam ou promovem o engajamento democrático. Para o tratamento de dados pessoais sensíveis, haverá interesse público inerente em determinadas situações (eg., administração da justiça, igualdade de oportunidade ou tratamento, prevenção de fraudes e partidos políticos), mas, em outras, o interesse público estará presente, se demonstrada sua presença no caso concreto (eg., prevenir ou detectar atos ilícitos, salvaguarda de crianças e indivíduos em risco e seguro).

Já a legislação sobre acesso à informação (*Freedom of Information Act*) estabelece que dados pessoais constantes de arquivos e bases de dados públicos poderão ser divulgados quando o interesse público for igual ou superior ao risco gerado à privacidade de indivíduos, e desde que: **(i)** observados os princípios de proteção de dados pessoais, e **(ii)** não haja objeção ao tratamento; ou **(iii)** os dados integrem as exceções ao direito de acesso. Como esclarecido

pelo ICO, o interesse público poderá assumir diversas formas, como a promoção da transparência, *accountability* e acesso à informação, a proteção do processo democrático, a tomada qualificada de decisão por órgãos públicos, a garantia do melhor uso de dinheiro público. Não serão consideradas de interesse público a informação de interesse *para* o *público* (curiosidade) ou interesses privados, visto que o interesse público é aquele que beneficia a sociedade como um todo, e não apenas uma única pessoa. De todo modo, dados pessoais somente poderão ser divulgados se os benefícios sociais superarem os prejuízos à privacidade em teste de proporcionalidade.

Já no Canadá, a legislação federal que regula o tratamento de dados pelo poder público (*Privacy Act*) autoriza a divulgação de dados pessoais mediante consentimento ou em situações específicas, como em casos nos quais o interesse público na divulgação claramente supere os riscos à privacidade resultantes da divulgação. Para avaliar se a divulgação claramente supera os riscos à privacidade, o agente público deverá primeiro avaliar o risco no caso concreto, que envolve entender a sensibilidade da informação, a expectativa do indivíduo, e grau e probabilidade do dano. Em relação à sensibilidade da informação, deve-se avaliar se há informações detalhadas ou altamente pessoais, e a sensibilidade do contexto em que a informação foi obtida. Para avaliar a expectativa do indivíduo, deve-se identificar elementos como o contexto da coleta e as expectativas de confidencialidade sobre os dados, e, para avaliar a probabilidade ou grau do dano, deve-se considerar os riscos em comparação com os benefícios da divulgação, inclusive de posterior divulgação inadequada.

A despeito do requisito de o benefício da divulgação claramente superar seus riscos reais, o teste de balanceamento no Canadá tenderá a privilegiar a divulgação de dados em relação à privacidade e proteção de dados pessoais quando o acesso à informação for necessário para promover *accountability* política e burocrática, viabilizar a participação social em processos políticos, ou evitar prejuízos sociais, como à saúde e à segurança pública. Por outro lado, essas autoridades protegem a privacidade em relação à divulgação de informações em casos nos quais o propósito da divulgação poderia ser alcançado por outros meios, se a divulgação resultasse em prejuízo financeiro ou contratual ao poder público ou quando as informações já estavam disponíveis publicamente.

No Brasil, decisões analisadas mostram que o STF e a CGU entendem haver interesse público na divulgação de dados pessoais pelo governo de importância histórica e/ou quando buscar: (i) transparência e *accountability* sobre gastos públicos e sobre o financiamento de campanhas eleitorais e candidatos a cargos eletivos, e (ii) eficiência na prestação de serviços

públicos. Isso pôde ser verificado, por exemplo, nas decisões sobre o compartilhamento de dados entre entes públicos, regulado pelo Decreto nº 10.046/2019, e sobre a publicação de salários de servidores públicos, de dados de beneficiários de programas sociais e de critérios para a promoção funcional de servidores públicos. Nessas situações, considerando-se as particularidades do caso concreto, se reconheceu que os benefícios sociais da divulgação seriam suficientes para justificar uma limitação à privacidade e proteção de dados pessoais, desde que adotadas medidas para mitigar eventuais riscos (note-se que, somente nos julgamentos realizados após a edição da LGPD, a efetividade das salvaguardas adotadas foi considerada como fator relevante na determinação sobre o interesse público na divulgação).

Por outro lado, se a divulgação resultar afronta a norma ou a determinações contratuais de confidencialidade (e.g., decisão sobre membros de bancas avaliadoras e sobre documentos armazenados em arquivos públicos), em riscos elevados à privacidade e/ou as salvaguardas propostas não forem consideradas satisfatórias (e.g., decisões sobre divulgação de dados do Inep), o teste de proporcionalidade pendeu em favor da restrição de acesso aos dados (e.g., decisão sobre envio de dados pelo Denatran à Abin). Esse foi o caso das decisões sobre divulgação de membros de banca examinadora de concurso público, de microdados sobre o sistema de ensino, e de comunicações estabelecidas entre a embaixada do Brasil no Egito e o MRE. Nesses casos, o sigilo ou confidencialidade eram destinados a assegurar confiança aos cidadãos sobre a privacidade de suas informações, de modo que a sua inobservância afrontaria a legítima expectativa dos titulares de dados sobre como eles seriam utilizados. No entanto, é possível que regras de sigilo ou de confidencialidade sejam irregulares, podendo ser afastado por autoridade competente.

Como se verifica, há nas decisões brasileiras semelhança em relação ao entendimento de autoridades do Canadá e do Reino Unido, segundo os quais haverá interesse público na publicação e no compartilhamento de dados pessoais por governos em casos de fomento ao ***accountability***, à **participação social** e **proteção do processo democrático**, à **tomada qualificada de decisão por órgãos públicos**, e à garantia do **melhor uso de dinheiro público**. Igualmente, não será de interesse público a informação de interesse para o público (em outras palavras, a informação obtida para fins de curiosidade). Pela experiência estrangeira, outras situações em que haveria interesse público na divulgação, a depender das particularidades do caso concreto, são a administração da justiça.

Outros aspectos identificados nas analisadas decisões proferidas pelo STF e pela CGU consistem na: (i) avaliação não aprofundada sobre a presença de dados pessoais no caso

concreto; (ii) à qualificação equivocada de certos dados pessoais como sensíveis e o entendimento de que não deverá haver divulgação de dados dessa natureza; (iii) pouca reflexão sobre a necessidade dos dados para o alcance da finalidade almejada ou sobre formas de concretizar a publicação ou o compartilhamento em observância à privacidade e proteção de dados pessoais.

Em relação ao primeiro aspecto, destacam-se decisões proferidas anteriormente à LGPD que apresentam imprecisão conceitual sobre o que qualificam dados pessoais. No caso, entendeu-se que a informação sobre despesas feitas por ocupantes de cargos públicos não seria dado pessoal. No entanto, nos termos da LGPD, esses dados serão pessoais se disserem respeito a uma pessoa natural identificável, mesmo que no exercício de atividade pública ou se tornadas acessíveis ao público. Isso não significa que esses dados não possam ser divulgados, mas que a divulgação deverá ocorrer em respeito às normas sobre privacidade e proteção de dados pessoais. Além disso, em outra situação, removeu-se acesso a bases de dados anteriormente publicadas em decorrência da constatação sobre a possibilidade de identificação dos dados. Nesse caso, para que se possa privilegiar eventual interesse público no acesso, faz-se necessário que o controlador avalie os riscos reais da divulgação e razoabilidade dos esforços necessários para a reidentificação dos dados.

Em relação ao segundo aspecto, foi possível identificar decisões (anteriores à LGPD) que qualificaram dados como sensíveis pelo simples fato de sua divulgação gerar riscos mais elevados à privacidade e proteção de dados pessoais. No entanto, são dados pessoais sensíveis apenas aqueles qualificados como tal pela LGPD, como a raça, religião e orientação sexual de uma pessoa. Além disso, a qualificação de um dado pessoal como sensível não impede sua publicação ou seu compartilhamento. Embora o tratamento de dados sensíveis tenha o potencial de gerar maiores danos aos titulares, nem todo tratamento desses dados imporá elevados riscos a direitos e liberdades de cidadãos.

Assim, não se deve pressupor que o tratamento realizado com dados pessoais sensíveis será sempre de elevado prejuízo ao titular de dados e, por consequência, tais dados não poderiam ser publicados ou compartilhados. A divulgação de certos dados pessoais sensíveis, a depender das particularidades do caso concreto, poderá ser qualificada como de interesse público. De todo modo, a análise sobre o interesse público na divulgação deverá ser mais rigorosa e os cuidados na divulgação serão mais rígidos. Interessante notar que esse mesmo entendimento foi identificado na experiência estrangeira. Por exemplo, no Reino Unido, a lista de finalidades que permite usar a base legal do exercício de função em benefício do

interesse público é mais detalhada (e menos flexível) em relação às finalidades que justificam o uso dessa base legal para dados triviais e exige a observância de maiores cuidados, a exemplo da necessidade de justificar o motivo pelo qual o consentimento não será a base legal mais adequada.

Finalmente, em relação ao terceiro aspecto, notou-se pouca reflexão sobre a necessidade dos dados e do tratamento para alcançar a finalidade almejada, assim como sobre a efetividade das salvaguardas adotadas para assegurar a privacidade e proteção de dados pessoais de cidadãos. Essa avaliação é de suma importância para: (i) a avaliação da proporcionalidade da divulgação e para que ela ocorra em observância à LGPD; (ii) a mais precisa ponderação entre os riscos e os benefícios a direitos e liberdades decorrentes do compartilhamento ou da publicação de dados mantidos pelo poder público. Esses cuidados também devem ser observados no momento da definição do escopo da divulgação (i.e., avaliação de finalidade e necessidade) e da divulgação de dados pessoais em observância à privacidade e proteção de dados pessoais (i.e., adoção de salvaguardas para mitigar os riscos do tratamento).

Determinado o interesse público na divulgação de dados pessoais, será necessário adotar procedimentos destinados a assegurar que os dados sejam divulgados e subsequentemente tratados em observância às normas de proteção de dados pessoais. Essa etapa envolve o estabelecimento de bases legais, a verificação da observância aos princípios de proteção de dados pessoais (na divulgação e nos possíveis usos subsequentes), garantia de direitos aos titulares de dados e a adoção de salvaguardas destinadas a reduzir os riscos inerentes à divulgação pretendida (por exemplo, o estabelecimento restrições contratuais ou a utilização de soluções tecnológicas para limitar o acesso e a manipulação de dados). A depender do caso concreto, também será necessário elaborar relatório de impacto à proteção de dados pessoais.[450]

[450] Por exemplo, ele será exigido quando o tratamento envolve: **(a)** riscos elevados a direitos de titulares, **(b)** perfilização ou tomada de decisão automatizada em casos nos quais há consequências jurídicas relevantes, **(c)** uso de grande quantidade de dados sensíveis, **(d)** monitoramento amplo e sistemático de locais públicos, ou **(e)** o compartilhamento sistemático de grande quantidade de dados. Assim, essa avaliação geralmente será realizada com o apoio de relatório de impacto, especialmente vista da grande quantidade de dados que órgão públicos possuem e porque, geralmente, o titular de dados **(i)** não possui escolha em fornecer seus dados; e **(ii)** tampouco tem a legítima expectativa de que seus dados serão utilizados por terceiros, públicos ou privados.

PARTE V O COMPARTILHAMENTO E A PUBLICAÇÃO DE DADOS PELO PODER PÚBLICO EM OBSERVÂNCIA À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS

15 ESTRUTURA DE GOVERNANÇA, GESTÃO DE RISCOS E TRANSPARÊNCIA

Após identificar que nas bases de dados ou arquivos que se deseja compartilhar ou publicar há dados pessoais cujo acesso atende ao interesse público, deverão ser adotados cuidados para assegurar a privacidade e a proteção de dados pessoais. Em outras palavras, não basta avaliar no caso concreto qual o escopo do interesse público, mas também, caso ele resulte no compartilhamento ou na publicação de dados pessoais, será necessário implementar medidas para assegurar a privacidade e proteção de dados pessoais dos cidadãos.

Mais precisamente, os cuidados a serem adotados para a publicação ou o compartilhamento de dados pessoais pelo poder público em observância à privacidade devem ser considerados desde a definição do escopo da divulgação e da avaliação sobre a existência de interesse público nessa atividade de tratamento de dados pessoais. De todo modo, após a análise sobre a presença do interesse público na divulgação, esses cuidados devem ser implementados como condição à legitimidade e legalidade da divulgação realizada.

Como mencionado, a legislação vigente não apresenta regras claras sobre como os governos podem publicar ou compartilhar dados pessoais em respeito à privacidade e à proteção de dados pessoais. Elas estão geralmente focadas em romper com paradigmas anteriores de sigilo ou burocracia governamental, ou preveem parâmetros gerais aplicáveis a qualquer atividade de tratamento de dados pessoais. Por essa razão, este e os próximos capítulos buscarão estabelecer parâmetros para a adoção dos referidos cuidados, tendo como base os exemplos internacionais estudados, e o disposto na LGPD e nas demais normas aplicáveis ao poder público, como a Lei de *Habeas Data* e a Lei de Acesso à Informação. Para tanto, pretende-se estabelecer diálogo entre a LGPD e as normas aplicáveis à divulgação de dados pelo governo.

Cumpre ressalvar que este e os seguintes capítulos não possuem a pretensão de esgotar todos os pontos de interface entre a LGPD e demais normas que regulam a atuação governamental. O objetivo será simplesmente apresentar balizas que devem ser consideradas quando da efetivação do compartilhamento ou da publicação de dados pessoais pelo poder

público. Além disso, como certas balizas estabelecidas pela LGPD já foram abordadas anteriormente nesta tese (e.g., princípios da finalidade e da necessidade), elas não serão novamente enfrentadas em maior profundidade. Por isso, a seguir serão abordadas obrigações relacionadas a governança, *accountability* e transparência, fundamentos legais para o tratamento de dados pessoais, direitos assegurados aos cidadãos enquanto titulares de dados pessoais, e salvaguardas a serem adotadas para mitigar os riscos decorrentes da publicação e do compartilhamento pelo poder público de dados pessoais de cidadãos.

15.1 Estrutura de governança para a proteção de dados pessoais

A LGPD recomenda aos agentes de tratamento de dados a adoção de programa de governança em que estabeleçam as responsabilidades e os procedimentos para assegurar que suas práticas serão realizadas segundo as exigências da lei. Essa determinação está em linha com boas práticas internacionais, na medida que a adoção de uma boa estrutura de governança pode contribuir para fomentar e fortalecer uma coordenada implementação de medidas técnicas e organizacionais para melhor controlar e gerenciar o ciclo de valor dos dados (OCDE, 2019).[451]

Entre as medidas de um programa de governança estabelecida conforme a LGPD estão a nomeação de um encarregado para atuar como canal de comunicação com indivíduos e autoridades, a observância de normas e padrões técnicos de segurança da informação, e a implementação de meios para que titulares exerçam seus direitos (art. 50). A governança adotada deverá também observar a escala, volume e sensibilidade das operações, e implementar políticas e salvaguardas baseadas em avaliação sistemática de impactos e riscos à privacidade, e estar devidamente registrada para que o controlador possa demonstrar, quando necessário, que suas atividades observam o disposto na lei.

No entanto, em vista das diferenças entre controladores de diferentes tamanhos e setores de atuação, e de forma a privilegiar medidas de auto regulação, a LGPD apenas apresenta regras gerais sobre o conteúdo e formato dos programas de governança. Assim, a lei não esclarece como as disposições sobre governança deverão ser implementadas pelo poder público, ainda que tais medidas sejam de extrema importância para a adoção de modelos de governo baseados no tratamento de dados pessoais. Como esclarece a OCDE (2019), a

[451] Além disso, a própria LGPD determina que a adoção de políticas de boas práticas e governança pode auxiliar na mitigação de sanções em casos de descumprimento à lei, o que figura como um incentivo adicional à sua implementação por parte dos agentes de tratamento de dados.

previsão de uma estrutura de governança por governos que desejam se orientar pelo uso de dados é imperativa e "pode ajudar a extrair valor dos ativos de dados, permitindo maior acesso, compartilhamento e integração aos dados no nível organizacional, além de aumentar a eficiência e a responsabilidade geral." (tradução nossa)

Diante disso, quando da entrada em vigor da LGPD, e diante da ausência de clareza a respeito dos contornos de programas de governança de entes públicos, a Secretaria de Governo Digital do Ministério da Economia (SGD) publicou o Guia de Elaboração de Programa de Governança em Privacidade,[452] a fim de auxiliar órgãos públicos na adoção de estrutura de governança e na sua adequação à LGPD.[453] No Guia, a SGD estabelece que a nomeação de encarregado deverá observar o art. 2º do Decreto nº 10.332/2020, que considera essa função como inerente a um Comitê de Governança Digital. Além disso, o Guia recomenda diversas práticas para a compatibilização da legislação de dados às particularidades de governos, tais como (i) o alinhamento de expectativas da alta administração do órgão; (ii) a avaliação de maturidade da organização[454]; (iii) a adoção de medidas de segurança; (iv) a elaboração de Inventário de Dados Pessoais, conforme modelo simplificado proposto pelos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP); e (v) e o levantamento de contratos públicos relacionados a dados pessoais.

Essas medidas estão alinhadas com o proposto pela OCDE (2019) em suas recomendações para a utilização responsável de dados por governos, o que envolve medidas como a adoção de: (a) estratégias nacionais que definem lideranças, expectativas e objetivos, (b) edição de normas e publicação de políticas que regulam estrutura, procedimentos, responsabilidades e técnicas para a proteção de dados pessoais, incluindo a nomeação de um encarregado de proteção de dados, e (c) treinamentos de pessoal e compartilhamento de conhecimento entre instituições. De fato, algumas dessas medidas já são adotadas pelo

---

[452] Vide: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaProgramaGovernanaemPrivacidade.pdf. Acesso em 24.04.2021

[453] Referidos materiais podem ser encontrados no seguinte link. https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd. Acesso em 10.01.2021.

[454] “, com o intuito de fornecer um diagnóstico do atual estágio de adequação à LGPD, trazendo subsídios para a formalização e cálculo de um índice de maturidade, oferece um questionário aos órgãos do SISP. Esse diagnóstico disponível no portal gov.br é uma versão de degustação e tem o propósito de auxiliar constantes medições do índice de maturidade do órgão ou entidade em relação à LGPD. Além de retratar o nível de adequação à LGPD, o índice de maturidade é também utilizado como um índice de performance e será apresentado na etapa de Monitoramento do PGP, item 2.3.1 deste Guia.” Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnostico-deadequacao-a-lgpd. Acesso em 02.05.2021.

governo brasileiro, a exemplo da publicação das estratégias de governo digital em 2016 e em 2020.

Entre as práticas que devem ser adotadas em um programa de governança, destaca-se a nomeação de um **encarregado** pela proteção de dados pessoais. Trata-se de medida de particular relevância, na medida em que o encarregado será o responsável por atuar como canal de comunicação com os titulares de dados e com a ANPD (art. 5º, VIII), além de possuir atribuições como: (i) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; (ii) receber comunicações da autoridade nacional e adotar providências; (iii) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e (iv) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (art. 41, §2º, I a IV). No entanto, a LGPD não estabelece parâmetros para a nomeação do encarregado ou características mínimas que deverão possuir. Por isso, a ANPD elaborou guia sobre o tema, no qual reforçou a necessidade de indicação de encarregados por agentes públicos ou privados, que poderão ser uma pessoa física ou jurídica, desde que dotado de liberdade na realização de suas atribuições, que deverão ser realizadas com eficiência (ANPD, 2022.1).

Além disso, a função do encarregado foi regulada, no âmbito dos órgãos e entidades do Sistema de Recursos de Tecnologia da Informação - SISP e, de forma geral, da administração pública federal direta, autárquica e fundacional pela Secretaria de Governo Digital do Ministério da Economia pelas Instruções Normativas (IN) nº 100/2020 e 117/2020. As Instruções estabelecem, especialmente, a necessidade de indicação, por cada autoridade máxima em seu respectivo órgão ou entidade do governo federal, de encarregado independente da estrutura interna de Tecnologia da Informação e com conhecimentos multidisciplinares a respeito de sua função, inclusive jurídicos e de gestão de riscos. A IN nº 117/2020 também enfatiza quais devem ser as atribuições e prerrogativas do encarregado, tais como acesso direto à alta administração, pronto apoio das unidades administrativas no atendimento das solicitações de informações e contínuo aperfeiçoamento relacionado aos temas de privacidade e proteção de dados pessoais.

Um segundo elemento relevante em programas de governança de dados pessoais consiste na elaboração de **políticas** que regulam e informam sobre como dados pessoais são tratados por determinado controlador (art. 50, I, *a* e *d*, LGPD). Elas possuem relevância tanto para fins de prestação de contas como para transparência sobre as atividades de tratamento.

De todo modo, essas políticas podem ser internas, para consumo por sujeitos como os funcionários ou prestadores de serviço do controlador, e serem destinadas a estabelecer regras, procedimentos, técnicas e responsabilidades para que suas atividades de tratamento sejam realizadas em conformidade com o disposto na legislação específica. Por outro lado, elas também podem ser externas, para consumo por titulares de dados, autoridades e outros possíveis interessados, e serem destinadas a esclarecer as finalidades e as condições das atividades de tratamento que realizam.

Outro aspecto central a um programa de governança, tal qual estabelecido pela LGPD em seu princípio de prestação de contas, consiste na elaboração pelo controlador de dados pessoais de **documentação de prestação de contas**. Entre suas principais funções estão: (i) registrar as atividades de tratamento de dados pessoais, (ii) detalhar as condições em que ocorre e as salvaguardas adotadas para reduzir possíveis riscos a direitos fundamentais de titulares de dados pessoais, e (iii) criar evidências capazes de demonstrar a adequação do tratamento à LGPD. Em outras palavras, a documentação de prestação de contas (também chamada de *accountability*) assume particular importância porque não somente atua como registro e detalhamento das atividades de tratamento, mas também como meio de comprovar a conformidade das atividades de tratamento com o disposto na legislação.

Essa atividade é comumente elaborada, em cumprimento ao art. 37 da LGPD, por meio do denominado de Registro de Operações de Tratamento (comumente referida como *Record of Processing Activities ou RoPA*), no qual se registram, entre outros, as atividades de tratamento realizadas, as suas finalidades, os dados envolvidos e o período de sua retenção, além das bases legais adotadas, os riscos existentes e as salvaguardas implementadas. No caso de compartilhamento de dados pelo Poder Público, a ANPD destaca que o registro das atividades de tratamento de dados pessoais deverá ocorrer em conjunto com as análises técnica e jurídica que motivaram o compartilhamento e a demonstração da aderência às normas de proteção de dados (ANPD, 2022.3).

Por sua vez, como será abordado adiante, no caso de diagnóstico de que o tratamento impõe risco elevado aos direitos e liberdades de titulares de dados, deverá ser elaborado **Relatório de Impacto à Proteção de Dados Pessoais** (ou RIPD) e, para as atividades de tratamento de dados fundamentadas na base legal de legítimo interesse, ser elaborado e registrado o teste de legítimo interesse, que na prática e por influência da experiência europeia, tem sido elaborado sob o formato e nomenclatura de LIA (*Legitimate Interest Impact Assessment*).

15.2 Prestação de contas e responsabilização

Como mencionado anteriormente, o compartilhamento e a publicação de dados pessoais pelo poder público deve ser realizado em observância aos princípios estabelecidos na LGPD (e.g.: finalidade, necessidade,[455] livre acesso, transparência,[456] segurança,[457] responsabilização e prestação de contas, e não discriminação), que deverão ser interpretados considerando as especificidades do tratamento de dados pessoais pelo poder público, especialmente à luz dos demais princípios e normas incidentes sobre as atividades exercidas pelo poder público - a exemplo dos princípios da legalidade, impessoalidade e publicidade (WIMMER, 2020). Alguns dos princípios centrais ao debate sobre divulgação de dados pelo poder público já foram abordados nesta tese, a exemplo dos princípios da finalidade e necessidade, e neste momento serão debatidos alguns aspectos do princípio de prestação de contas e responsabilização.

Segundo o princípio de prestação de contas, controladores e operadores de dados pessoais possuem o dever de adotar medidas e registros que demonstrem que suas atividades estão adequadas às exigências da legislação de proteção de dados pessoais. Esse princípio é central no desenho das mais modernas normas de proteção de dados pessoais, que são menos prescritivas a respeito das medidas específicas que devem ser adotadas e viabilizam ao controlador, com base nas particularidades das atividades de tratamento de dados que desenvolve, empregar salvaguardas proporcionais ao risco que efetivamente oferecem.

Segundo Bruno Bioni (2021), o princípio da prestação de contas, ainda que relacionado ao conceito de *accountability* constante da GDPR, se diferencia dele por ser mais prescritivo. O *accountability* seria compreendido como uma virtude do agente de tratamento

---

[455] Como mencionado anteriormente, o princípio da finalidade exige o tratamento de dados pessoais nos limites do informado aos seus titulares, sendo vedados usos posteriores para finalidades incompatíveis com aquelas informadas. Além disso, essa finalidade deverá estar respaldada em legislação vigente e de acordo com as legítimas expectativas dos titulares de dados. Ele está diretamente relacionado aos princípios da adequação e da necessidade, que requerem a compatibilidade do tratamento com as finalidades informadas ao titular e a limitação do uso de dados ao estritamente necessário para a realização dessas finalidades.

[456] É necessário também observar o princípio da transparência, que exige aos agentes de tratamento de dados a prestação de informações claras, precisas e facilmente acessíveis sobre o uso de seus dados, observados os segredos comercial e industrial. Essa prestação de informações é fundamental para que o titular possa compreender como seus dados são usados e como exercer direitos de forma mais qualificada.

[457] O princípio da segurança recomenda a adoção de medidas 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 difusão. Dialoga, por sua vez, com o princípio da prevenção, que se refere à adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Esses princípios, conjuntamente com o princípio da prestação de contação de contas, são essenciais para assegurar o que se chama de privacy by design, que consiste na adoção de medidas técnicas e organizacionais para assegurar proteção de dados desde a concepção de um projeto.

que consegue colocá-lo em prática, mas não como gerador de vínculo obrigacional dinâmico estabelecido com os titulares de dados. Já a prestação de contas prevista na LGPD seria um mecanismo ou ferramenta de adoção exigida aos agentes de tratamento de dados para demonstrar sua conformidade com o disposto na legislação. Por isso, o princípio da prestação de contas seria uma obrigação de demonstração de que o agente de tratamento de dados adotou, previamente à utilização dos dados pessoais, medidas eficazes e capazes de comprovar a observância das normas de proteção de dados pessoais.

De todo modo, tanto o *accountability* quanto a prestação de contas buscam assegurar aos agentes de tratamento flexibilidade e autonomia na avaliação dos riscos e implementação de medidas de mitigação impostas pelas suas atividades de tratamento. Ao mesmo tempo em que exige ao agente de tratamento a adoção de medidas capazes de demonstrar que suas práticas estão em conformidade com a legislação, não estabelece balizas rígidas para a avaliação de risco e proposição de medidas de mitigação. Com isso, a legislação buscou assegurar porosidade e atualidade de suas disposições ao desenvolvimento de novas tecnologias e, com isso, não se colocar como instrumento que impede ou retarda a inovação e o desenvolvimento tecnológico no país. Essa proposta normativa está em linha com os objetivos da LGPD, entre os quais destaca-se o desenvolvimento econômico e tecnológico e a inovação (art. 2º, V). Em contrapartida a esse espaço de autonomia para os agentes de tratamento atuarem, eles se incumbem do ônus de prestar contas e demonstrar a observância das prescrições da LGPD.

Já o princípio da responsabilização está relacionado à possibilidade de fiscalização sobre o cumprimento das normas de proteção de dados pessoais pelo controlador, inclusive tendo em vista a eficácia das medidas adotadas. Assim, os princípios da prestação de contas e da responsabilização, embora estejam situados no mesmo dispositivo da LGPD (art. 5º, X) e possuam finalidade precípua relacionada, consistente em assegurar e comprovar a adoção pelos agentes de tratamento de medidas para a proteção de dados pessoais tratados, possuem lógicas distintas.

De um lado, a prestação de contas está associada à lógica *ex ante* de regulação de proteção de dados, na medida em que exige a avaliação prévia sobre os riscos resultantes da atividade pretendida, de forma a prevê-los, evitá-los e mitigá-los com antecedência. De outro lado, o princípio da responsabilização está atrelado a noções mais tradicionais de responsabilidade civil, em que se realiza o controle da atividade após o cometimento do ato lesivo e destinado à reparação de danos. Portanto, os princípios de prestação de contas e de

responsabilização, em conjunto, atuam para viabilizar autonomia e flexibilidade aos agentes de tratamento, ao mesmo tempo em que se protege a privacidade de indivíduos.

Tal como os demais princípios da LGPD, a prestação de contas e a responsabilização também incidem sobre as atividades de tratamento de dados pessoais realizadas por entes públicos, de forma que o compartilhamento e a publicação de dados pessoais deverão ser precedidos da adoção de medidas destinadas a registrar seus contornos, avaliar os riscos que oferece aos titulares de dados e demonstrar como as salvaguardas propostas mitigam esses riscos. Como mencionado, essa função poderá ser realizada em RoPAs, LIAs e/ou RIPD, a depender das características da atividade de tratamento.

Análise de riscos e elaboração de Relatório de Impacto à Proteção de dados

O **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)** consiste entre os principais mecanismos documentais previstos pela LGPD para que o controlador avalie e demonstre a conformidade entre o determinado na lei e o tratamento de dados concretamente realizado.[458] Segundo a LGPD, ele deve descrever os processos de tratamento que podem gerar elevados riscos às liberdades civis e aos direitos fundamentais dos titulares de dados, assim como as medidas, salvaguardas e mecanismos de mitigação dos riscos identificados (arts. 5º, XVII e 38). Assim, o RIPD é uma dentre as ferramentas para demonstrar adequação ao princípio de prestação de contas, e acaba por contribuir para o desenvolvimento de uma cultura de governança de proteção de dados pessoais (GOMES, 2019).

No entanto, a LGPD não esclarece o que são atividades de elevado risco a liberdades civis e a direitos fundamentais dos titulares de dados e também não delimita as características mínimas desses relatórios. Na verdade, certos autores argumentam que a LGPD não prevê obrigação legal de elaboração do RIPD, mas que atribui à ANPD a competência de estabelecer diretrizes para auxiliar na determinação de quando sua elaboração será necessária e a faculdade de requerer sua elaboração em situações específicas (GOMES, 2019).

Por isso, em junho de 2021, a ANPD organizou reuniões técnicas para discutir parâmetros regulatórios do RIPD e, posteriormente, editar regulamento que oriente os agentes

[458] A elaboração de relatórios de impacto como mecanismo de mitigação de riscos era prevista na Diretiva 95/46/EC, que previa o *Privacy Impact Assessment* como ferramenta de boa prática no cumprimento das obrigações de proteção de dados. Por sua vez, a GDPR apresentou uma nova versão de relatório com maior precisão sobre os casos concretos em que era mandatória a sua elaboração, conhecido como *Data Protection Impact Assessmen*t (WP 29, 2016).

de tratamento na elaboração do relatório nos casos em que ele for necessário.[459] Para tanto, as reuniões técnicas discutiram perguntas como: (i) deverá a ANPD estabelecer uma metodologia que deverá ser seguida para a elaboração do RIPD?; (ii) quais os elementos mínimos que um RIPD deverá conter?; e (iii) em quais circunstâncias e condições os RIPDs elaborados por governos deverão ser publicados? [460]

Em relação à metodologia de elaboração do Relatório de Impacto, os participantes das reuniões técnicas argumentaram em favor do reconhecimento pela ANPD da utilização de uma dentre as diversas metodologias existentes que se baseiam na análise de riscos (eg., COSO, SWOT, ISO 31000, FMA etc.), sem, entretanto, indicar um único método que deveria ser mandatório. Apontaram também que a abordagem baseada em riscos, ainda que não seja a única existente, é aceita por autoridades europeias de proteção de dados.[461] Quanto aos elementos mínimos que deverão estar presentes no relatório de impacto, os participantes das reuniões técnicas concordaram que deverá conter, ao menos: (i) descrição das atividades de tratamento, seu contexto e objetivos, e metodologias adotadas na sua execução, (ii) análise sobre a necessidade do tratamento, os riscos que oferece e medidas para sua mitigação; e (iii) identificação e justificação da base legal utilizada para o tratamento. No que diz respeito aos RIPDs elaborados pelo poder público, os participantes reconheceram que deverão ser publicados porque as atividades realizadas pelo poder público têm uma presunção de transparência, nos termos da LAI e do art. 23 da LGPD.[462]

Quando da elaboração desta tese, a ANPD ainda está avaliando essas e outras contribuições apresentadas e elaborando materiais (e/ou editando consultas públicas sobre novos atos normativos) para regular o tema. De todo modo, a despeito desse momento inicial em que se encontra o debate sobre como e em quais condições elaborar um RIPD, entende-se que, para determinar a necessidade de se elaborar relatório de impacto, o controlador poderá antes elaborar um RoPA para identificar os riscos decorrentes do tratamento e apontar o seu nível de risco. Considerando que, como se abordará adiante, o compartilhamento e a

---

[459] Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em 04.01.2023.

[460] As gravações das reuniões estão disponíveis no Youtube da ANPD. Um resumo dos principais pontos defendidos pode ser encontrado em GARROTE, Marina Gonçalves *et al*. ANPD na regulamentação do Relatório de Impacto à Proteção de Dados Pessoais. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/anpd-relatorio-impacto-protecao-dados-pessoais-13072021. Acesso em: 27.10.2022.

[461] Como explicou Maria Cecília Oliveira, há também outras abordagens disponíveis, a exemplo da baseada na avaliação de riscos e benefícios e da baseada em direitos

[462] O mesmo não se aplica, todavia, a entidades privadas, especialmente diante da proteção de segredo comercial e industrial.

publicação de dados pessoais mantidos pelo poder público poderão ser considerados como atividade de tratamento de elevado risco, especialmente diante da mais frágil legítima expectativa do titular sobre o reuso de dados fornecidos ao Estado de forma mandatória ou como condição de acesso a direitos, muitas vezes será necessário ao poder público elaborar relatório de impacto para essas atividades de tratamento. A ANPD reforça esse entendimento ao argumentar que, se a coleta de dados é obrigatória e sua eliminação não seja possível, devem ser adotadas medidas de mitigação que podem ser registradas em RIPD (ANPD, 2022.3).

Diagnosticado o elevado risco a direitos e liberdades dos titulares de dados, o controlador deverá registrá-lo no relatório de impacto, no qual o órgão ou entidade pública deverá descrever o contexto do tratamento (e.g., quem são os titulares de dados, qual a natureza dos dados e as condições da coleta), avaliar a necessidade, proporcionalidade e interesse público do tratamento, identificar seus riscos e benefícios, e apontar as salvaguardas propostas para mitigar esses riscos. Importante destacar que a obrigação de elaboração de relatório de impacto não poderá atuar como uma barreira ou elemento de atraso na publicação ou no compartilhamento de dados pessoais pelo poder público em casos nos quais houver interesse público (como se verifica, por exemplo, com os microdados do Inep, que foram removidos até que o RIPD e outras medidas destinadas à proteção de dados pessoais fossem implementadas pelo Ministério da Educação).

De todo modo, esse relatório poderá ser publicado posteriormente, como uma forma de cumprir com o princípio de transparência e de assegurar meios para *accountability* social sobre como dados pessoais são tratados por determinados órgãos ou entidades públicas. A ANPD corroborou com esse entendimento em Nota Técnica sobre a divulgação pelo Inep de microdados referentes ao Enem e ao Censo Escolar: "[a publicação do RIPD] contribui para ampliar a transparência dos critérios adotados e considerados pelo Inep para fundamentar a sua decisão" (ANPD, 2022.5). No entanto, não é possível exigir a publicação da integralidade do relatório, especialmente em casos nos quais a atividade é protegida por normas de sigilo ou cláusula de confidencialidade, ou quando a divulgação afrontar segredos comerciais ou industriais, de entidade pública ou de particulares.

Avaliação sobre o risco do compartilhamento ou da divulgação

Com vistas a assegurar aos controladores mais flexibilidade e autonomia na adoção de medidas destinadas ao tratamento de dados pessoais (e reconhecendo que o tratamento de

dados pessoais em geral costuma implicar algum nível de restrição ao direito à privacidade de indivíduos), a LGPD adotou a abordagem regulatória de risco. Isso significa que a legislação atribuiu aos controladores a função de calibrar, no caso concreto, riscos e salvaguardas do tratamento de dados pessoais que se pretende realizar. Com isso, evita-se proibir *ex ante* certas atividades de tratamento e permite-se espaço para a inovação e geração de benefícios sociais.

De todo modo, a LGPD estabelece que atividades avaliadas pelos controladores como sendo de alto risco exigirão cuidados adicionais e poderão, inclusive, resultar em sanções mais elevadas no caso de descumprimento do disposto na lei. A despeito disso, a LGPD não apresenta critérios para a avaliação do risco no caso concreto, limitando-se a informar que eles são associados ao exercício de liberdades civis pelos titulares de dados, como a liberdade de pensamento, liberdade religiosa, liberdade de expressão e liberdade de associação (GOMES, 2019). Sabe-se, todavia, que consiste em uma avaliação contextual, que exige a identificação no caso concreto das condições em que o tratamento de dados pessoais ocorre.

Em linha com esse entendimento, a ANPD publicou a Resolução CD/ANPD nº 02/2022,[463] destinada a regular as atividades realizadas por agentes de tratamento de pequeno porte, em que apresenta método para a identificação, com base nas características do caso concreto, de atividades de tratamento de alto risco (art. 4º). Para tanto, deverão ser considerados, de forma cumulativa, os critérios qualificados como: (a) gerais, que envolvem o tratamento em larga escala[464] ou que possam afetar significativamente interesses e direitos fundamentais dos titulares;[465] e (b) específicos, que consistem no uso de (b.1) tecnologias emergentes e inovadoras, (b.2) vigilância ou controle de zonas acessíveis ao público, (b.3) utilização de dados sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos, e (b.4) decisões tomadas unicamente com base em tratamento automatizado de dados pessoais.

Ou seja, para que um tratamento de dados seja considerado como de elevado risco, ele deverá cumular situações previstas como requisitos gerais e como requisitos específicos. Por meio dessa metodologia, a ANPD reconhece que fatores isolados (e.g., tratamento de dados

[463] Vide: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em 31.12.2023.

[464] O tratamento de larga escala será aquele que "[...] abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado" (art. 4º, § 1º).

[465] O tratamento de que possa afetar significativamente interesses e direitos fundamentais será aquele que "dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade" (art. 4º, § 2º).

de crianças ou a utilização de tecnologias emergentes e inovadoras) não qualificam, *per se*, atividade de tratamento de alto risco, sendo necessária sua cumulação com outros elementos do caso concreto (e.g., o tratamento em larga escala de dados de crianças será de elevado risco). No entanto, os critérios estabelecidos pela ANPD (com especial destaque ao conceito de tratamento de dados em larga escala) impõem consideráveis dificuldades, especialmente para o tratamento de dados pessoais pelo poder público.

Considerando que governos mantêm dados sobre todos os cidadãos brasileiros (e de estrangeiros residentes no país) e que fazem isso por período prolongado, será recorrente a qualificação de suas atividades enquanto tratamento em larga escala. Com isso, já se cumpre um dos requisitos para que o tratamento seja considerado de alto risco, bastando, para tanto, a presença de alguma das situações qualificadas como critérios específicos (e.g., tratamento de dados de adolescentes ou idosos).

De todo modo, caso esse seja efetivamente o critério a ser adotado pela legislação brasileira, a qualificação do tratamento como de alto risco é relevante essencialmente para fins de cumprimento com as obrigações previstas na LGPD, como a necessidade de o controlador elaborar relatório de impactos ou de notificar a autoridade de proteção de dados pessoais em casos de incidentes de segurança da informação. A eventual qualificação de uma atividade como sendo de elevado risco **não** leva o resultado do teste de proporcionalidade a concluir que o interesse público resulta necessariamente na restrição de acesso a dados pessoais. Em outras palavras, será possível publicar ou divulgar dados pessoais em casos de tratamento de dados qualificado pela ANPD como de alto risco, desde que presente o interesse público e adotadas salvaguardas efetivas. Caso contrário, o interesse público na divulgação de dados seria consideravelmente limitado (e.g., como a publicação de dados pessoais em portais de transparência podem ser qualificados como de larga escala e envolver dados sensíveis, essa atividade seria considerada de alto risco e não poderia ser realizada).

Para fins do teste de proporcionalidade, a avaliação dos riscos do compartilhamento e da publicação de dados pelo poder público, ainda que considere a qualificação de risco tal qual regulada pela ANPD (e.g., como/se essa atividade impacta negativamente direitos e liberdades de pessoas), deve contemplar também outros elementos. Por exemplo, deve-se observar não somente: (i) se o dado é sensível ou não, mas também avaliar a efetividade da técnica de anonimização adotada;[466] (ii) se o titular de dados é criança, adolescente ou idoso,

[466] Como argumentado anteriormente nesta tese, uma das primeiras medidas que devem ser adotadas quando da determinação sobre a publicação ou o compartilhamento de dados pelo poder público consiste em

mas também se encontra-se em alguma situação de vulnerabilidade social ou econômica; (iii) se o tratamento é realizado para fins de vigilância em espaços públicos, mas também se poderá ter efeitos discriminatórios ilícitos ou abusivos. Para além disso, o resultado do teste de proporcionalidade deverá levar em consideração os benefícios da divulgação e a efetividade das salvaguardas adotadas. Caso o tratamento seja de elevado risco, mas os benefícios sociais da divulgação forem igualmente elevados e o controlador implementar salvaguardas capazes de reduzir esses riscos, será possível que o teste de proporcionalidade indique haver interesse público na divulgação qualificada pela ANPD como sendo de alto risco.

Finalmente, tendo em vista algumas das decisões analisadas nesta tese, serão realizadas breves considerações sobre o risco envolvendo dados sensíveis e dados de beneficiários de programas sociais. De um lado, destaca-se que nem sempre a divulgação de dados sensíveis será de elevado risco. De outro lado, ressalta-se que a situação de vulnerabilidade social do beneficiário de programa social deverá ser considerada como elemento de risco, de modo que a presença de interesse público na publicação de dados sobre essas pessoas dependerá da adoção de medidas adicionais para proteger seus direitos e liberdades.

De fato, muitas vezes a divulgação de dados pessoais sensíveis envolve riscos mais elevados a direitos e liberdades de cidadãos. Segundo conceitua a LGPD, dados sensíveis dizem respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (LGPD, art. 5º, II). A esses dados é assegurada proteção adicional pela LGPD, visto que poderão mais facilmente ser utilizados para finalidades discriminatórias ilícitas ou abusivas, ou porque os possíveis danos pelo seu uso inadequado poderão ser mais gravosos ao seu

---

compreender se esses dados são pessoais, identificados ou identificáveis. Caso os dados divulgados não sejam qualificados como dados pessoais, não será necessário observar todo o disposto na LGPD. Assim, na situação em que dados são publicados ou compartilhados dados em formato anonimizado, mas que venham a posteriormente ser identificados por terceiros, incidirão riscos sobre direitos e liberdades de titulares de dados decorrentes do seu tratamento sem os cuidados exigidos pela LGPD. Com isso, parte relevante da avaliação do risco na divulgação de dados por governos perpassa justamente pela avaliação das chances de os dados serem re-identificados. Para tanto, em relação à publicação dos dados, o órgão ou entidade pública deve ponderar elementos como: (a) se a divulgação de nova base de dados poderá contribuir para a re-identificação dos dados que já publicou ou compartilhou; e (b) como a divulgação dessa nova base de dados pode contribuir ou elevar os riscos identificados em relação à base de dados já publicada ou compartilhada (GREEN et al., 2017). Assim, a avaliação de riscos perpassa por compreender fatores externos à divulgação pontual que se pretende realizar.

titular.[467] No entanto, essa maior tendência de o tratamento envolvendo dados sensíveis resultar em elevados riscos a direitos e liberdades de indivíduos não significa que qualquer uso de tais dados será necessariamente qualificado como de elevado risco (ou que a divulgação qualificada pela LGPD e pela ANPD como de elevado risco não possa ocorrer). É possível que certo tratamento de dados sensíveis imponha menores riscos que outras atividades de tratamento de dados pessoais envolvendo somente dados triviais, a depender de fatores como quem são os titulares de dados e qual a finalidade do tratamento.

No que diz respeito à avaliação sobre quem são os titulares de dados, o risco poderá aumentar caso o tratamento seja realizado sobre dados de pessoas em situação de vulnerabilidade (e.g., crianças, pessoas com deficiência ou pessoas em situação de vulnerabilidade econômica). Especificamente em relação a beneficiários de programas sociais, por se encontrarem em situação de vulnerabilidade econômica e/ou social, certas atividades de tratamento realizadas com seus dados pessoais poderão reforçar afrontas existentes a seus direitos básicos e também permitir a prática de discriminação. Por isso, quando do tratamento de dados pessoais de indivíduos qualificados como beneficiários de programas sociais, o risco oferecido a seus direitos e liberdades poderá ser maior a depender do contexto do tratamento realizado. Note que situações de vulnerabilidade poderão decorrer de outras características do titular, como o pertencimento a certo grupo social, segundo identificadores diversos como raça, idade, escolaridade, renda, identidade de gênero e orientação sexual, religião, filiação partidária, entre outras classificações possíveis. A depender da forma como esses dados são utilizados quando da análise de bases de dados públicas, cuidados adicionais poderão ser necessários para assegurar que grupos ou indivíduos não serão particularmente prejudicados.

15.3 Assegurar transparência sobre o compartilhamento e a publicação de dados

Observadas as etapas de identificar qual a base legal mais apropriada para o tratamento de dados pessoais, e preventivamente avaliar e registrar que as atividades de tratamento de dados pessoais estão adequadas às exigências da legislação de proteção de dados pessoais, será necessário, antes mesmo de iniciado o tratamento de dados pessoais, promover medidas que assegurem observância ao princípio da transparência (LGPD, art. 6º, VI). Conforme será

[467] De fato, a ANPD vem reconhecendo essa maior probabilidade de o tratamento de dados pessoais sensíveis gerar riscos ou danos relevantes a titulares de dados, como se verifica em suas publicações sobre incidentes de segurança e sobre agentes de pequeno porte (2022.2). Vide: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em 04.03.2021.

demonstrado a seguir, trata-se de princípio essencial para a observância dos demais princípios, direitos e obrigações previstos nas normas de proteção de dados pessoais, na medida em que fornece aos titulares de dados, autoridades e outros possíveis interessados informações sobre como os dados são utilizados por determinado agente.

Para os titulares de dados, a informação é essencial para o exercício da autodeterminação informativa porque fornece substrato para a tomada de decisão consciente e voluntária a respeito de como dispor de seus dados pessoais, a exemplo da escolha pela utilização de determinado serviço e pela forma de exercício de seus direitos.[468] Sob essa perspectiva, o princípio da transparência possui viés preventivo, na medida em que antecede e municia a tomada de decisão em relação à disponibilização de dados pelo seu titular, e um viés de monitoramento ou repressivo, visto que permite ao titular de dados acompanhar a forma como seus dados são tratados e, eventualmente, solicitar a cessação destas atividades.

Para outros possíveis *players* - reguladores, pesquisadores, parceiros comerciais e jornalistas - o fornecimento de informações consiste em prestação de contas em relação às atividades desenvolvidas. Por exemplo, a transparência sobre como o controlador utiliza dados pessoais fornece elementos para que órgãos reguladores possam diagnosticar se empresas estão agindo com boa-fé e/ou em conformidade com a legislação, ou apresenta substrato para que pesquisadores avaliem a eficiência de determinados desenhos regulatórios (e.g., as políticas de privacidade efetivamente contribuem para a tomada de decisão do titular de dados a respeito da utilização de determinado serviço?).

Assim, nota-se que o princípio da transparência possui relação íntima com a boa-fé necessária ao tratamento dos dados pessoais, e com os princípios da finalidade, necessidade, livre acesso, responsabilização e prestação de contas. Isso porque ele é (i) destinado a promover informações para que o titular de dados possa melhor compreender, escolher e eventualmente questionar os usos atribuídos aos seus dados pessoais,[469] e (ii) instrumental para que os agentes de tratamento consigam demonstrar que suas operações são conduzidas de boa-fé e de acordo com as normas de proteção de dados pessoais.

---

[468] Esse aspecto do princípio da transparência foi ressaltado pelo Ministro Gilmar Mendes no Julgamento da ADI nº 6387 (julgamento em 07.05.2020), que avaliou a constitucionalidade da Medida Provisória nº 959/2020, que determinava às empresas provedoras de serviços de telecomunicação o dever compartilhar determinados dados pessoais de seus clientes ao IBGE. A ação foi julgada procedente por maioria (vencido o Ministro Marco Aurélio Mendes de Farias Mello).

[469] Working Party 29 Guidelines on Transparency under Regulation 2016/679. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227. Acesso em 21.06.2020.

Além disso, o princípio da transparência está relacionado à prestação de informações de forma abrangente, envolvendo a descrição sobre as práticas realizadas com dados pessoais, a explicação sobre quais são e como exercer os direitos de titulares de dados e a notificação sobre eventual incidente de segurança da informação. Essa pluralidade de funções, n LGPD, pode ser ilustrada pelos arts. 6º, VI (que qualifica o princípio da transparência) e 18, VII e VIII (que estabelece que determinadas informações são direitos dos titulares de dados) e 48 (estabelece o dever de notificação ao titular de dados quando houver determinadas modalidades de incidentes de segurança da informação), ou pelos arts. 8º e 10 da LAI (que prevêem a transparência ativa e passiva).[470]

Tendo isso em vista, cumpre esclarecer que neste tópico serão abordados essencialmente os primeiros dois aspectos desse princípio (dever de prestar informação e o fornecimento de informação como um direito dos titulares de dados), consistente no fornecimento ativo de informações sobre quais dados e em quais condições serão tratados. O aspecto do princípio da transparência relacionado à ocorrência de incidente de segurança da informação, embora crucial quando se aborda qualquer atividade de tratamento de dados pessoais realizadas pelo poder público - especialmente em vista das inúmeras e sucessivas ocorrências de incidentes com bases de dados governamentais -, não será abordado nesta tese porque não afeta diretamente o processo de decisão e execução da publicação ou compartilhamento de dados pessoais. Não se ignora que certas práticas irregulares de reuso de dados pessoais divulgados pelo poder público poderão ser qualificadas como incidente de segurança da informação que enseje deveres de notificação aos titulares de dados e autoridades - de fato, as medidas propostas nesta tese são, em algum grau, destinadas a evitar a ocorrência de tais incidentes -, mas entende-se que esse debate não se posiciona no cerne da resposta à pergunta de pesquisa.

Em relação às facetas ora abordadas do princípio da transparência, os agentes de tratamento deverão fornecer informações completas e adequadas sobre como usam dados pessoais, incluindo o compartilhamento de dados (LGPD, art. 18, VII), que deverá ocorrer em local de fácil acesso, em linguagem clara e de forma que permita a fácil compreensão pelo seu público-alvo (LGPD, art. 6º). No caso em que a base legal aplicável for o consentimento, o controlador deverá também informar o titular de dados sobre a possibilidade de não fornecer consentimento e as consequências decorrentes dessa escolha (LGPD, art. 18, VIII).

---

[470] Já na GDPR isso pode ser verificado de forma abrangente nos recitais, nº 39, 58 e 60 e nos arts. 12 a 22 e 34.

Interessante notar que esse dever de transparência ("fornecimento de informações adequadas e claras") já estava previsto no Código de Defesa do Consumidor (art. 6º, III) e foi um dos fundamentos para o reconhecimento de direitos relacionados a dados ao tratamento de dados pessoais de consumidores (MENDES, 2008). Esse direito foi posteriormente reconhecido pelo Marco Civil da Internet, que assegurou ao usuário da internet o direito de obter informações claras e completas sobre o tratamento de dados pessoais (art. 7º, VIII).[471]

Disso decorre uma série de desdobramentos práticos que passarão a ser abordados a seguir. *Primeiramente*, o comunicado deverá evitar termos técnicos e linguagem abstrata que permita divergência de interpretação. Mais que isso, deverá considerar o público-alvo do serviço, como é o caso de serviços destinados a crianças,[472] que deverá priorizar recursos linguísticos e visuais compreensíveis e de interesse desse público (LGPD, art. 14, § 6º), e considerar a inclusão de pessoas com determinadas modalidades de deficiências, caso em que recursos auditivos também podem ser desejáveis.[473]

Em *segundo lugar*, o conteúdo oferecido deverá permitir que o titular de dados tenha, de antemão, clareza sobre os tipos de riscos envolvidos no fornecimento e processamento de dados. A observância dessas exigências pelo poder público apresenta desafios próprios, como assegurar que qualquer cidadão tenha acesso e compreenda a informação, independente de fatores como classe social, acesso à tecnologia, escolaridade e idade. Além disso, será necessário assegurar que o agente público (ou *website* e aplicativo) esteja devidamente instruído para assegurar que o cidadão receberá e compreenderá, antes do fornecimento de dados, como eles serão usados pelo governo.

No mesmo sentido, quando dados pessoais forem compartilhados com outros controladores, o titular de dados deverá ser informado sobre essa divulgação de dados e as finalidades para as quais serão utilizados (LGPD, art. 9º, V) - lembrando-se que, em observância ao princípio da finalidade, esses usos devem ser compatíveis com aqueles que

---

[471] Inclusive, estabelece que o não cumprimento de parâmetros mínimos informacionais poderá resultar na nulidade do consentimento fornecido pelo titular de dados (cf. art. 7º, VII, o consentimento deverá ser livre, expresso e informado).

[472] Embora eventual consentimento, quando necessário, seja fornecido pelos representantes legais da criança, ela segue possuindo direitos de obter informações a respeito de como seus dados pessoais são utilizados. Essa afirmação possui respaldo no art. 13 da Convenção sobre Direitos de Crianças da ONU, disponível em: https://www.ohchr.org/en/professionalinterest/pages/crc.aspx. Acesso em 07.06.2020.

[473] O art. 12 da GDPR determina que o controlador deverá adotar medidas para o fornecimento de informações em forma concisa, transparente, inteligível, em formato de fácil acesso, em linguagem clara. Também determina que a informação deverá ser fornecida gratuitamente (salvo nos casos em que o exercício de direitos é realizado pelo titular de dados de forma abusiva), de forma escrita ou outras formas e, quando apropriado, em formato eletrônico. Além disso, é recomendável a disponibilização de ícones padronizados e legíveis por máquina, com vistas a fornecer informações de forma fácil, inteligível e facilmente legível.

justificaram a sua coleta. Além disso, eventuais mudanças no tratamento de dados pessoais que resultem em alteração de finalidade e, especialmente, possam gerar algum prejuízo material ao titular de dados, devem ser devidamente refletidas na política de privacidade e devidamente informadas aos seus titulares (art. 8º, § 6º).

Em *terceiro lugar*, a informação deve ser facilmente encontrada e ser disponibilizada de forma a evitar fadiga informacional. Na prática, as informações podem ser fornecidas em política de privacidade, com apresentação de forma sistematizada e concisa das informações sobre como os dados são utilizados, e que deverá ser encontrada com poucos cliques do usuário no *site* ou aplicativo utilizado.[474] Essa solução permite maior detalhamento na descrição das atividades e facilita o acesso continuado a essas informações por quaisquer interessados, como o titular de dados, pesquisadores e autoridades. De todo modo, para compatibilizar a qualidade e quantidade de informação com a sua fácil compreensão, a política poderá ser divulgada em formatos distintos, inclusive com o auxílio de ferramentas técnicas, e ser complementada por outros recursos, destinados a traduzir o conteúdo da política para diferentes contextos de coleta de dados e de público-alvo.

As informações também podem ser reiteradas em recursos visuais diversos, como a disponibilização de vídeos, infográficos, banners e *pop-ups*. Por exemplo, um recurso cada vez mais utilizado são as *privacy-dashboards*, que oferecem ferramentas para que o usuário possa modular suas preferências em relação ao uso e compartilhamento de seus dados pessoais. Essa opção tem ganhado espaço por permitir soluções granulares de consentimento (no lugar de aceitar ou rejeitar qualquer atividade de tratamento de dados pessoais que exige o consentimento), além de estimular o titular de dados a engajar com as informações ao navegar na ferramenta e escolher suas preferências. Essa é a proposta da Lei de Governo Eletrônico, que recomenda a criação de plataformas com ferramentas de transparência e de controle do tratamento de dados pessoais (art. 25). Segundo a Lei, as ferramentas devem disponibilizar mecanismos para que cidadãos possam requisitar seus dados (art. 25, §1º) e informações sobre as fontes dos dados pessoais, a finalidade do tratamento e a indicação de outros órgãos ou entes com os quais houve o compartilhamento de dados (art. 25, §2º).

Também é necessário avaliar maneiras de fornecer informações em casos nos quais a coleta de dados não ocorre por meio de uma interface *online*, como é o caso da prestação de serviços físicos (e.g., lojas e repartições públicas) ou da instalação de dispositivos de IoT ou

[474] Por exemplo, é possível manter o link para a política de privacidade acessível no cabeçalho ou rodapé de todas as páginas do site e/ou nos primeiros resultados da aba de configurações do aplicativo.

câmeras de reconhecimento facial na infraestrutura urbana. Nesses casos, é possível que informações sejam fornecidas em formato físico, como papéis impressos ou divulgados em totens, oralmente quando da coleta do dado, ou por meio da disponibilização de URL ou Códigos QR próximos a sensores e outros dispositivos que realizam o tratamento de dados pessoais.

Em *quarto lugar*, os agentes de tratamento de dados pessoais deverão fornecer informações sobre: (i) a finalidade específica, forma e duração da atividade de tratamento de dados pessoais, respeitado o segredo industrial; (ii) identificação e informações de contato do controlador, bem como as responsabilidades dos agentes de tratamento de dados pessoais; (iii) informações prévias, claras e inequívocas sobre o uso compartilhado de dados pelo controlador; e (iv) os direitos dos titulares de dados pessoais, conforme definidos pela LGPD - nos casos em que o tratamento de dados for essencial para o fornecimento de produto ou para o exercício de direito, essa informação deverá estar destacada[475]-[476].

Finalmente, essa disponibilização deverá ocorrer de forma gratuita - salvo quando impuser prejuízos para o controlador - e preferencialmente por escrito (quando solicitado pelo titular de dados, pode ser via oral) e/ou eletronicamente.

No caso do poder público, esse princípio é reforçado em vista de sua interface com o direito fundamental de acesso à informação (art. 5º, XXXIII) e com o princípio da publicidade dos atos administrativos (art. 37). Disso decorre que todo cidadão possui o direito de obter informações provenientes de órgãos públicos, salvo em hipóteses prescritas em lei, e que os órgãos públicos possuem o dever de ativamente publicizar dados e informações a respeito de sua atuação. Como consequência, determinações sobre transparência constantes de leis como a LAI e a Lei nº 13.460/2017 (sobre direitos do usuário de serviços públicos), também se aplicam igualmente às atividades realizadas que envolvem o tratamento de dados pessoais

[475] O art. 13 da GDPR determina que o controlador deverá, quando da coleta de dados, informar o titular de dados **(i)** a identidade e informações de contato do controlador e do encarregado de proteção de dados, **(ii)** as finalidades e bases legais aplicáveis ao tratamento de dados (quando aplicável, o legítimo interesse que fundamenta a utilização dessa base legal), **(iii)** os recipientes ou categorias de recipientes dos dados pessoais, **(iv)** o intuito do controlador em transferir dados internacionalmente. Além disso, quando o dado for obtido, o controlador deverá também informar sobre **(v)** o período que o dado pessoal será armazenado ou os critérios para determinar esse período; **(vi)** o direito de solicitar o exercício de seus direitos enquanto titular de dados pessoais; **(vii)** o direito de peticionar perante autoridades competentes, e **(viii)** a existência de tratamento automatizado de dados pessoais, incluindo profiling, bem como as consequências que esse tratamento poderá impor ao titular de dados.

[476] O art. 14 da GDPR prescreve como deverá ser observado o princípio da transparência quando o dado não foi obtido diretamente do titular de dados, consistente em fornecer informações similares àquelas fornecidas quando o dado é coletado do titular de dados, além de informar, quando cabível, se os dados foram adquiridos de fontes acessíveis publicamente. A prestação dessas informações será dispensada em algumas situações, como a prestação da informação for impossível ou exigir esforço desproporcional.

mantidos pelo poder público. Isso significa que a própria legislação de transparência exige ao poder público a divulgação em seu *site* da internet, de informações sobre como informações de cidadãos são utilizadas.

Tal conclusão possui respaldo na descrição feita pela LAI sobre quais informações são submetidas ao dever de transparência (art. 7º), que são aquelas: **(i)** contidas em registros ou documentos, produzidos ou acumulados por seus órgãos ou entidades, recolhidos ou não a arquivos públicos; **(ii)** produzida ou custodiada por pessoa física ou entidade privada decorrente de qualquer vínculo com o poder público, mesmo que o vínculo tenha se encerrado; **(iii)** primária, íntegra, autêntica e atualizada; **(iv)** sobre atividades exercidas pelo governo, inclusive as relativas à sua política, organização e serviços; **(v)** sobre administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos; **(vi)** sobre a implementação, acompanhamento e resultados dos programas, projetos e ações dos órgãos e entidades públicas, bem como metas e indicadores propostos; e **(vii)** sobre o resultado de inspeções, auditorias, prestações e tomadas de contas realizadas pelos órgãos de controle interno e externo, incluindo prestações de contas relativas a exercícios anteriores.[477]

Igualmente, a Lei nº 13.460/2017 estabelece que os serviços públicos e o atendimento do usuário serão realizados segundo o princípio da transparência (art. 4º) e que são direitos do usuário o acesso e obtenção de informações sobre a sua pessoa (art. 6º, III) e a obtenção de informações precisas e de fácil acesso sobre os serviços prestados (art. 6º, VI e art. 7º). Do mesmo modo, como mencionado, a Lei nº 14.129/2021 (sobre governo digital) possui entre seus princípios a transparência sobre a execução de serviços públicos (art. 3º, IV) e o uso de linguagem clara e compreensível a qualquer cidadão (art. 3º, VII). A lei também exige às plataformas de governo digital, como mencionado, oferecer ferramentas com informações sobre o tratamento de dados pessoais (art. 25). Além disso, reforça e incrementa obrigações da LAI de publicar bases de dados em formato legível por máquina sobre, entre outros, licitações e contratos realizados pelo poder público (art. 29, §2º, V) e inventário de bases de dados produzidos e geridos pela administração pública (art. 29, §2º, XI).

[477] Em relação à LAI, ela também determina que os órgãos e entidades públicos deverão divulgar ativamente, em local de fácil acesso no seu *site* na internet, informações como **(a)** dados gerais para o acompanhamento de programas, ações, projetos e obras; **(b)** registro de competências, endereços e telefones de suas unidades e horários de atendimento ao público; e **(c)** informações sobre procedimentos licitatórios e sobre contratos celebrados (art. 8º). Essas e outras informações devem ser constantemente atualizadas, estar em linguagem de fácil compreensão, e ser divulgadas de forma aberta, não proprietária, estruturada, em diversos formatos eletrônicos, de forma a ser legível por máquina e permitir o acesso automatizado.

Como se verifica, no escopo do dever de transparência governamental estão atividades que envolvem o tratamento de dados pessoais, como a confecção e o armazenamento de registros públicos (que podem possuir dados como nome, data de nascimento e biometria); o processamento, pelo governo ou por particular, de dados para prestação de serviços públicos (como a coleta dados de bilhetagem para o fornecimento de serviços de transporte público); o tratamento de informações para a execução e acompanhamento de programas sociais (como os dados para controle e fiscalização de beneficiários do bolsa família), entre outros.

Disso decorre, ao menos, a obrigação na divulgação sobre a ocorrência de atividades de tratamento de dados pessoais, pelo governo e/ou por particulares; a publicação dos contratos que envolvem o compartilhamento de dados pessoais (G2G, G2B ou B2G); bem como a designação e formas de contato do controlador e do encarregado pela proteção de dados. Além disso, caso informações a respeito de atividades de tratamento de dados pessoais não sejam disponibilizadas ativamente, o cidadão poderá encaminhar pedido de acesso à informação, que deverá ser respondido pelo órgão ou entidade pública dentro do prazo de 20 (vinte) dias, prorrogável por mais 10 (dez) dias mediante justificativa (LAI, art. 11).[478]

Note-se, portanto, que o dever de transparência pelo poder público não se restringe a publicar políticas de privacidade sobre o uso de *cookies* em *websites* e aplicações de dispositivos móveis. De fato, a publicação de tais documentos - como feito pelo Departamento de Estado dos Estados Unidos,[479] pelo Governo do Reino Unido,[480] e pela província de Ontário[481] - é considerada uma boa prática. No entanto, como demonstrado ao longo deste tópico, o dever de transparência sobre as atividades do poder público é mais amplo. Deverão ser fornecidas, em local de fácil acesso, informações claras e que sejam compreensíveis por qualquer cidadão a respeito de quais dados pessoais são tratados, para quais finalidades e em quais condições, além de apresentados os meios disponibilizados para o exercício de seus direitos.[482]

---

[478] Note-se que o pedido de acesso à informação possui semelhanças com o exercício de direitos de titulares, que serão mais detidamente abordados adiante. Na transparência passiva, o solicitante, mediante apresentação de simples identificação pessoal e sem necessidade de apresentar justificativa (LAI, art. 10, § 1º), poderá solicitar acesso às informações a respeito de determinada atividade de tratamento de dados pessoais e os agentes envolvidos (e.g., solicitação de acesso a contrato entre o Serpro e a Abin para o compartilhamento de dados pessoais de cidadãos brasileiros).

[479] Vide: disponível em: https://www.state.gov/privacy-policy/. Acesso em 06.11.2022.

[480] Vide: disponível em: https://www.gov.uk/help/privacy-notice. Acesso em 06.11.2022.

[481] Vide: disponível em: https://www.ontario.ca/page/privacy-statement. Acesso em 06.11.2022.

[482] Sobre o tema, vide pesquisa elaborada na Índia sobre políticas de privacidade em governos eletrônicos: https://onlinelibrary.wiley.com/doi/abs/10.1002/pa.2160. Acesso em 12.12.2022.

No entanto, como mencionado, essa transparência não deverá se limitar à publicação de política de privacidade. Ela deverá ser assegurada nas diversas instâncias de interação entre o poder público e cidadão, como em *pop-ups* de aplicativos de dispositivos móveis ou em informações prestadas por entrevistadores de candidatos ao recebimento de benefícios sociais. Outra forma de transparência consiste na criação de um portal contendo informações diversas pertinentes ao tratamento de dados pessoais, como a disponibilização de contratos com prestadores de serviços de armazenamento e processamento de dados, termos de parceria de compartilhamento de dados, listas descritivas e/ou com links para as bases de dados e documentos publicados em portais de transparência e dados abertos, políticas internas de tratamentos de dados, canal de contato do encarregado e Relatórios de Impacto.[483]

[483] Exemplos interessantes de implementação do princípio da transparência pelo poder público foram adotados pelo governo da província Canadense de British Columbia e pela autoridade de proteção de dados da Austrália (*Office of the Australian Information Commissioner*), que divulgaram materiais e políticas para auxiliar entes públicos desenvolverem suas funções na gestão da privacidade. A política elaborada pelo governo da província de British Columbia destaca a importância de se designar uma pessoa enquanto encarregada pela privacidade de uma entidade pública específica, de forma que haja publicidade sobre a existência dessa pessoa responsável e que ela possa ser apoiada pelos demais servidores na observância da legislação aplicável. Essa pessoa seria chamada de *Ministry Privacy Officers* (MPO) e teria competência de desenvolver políticas e procedimentos específicos da entidade para apoiar esta política e a conformidade com a lei. A política ainda estabelece o Escritório de Informação Corporativa e Gerenciamento de Registros (*Corporate Information and Records Management Office* - CIRMO), responsável por rever e atualizar a política anualmente em acordo com as contribuições dos MPO e outras partes interessadas. O CIRMO também deveria estabelecer e presidir uma Comunidade de Prática de Gerenciamento de Privacidade para facilitar o conhecimento, experiências e melhores práticas entre os profissionais de privacidade em todo o governo. Já a autoridade australiana publicou um documento para auxiliar outras entidades públicas da Austrália a estarem de acordo com a legislação de proteção de dados, como a nomeação de um encarregado com funções específicas de apoio a atividades relacionadas à privacidade,l a promoção de programas de educação e treinamento de privacidade, e o desenvolvimento de relatórios de impacto de privacidade para os casos em que o risco do tratamento daquela informação é elevado. Vide: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy, https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/resources/policies-guidelines/pmap_version_4.pdf e https://www.oaic.gov.au/privacy/privacy-for-government-agencies/privacy-code-checklist Acesso em 12.12.2022.

16 FUNDAMENTOS LEGAIS PARA O COMPARTILHAMENTO E A PUBLICAÇÃO DE DADOS

Para que sejam considerados legítimos, o compartilhamento ou a publicação de dados deverão estar fundamentados em legislação específica, observar as atribuições legais do ente público e estar contemplada em alguma das hipóteses legais para o tratamento de dados pessoais, observar a boa-fé e respeitar os princípios de tratamento de dados pessoais previstos na lei, como os já abordados princípios da finalidade, necessidade e transparência.[484]

Para o poder público, a existência de balizas legais para o desenvolvimento de suas atividades não é novidade (WIMMER, 2020). Ela está relacionada aos princípios da legalidade e da impessoalidade (art. 37, Constituição Federal), segundo o qual as condutas dos agentes públicos devem ser autorizadas pela ordem constitucional e pela lei (BINENBOJM, 2006). Esses princípios estão atrelados ao pressuposto democrático, no qual a lei aparece como uma representação da vontade do Poder Legislativo (eleito por expressão de soberania popular) e se impõe às atividades realizadas pelo administrador (BANDEIRA DE MELLO, 2007), que deverá se pautar pela busca do interesse social. Embora a legalidade administrativa inicialmente se pautou pela vinculação positiva,[485] segundo a qual somente seria permitido ao poder público realizar aquilo que a lei expressamente autoriza (atuação *secundum legem*), a evolução do papel do Estado[486] exigiu que sua compreensão fosse modificada para assegurar

---

[484] Essa exigência é similar ao determinado na legislação europeia, em que qualquer tratamento de dados deve ser lícito, transparente e observar a lealdade (Regulamento EU 2016/679 art. 5º, 1a). Nesse contexto, o tratamento lícito será aquele fundamentado em uma base legal específica - conforme será abordado em maiores detalhes a seguir - e não afrontar as normas vigentes no país. Já a lealdade significa que, mesmo nos casos em que é possível qualificar a atividade de tratamento de dados em uma base legal específica, ele deverá ser realizado de acordo com as legítimas expectativas dos titulares de dados e que não lhes promova prejuízo injustificável (ou seja, é possível que o tratamento ocorra em detrimento do titular de dados pessoais desde que seja justificável). A transparência, por sua vez, informar de forma clara e honesta ao titular de dados, desde o princípio, sobre os possíveis usos que serão atribuídos aos dados coletados. Ele é destinado a assegurar ao indivíduo algum grau de escolha sobre prosseguir com determinada atividade que envolva o tratamento de seus dados pessoais.

[485] Nas palavras de Bandeira de Mello (2014): "Em outras palavras, não basta a simples relação de não contradição, posto que, demais disso, exige-se ainda uma relação de *subsunção*. Vale dizer, para a legitimidade de um ato administrativo é insuficiente o fato de não ser ofensivo à lei. Cumpre que seja praticado com embasamento em alguma norma permissiva que lhe sirva de supedâneo."

[486] Odete Medauar (2016) explica esse contexto: "Embora permaneçam o sentido de poder objetivado pela submissão da Administração à legalidade e o sentido de garantia, certeza e limitação do poder, registrou-se evolução na ideia genérica de legalidade. Alguns fatores podem ser apontados, de modo sucinto. A própria sacralização da legalidade produziu um desvirtuamento denominado legalismo ou legalidade formal, pelo qual leis passaram, a ser vistas como justas por serem leis, independentemente do conteúdo. Outro desvirtuamento: o formalismo excessivo dos decretos, circulares e portarias, com exigências de minúcias irrelevantes. Por outro lado, com as transformações do Estado, o Executivo passou a predominar sobre o Legislativo; a lei votada pelo Legislativo deixou de expressar a vontade geral para ser vontade maiorias parlamentares, em geral controladas pelo Executivo. Este passou a ter ampla função normativa, como autor

maior liberdade à atuação administrativa, que passou a ser restringida pelos limites do direito e pelos princípios constitucionais (MEDAUAR, 2016).

Essa exigência é reforçada pela LGPD quando determina que o poder público somente poderá tratar dados pessoais para o atendimento de suas funções públicas, no atendimento do interesse público e com o objetivo de executar competências ou atribuições legais (art. 23). Assim, órgãos e entidades públicas somente poderão utilizar dados pessoais em observância ao princípio da legalidade e da impessoalidade, de forma que essa atividade deverá sempre ocorrer dentro dos limites do seu escopo de atuação estabelecido em lei.

A LGPD agrega a esse requisito, determinando que, para o tratamento de dados pessoais ser considerado legítimo, independente de ser realizado por agentes públicos ou privados, deve ser fundamentado em uma das bases legais, identificadas nos arts. 7º e 11 da LGPD. As bases legais previstas no art. 7º referem-se ao tratamento de dados pessoais triviais e as constantes do art. 11 são específicas para o tratamento de dados pessoais sensíveis. Essa diferenciação está entre as medidas apresentadas pela legislação para assegurar maior nível de proteção a dados e informações que poderão, caso utilizadas de forma não prevista e/ou desejada pelo titular de dados, lhe infringir maiores danos.

No entanto, há considerável similaridade entre as bases legais previstas para dados pessoais triviais[487] e sensíveis (i.e., quase todas as bases legais do art. 7º possuem equivalência com as bases legais do art. 11), mas com algumas limitações para o tratamento de dados pessoais sensíveis. Por exemplo, o art. 11 da LGPD não prevê entre as bases legais para o tratamento de dados sensíveis o legítimo interesse ou a proteção ao crédito, e prevê com restrição de alcance as bases legais de execução de políticas públicas e execução de contratos.

Para o poder público, a LGPD prevê base legal específica para determinadas atividades de tratamento de dados que realiza (a base legal de execução de políticas públicas), que deverá estar fundamentada em legislação específica. A despeito disso, a LGPD não esclarece se as demais bases legais são aplicáveis ao poder público, o que vem permitindo o surgimento de dúvidas, como: **(i)** o governo poderá se utilizar de todas as bases legais

---

de projetos de lei, como legislador por delegação, como legislador direto [...], como emissor de decretos, portarias e circulares que afetam direitos. Além do mais, expandiram-se e aprimoraram-se os mecanismos de controle de constitucionalidade de leis."

[487] Para fins desta tese, dados triviais serão os dados pessoais não qualificados como sensíveis. O termo foi extraído do Anteprojeto de Lei de Proteção de Dados Pessoais, mas não aparece no texto final da legislação.

previstas na LGPD ou apenas aquela constante dos art. 7º, III e 11, II(b)?; e **(ii)** o disposto no art. 26 da LGPD constitui uma base legal autônoma?

De imediato, destaca-se que, em relação às bases legais aplicáveis às atividades de tratamento realizadas pelo poder público, **o entendimento ao qual se filia esta tese é que o poder público poderá se utilizar de outras bases legais para além do art. 7º, III e do art. 11, II(b)**.[488]-[489] Ainda que as bases legais de cumprimento de obrigação legal ou regulatória e de execução de políticas públicas alcance grande parte das atividades realizadas por governos (TEFFÉ; VIOLA, 2020), outras bases legais podem ser igualmente aplicáveis, como a tutela da saúde (arts. 7º, IV e 11, II, f) ou a realização de estudos por órgão de pesquisa (arts. 7º, VIII e 11, II, c).

Corrobora esse entendimento o fato de que, no moderno entendimento sobre os contornos do princípio da legalidade, não é necessário que o ato administrativo esteja especificamente delineado pela legislação. Ao administrador é exigido que suas atividades tenham lastro no ordenamento jurídico e na Constituição Federal. Assim, ainda que as bases legais de execução de políticas públicas e de cumprimento de obrigação legal sejam as mais apropriadas para embasar o uso de dados pessoais pelo poder público - na medida em que exigem que a atividade esteja fundamentada em leis, regulamentos, contratos ou instrumentos congêneres -, é possível ao poder público fundamentar suas atividades de tratamento de dados em outras bases legais.

Outro fato que contribui para esse entendimento está na similaridade que as bases legais previstas na LGPD possuem com as exceções ao sigilo de dados pessoais previsto na LAI (BARROS; SILVA; SCHMIDT, 2019). Assim como a LGPD, a Lei de Acesso à Informação permite aos órgãos e entes públicos disponibilizar acesso a informações pessoais mediante consentimento da pessoa sobre quem elas se referem (art. 31, §1º, II) ou quando

---

[488] Nesse mesmo sentido se posicionou a Autoridade Nacional de Proteção de Dados Pessoais no guia que publicou sobre o tratamento de dados pessoais pelo poder público (2022). Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 08.06.2022.

[489] Segundo Miriam Wimmer (2019): "não é possível desconsiderar o fato de que a própria evolução da tecnologia poderá eventualmente ensejar o surgimento de relacionamentos menos formais e mais facultativos entre cidadãos e o Poder Público, ensejando a necessidade de invocação de outras bases legais para além daquelas especificamente direcionadas ao Estado. Consultas a informações públicas, realização de agendamentos e emissão de certidões já ocorrem por meio de aplicativos no telefone celular; órgãos públicos já possuem perfis em redes sociais, por meio dos quais interagem dinamicamente com cidadãos, por meio de "curtidas" e compartilhamentos de postagens; chatbots já são utilizados para recebimento de reclamações e denúncias. Em relacionamentos entre cidadão e Poder Público mediados pela tecnologia, pode eventualmente haver necessidade de coleta e tratamento de dados pessoais de formas não previstas textualmente em normas jurídicas".

essas informações forem necessárias para: (i) a prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico; (ii) a realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; (iii) o cumprimento de ordem judicial; (iv) a defesa de direitos humanos; ou (v) a proteção do interesse público e geral preponderante (art. 31, §3º). Não se argumenta aqui que as hipóteses do art. 31 da LAI possuem o exato mesmo escopo das bases legais previstas na LGPD. Há diferenças entre essas hipóteses legais, especialmente diante da inexistência de paralelo para as bases legais de legítimo interesse (LAI, art. 7º, IX), execução de contrato (LAI, art. 7º, V) e proteção de crédito (LAI, art. 7º, X) - o que, contudo, não invalida a possibilidade de realizar referida comparação.

De todo modo, a despeito da possibilidade de fundamentar atividades de tratamento de dados pessoais realizadas pelo poder público em qualquer das bases legais, as bases legais de execução de políticas públicas e de cumprimento de obrigação legal ou regulatória, serão as mais recorrentes porque a atividade de tratamento geralmente está fundamentada em suas atribuições legais. De todo modo, as demais bases legais devem ser utilizadas apenas excepcionalmente e somente quando o tratamento decorra de um relacionamento realizado de forma voluntária pelo cidadão (WIMMER, 2021).[490]

Além disso, diferentemente do posicionamento de Miriam Wimmer (2021), segundo o qual o art. 23 da LGPD "estabelece uma hipótese complementar para o tratamento de dados pelo Poder Público, ao acrescentar às previsões dos arts. 7º e 11 o objetivo de “executar as competências legais ou cumprir as atribuições legais do serviço público”,[491] esta tese entende que os arts. 23 e 26 da LGPD não constituem bases legais alocadas fora dos arts. 7º e 11, mas tão somente cuidados adicionais que deverão ser observados no tratamento de dados pelo

[490] Nas palavras de Miriam Wimmer (2021): "A prestação de serviços comerciais por empresas públicas atuando em regime de concorrência, por exemplo, é um caso claro em que a relação entre cidadão e Estado se dá de maneira voluntária e, não por acaso, a própria LGPD determinou que em tais hipóteses aplicam-se as regras dispensadas às pessoas de direito privado (art. 24). (...) Em síntese, quando determinada relação entre cidadão e Poder Público é verdadeiramente facultativa, poderia ser considerado legítimo o tratamento de dados fundamentado em outras bases legais, inclusive com base no consentimento livre e informado." De forma similar se posicionaram Ana Flávia Paiffer dos Santos, Isabela Canesin Dourado Figueiredo Costa, Leonardo Relvas dos Santos, Marinho Dembinski Kern, Yasmin Bewiahn Saba Relvas (2021).

[491] Segundo Miriam Wimmer (2019): "Conquanto não seja desarrazoado invocar, como base legal para o tratamento de dados pessoais pelo Poder Público, o “cumprimento de obrigação legal ou regulatória pelo controlador” (art. 7º, inciso II, c.c. art. 11, inciso II, alínea a), parece mais adequado buscar no art. 23 da LGPD, inserido no capítulo específico relativo ao Poder Público, uma base legal complementar: a de tratamento de dados pessoais com o objetivo de “executar as competências legais ou cumprir as atribuições legais do serviço público”, observando-se a finalidade pública e a persecução do interesse público."

governo.[492] Esta tese concorda com Chiara de Teffé e Mário Viola (2020) no sentido de que o rol de bases legais previsto nos arts. 7º e 11 da LGPD é taxativo.[493] Além disso, as bases legais previstas nos arts. 7º e 11 da LGPD já contemplam as atividades de tratamento cuja realização se busca garantir com esse entendimento de que o art. 23 da LGPD prevê bases legais adicionais para o tratamento de dados pessoais realizado pelo poder público (i.e.: cumprimento de obrigação legal ou regulatória e execução de políticas públicas). Esse é também o entendimento apresentado no Guia de Boas Práticas da CCGD, segundo o qual o tratamento de dados pelo poder público, ainda que limitado pelas hipóteses descritas nos arts. 23 a 26 da LGPD, deverá ser enquadrados em qualquer uma das bases legais descritas nos arts. 7 º ou 11, conforme caracterização do dado como pessoal ou pessoal sensível.[494]

Feitos esses esclarecimentos, a seguir serão apresentados os contornos das bases legais previstas na LGPD, mas com foco e destaque naquelas mais relevantes (ou alvo de maiores debates) para fins de tratamento de dados pessoais pelo governo, consistentes na: **(a)** existência de obrigação legal ou regulatória; **(b)** execução de políticas públicas, **(c)** consentimento; e **(d)** legítimo interesse.[495] A escolha por aprofundar essas bases legais se

---

[492] Nesse mesmo sentido se posicionou a ANPD no guia que publicou sobre o tratamento de dados pessoais pelo poder público (2022): "O tratamento de dados pessoais pelo Poder Público deve se amparar em uma das hipóteses previstas no art. 7o ou, no caso de dados sensíveis, no art. 11 da LGPD. Esses dispositivos devem ser interpretados em conjunto e de forma sistemática com os critérios adicionais previstos no art. 23, que complementam e auxiliam a interpretação e a aplicação prática das bases legais no âmbito do Poder Público, conforme será demonstrado." Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 06.08.2022.

[493] Nas palavras de Teffé e Viola (2020): "Entende-se que tanto o rol do Art. 7.º quanto o do Art. 11 são taxativos, sendo dotados de algumas hipóteses mais abertas e com certo grau de subjetividade (como, por exemplo, o legítimo interesse). [...] Contudo, entendemos que o tratamento de dados pessoais para tais atividades já estaria contemplado, em grande parte, nas hipóteses relativas ao cumprimento de uma obrigação legal (Art. 7.º, II, e Art. 11, II, "a"), já que a atuação da administração pública decorre de um mandamento legal, e ao tratamento e uso compartilhado de dados necessários à execução de políticas públicas (Art. 7.º, III, e Art. 11, II, "b").8 A previsão contida no art. 23 traria apenas requisitos adicionais e específicos para o tratamento de dados pessoais realizado por parte da administração pública, complementando a base legal selecionada no art. 7.º ou 11 da lei.

[494] Conforme a redação do Guia: "A LGPD autoriza, em seu art. 23, os órgãos e entidades da administração pública a realizar o tratamento de dados pessoais unicamente 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 as hipóteses de tratamento sejam informadas ao titular**." Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf. Acesso em 24.04.2021.

[495] Quando analisando o tratamento de dados pelo poder público, a ANPD também focou na avaliação das mesmas bases legais, como se verifica: "Considerando os questionamentos encaminhados à ANPD e as peculiaridades do tratamento de dados pessoais pelo Poder Público, bem como o previsto na Agenda Regulatória do biênio 2021-2022,6 a análise a seguir será limitada às seguintes bases legais: consentimento, legítimo interesse, cumprimento de obrigação legal e regulatória e execução de políticas públicas." Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf. Acesso em 24.04.2021. De forma similar fez o Ministro Gilmar Mendes no julgamento da ADPF nº 695: "Dentre as bases legais específicas, a LGPD estabelece duas matrizes centrais: o tratamento de dados (i) para a execução de políticas públicas e (ii) para a execução de competências legais do serviço público." Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15343579920&ext=.pdf. Acesso em 06.08.2022.

justifica principalmente porque as atividades realizadas por órgãos públicos, em vista do princípio da legalidade, devem atuar segundo autorizações previamente estabelecidas na legislação. A utilização pelo poder público das bases legais de cumprimento de obrigação legal ou regulatória, de execução de políticas públicas ou de execução de contrato estão, portanto, relacionadas ao seu dever de atuar em conformidade com o princípio da legalidade.[496]

Já as bases legais do consentimento e legítimo interesse serão abordadas por estarem entre as mais comumente utilizadas para fundamentar o reuso de dados divulgados pelo poder público. De um lado, o consentimento possui relevância histórica e possui a capacidade de assegurar aos titulares de dados maior autonomia sobre como seus dados são utilizados. De outro lado, o legítimo interesse é bastante utilizado por agentes privados por ser uma base legal coringa, que atribui maior flexibilidade ao controlador. No entanto, como se demonstrará, essas duas bases legais geralmente não são adequadas para fundamentar atividades de tratamento de dados realizadas pelo poder público.

Em relação às demais bases legais, ainda que elas sejam aplicáveis a atividades de certos órgãos ou entidades públicas (e.g., o tratamento de dados pessoais realizado para pesquisa desenvolvida por instituição de ensino pública ou necessários para procedimentos médicos realizados em hospitais públicos), não serão objeto de estudo detalhado nesta tese. Isso se dá porque elas são inerentes a determinados setores (e.g., pesquisa e saúde), que demandam análise e desafios próprios não necessariamente relacionados ao tema ora debatido.

16.1 Limites do consentimento no uso de dados mantidos por governos

A despeito de as bases legais de cumprimento de obrigação legal e de execução de políticas públicas serem as primeiras que vêm à mente quando se trata de atividades de tratamento de dados pessoais realizadas pelo poder público, a primeira base legal que será abordada neste capítulo será a do consentimento. Essa escolha se deve ao fato de que ela é a base legal mais conhecida (em leis mais antigas, é inclusive a única base legal), e objeto de grandes divergências a respeito de seu alcance e forma de obtenção, especialmente quando o controlador de dados pessoais é órgão ou entidade pública.

---

[496] Ainda que sem maiores explicações, essas foram as mesmas bases legais abordadas pela ANPD em seu guia sobre o tratamento de dados pelo poder público. Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 08.06.2022.

Na busca por assegurar aos indivíduos controle sobre como seus dados serão utilizados por terceiros, o consentimento esteve entre as primeiras ferramentas previstas pela doutrina e em leis de proteção de dados pessoais (MENDES; FONSECA, 2020). Como mencionado, o entendimento moderno do direito à privacidade assegura ao indivíduo a possibilidade de determinar como informações sobre si são comunicadas e utilizadas por terceiros (WESTIN, 1967). Para promover essa autonomia aos indivíduos, as primeiras leis de proteção de dados pessoais estavam fundamentadas no ideal de *"notice and consent"*, segundo o qual indivíduos devem receber informações claras a respeito das finalidades e condições em que seus dados são tratados para posteriormente poder escolher livremente se autorizam ou não a sua realização (SCHWARTZ, 2000). Assim, nesse modelo, a proteção de dados pessoais está atrelada ao paradigma do controle pelo indivíduo sobre como seus dados são utilizados por terceiros, e o consentimento aparece como o meio mais apto à materialização desse controle.[497]

No Brasil, antes da edição da LGPD, o consentimento era tido como a única forma de tratar dados pessoais de forma lícita, em vista do disposto no Marco Civil da Internet, e também por essa ter sido, até a edição da GDPR em 2016, uma tendência normativa em diversos países. De fato, o Marco Civil exigia que qualquer atividade de tratamento de dados pessoais fosse precedida de consentimento **expresso**, **livre** e **informado**[498] do titular de dados pessoais (art. 7º, IX), obtido de forma destacada das demais cláusulas contratuais.[499]-[500] Esse

---

[497] Nesse sentido se manifestou Laura Schertel Mendes e Gabriel da Fonseca (2020): "Sobretudo a partir da dita "terceira geração" de leis regulando o tema, essa convergência se deu em torno de bases teóricas e de fundamentos jurídicos calcados no consentimento: o paradigma do consentimento. Nesse contexto, o consentimento passou a ser utilizado para legitimar, justificar e alicerçar a proteção de dados pessoais. Sem se olvidar da variedade de importantes avanços relativizando a ênfase no consentimento como garantia de autonomia e de proteção do titular dos dados, não é forçoso afirmar que o seu protagonismo permaneceu como "traço marcante da abordagem regulatória". Nesse paradigma, o indivíduo se encontra no centro do processo decisório acerca do que é feito com seus dados pessoais.34 Entretanto, nos casos em que o tratamento não está explicitamente autorizado por alguma base normativa, na prática, o positivo ideal de empoderamento do titular resulta na obtenção de seu consentimento individual diante dos termos do tratamento, depois de previamente informado a respeito da finalidade da coleta (notice and consent). O instrumento do consentimento tornou-se, assim, vetor dominante na busca pela materialização dessa almejada autonomia do titular dos dados, sobretudo no âmbito da Internet."

[498] Os requisitos serão abordados a seguir.

[499] Lei nº 12.965/2014, art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; [...] IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;"

[500] Segundo relatório do InternetLab (2018): "Apesar de haver obrigatoriedade da obtenção do consentimento no Marco Civil, o *modo* como ele deve ser obtido não é exatamente regulado em lei, dando lugar a formatos variados, que melhor ou pior garantem uma decisão informada do usuário ou da usuária; é para isso que

consentimento como único fundamento legal para o tratamento de dados pessoais, salvo em casos de dispensa expressa pela legislação, segue sendo comum na América Latina (e.g., Colômbia, México e Argentina) e em países como o Canadá[501] e Singapura[502], cuja lei de proteção de dados pessoais foi editada antes da aprovação da GDPR.

No entanto, a compreensão do consentimento como única base legal impõe dificuldades em sua implementação, além de ser incapaz de assegurar com eficácia a autodeterminação informativa aos titulares de dados. No limite, o consentimento como condição ao tratamento de dados pessoais é incompatível com os seus próprios requisitos de validade. Por exemplo, como poderá o controlador obter um consentimento livre ao titular de dados se o tratamento for essencial à execução do serviço solicitado?[503] Assim, em países em que o consentimento persiste sendo a única base legal aplicável, a liberdade de consentir se flexibiliza e acaba por se traduzir em uma condição para que o indivíduo possa contratar. Alternativamente, como ocorre na Colômbia e no México, o consentimento é dispensado para certas atividades, como no tratamento de dados pelo poder público ou no reuso de dados pessoais de acesso público, caso em que a proteção à privacidade de cidadãos se centra principalmente em práticas transparência e em garantia a direitos restritos aos titulares de dados.

Outro desafio está na forma de obter consentimento expresso para cada uma das atividades de tratamento realizadas, sem que o usuário se sinta assoberbado em função da quantidade de informações e decisões que lhe serão exigidas. Se o usuário precisar autorizar cada uma das atividades que serão realizadas, deverá interagir com uma série de informações e poderá se sentir desestimulado a seguir com a contratação ou poderá acabar por fornecer

---

vamos olhar.". Disponível em: https://internetlab.org.br/pt/noticias/especial-obtencao-do-consentimento-sobre-tratamento-de-dados/. Acesso em 11.09.2022.

501 Vide https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html. Acesso em 23.04.2022.

502 Vide https://sso.agc.gov.sg/Act/PDPA2012. Acesso em 23.04.2022.

503 Nesse sentido argumenta o relatório do InternetLab (2018):"Quando se analisa o uso dessa base legal pelo *poder público*, coloca-se um paradoxo. A exploração da via do consentimento para alcançar ampla base legal para explorar dados pessoais, tal como muitas vezes feito por empresas privadas, é incompatível com a administração pública, que deve perseguir o interesse público, resguardar direitos fundamentais, e sempre respeitar princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência, conforme preceitua a Constituição Federal (art. 37, caput). Ao mesmo tempo, a exigência do consentimento como via exclusiva e irremediável de obtenção de autorização para tratamento de dados pessoais pode colocar obstáculos para a realização eficiente de políticas públicas na era digital. Assim, ao olhar para a forma como o consentimento é obtido em apps do governo, é necessário levar em conta que a administração pública tem um ônus redobrado em garantir que titulares de dados tenham controle efetivo sob seus dados pessoais, sem entretanto que isso inviabilize a prestação de serviços públicos de forma eficiente" Disponível em: https://internetlab.org.br/pt/noticias/especial-obtencao-do-consentimento-sobre-tratamento-de-dados/. Acesso em 11.09.2022.

consentimento irrefletido.[504] Nesse cenário, ocorre o efeito chamado de "fadiga do consentimento", segundo o qual, diante da quantidade de informação recebida e das ações que lhe são demandadas, e para que possa ter acesso facilitado ao conteúdo ou serviço desejado, o indivíduo acaba por aceitar todos os pedidos que lhe são feitos a respeito de seus dados pessoais.

Com isso, o consentimento acaba por não atuar da forma como idealizado (ou seja, como um mecanismo de informação e controle pelo indivíduo sobre como seus dados são utilizados). Mais que isso, essa sobrecarga informacional e pedidos repetidos de escolha podem levar indivíduos a perderem interesse em exercer controle sobre o uso de seus dados, de forma a colocar em descrédito o conceito de autonomia informacional que fundamenta todo o sistema de proteção de dados pessoais.[505]

Tendo isso em vista, as mais modernas normas de proteção de dados pessoais apresentam o consentimento como uma dentre as possíveis bases legais existentes (e.g., GDPR,[506] Panamá,[507] Tailândia,[508] Equador[509] e África do Sul),[510] mas apresenta requisitos adicionais à sua obtenção junto ao titular de dados.[511] É justamente essa a solução adotada pela LGPD quando previu outras bases legais com o mesmo grau de hierarquia (TEFFÉ; VIOLA, 2020) e estabeleceu que o consentimento deverá ser efetivamente livre e revogável.

---

504 Por exemplo, a má experiência de usuários com *banners* e *pop ups* referentes a cookies estimula usuários a fecharem a página de internet ou aceitarem todas as modalidades de cookies disponíveis para que possam acessar rapidamente o conteúdo desejado.

505 Nesse sentido se manifestou Laura Schertel Mendes e Gabriel da Fonseca (2020): "Não obstante sua importância para o florescimento e consolidação da disciplina normativa voltada à proteção de dados, os pressupostos que delineiam o paradigma do consentimento, atualmente, demonstram-se insuficientes para garantir um regime protetivo efetivo e material, em especial, para assegurar um verdadeiro controle sobre o fluxo de dados pessoais pelo seu titular. Nesta seção, serão destacados três pontos que elucidam as insuficiências do consentimento como foco regulatório: (i) as limitações cognitivas do titular dos dados pessoais para avaliar os custos e benefícios envolvidos quanto aos seus direitos de personalidade; (ii) as situações em que não há uma real liberdade de escolha do titular, por exemplo, em circunstâncias denominadas "take it or leave it"; e (iii) as modernas técnicas de tratamento e análise de dados a partir de Big Data que fazem com que a totalidade do valor e a possibilidade de uso desses dados não sejam completamente mensuráveis no momento em que o consentimento é requerido."

506 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679. Acesso em 04.05.2022.

507 Vide: https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf. Acesso em 23.04.2022.

508 Vide: https://www.dataguidance.com/legal-research/personal-data-protection-act-2019. Acesso em 23.04.2022.

509 Vide: http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoicm8iLCJ1dWlkIjoiOTE1ZTIyMDQtY2Q1Zi00ZGMzLWFkYTAtNDE1OTRkNjgyNTEwLnBkZiJ9. Acesso em 23.04.2022.

510 Vide: https://www.dataguidance.com/sites/default/files/popia_2013.pdf. Acesso em 23.04.2022.

511 De forma a lidar com essa ineficácia do consentimento, entre as medidas propostas por leis mais recentes de proteção de dados pessoais esteve a previsão de outras bases legais segundo as quais o tratamento de dados pessoais seria legítimo, a exemplo da execução de contrato ou do legítimo interesse. Essa foi justamente a escolha adotada pelo legislador brasileiro, ao prever nos artigos 7º e 11 da LGPD o consentimento como apenas uma das bases legais capazes de justificar o tratamento legítimo de dados pessoais.

Isso significa que o titular de dados poderá escolher por não consentir com o tratamento de dados ou solicitar a sua revogação, sem que isso signifique a impossibilidade de utilizar os serviços. Interessante notar que essa escolha normativa também está prevista, de alguma forma, na LAI (mesmo que anteriormente à edição do Marco Civil), quando estabelece hipóteses nas quais o consentimento do titular de dados não será necessário para a publicação de dados pessoais.

Nesse contexto, a LGPD estabeleceu que o consentimento consiste em manifestação **livre**, **informada** e **inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII), sendo **vedadas autorizações genéricas, enganosas ou abusivas**.[512] Para dados sensíveis, o consentimento deverá também ser obtido de forma específica e destacada.[513] Como se verifica, os requisitos de validade do consentimento na LGPD são bastante similares aos previstos no Marco Civil da Internet, com algumas diferenças terminológicas e práticas.

De todo modo, como será demonstrado a seguir, o pleno alcance desses requisitos pelo poder público é bastante desafiador, motivo pelo qual o consentimento muitas vezes não será a base legal mais apropriada para as atividades de tratamento de dados pessoais que desenvolve.

Em relação ao qualificador **livre**, ele impõe que a aceitação fornecida deverá implicar uma escolha (que poderá inclusive ser de não autorizar o tratamento) genuína do indivíduo e desimpedida de estímulos externos para que forneça o consentimento. Desse modo, qualquer elemento que influencie ou pressione de maneira inapropriada (como condicionar o uso do serviço ao fornecimento de consentimento) o titular de dados e que o impeça de plenamente exercer o seu livre arbítrio pode culminar em um consentimento inválido. Por isso, sempre que houver disparidade de poder entre as partes, ou quando o tratamento de dados for necessário à prestação do serviço, o consentimento não será a base legal apropriada.

---

[512] "Por fim, o consentimento também precisa ser específico, isto é, precisa indicar exatamente o propósito do processamento de dados. Assim, um cheque em branco não atende aos requisitos de validade do consentimento. Tampouco é válido o consentimento dado pelo consumidor, com base em informações enganosas veiculadas pelo fornecedor, nos termo do art. 37, § 1.° do Código de Defesa do Consumidor." (MENDES, 2018).

[513] Nesse sentido: "Mais uma vez, declarações genéricas para tratamento de dados pessoais sensíveis serão tidas como desprovidas de validade, na medida em que devem necessariamente se referir a uma concreta finalidade. Essa relação causal é condição necessária para a efetividade do consentimento" (MULHOLLAND, 2019).

O alcance desse requisito é um dos principais desafios para a utilização do consentimento para o tratamento de dados pessoais realizados pelo poder público.[514] A disparidade de poder entre governos e cidadãos e a necessidade do tratamento de dados para o desempenho de suas atividades muitas vezes removem a autonomia do cidadão em decidir se deseja consentir.[515] Por exemplo, para a obtenção do título de eleitor, o cidadão deverá fornecer dados como nome, endereço e biometria. A recusa de fornecimento desses dados impede que o Estado efetue o registro eleitoral do indivíduo que, por sua vez, será impedido de votar e exercer outros atos da vida civil. Nesse caso, o cidadão não é livre para escolher sobre o fornecimento e subsequente tratamento de seus dados.

Por sua vez, o qualificador **informado** exige que sejam fornecidas ao titular de dados informações claras e acessíveis, assim como necessárias e suficientes, antes do fornecimento do consentimento, a respeito de quais dados serão tratados, para quais finalidades e as condições nas quais o tratamento irá ocorrer. Isso significa dizer que o indivíduo deverá ter acesso a informações necessárias para que possa tomar uma decisão consciente sobre o fornecimento de consentimento.[516]-[517] O art. 9º da LGPD apresenta elementos que orientam a sua concretização, consistentes no fornecimento de informações claras, adequadas e ostensivas sobre a finalidade, forma e duração do tratamento, a identificação e informações de contato do controlador, os direitos assegurados aos titulares de dados, e a responsabilidade

---

514 Nesse sentido se manifestou Miriam Wimmer (2021): "[...] o consentimento é uma hipótese normalmente tratada com desconfiança no contexto do tratamento de dados pessoais pelo Poder Público, dados o desbalanceamento na relação entre cidadão e Poder Público e a consequente dificuldade de se caracterizar tal consentimento como livre"

515 Nesse sentido o Considerando 43 da GDPR: "A fim de garantir que o consentimento seja dado livremente, o consentimento não deve fornecer uma base legal válida para o tratamento de dados pessoais em um caso específico em que haja um desequilíbrio claro entre a pessoa em questão e o responsável pelo tratamento, em particular quando o responsável pelo tratamento for uma autoridade pública e, portanto, é improvável que o consentimento tenha sido dado livremente em todas as circunstâncias dessa situação específica. Presume-se que o consentimento não foi dado livremente se ele não permitir o consentimento separado para diferentes operações de processamento de dados pessoais, apesar de ser apropriado no caso individual, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento, apesar de tal consentimento não ser necessário para tal execução." (tradução nossa).

516 Conforme Chiara Teffé e Mário Viola (2020): "Na linguagem legislativa, o vocábulo informado significa que o titular do dado tem de ter ao seu dispor as informações necessárias e suficientes para avaliar corretamente a situação e a forma como seus dados serão tratados. A informação é fator determinante para a expressão de um consentimento livre e consciente, direcionado a tratamento específico, para determinado agente e sob determinadas condições. Destaca-se, aqui, a importância dos princípios da transparência, adequação e finalidade para restringir tanto a generalidade na utilização dos dados quanto tratamentos opacos. Para diminuir a assimetria técnica e informacional existente entre as partes, exige-se que ao cidadão sejam fornecidas informações transparentes, adequadas, claras e em quantidade satisfatória acerca dos riscos e implicações do tratamento de seus dados."

517 Essas informações geralmente são fornecidas na política de privacidade e na interface de comunicação com o indivíduo (e.g., nas páginas de cadastro de aplicativos de dispositivos móveis).

dos agentes envolvidos no tratamento.[518] Na prática, o consentimento previsto na LGPD é traduzido em uma escolha real pelo titular de dados, não podendo se colocar como condição ao fornecimento do produto ou de serviço (art. 9º §3º).

Esse requisito exerce papel importante nos casos de tratamento de dados por governos, na medida em que prestar informações claras consiste em uma das formas de reduzir a disparidade de poder existente entre governos e cidadãos. Em outras palavras, para que o poder público possa fundamentar atividades nessa base legal, será necessário que o cidadão compreenda e tenha confiança de que sua decisão a respeito do consentimento não irá impactar seu acesso a direitos, serviços públicos ou políticas públicas. Essa tarefa poderá ser desafiadora, especialmente se os dados pessoais forem obtidos durante procedimentos que impactam o acesso do cidadão a serviços públicos ou programas sociais.

Outra exigência traduzida por esse requisito do consentimento consiste na adequação das informações ao seu público-alvo. Isso se faz particularmente relevante nas relações jurídicas em que há desequilíbrio de conhecimento, caso em que o requisito de informação só é cumprido em vista das circunstâncias fáticas e necessidades das partes que compõem aquela relação (TOMASEVICIUS FILHO, 2007). Por exemplo, se os titulares de dados forem menores de idade ou pessoas analfabetas, o controlador deverá assegurar que a informação seja comunicada de forma a garantir o acesso por aqueles que não conseguem ler e a devida compreensão por aqueles em distinto estágio de desenvolvimento cognitivo. No caso do tratamento de dados pelo poder público, assegurar consentimento informado exige compreender qual segmento da população está impactado, o que poderá abranger pessoas de diferentes origens e níveis de escolaridade, e também populações de locais afastados ou em situação de vulnerabilidade.

Em relação ao qualificador **inequívoco**, ele possui similaridades com o termo "expresso" previsto no Marco Civil. Por consentimento expresso, entendia-se que o indivíduo deveria oferecer uma manifestação de vontade manifesta a respeito da sua decisão, não sendo autorizado àquele que realizaria a coleta de dados pessoais presumir ou obter manifestação implícita de consentimento. Esse requisito muitas vezes é materializado pela exigência de que

[518] Segundo Chiara de Teffé e Mário Viola (2020): "Na lógica do consentimento informado, o artigo 9º da LGPD dispõe que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca da: finalidade específica do tratamento (I); forma e duração do tratamento, observados os segredos comercial e industrial (II); identificação do controlador (III); informações de contato do controlador (IV); informações acerca do uso compartilhado de dados pelo controlador e a finalidade (V); responsabilidades dos agentes que realizarão o tratamento (VI); e direitos do titular, com menção explícita aos direitos contidos no art.18 (VII)."

o titular de dados clique um botão de aceite ou um *checkbox* não previamente preenchido.[519] No entanto, como aponta Bruno Bioni (2019), "apesar dessa diferença semântica, entre os qualificadores expresso e específico, a consequência normativa tende a ser a mesma. Isso porque o que está em jogo é reservar um tipo de autorização singular em situações igualmente singulares no que tange ao tratamento de dados". Isso significa que, para que o consentimento seja inequívoco, a autorização fornecida deverá ser clara e expressa, não bastando sua presunção pelo fato de o indivíduo se cadastrar ou utilizar determinado serviço, e poderá ser obtida de forma escrita ou de outra forma que demonstre a manifestação de vontade (TEFFÉ; VIOLA, 2020). Um dos desafios atrelados a esse requisito, ainda que alcance agentes de tratamento tanto do setor público como particulares, consiste em gerenciar e comprovar a obtenção desses consentimentos inequívocos.

Além disso, a LGPD ressalta que o consentimento também deverá se referir a **finalidades determinadas**, não sendo permitido ao controlador obter autorizações genéricas (art. 8º, §4º). Segundo Bruno Bioni (2021) "qualquer declaração de vontade deve ter um direcionamento, já que não se consente no vazio e de forma genérica". Isso significa que será necessário ao controlador identificar cada uma das atividades de tratamento de dados pretendidas, para as quais o titular deverá ser capaz de livremente escolher com quais irá consentir, ao invés de manifestar o seu consentimento em relação a todas as atividades de maneira unificada. Dito de outra forma, ao titular deve ser dada a opção de consentir de forma granular e independente para as diferentes finalidades de tratamento dos seus dados.[520]

Após a obtenção do consentimento, caso haja mudança na finalidade, de modo a tornar a finalidade não mais compatível com a informada previamente ao titular de dados, o controlador deverá informar previamente o titular sobre as mudanças de finalidade e solicitar novo consentimento, podendo o titular revogar o consentimento previamente concedido caso

---

[519] Sobre esse respeito, a Corte de Justiça da União Europeia, no julgamento do caso C-61/19, argumentou: "A esse respeito, enquanto o considerando 32 desse regulamento afirma que o consentimento poderia ser dado, entre outras coisas, por meio de um "tic tac" em uma caixa ao visitar um site na Internet, ao contrário, ele exclui expressamente a possibilidade de que "o silêncio, caixas pré-ticadas ou inatividade" constituam consentimento. Como o Tribunal decidiu, em tal situação, parece impossível, na prática, verificar objetivamente se um usuário de um website deu seu consentimento para o processamento de seus dados pessoais, não desmarcando uma caixa de seleção previamente colada nem, em qualquer caso, se tal consentimento foi informado. Não é inconcebível que um usuário não tenha lido as informações que acompanham a caixa de seleção pré-selecionada, ou mesmo não tenha notado essa caixa de seleção, antes de continuar com sua atividade no site visitado (ver, para esse efeito, o julgamento de 1 de outubro de 2019, *Planet49*, C‑673/17, EU:C:2019:801, paragraphs 55 and 57)." (tradução nossa). Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=233544&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4599345. Acesso em 21.08.2022.

[520] Essa é uma diferença prática significativa se comparado com o modelo anterior de consentimento que, por ser exigido para todas as atividades de tratamento de dados (na medida em que era a única base legal), muitas vezes era coletado pelo aceite do texto da política de privacidade.

discorde das alterações existentes (art. 9°, §2º). Essa exigência está atrelada ao princípio da finalidade (art. 6°, I), segundo o qual toda atividade de tratamento de dados pessoais deve ser direcionada para um propósito específico, explícito e informado ao titular.

Aqui também verifica-se um desafio em relação à utilização de consentimento por governos, especialmente em casos nos quais os dados poderão ser compartilhados com outros órgãos ou entidades públicas em sistemas interoperáveis ou publicados em portais de transparência e dados abertos. Caso a coleta de dados seja fundamentada no consentimento, será necessário ao poder público obter nova autorização do indivíduo para viabilizar quaisquer novas finalidades de tratamento não propriamente compatíveis com a finalidade que justificou a coleta do consentimento. No limite, se o consentimento fosse genericamente utilizado para o tratamento de dados pelo poder público, a necessidade de nova autorização para o reuso de dados restringiria sensivelmente o compartilhamento e a publicação de dados, e dificultaria o alcance do objetivo de eficiência governamental, na medida em que a coleta e gestão desses novos consentimentos geraria esforço desproporcional por parte do governo.

Além disso, a LGPD estabelece que o consentimento pode ser **revogado** a qualquer momento pelo titular, devendo tal revogação ser de fácil manifestação, além de não impor qualquer custo ou resultar em retaliações ao solicitante (art. 18, IX). É recomendado que seja permitido ao titular revogar o consentimento utilizando-se do mesmo processo ou formato utilizado para a sua obtenção.[521] Vale ressaltar que, caso os dados cujo consentimento para tratamento foi revogado tenham sido compartilhados com terceiros, o controlador deverá comunicar esses terceiros para que repitam procedimento similar, salvo quando essa comunicação seja impossível ou implique esforço desproporcional por parte do controlador (art. 18, §6°).

Esse requisito do consentimento está atrelado ao já mencionado requisito de liberdade. Isso porque, se o titular de dados deverá possuir autonomia em autorizar o tratamento de dados, similar liberdade deverá ser garantida para que possa remover essa autorização. Esse é mais um dentre os motivos para que o consentimento não seja a base legal mais apropriada para fundamentar atividades de tratamento de dados realizadas por governos. Como os dados são, na maioria das vezes, necessários ao cumprimento das atribuições legais do órgão ou

[521] Autoridade de Proteção de Dados Polonesa multou entidade por dificultar a revogação de consentimento https://edpb.europa.eu/news/national-news/2019/polish-dpa-withdrawal-consent-shall-not-be-impeded_en. Acesso em 11.07.2020.

entidade público, não será permitido ao cidadão revogar o consentimento anteriormente dado. Nas palavras de Miriam Wimmer (2020):

> [...] a possibilidade de revogação do consentimento a qualquer tempo representa outro grande inconveniente para seu uso como base legal para o tratamento de dados pessoais pelo Poder Público. A depender do caso, o embasamento de uma política pública estruturante no consentimento individual traria uma instabilidade incompatível com os objetivos buscados.

Caso não sejam observados todos os requisitos apresentados, o consentimento será nulo. Em outras palavras, se não obtida manifestação expressa para finalidades específicas, que não sejam enganosas ou abusivas, que tenham sido previamente informadas de forma clara e acessível ao titular de dados, e que seja revogável a qualquer momento, ele não terá validade. Além disso, a utilização indevida dessa base legal poderá afrontar direitos do titular de dados, visto que, após consentir para determinada atividade de tratamento, terá a expectativa de que poderá solicitar a sua revogação a qualquer tempo, o que nem sempre será possível.[522] Isso sem contar que a utilização de outras bases legais é acompanhada de obrigações adicionais ao controlador, como a elaboração de Relatórios de Impactos e testes de legítimo interesse, destinados a garantir, entre outros, se atividade observa a proporcionalidade, adequação, necessidade e legítima expectativa do titular de dados.

Assim, embora seja uma das mais notórias bases legais (especialmente porque intimamente relacionada com o conceito de autodeterminação informativa, na medida em que confere ao titular de dados certo controle sobre como serão utilizados seus dados), a sua utilização deve ocorrer com cautela pelo poder público. Na verdade, quando se trata do uso de dados por governos, o consentimento muitas vezes não será a base legal mais apropriada para fundar a atividade de tratamento. Isso porque, geralmente, a coleta e posterior utilização ou manutenção de dados por órgãos do poder público ocorre como: **(i)** consequência de uma obrigação legal, imposta ao ente público ou ao particular atuando em nome ou em parceria com o poder público, e o titular de dados; ou **(ii)** condição para que cidadãos possam gozar seus direitos, usufruir de serviços públicos ou se beneficiar de políticas públicas. Assim, além da disparidade de poder entre Estado e cidadãos, muitas vezes, o tratamento de dados é

[522] A utilização incorreta do consentimento já foi motivação para a punição de empresa pela Autoridade de Proteção de Dados Grega ("Hellenic DPA"). De acordo com a autoridade, além de o consentimento ser nulo porque não obtido de forma livre, a solicitação do consentimento gera falsas expectativas no titular de dados, que poderá posteriormente remover seu consentimento. Vide: https://edpb.europa.eu/news/national-news/2019/company-fined-150000-euros-infringements-gdpr_en. Acesso em 11.07.2020.

condição para que entes públicos possam exercer suas competências legais, inclusive assegurar o exercício de direitos individuais ou coletivos pelos cidadãos.[523]-[524]

Se o cidadão se recusar a consentir com o uso de seus dados pessoais, o órgão ou entidade pública poderá se ver limitado no exercício de suas atribuições legais. Por outro lado, poderá ocorrer de o cidadão consentir com o uso de seus dados simplesmente por saber que essa autorização é uma condição para que possa exercer determinado direito ou usufruir de certos serviços ou políticas públicas. Em verdade, tanto o poder público não pode depender de autorização do titular de dados para utilizar os dados, como o titular de dados não possui uma escolha efetiva em relação ao tratamento de seus dados. Com isso, não estarão presentes as condições do consentimento, especialmente a liberdade na manifestação de vontade.

Nesse sentido se manifestou Miriam Wimmer (2019):

> Entretanto, dada a disparidade de forças e a natureza não voluntária da maior parte das interações entre o poder público e o cidadão, a própria ideia de consentimento "livre" pode ser colocada em xeque. A legislação brasileira não veda a invocação da base legal do consentimento por órgãos públicos, contudo entende-se que sua importância tende a ser residual, dado que os atos do poder público devem, em regra, estar ancorados na execução de competências legais ou no cumprimento de atribuições legais do serviço público.

Essa, foi também uma das preocupações demonstradas por participantes da Consulta Pública realizada pelo Ministério da Justiça para a elaboração do Anteprojeto de Lei de Proteção de Dados Pessoais, como relatado pela associação InternetLab (2016) em relatório de acompanhamento do debate público realizado à época:

---

[523] Nesse sentido se manifestam Black & Stevens (2013): "Além disso, há preocupações particulares com o consentimento do setor público. O Ministério da Justiça declarou que, "em certas circunstâncias (como o compartilhamento de dados no contexto de funções reguladoras ou de execução) é improvável que o consentimento seja uma condição apropriada e os órgãos públicos desejarão confiar em outras condições". A razão para esta relutância decorre da natureza da relação entre o responsável pelo tratamento de dados e o envolvido no setor público, onde é provável que o envolvido seja dependente do responsável pelo tratamento de dados para a prestação de serviços públicos, sejam eles de saúde, finanças ou habitação, por exemplo." (tradução nossa).

[524] Igualmente se posicionou relatório publicado pelo governo do Reino Unido (2020) sobre formas de endereçar confiança no tratamento de dados pelo poder público: "As organizações do setor público raramente utilizam o consentimento como base para o processamento de dados. Na maioria dos casos isso seria inadequado, uma vez que o processamento de dados é uma condição prévia para a prestação de um serviço e, portanto, há um desequilíbrio de poder entre o governo e o cidadão. Nessas circunstâncias, o consentimento não seria considerado como dado livremente. Ao invés disso, o desempenho de uma tarefa pública é a base legal para o processamento de dados. Isto também pode permitir o processamento por um terceiro processador de dados, muitas vezes uma organização do setor privado, agindo em nome da organização do setor público." (tradução nossa). Disponível em: https://www.gov.uk/government/publications/cdei-publishes-its-first-report-on-public-sector-data-sharing/addressing-trust-in-public-sector-data-use?utm_source=Digest&utm_campaign=7063bf665b-RSS_EMAIL_CAMPAIGN&utm_medium=email&utm_term=0_d90a01c7ff-7063bf665b-87770509#introduction--context. Acesso em 06.08.2022.

> Houve sugestões quanto à base legal do consentimento, em que a RELX Group, Centre for Information Policy Leadership e MPA sugeriram uma nova hipótese para interesse público: "O consentimento também não deve ser obrigatório quando o tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados" [Centre for Information Policy Leadership]. Essa exceção está, aliás, alinhada com a Lei de Acesso à Informação (Lei n° 12.527/2011), que elimina a necessidade de consentimento em diversas circunstâncias, inclusive "à proteção do interesse público e geral preponderante" (Artigo 31, V). Sem essa nova exceção, não seriam permitidas, por exemplo, o tratamento de dados para a prevenção à fraudes e até investigações criminais.

No entanto, é possível que haja casos em que a base legal aplicável será o consentimento e ele poderá ser oferecido livremente.[525] São situações em que não há significativa disparidade de poder na relação entre cidadão e governo, e quando a atividade realizada não é fruto de obrigação legal ou regulatória, ou quando não necessária para o exercício de políticas públicas.[526] Um exemplo consiste no compartilhamento de dados de beneficiários de programas sociais com terceiros para finalidades comerciais, a exemplo de ofertas de crédito especiais para cidadãos vinculados ao Bolsa Família (FRAGOSO *et al.*, 2021). Nesse caso, o titular de dados deverá compreender que a oferta de consentimento é efetivamente livre e que a negativa não irá afetar direitos ou acesso a serviços públicos por parte do cidadão.

Por outro lado, o consentimento poderá ser a base legal mais apropriada para a utilização desses dados pelos receptores de dados (fruto de compartilhamento ou de publicação de dados pelo poder público) para finalidades secundárias não compatíveis com o motivo que justificou a coleta dos dados. Isso porque, a depender da nova finalidade do tratamento dos dados, outras bases legais poderão não ser aplicáveis, como o exemplo do legítimo interesse, especialmente porque o titular de dados nem sempre terá a legítima

---

[525] Nesse sentido se manifestou a Autoridade de Proteção de Dados Pessoais da Eslovênia: "Assim, os dados pessoais podem ser processados no setor público se o processamento de dados pessoais e os dados pessoais que estão sendo processados estiverem previstos por lei. A lei pode estipular que certos dados pessoais só podem ser processados com o consentimento pessoal do indivíduo. Os detentores da autoridade pública também podem processar dados pessoais com base no consentimento pessoal de um indivíduo sem base legal, quando não se trata do desempenho de suas tarefas como detentores da autoridade pública. Excepcionalmente, porém, os dados pessoais necessários para o exercício de poderes, tarefas ou obrigações legais do setor público serão processados, desde que tal processamento não interfira com o interesse legítimo do indivíduo, ao qual os dados pessoais se referem." (tradução nossa). Disponível em: https://gdprhub.eu/index.php?title=IP_-_0610-376/2020/35. Acesso em 21.08.2022.

[526] Outro exemplo foi fornecido por Miriam Wimmer (2021): "Outra hipótese em que o consentimento poderia configurar base legal adequada para o tratamento de dados pelo Poder Público se dá nos casos em que ao cidadão é dada a opção de acessar determinado serviço por meios alternativos (por exemplo, optando por um aplicativo de Internet em vez do atendimento presencial em uma agência física). Nesse caso, ao dar ao cidadão a opção por uma via alternativa de fruição de determinado serviço, seria razoável entender que ele pudesse consentir com o uso de determinados dados que não seriam necessários em um atendimento presencial (por exemplo, dados técnicos relativos ao terminal utilizado e ao sistema operacional necessários para a prestação do serviço por meio de aplicativo eletrônico)."

expectativa de que seus dados serão utilizados dessa nova forma. Por exemplo, num novo debate a respeito de monetização em parcerias público-privadas está a possibilidade de uso de dados obtidos na prestação dos serviços públicos para finalidades comerciais não diretamente relacionadas com a prestação desses serviços. Nesses casos, uma das possíveis soluções para buscar viabilizar esse uso secundário aos dados seria, em conjunto com outras medidas, a obtenção do consentimento livre e informado dos titulares de dados.

16.2 Cumprimento de obrigação legal e execução de políticas públicas

Como mencionado, as bases legais de execução de políticas públicas e de cumprimento de obrigação legal são as mais apropriadas para embasar o uso de dados pessoais pelo poder público (ainda que não sejam as únicas aplicáveis), na medida em que exigem que a atividade esteja embasada em legislação. Considerando que o princípio da legalidade exige ao poder público atuar em observância ao ordenamento jurídico, será mais recorrente a fundamentação de atividades de tratamento de dados pelo poder público em alguma dessas duas bases legais.

Nesse respeito, como mencionado, esta tese discorda de Miriam Wimmer (2021) quando argumenta que "[o] art. 23 da LGPD [...] estabelece uma hipótese complementar para o tratamento de dados pelo Poder Público, ao acrescentar às previsões dos arts. 7º e 11 o objetivo de “executar as competências legais ou cumprir as atribuições legais do serviço público”". Esse objetivo está devidamente contemplado pelas bases legais ora abordadas, em leitura conjunta com o art. 23, que, por sua vez, não acrescenta nova base legal às previstas nos arts. 7º e 11 da LGPD, mas apenas estabelece as condições segundo as quais o tratamento de dados pelo poder público deverá ocorrer (ie.: no interesse público, para a execução de políticas públicas e de competências legais ou atribuições legais do serviço público).

De fato, quando essas duas bases legais são utilizadas pelo poder público, elas apresentam grande semelhança, na medida em que, nos dois casos, o tratamento de dados será necessário para o cumprimento das competências e atribuições legais do órgão ou entidade pública. Por outro lado, elas possuem diferenças importantes e que resultam na adoção de cuidados específicos por parte do gestor público, especialmente no que diz respeito ao dever do órgão e entidade pública em justificar a necessidade e adequação do tratamento pretendido.

No entanto, a LGPD não apresenta critérios claros sobre como essas bases legais deverão ser interpretadas, especialmente quando utilizadas pelo poder público. Nesse tópico

se buscará construir parâmetros para auxiliar nessa compreensão. Para tanto, e com vistas a auxiliar nesse esforço interpretativo, este tópico observará os contornos de similares bases legais previstas na legislação europeia que, como mencionado, inspirou diversas disposições da LGPD. Para ilustrar essa semelhança entre bases legais da LGPD e da GDPR, a seguir há quadro comparando as bases legais de cumprimento de obrigação legal e de execução de políticas públicas previstas na LGPD e GDPR:

Quadro 8: comparativo das bases legais previstas na LGPD

LGPD, art. 7º	**GDPR, art. 6**
Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:	1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;	c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;	e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
LGPD, art. 11	**GDPR, art. 9**
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:	1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. 2. O disposto no n.o 1 não se aplica se se verificar um dos seguintes casos:
a) cumprimento de obrigação legal ou regulatória pelo controlador;	b) Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na

	medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados;
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;	g) Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;

Como se verifica, as bases legais previstas nos arts. 7º e 11 da LGPD são consideravelmente similares às bases legais previstas nos arts. 6 e 9 da GDPR. O art. 6(1)(c) da GDPR estabelece que dados pessoais triviais poderão ser tratados para o cumprimento com obrigação jurídica, e o art. 9(2)(b) da mesma lei autoriza o tratamento de dados pessoais sensíveis para finalidades de cumprir com obrigações ou para exercer direitos do controlador ou do titular de dados nas áreas de seguridade pública e emprego. Por sua vez, os arts. 6(1)(e) e o art. 9(2)(g) da GDPR fundamentam o tratamento de dados pessoais realizados para o exercício de funções do interesse público ou da autoridade pública à qual está investido o responsável pelo tratamento. Assim, ainda que com diferenças importantes, como se verá adiante, as bases legais dos art. 6(1)(c)(e) e art. 9(2)(b)(g) da GDPR possuem semelhanças em relação às bases legais de cumprimento de obrigação legal e de execução de políticas públicas, previstas nos arts. 7º, II e III e 11, II, a e b da LGPD.

A seguir serão apresentadas as duas bases legais, com o objetivo de identificar seus pontos de semelhança e diferença, assim como as obrigações acessórias decorrentes da fundamentação da atividade de tratamento em uma ou de outra dessas duas bases legais.

Cumprimento de obrigação legal

A base legal do cumprimento de obrigação legal ou regulatória (art. 7º, II e art. 11, II, a) assume particular relevância no tratamento de dados pessoais mantidos pelo poder público, visto que a administração pública é regida pelo princípio da legalidade - ou seja, suas ações

devem estar pautadas em normas autorizadoras específicas.[527] Mais que isso, muitos dados são tratados pelo poder público ou a ele enviados por força de exigências legais expressas de fornecimento de dados, como o exemplo da circulação de dados pessoais de cidadãos entre entidades públicas responsáveis por executar programas de benefício social ou a coleta de foto, endereço e digital como condição para que o cidadão possa votar.

No entanto, como mencionado, a LGPD não apresenta maiores esclarecimentos sobre os contornos da base legal de cumprimento de obrigação legal ou sobre cuidados ou obrigações adjacentes à fundamentação do tratamento de dados pessoais nessa base legal. Essa definição se faz particularmente importante nas situações em que dados são tratados por entes públicos porque, no limite, sempre deverá ser possível relacionar a atividade a uma determinação legal - especialmente em vista da moderna leitura administrativista sobre os contornos do princípio da legalidade e do conceito de discricionariedade administrativa, que permitem maior flexibilidade na atuação do agente público, na medida em que os permite agir dentro de certo nível de subjetividade, desde que observado o ordenamento jurídico.

No entanto, essa base legal não foi prevista para assumir tamanha amplitude - isso pode ser depreendido, por exemplo, pela existência de outra base legal aplicável ao poder público, como a de execução de políticas públicas pela administração pública - e não poderá ser interpretada como uma autorização abrangente para qualquer atividade de tratamento de dados pessoais realizada por órgãos e entidades públicas. Entre os motivos para tanto consiste o fato de que um dos mecanismos previstos por leis de proteção de dados para assegurar a autodeterminação informativa aos indivíduos sobre como seus dados circulam é a previsão de bases legais que delimitam as situações nas quais será permitido tratar dados pessoais. Assim, a previsão de base legal que englobe todas as atividades desenvolvidas pelo poder público seria contrária à própria lógica da legislação de proteção de dados pessoais, especialmente se considerarmos que, como se demonstrou nesta tese, historicamente buscou-se evitar a prática de abusos no uso de dados pessoais por governos.

Na Europa, a base legal similar à de cumprimento de obrigação legal ou regulatória está prevista nos arts. 6(1)(c) e 9(2)(g) da GDPR, que autorizam dados pessoais a serem tratados para o cumprimento com obrigação jurídica. Por sua vez, os Considerandos 41 e 45 da mesma lei esclarecem que a atividade de tratamento de dados pessoais realizada com

[527] Conforme mencionado, no mesmo sentido se manifestou o Comitê de Governança de Dados, por meio do Guia de Boas Práticas para Implementação da LGPD na administração pública Federal. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em 13.08.2020

fundamento nesses dispositivos deverá estar fundamentada em legislação, que não precisa ser editada pelo poder legislativo, desde que seja clara, precisa e de aplicação previsível pelo jurisdicionado. Essa exigência, segundo a Corte de Justiça da União Europeia, no caso C-175/20, busca assegurar transparência sobre o tratamento de dados e previsibilidade para os titulares de dados sobre como seus dados serão utilizados por terceiros e sobre como poderão exercer seus direitos.[528] Para tanto, a lei ou regulamento que fundamenta a utilização dessa base legal deverá ser clara e estabelecer garantias mínimas para assegurar a proteção de dados pessoais.

A GDPR também esclarece que não será necessária a existência de lei para cada atividade de tratamento de dados, sendo autorizada a presença de norma única que determine as condições gerais desse tipo de tratamento de dados (Considerando 45), como os tipos de dados pessoais que são objeto do tratamento, os titulares de dados envolvidos, os possíveis recipientes dos dados, as finalidades do tratamento, o período de armazenamento e outras medidas que assegurem o devido tratamento dos dados pessoais (art. 6). No entanto, não será permitido o uso dessa base legal se a atividade de tratamento estiver fundamentada em arranjos contratuais ou em legislação de país estrangeiro, caso em que se aplicará outra base

[528] ”A questão que está no cerne dessa avaliação, que requer atenção especial, é se o artigo 15(6) da Lei de impostos e taxas, juntamente com os pedidos específicos de informação, cumpre a exigência de previsibilidade (43) ao examinar a base legal. A legislação que permite a transferência de dados deve estabelecer regras claras e precisas que regulamentem o escopo e a aplicação da medida em questão e impor salvaguardas mínimas, de modo que as pessoas cujos dados pessoais são afetados tenham garantias suficientes de que esses dados serão efetivamente protegidos contra o risco de abuso. (44) Portanto, a base jurídica tomada como um todo (legislativa e administrativa combinada) deve ser formulada com suficiente precisão para todas as pessoas envolvidas: as autoridades públicas no que diz respeito ao que podem solicitar, as empresas em relação ao que podem fornecer e, acima de tudo, as pessoas envolvidas, para que saibam quem pode ter acesso aos seus dados e para que fins. É possível lembrar que as informações sobre o processamento de dados são, de fato, um requisito fundamental no âmbito da GDPR. As pessoas em questão devem estar cientes da existência de tal processamento e que a informação é o pré-requisito para exercer mais direitos de acesso ou de apagamento ou retificação. (45) A menos que o artigo 23 da GDPR tenha sido de alguma forma transposto para a legislação nacional a fim de restringir os direitos das pessoas em questão sob o Capítulo III da GDPR, decorre dos artigos 13 e 14 da GDPR que o controlador do processamento deve fornecer informações à pessoa em questão. No contexto de sucessivas transferências de dados, pode ser difícil determinar sobre quem recai o dever de informação. (46) Além disso, em termos práticos, na ausência de quaisquer restrições adotadas sob o artigo 23(1) da GDPR, que na legislação nacional deve cumprir a exigência do artigo 23(2) da GDPR, uma autoridade pública que obteve os dados pode ter a obrigação de fornecer as informações apropriadas sob o artigo 14 da GDPR a todas as pessoas em questão. Se não houver uma base legal clara e previsível que permita tais transferências de dados, dificilmente se pode esperar que o responsável pelo tratamento que coletou os dados informe já a pessoa em questão de acordo com o artigo 13 da GDPR. Em conclusão, portanto, em minha opinião, o artigo 6(1)em e (3) da GDPR não impede que as regras nacionais estabeleçam, sem qualquer limite de tempo, a obrigação de os prestadores de serviços de publicidade na Internet comunicarem determinados dados pessoais a uma autoridade fiscal, desde que haja uma base legal clara na legislação nacional para tal tipo de transferência de dados e os dados solicitados sejam adequados e necessários para que a autoridade fiscal cumpra suas tarefas ofici”is". (tradução nossa). Julgado disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=245557&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2607038. Acesso em 07.08.2022.

legal, como o legítimo interesse.[529]-[530] Por exemplo, a Suprema Corte da Holanda determinou que também não se aplica a base legal prevista no art. 6(1)(c) para normas decorrentes de autorregulação que foram aceitas e são adotadas pela autoridade.[531]

Finalmente, nos termos da legislação europeia, a lei utilizada como fundamento para a base legal de cumprimento de obrigação jurídica, ao estabelecer uma obrigação de tratamento de dados, deverá identificar a necessidade, proporcionalidade e finalidade dessa atividade (WP 29, 2016). Isso significa que o tratamento de dados deverá ser uma exigência legal, não podendo ser uma faculdade,[532] e o controlador não deverá ter discricionariedade sobre como cumprir com essa obrigação legal.[533] Caso contrário, se a legislação apenas definir condições

---

[529] Nesse sentido se posicionou o IC“: "Uma obrigação contratual não compreende uma obrigação legal neste contexto. Você não pode contratar fora da exigência de uma base legal. No entanto, você pode procurar uma base legal diferente. Se o contrato for com o indivíduo, você pode considerar a base legal para os contratos. Para contratos com outras partes, você pode querer considerar os interesses legítimo”.." Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/. Acesso em 07.08.2022.

[530] Nesse sentido, se posicionou a Autoridade de Proteção de Dados Pessoais do Reino Unido (ICO“: "Uma obrigação contratual não compreende uma obrigação legal neste contexto. Você não pode contratar fora da exigência de uma base legal. No entanto, você pode procurar uma base legal diferente. Se o contrato for com o indivíduo, você pode considerar a base legal para os contratos. Para contratos com outras partes, você pode querer considerar os interesses legítim”s." (tradução nossa). Disponível aqui: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/. Acesso em 14.08.2022.

[531] “Nos Países Baixos, o sistema de registo de crédito do qual participam os credores em cumprimento da legislação e regulamentação referida em 3.1.6 supra e que consultam para a sua implementação é constituído pelo CKI do BKR. O CKI não tem base legal. Baseia-se na autorregulação do setor financeiro, que o legislador aceitou. O BKR estabeleceu o Regulamento Geral do CKI (doravante: Regulamentos do CKI).8 De acordo com o art. 2 § 1º Regulamentos do CKI, trata-se de um acordo contratual que regula exclusivamente a relação entre o BKR e seus clientes empresariais. (...) Art. 4:32 parágrafo 1 Wft e art. 4:34 parágrafo 1 Wft, conforme detalhado no art. 114 BGfo, embora obrigue os credores a participar e consultar um sistema de registro de crédito, essas disposições legais não são suficientemente claras e precisas e sua aplicação não é suficientemente previsível para aqueles a quem essas disposições legais se aplicam, como o art. 6 parágrafo 3 GDPR (ver 3.1.5). Afinal, não fica claro por aquelas disposições legais quais dados pessoais devem ou podem ser registrados no CKI, quais são as condições para tal registro e em que condições e em que prazos os dados pessoais devem ser apagados. Isso é regulamentado nos regulamentos do CKI, mas esses regulamentos não são baseados em uma base legal; o registro de dados pessoais no CKI ocorre com base em um acordo entre o BKR e os provedores de crédito (ver 3.1.8). Na ausência de uma obrigação legal de tratamento de dados na acepção do art. 6 n.º 1, preâmbulo e alínea c do RGPD, esta disposição não pode servir de base para o tratamento lícito de dados pessoais no CKI do BKR.” (tradução nossa). Julgado disponível em: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2021:1814. Acesso em 07.08.2022.

[532] Conforme aponta a Working Party 29: “Os compromissos unilaterais voluntários e as parcerias público-privadas que processam dados além do que é exigido por lei não são, portanto, cobertos pelo Artigem(c). Por exempl–, se - sem uma obrigação legal clara e específica de fa–ê-lo - um provedor de serviços de Internet decidir monitorar seus usuários em um esforço para combater o download ilegal, o Aremo 7(c) não será uma base legal apropriada para esta finalidade.” (tradução nossa). Vide: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Acesso em 12.07.2020.

[533] Nesse sentido argument“ o ICO: "Embora o processamento não precise ser essencial para que você cumpra a obrigação legal, ele deve ser uma forma razoável e proporcional de alcançar o cumprimento. Você não pode confiar nesta base legal se tiver discrição para processar os dados pessoais, ou se houver outra maneira razoável de”cumprir." (tradução nossa). Disponível em: https://ico.org.uk/for-organisations/guide-to-data-

gerais para seu cumprimento e a atividade de tratamento constituir uma das possíveis formas de executar essa obrigação, a base legal mais apropriada seria a execução de função para o interesse público e exigiria a realização de um teste de balanceamento de interesses.

Entre os aprendizados decorrentes da análise sobre como a GDPR regula essa base legal está em entender seus limites, a saber: (i) deverá haver obrigação clara, precisa e de aplicação previsível pelo jurisdicionado; (ii) o tratamento de dados deverá ser uma exigência legal imposta ao controlador, que não terá discricionariedade quanto ao seu cumprimento; (iii) a base legal não se aplicará se a atividade de tratamento constituir uma das possíveis formas de executar essa obrigação, (iv) a base legal não se aplicará se fundamentada em obrigações constantes de contratos, convênios ou instrumentos congêneres; e (v) a obrigação deverá estar prevista em legislação nacional.

Assim, quando a divulgação de dados ocorrer por força de legislação que estabelece com clareza quais dados serão divulgados, para quem, para quais finalidades e por quanto tempo, a base legal aplicável geralmente será o cumprimento de obrigação legal ou regulatória. Nesse caso, a ponderação entre a privacidade do cidadão e o interesse público no acesso aos dados é realizada pelo legislador ou pelo administrador em sua capacidade legislativa (ainda que a norma possa ser posteriormente questionada em juízo), cabendo ao gestor público menor grau de discricionariedade em relação às condições de tratamento dos dados.

Na prática, isso significa que a administração pública poderá ter maior ou menor grau de discricionariedade, a depender do detalhamento normativo em relação às suas atividades. Quanto mais detalhadas as normas editadas pelo legislador, menor a possibilidade de escolha do administrador em relação à competência, forma e conteúdo de seus atos (MARRARA, 2012). Isso possui reflexos na escolha da base legal aplicável, na medida em que o grau de detalhamento em lei sobre as atividades de tratamento de dados pessoais que deverão ser realizadas (a) importará na incidência da base legal de obrigação legal ou regulatória ou em outra base legal, como a de execução de políticas públicas; e (b) exigirá maior ou menor envolvimento do administrador na (b1) avaliação sobre os riscos que a atividade impõe aos titulares de dados, (b2) ponderação sobre o interesse público envolvido no uso dos dados, e (b3) escolha sobre quais salvaguardas adotar para proteger os titulares.

---

protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/. Acesso em 07.08.2022.

Assim, o teor da legislação que justifica a divulgação de dados resultará em bases legais e responsabilidades distintas para o gestor público. Em relação às normas que abordam a divulgação de dados, elas geralmente: (i) determinam com algum grau de clareza quais dados serão divulgados para quais terceiros, particulares ou entes públicos, e para quais finalidades; ou (ii) estabelecem políticas e/ou medidas cujo cumprimento poderá envolver a realização de atividades de tratamento de dados pessoais. Para que seja possível fundamentar a divulgação de dados no cumprimento de obrigação legal ou regulatória, deverá estar presente a primeira situação - ou seja, deverá haver uma norma que preveja quais dados deverão ser divulgados, em quais condições e para quais finalidades.

Por isso, a Lei de Acesso à Informação geralmente não consiste em obrigação capaz de fundamentar a divulgação de dados pessoais na base legal de cumprimento de obrigação legal ou regulatória. Isso se dá porque ela apresenta uma obrigação geral de publicação de dados, que eventualmente poderá ser cumprida até mesmo com a supressão de dados pessoais. Por outro lado, o mesmo não se aplica ao Decreto nº 7.724/2012, que regulamenta a LAI no âmbito da administração pública federal, naquilo que determina a publicação nos sites dos órgãos e entidades públicos a remuneração e subsídio recebidos por servidores públicos, incluídos os auxílios, ajuda de custos e outras vantagens pecuniárias, de maneira individualizada (art. 7º, § 3º, VI). A obrigação é clara, específica e não pode ser alcançada de outra forma senão pela publicação de determinados dados pessoais de servidores públicos.

A avaliação sobre o interesse público na divulgação de remuneração de servidores públicos foi realizada anteriormente à edição do Decreto (e confirmada posteriormente pelo Supremo Tribunal Federal). No entanto, ainda resta ao gestor público determinar quais dados serão divulgados (e.g., nome, número de identidade, remuneração, residência etc.) e em qual formato (e.g., em planilhas com formato aberto ou em portal que apenas permite busca individualizada). Esse nível de discricionariedade atribuído ao gestor público não afasta a aplicação da base legal de cumprimento de obrigação legal ou regulatória.

Execução de Políticas Públicas

Outra base legal que assume particular relevância quando estamos falando do tratamento de dados pessoais mantidos pelo poder público consiste na base legal de execução de políticas públicas (art. 7º, III e art. 11, II, b). Para o tratamento de dados triviais, a LGPD estabelece que a política pública que dá causa ao tratamento de dados que será fundamentado nessa base legal poderá ser prevista em leis e regulamentos ou respaldada em contratos,

convênios ou instrumentos congêneres. Já para dados sensíveis, a autorização se limita a políticas públicas previstas em leis e regulamentos. Como se verifica, assim como a base legal de cumprimento de obrigação legal ou regulatória, a base legal de execução de políticas públicas também somente será aplicável quando o tratamento estiver fundamentado em legislação.

Primeiramente, cumpre apontar a existência de duas diferenças entre a base legal de execução de política pública prevista para o tratamento de dados pessoais triviais (art. 7º, II) e para o tratamento de dados pessoais sensíveis (art. 11, II, b). Primeiro, para o tratamento de dados pessoais triviais, a utilização dessa base legal poderá pretender alcançar objetivos previstos em leis e regulamentos ou em contratos, convênios ou instrumentos congêneres. Já para os dados pessoais sensíveis, somente será possível se utilizar a base legal de execução de política pública se a atividade de tratamento for necessária para alcançar um objetivo previsto em lei ou regulamento. Com isso, busca-se reduzir a discricionariedade administrativa no tratamento de dados pessoais sensíveis, na medida em que o objetivo que se busca alcançar pelo tratamento deverá ser estabelecido por procedimento legislativo prévio.

Além disso, a redação do art. 11, II, b, que estabelece os contornos dessa base legal para o tratamento de dados pessoais sensíveis se refere ao "tratamento compartilhado de dados", o que poderia levar à compreensão de que somente seria possível utilizar essa base legal nos casos em que o tratamento consiste no compartilhamento de dados pessoais. No entanto, essa interpretação literal do texto legal não pode prosperar, por dois principais motivos: (i) o termo compartilhamento não está qualificado na lei, dificultando a circunscrição das situações que estariam contempladas por essa base legal; e (ii) a norma não alcançaria o seu objetivo de permitir que órgãos ou entidades públicas (sem precisar transferir dados a terceiros) possam se utilizar de dados pessoais sensíveis para finalidades que beneficiem a sociedade. Nesse sentido se posicionou Miriam Wimmer (2021):

> Em primeiro lugar, é necessário chamar atenção para a confusão terminológica do legislador quanto ao uso da expressão “tratamento compartilhado” no art. 11 da LGPD. Com efeito, a partir da leitura da lei, é possível compreender que o “uso compartilhado de dados”, previsto no art. 5.º, XVI, é uma modalidade de “tratamento” de dados, conforme definição do art. 5.º, X. Não faria sentido imaginar que a legislação tivesse pretendido limitar o tratamento de dados sensíveis pelo Poder Público à hipótese de uso compartilhado. Uma interpretação sistemática dos artigos em questão conduz, portanto, ao entendimento de que o art. 11 se refere tanto ao tratamento quanto ao uso compartilhado de dados sensíveis pelo Poder Público.

Outro aspecto que chama atenção é que as bases legais previstas nos art. 7º, III e art. 11, II, b são redigidas de tal forma a direcionar sua aplicação à administração pública (i.e.:

"pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas" e "necessários à execução, pela administração pública, de políticas públicas").[534] No entanto, esse entendimento não deve prosperar, de forma que essa base legal deve se aplicar também aos demais Poderes Estatais (e.g., Poderes Legislativo, Ministério Público e Judiciário) quando atuam no desenvolvimento de políticas públicas (ANPD, 2022.3).

No entanto, também para essa base legal, a LGPD não apresenta maiores esclarecimentos sobre seus contornos. Essa especificação sobre sua aplicação é de suma importância para que ela, junto com a base legal de cumprimento de obrigação legal ou regulatória, não seja interpretada como uma ampla autorização para o poder público tratar dados pessoais. De fato, a despeito do silêncio legal, essa base legal se aplica em hipóteses específicas e atrai para o poder público a necessidade de justificar a necessidade e proporcionalidade do tratamento de dados pretendido. Conforme será argumentado adiante, essa avaliação deverá ocorrer antes do tratamento de dados e assumir contornos similares a um teste de balanceamento exigido para a utilização da base legal do legítimo interesse.

Na Europa, o desempenho de atividade para o alcance de interesse público consiste em base legal para o tratamento de dados pessoais (arts. 6(1)(e) e 9(2)(g) da GDPR). Ela estará presente quando o tratamento for realizado para o exercício de função atribuída ao controlador, que deverá ser necessária para: **(i)** o alcance do interesse público previsto em lei; ou **(ii)** no exercício de suas atribuições legais do controlador.[535] Caso o controlador, ente público ou privado, esteja atuando segundo suas atribuições legais, desde que comprovado

---

[534] Como apontado por Miriam Wimmer"(2019): "Conforme amplamente debatido anteriormente, o Poder Público não se resume à administração pública e as inúmeras atividades por ele desempenhadas transcendem, em grande medida, a execução de políticas públicas. De fato, por meio de suas diferentes ramificações no âmbito do Executivo, do Legislativo e do Judiciário, o Poder Público ocupa-se de uma miríade de atividades envolvendo o exercício de poder de polícia administrativo, a realização de pagamentos, a gestão de servidores públicos e a prestação de tutela jurisdicional, para citar apenas alguns exemplos que dificilmente podem ser caracterizados como execução de políticas públicas.

[535] Segundo a Working Party 29, na Opinião 04/2014: [...] abrange situações em que o próprio controlador tem uma autoridade oficial ou uma tarefa de interesse público (mas não necessariamente também uma obrigação legal de processar dados) e o processamento é necessário para exercer essa autoridade ou executar essa tarefa. Por exemplo, uma autoridade fiscal pode recolher e processar a declaração de impostos de um indivíduo a fim de estabelecer e verificar o valor do imposto a ser pago. Ou uma associação profissional, como uma ordem de advogados ou uma câmara de profissionais médicos investida de autoridade oficial para fazê-lo, pode realizar procedimentos disciplinares contra alguns de seus membros. Outro exemplo poderia ser um órgão governamental local, como uma autoridade municipal, encarregado de administrar um serviço de biblioteca, uma escola, ou uma pisci"a local." (tradução nossa). Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Acesso em 14.08.2022.

que a atividade de tratamento de dados pretendida é necessária para tanto,[536]-[537] não será preciso realizar teste de interesse público (ICO, 2022).

De imediato, nota-se que será permitido a entes privados tratarem dados pessoais com fundamento nessa base legal se estiverem exercendo atividades descentralizadas (ICO, 2022).[538] Além disso, destaca-se que a avaliação da necessidade possui papel relevante na determinação sobre a aplicação da base legal dos arts. 6(1)(e) e 9(2)(g) ao caso concreto,[539] na medida em que a base legal somente se aplicará se os dados manejados e o tratamento

[536] A Autoridade de Proteção de Dados Austríaca reforça a importância em se demonstrar a necessidade do tratamento para o alcance do objetivo que justificou a utilização da base legal de cumprimento de uma publ“c task: "O artigo 6 (1) (e) GDPR, que é aplicado na área soberana, também se baseia em tal necessidade de processamento de dados. De acordo com isto, o processamento só é legal se for necessário para o desempenho de uma tarefa que seja de interesse público ou no exercício da autoridade oficial. A condição de necessidade exige, de acordo com a finalidade protetora da GDPR (Art. 1 § 2), limitar o processamento de dados pessoais ao que é absolutamente necessário. O processamento deve, portanto, ser necessário tanto para o desempenho de tarefas de interesse público quanto para o exercício da autoridade oficial, para que a pessoa responsável possa desempenhar essa tarefa de forma eficiente. Isto deve ser avaliado de acordo com critérios objetivos, a partir dos quais existe uma conexão entre os dados e a finalidade perseguida com o processamento (ver Heberlein em Ehmann / Selmayr, DS-GVO² Art 6 Rz 23; ver também § 1 Parágrafo 2 última frase DSG, segundo a qual a invasão do direito fundamental só pode ser realizada da forma mais branda possível para o objetivo). De acordo com a jurisprudência do Supremo T“ibunal, "n”cessário" no sentido do Art. 9 Parágrafo 2 lit. f GDPR significa que sem os dados a afirmação da reivindicação ou uma defesa contra ela não seria possível ou significativamente mais difícil (OGH, 24 de julho de 2019, 6Ob45 / 19i). Tal avaliação da necessidade de seu processamento não é possível sem o conhecimento dos dados e das circunstâncias mais detalhadas de seu proce”samento." (tradução nossa). Disponível em: https://gdprhub.eu/index.php?title=BVwG_-_W256_2240235-1. Acesso em 14.08.2022.

[537] O Tribunal de Amsterdam também estou a necessidade do tratamento de dados pretendido para identificar a aplicabilidade da base legal prevista no art. 6(2)(e). Disponível em: https://gdprhub.eu/index.php?title=Gerechtshof_Amsterdam_-_200.280.852/01. Vide também: https://gdprhub.eu/index.php?title=OLG_Schleswig_-_17_U_15/21. Acesso em 14.08.2022.

[538] Segundo a Working Party 29, na Opinião “4/2014: "Estas situações estão se tornando cada vez mais comuns, também fora dos limites do setor público, considerando a tendência de terceirização de tarefas governamentais para entidades do setor privado. Este pode ser o caso, por exemplo, no contexto de atividades de processamento no setor de transporte ou saúde (por exemplo, estudos epidemiológicos, pesquisa). Este fundamento também pode ser invocado num contexto de aplicação da lei, como já sugerido nos exemplos acima. Entretanto, a medida em que uma empresa privada pode ser autorizada a cooperar com as autoridades de aplicação da lei, por exemplo, na luta contra a fraude ou conteúdo ilegal na Internet, requer uma análise não apenas nos termos do Artigo 7, mas também do Artigo 6, considerando a limitação de propósito, legalidade e requisitos de”justiça." (tradução nossa). Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Acesso em 14.08.2022.

[539] De acordo com Schiopu (2018): "Em alguns países, a lei nacional estabelece que as autoridades públicas são responsáveis pelo tratamento de dados pessoais no contexto de suas funções - competência legal explícita (Grupo de Trabalho de Proteção de Dados do Artigo 29, 2010, p. 10). Por outro lado, mais freqüentemente é o caso quando a lei, em vez de nomear diretamente o responsável pelo tratamento ou estabelecer os critérios para sua nomeação, estabelece uma tarefa ou impõe um dever a uma entidade de coletar e processar determinados dados. Além disso, uma entidade pode ser encarregada de certas tarefas públicas que não podem ser cumpridas sem a coleta de pelo menos alguns dados pessoais. No que nos diz respeito, acreditamos que as autoridades da administração pública podem confiar no fundamento previsto no artigo 6 parágrafo (1) letra e) GDPR somente na medida em que, embora a lei não preveja a obrigação de processar dados pessoais, este processamento é intrínseco ao desempenho de uma tarefa de interesse público ou ao exercício da autoridade oficial investida do controlador. Assim, as autoridades da administração pública poderão recorrer ao artigo 6 parágrafo (1) letra e) da GDPR quando, embora sua tarefa, função ou poder relevante que envolve o processamento de dados pessoais esteja estabelecido em lei, elas não podem identificar, além disso, a disposição legal específica que estabelece claramente sua obrigação de processar dados pessoais." (tradução nossa).

realizado forem razoavelmente necessários. Se houver outra forma razoável e menos intrusiva de alcançar o mesmo resultado, essa base legal não será aplicável. Sobre esse respeito, o Conselho de Estado da Holanda afirmou que, embora caiba ao controlador demonstrar que o tratamento é necessário para o alcance do objetivo almejado, não será necessário a ele prever e avaliar todas as possíveis alternativas ao tratamento (RvD, 20215).

Outra característica dessa base legal é que não será necessária a existência de lei expressa sobre o tratamento de dados pessoais específicos, desde que ele seja esperado para o exercício de funções legais atribuídas ao controlador. É permitido que a lei apenas indique objetivos gerais que deverão ser alcançados por aquele que estiver exercendo a função pública ou buscando o alcance de determinado interesse público.[540] Essa é uma das principais diferenças dessa base legal em relação à base de cumprimento de obrigação legal (art. 6(1)(c), GDPR), na medida em que esta última precisa estar prevista em norma que indique as características e necessidade do tratamento.

De todo modo, como se verifica, na base legal de exercício de função no interesse público, o tratamento de dados pessoais consiste em uma das possíveis formas de alcançar o objetivo geral estabelecido pela legislação. Isso significa que o controlador terá discricionariedade sobre como cumprir com a obrigação, desde que observar os requisitos de necessidade, razoabilidade e proporcionalidade. Por esse motivo, **(i)** essa base legal se aproxima também da base legal do legítimo interesse, visto que oferece autorização mais ampla ao tratamento de dados pessoais, desde que o controlador promova prévio teste de balanceamento e demonstre a necessidade do tratamento de dados; e **(ii)** o balanceamento entre interesses não será realizado pelo responsável pela edição do ato legal (diferente da base legal prevista no art. 6(1)(e), em que o legislador realiza essa avaliação previamente à edição do ato legal), mas pelo gestor público antes de iniciado o tratamento.

Entre os aprendizados decorrentes da análise sobre como a GDPR regula essa base legal está em entender seus limites, a saber: **(i)** o agente público deverá estar atuando dentro

[540] De acordo com Schiopu (2018): "Quando os dados pessoais são processados a fim de executar uma tarefa específica de interesse público que está estabelecida por lei ou para processar dados pessoais no exercício da autoridade oficial (funções e poderes públicos estabelecidos por lei), o controlador não precisa de um poder legal específico para processar dados pessoais, mas sua tarefa, função ou poder subjacente deve ter uma base legal clara (Information Commissioner's Office, 2018, p. 75). Se o controlador tem um poder legal específico para processar dados pessoais ou precisa processar os dados pessoais para cumprir uma obrigação legal, então o fundamento legal para o processamento será o cumprimento de uma obrigação legal à qual o controlador está sujeito de acordo com o artigo 6 parágrafo (1) letra c) GDPR. Entretanto, a última edição do Handbook on European data protection law (2018, p. 151) menciona que "as obrigações legais dos responsáveis pelo tratamento de dados do setor público também podem ser abrangidas pelo artigo 6 (1) (e) da GDPR" (tradução nossa).

de suas atribuições legais ou exercendo função para o interesse público previsto em lei; **(ii)** a atividade não precisa estar expressamente prevista em lei, podendo se tratar de uma autorização legal ampla; **(iii)** a atividade deverá ser necessária para o alcance do objetivo legal, não sendo aplicável se for possível alcançar o mesmo objetivo de outra forma razoável e menos intrusiva; e **(iv)** será permitido a particular utilizar essa base legal, desde que comprovado que esteja atuando em substituição ao poder público no alcance do interesse público ou para o cumprimento de determinação legal.

Assim, quando a norma for mais aberta, determinando apenas objetivos gerais à atuação do poder público, a base legal aplicável à divulgação dos dados será a execução de políticas públicas e caberá ao gestor público maior grau de discricionariedade sobre qual atividade realizar e como ela deverá ser executada.[541] Nesse caso, a ponderação entre a privacidade do cidadão e o interesse público no acesso aos dados é realizada pelo agente público em sua capacidade executiva e mediante o exercício de discricionariedade em relação às condições de tratamento dos dados. Por isso, o administrador será o responsável por justificar a necessidade do tratamento pretendido, avaliar os riscos que a atividade impõe aos titulares de dados, ponderar sobre o interesse público envolvido no uso dos dados, e apontar sobre quais salvaguardas adotar para proteger os titulares.

Na prática, isso significará a elaboração de documentação que justifique e comprove a necessidade e proporcionalidade do tratamento para cumprir com os objetivos de determinado dispositivo legal (que, para dados triviais, poderá inclusive em contratos e convênios). Nos casos em que se diagnosticar que a atividade impõe elevado risco à liberdade e direitos de cidadãos, essa tarefa poderá ser realizada com o apoio de um Relatório de Impacto. Além disso, em vista desses cuidados adicionais exigidos para a fundamentação do tratamento na base legal de execução de políticas públicas, que oferecem maior proteção a direitos de titulares de dados, ela poderá ser utilizada em substituição à base legal de cumprimento de obrigação legal ou regulatória quando houver norma que exija o tratamento de dados pessoais, mas ofereça a maior discricionariedade na sua execução prática.

[541] Por exemplo, a autorização da LAI para que governos publiquem dados pessoais quando eles forem de interesse público permite grande espaço de avaliação ao gestor público sobre quais dados inserir no portal de transparência e em qual formato.

16.3 Legítimo Interesse do controlador e de terceiros

Finalmente, a base legal de legítimo interesse pode ser utilizada quando o tratamento de dados for necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso em que prevaleçam direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (art. 7º, IX). Entre as atividades de tratamento de dados que podem ser fundamentadas na base legal do legítimo interesse estão a (i) segurança física e segurança de rede; (ii) marketing e propaganda; (iii) mensagens comerciais não solicitadas, incluindo propaganda de campanha política ou para arrecadamento de caridade; (iv) o tratamento posterior de dados tornados públicos (WP 29, 2014).

Trata-se de base legal mais flexível, motivo pelo qual a legislação não autoriza sua utilização para o tratamento de dados pessoais sensíveis e estabelece algumas condições para que possa ser utilizada.[542] Para tanto, a LGPD determina que o legítimo interesse deve ser aplicado para finalidades legítimas que incluem, mas não se limitam, ao apoio e promoção de atividades do controlador, e à proteção do exercício regular dos direitos do titular ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais (art. 10, I e II). Além disso, a LGPD aponta, caso aplicável o legítimo interesse, que somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados (art. 10, §1º), e que o controlador dos dados deve estabelecer medidas para garantir a transparência no tratamento de dados baseado no legítimo interesse. Assim, essa base legal exige prévia: (i) compreensão do que pode ser considerado legítimo interesse do controlador ou de terceiro; e (ii) avaliação sobre em que medida este legítimo interesse pode ser alegado, diante dos direitos e liberdades fundamentais do titular.[543]

Apesar dessas determinações, a LGPD não traz critérios claros e específicos para que se consiga avaliar se há um cumprimento das condições apresentadas pelo art. 10. Por esse

---

[542] De forma similar se posicionaram Carlos Affonso Souza, Mário Viola e Vinícius Padrão (2019): "Com efeito, a hipótese autorizativa dos interesses legítimos pode ser vis-ta como um dos requisitos mais flexíveis para justificar o tratamento de da-dos pessoais. No entanto, justamente em razão dessa flexibilidade, a hipótese torna- se mais complexa, dado que será necessário um exercício argumentativo constante para a sua incidência."

[543] O relator do Projeto de Lei da LGPD, Deputado Orlando Silva, destaca que o "legítimo interesse, contudo, não deve ser lido como um cheque em branco. Em outras palavras, não pode ser utilizado como um subterfúgio para que todo e qualquer tratamento de dados pessoais seja autorizado. Esta a razão dos parágrafos do artigo, mediante os quais se destaca que o legítimo interesse deve sempre vir acompanhado dos princípios da adequação, necessidade e transparência bem como da possibilidade de fiscalização. Ademais, prevemos que deverá se basear em situação concreta e desde que atendidas as legítimas expectativas do titular". Para mais informações, vide: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=SBT+1+PL406012+%3D%3E+PL+4060/2012. Acesso em 04.01.2023.

motivo, assim como realizado para as bases legais de cumprimento de obrigação legal e regulatória e execução de políticas públicas, será realizada análise sobre seus contornos na legislação europeia que, como mencionado, inspirou diversas disposições da LGPD.

O GDPR prevê o legítimo interesse como um dos fundamentos jurídicos para o tratamento de dados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular de dados e sejam levadas em consideração as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável pelo tratamento. Para tanto, o interesse do controlador ou de terceiros deve ser suficientemente claro (isto é, interesses especulativos ou vagos não são considerados suficientes), além de ser real e presente, correspondente a atividades atuais da empresa ou benefícios que são esperados em um futuro próximo.[544]

O teste de legítimo interesse tem sua aplicação dividida em quatro etapas: (a) verificação da **legitimidade do interesse,** que envolve identificar se há direitos fundamentais e/ou normas que justificam esse tratamento, se a finalidade é legítima, e se o tratamento beneficia a comunidade e não somente interesses particulares; (b) **necessidade** do tratamento, momento no qual se avalia os impactos positivos e negativos do tratamento sobre direitos e liberdades dos indivíduos, considerando-se a natureza dos dados, a probabilidade de risco, quem são os titulares de dados (e.g., crianças ou pessoa em situação de vulnerabilidade) as condições do tratamento (e.g., dados disponíveis publicamente ou grandes quantidades de dados), o equilíbrio de poder entre controlador e titular, e as legítimas expectativas dos titulares de dados; (c) **balanceamento**, o que inclui verificar a avaliação de equilíbrio entre as pretensões do controlador e os direitos dos titulares de dados; e (d) implementação de **salvaguardas**, o que implica assegurar transparência sobre o tratamento e a adoção de ações que mitiguem seus riscos (e.g., minimização de dados, medidas técnicas e organizacionais e anonimização).

Como se pode observar, o teste de legítimo interesse possui considerável similaridade com o teste de proporcionalidade para fins de sopesamento de princípios constitucionais (MATIUZZO, PONCE, 2020). De fato, o teste de proporcionalidade no modelo abordado nesta tese é segmentado em três etapas (e não quatro, como no teste de legítimo interesse ou no teste de proporcionalidade adotado por Tribunais europeus), consistentes em avaliar se a medida observa os requisitos de adequação, necessidade e proporcionalidade em sentido

[544] Para mais informações, acesse: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Acesso em 04.01.2023.

estrito. Se comparados o teste de legítimo interesse e o teste de proporcionalidade: (i) a etapa de adequação se aproxima à avaliação da legitimidade do interesse, na medida em que avaliam se o interesse almejado pode ser alcançado pelo tratamento, que deverá ser suficientemente específico, concreto e lícito; (ii) a avaliação sobre a necessidade do tratamento se equipara ao teste de necessidade, visto que buscam identificar riscos do tratamento e a existência de medidas alternativas que podem alcançar o mesmo objetivo de formas menos onerosas aos titulares de dados; e (iii) o teste de proporcionalidade em sentido estrito incluiria tanto as avaliações de balanceamento e de existência de salvaguardas, visto que buscam harmonizar os riscos do tratamento em relação aos interesses do controlador ou de terceiros.

E não poderia ser diferente, pois as bases legais são uma dentre as medidas destinadas a assegurar aos indivíduos mais autonomia sobre como seus dados são tratados, e a base legal de legítimo interesse é mais flexível que as demais bases legais. Assim, como o legítimo interesse, em tese, permite maior flexibilização a direitos e liberdades de titulares de dados, o sopesamento de interesses é recomendado. Do mesmo modo, também para reduzir os riscos associados à maior flexibilidade dessa base legal, a LGPD não permite que ela seja utilizada para o tratamento de dados sensíveis e impõe ao controlador maior ônus quando do seu uso.

Esse é um dos motivos pelo quais na GDPR, o legítimo interesse não é aplicável às atividades de tratamento de dados realizadas por entes públicos na consecução das suas atribuições (Conosiderando 47 e art. 6, GDPR).[545] A mesma restrição não era prevista na Diretiva 95/46/EC, que regulava a proteção de dados pessoais na Europa até a edição da GDPR. Como apontado pela WP29 na Opinião nº 06/2014 sobre o legítimo interesse, a mudança se deve ao fato de que as bases legais de cumprimento de obrigação legal e de função realizada em benefício do interesse público serem mais apropriadas para atividades de tratamento realizadas pelo poder público:

> A proposta de alteração legislativa destaca a importância do princípio geral de que as autoridades públicas, em regra, só devem proceder ao tratamento de dados no exercício das suas funções se tiverem a devida autorização legal para o fazer. A adesão a este princípio é particularmente importante - e claramente exigida pela jurisprudência do Tribunal Europeu dos Direitos Humanos - nos casos em que a privacidade dos titulares de dados está em jogo e as atividades da autoridade pública interferem em sua privacidade. Também é necessário autorização suficientemente detalhada e específica por lei - também nos termos da atual Diretiva - caso o tratamento por autoridades públicas interfira na privacidade dos titulares dos dados.

[545] Essa é uma inovação da GDPR, na medida em que não havia similar determinação na Diretiva anterior que regulava o tratamento de dados pessoais na Europa.

A LGPD silencia sobre o tema, não esclarecendo a respeito da sua aplicação para atividades realizadas por órgãos e entidades públicas ou por particulares em benefício do poder público. Nesse sentido, seria hipoteticamente possível ao poder público utilizar-se da base legal de legítimo interesse, desde que: (i) superado o teste do legítimo interesse; e (ii) não aplicáveis outras bases legais como as de cumprimento de obrigação legal e regulatória e execução de políticas públicas. No entanto, acredita-se que a combinação dessas duas condições seria particularmente desafiadora, especialmente pelo fato de as referidas bases legais estarem relacionadas ao princípio da finalidade, aplicável aos atos da administração pública. Soma-se a isso o fato de a base legal de execução de políticas públicas já oferecer ao agente público maior flexibilidade para o tratamento de dados pessoais e exigir do controlador a adoção de medidas similares àquelas exigidas para a utilização da base legal do legítimo interesse.

Por outro lado, o legítimo interesse poderá ser utilizado por particulares receptores de dados compartilhados ou publicados pelo poder público, desde que permitido pelo teste de legítimo interesse e observados o princípio da finalidade, a boa-fé e o interesse público que justifiquem a publicação e o compartilhamento de dados. Como será mais detidamente abordado adiante neste capítulo, embora essa exigência esteja expressamente prevista na LGPD para dados acessíveis ao público (art. 7º, §§ 3º e 7º), uma análise sistemática da LGPD impõe que o mesmo seja observado para qualquer atividade de reuso a dados divulgados pelo poder público.

Dito isso, será necessário ao interessado em reutilizar os dados se utilizando da base legal do legítimo interesse atribuir particular atenção aos seguintes elementos da avaliação das etapas de legitimidade e necessidade, do teste de legítimo interesse: (a) a legitimidade do tratamento secundário que deseja realizar, que deverá beneficiar não somente seus interesses particulares e ser compatível com as finalidades que justificaram a divulgação; e (b) a avaliação das legítimas expectativas dos titulares de dados, na medida em que os dados foram originalmente coletados pelo poder público por força de legislação ou como condição para o exercício de direitos, utilização de serviços públicos ou obtenção de benefícios sociais.

Para tanto, exerce papel importante a transparência, a elaboração de documentos de *accountability* e a garantia de meios para que titulares possam exercer seus direitos. A transparência, que deverá ser assegurada pelo poder público e pelo novo controlador, garante que cidadãos tenham clareza: (i) que seus dados poderão ser compartilhados ou publicados pelo governo e reutilizados por terceiros; (ii) sobre as novas finalidades de reuso de seus

dados; e (iii) dos direitos que possui para limitar eventual reuso de dados e os meios que dispõem para exercê-los. Os documentos de *accountability* auxiliam o controlador a avaliar a presença de interesse legítimo no reuso e registram esse esforço para fins de prestação de contas, e os mecanismos de exercício de direitos fornecem ao titular de dados algum controle sobre como os dados que forneceu a governos serão reutilizados por terceiros.

17 DIREITOS DE CIDADÃOS SOBRE O COMPARTILHAMENTO E PUBLICAÇÃO DE DADOS

Como mencionado anteriormente, a compreensão da proteção de dados pessoais como uma releitura do direito à privacidade passa pelo reconhecimento do direito à autodeterminação informativa dos cidadãos. Com isso, a anterior concepção da privacidade, enquanto uma simples prerrogativa dos indivíduos em manter sigilo sobre sua vida privada, é substituída pelo direito de cidadãos terem conhecimento e exercerem influência sobre como e para quais finalidades suas informações são utilizadas por terceiros.

Embora esse direito de autodeterminação informativa tenha, em um primeiro momento, sido instrumentalizado por meio da coleta de consentimento do titular de dados, apostar somente nessa solução se mostrou pouco efetivo. Entre os motivos para tanto esteve o aumento na quantidade de dados pessoais que são tratados e no aumento da complexidade em que dados são processados e inferências são criadas. Diante disso, e com o objetivo de permitir maior transparência sobre as atividades de tratamento de dados realizadas e de assegurar novas formas para que o indivíduo possa exercer algum grau de controle sobre o uso de seus dados, leis em diversos países passaram a prever alguns direitos aos titulares de dados.

Os primeiros direitos assegurados estavam relacionados à confirmação sobre a existência do tratamento dos seus dados pessoais, o acesso aos dados, e a correção de dados incompletos, inexatos ou desatualizados.[546] Esses direitos foram previstos em instrumentos diversos, como o *habeas data,* presente em leis diversas na América Latina. No Brasil, ele busca assegurar ao cidadão mecanismos para acessar e corrigir informações suas que o governo mantém (Constituição Federal, art. 5º, LXXII), o que é em grande medida explicado pelo contexto ditatorial que precedeu a elaboração da Constituição Federal.[547] No entanto, em outros países da América Latina, como o exemplo da Colômbia, o *habeas data* busca assegurar direitos em face de usos de seus dados por agentes públicos ou privados.

---

[546] "Durante os anos 70 e 80, inúmeras leis de privacidade foram aprovadas nos EUA e na UE, e quase todas elas continham direitos, especialmente os direitos de acesso e correção. Nos anos 80, muitos países latino-americanos adotaram um conjunto central de direitos de privacidade em suas constituições conhecido como "writ of habeas data "16 O nome do writ significa "você tem os dados "1Os direitos de dados de Habeas apareceram pela primeira vez em 1988 na constituição do Brasil e logo se espalharam para outros países, como Colômbia (1991), Paraguai (1992), Peru (1995), Argentina (1994) e Equador (1996, tradução nossa)". (SOLOVE, 2022).

[547] Vide explicação sobre o direito de habeas data nas palavras da autoridade colombiana de proteção de dados pessoais: https://www.sic.gov.co/manejo-de-informacion-personal. Acesso em 02.05.2021.

De todo modo, as mais modernas leis de proteção de dados pessoais, inspiradas pelo exemplo da GDPR, prevêem novos meios para que os titulares de dados pessoais possam exercer controle sobre como seus dados pessoais são tratados, como os seguintes exemplos: (i) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade; (ii) portabilidade dos dados; (iii) eliminação dos dados tratados através da base legal do consentimento; (iii) direito de peticionar autoridades competentes contra o controlador dos dados; ou (iv) direito de oposição ao tratamento de dados justificado em outras bases legais que não o consentimento (SOLOVE, 2022).

Na LGPD, esses direitos estão previstos essencialmente (ainda que não exclusivamente) no art. 18 e, para o poder público (art. 23, §3º), deverão ser observadas também a legislação específica, como a Lei do *Habeas Data* (Lei nº 9.507/1997), e a Lei de Acesso à Informação (Lei nº 12.527/2011). No entanto, a LGPD não esclarece a forma de compatibilizar o exercício dos direitos de titulares com as referidas normas, cabendo ao gestor encontrar soluções na prática ou em observância de posterior regulação de órgãos com competência para editar regulação sobre o tema.

Em breve síntese, o titular tem o direito de obter, a qualquer momento, a confirmação sobre a existência do tratamento dos seus dados pessoais pelo controlador (art. 18, I, LGPD) e o acesso aos dados pessoais em tratamento (art. 18, II, LGPD). O controlador também deve fornecer ao titular a possibilidade de corrigir dados incompletos, inexatos ou desatualizados (art. 18, III, LGPD), cuja finalidade é garantir a qualidade dos dados pessoais. Outros direitos assegurados aos titulares de dados, e que são atrelados à desconformidade do tratamento com a lei, consistem na possibilidade de se opor a tratamento que não seja fundamentado em seu consentimento, solicitar a anonimização, o bloqueio ou a eliminação de dados desnecessários e excessivos ou então tratados em desconformidade com a legislação aplicável (art. 18, IV e VI, LGPD). Finalmente, a LGPD também prevê aos titulares o direito de solicitar a portabilidade dos seus dados pessoais para outro prestador de serviços ou fornecedor de produtos, respeitados os segredos de indústria e comércio (art. 18, V, LGPD).

No entanto, a despeito da sua relevância, a garantia desses direitos não pode ser entendida como a principal ferramenta para que titulares de dados possam exercer controle sobre como seus dados pessoais são utilizados (assim como ocorre com o consentimento, que possui eficácia limitada quando utilizado como principal fundamento legal). Como aponta Solove (2022), embora os direitos de titulares tenham um papel central na proteção de dados pessoais, não é possível atribuir a eles maior responsabilidade do que são capazes de exercer.

Esses direitos apostam na capacidade de indivíduos efetivamente compreenderem (e.g., dúvida sobre seu conteúdo e sobre os riscos decorrentes do tratamento de dados realizado por terceiros) e terem disponibilidade para exercer seus direitos, especialmente considerando a quantidade de controladores de dados pessoais em face de quem os direitos serão exercidos.[548] Além disso, os direitos de titulares são soluções focadas em indivíduos para problemas que muitas vezes alcançam terceiros ou toda uma coletividade. No atual momento de desenvolvimento tecnológico, a análise de dados poderá dizer respeito a mais de um indivíduo ou revelar informações a outras pessoas com características semelhantes ou que integram o mesmo grupo social. No entanto, o exercício de direitos por um indivíduo possui impacto limitado e não alcança os demais membros da coletividade (SOLOVE, 2022).

De fato, nesta tese se entende a garantia de direitos a titulares de dados como ferramenta necessária, mas com capacidade restrita de assegurar controle ao cidadão sobre seus dados pessoais quando tratados e divulgados pelo poder público. Isso se dá justamente pelo fato de que, na maioria das vezes, a possível inadequação no tratamento de dados pessoais não ocorrerá somente em relação a uma pessoa, mas afetará toda ou uma parcela da sociedade. Assim, soluções pautadas em iniciativas individuais de cidadãos não serão suficientes para resolver eventual problema sistêmico do tratamento.

Além disso, como muitas vezes a divulgação de dados será fundamentada em obrigação legal, determinados direitos não serão aplicáveis, a exemplo da revogação do consentimento ou da deleção de dados. Por isso, no caso de tratamento de dados pelo poder público, para além da garantia de ferramentas para que cidadãos possam exercer seus direitos, são tão ou mais importantes iniciativas de *accountability* e transparência. Essas medidas são cruciais para que entidades com legitimidade para defender direitos coletivos em juízo ou reguladores possam avaliar e questionar a adequação das atividades realizadas por determinado órgão ou entidade pública. Além disso, considerando que muitas atividades de tratamento de dados pessoais realizadas pelo poder público são fundamentadas em legislação,

[548] "Em muitos casos, um indivíduo deve exercer não apenas um direito, mas vários direitos. Estes múltiplos direitos devem ser exercidos com centenas, se não milhares, de organizações. Mesmo quando uma pessoa exerce direitos com cada organização, os dados que essas organizações coletam e os usos dos dados mudam com o tempo. Por exemplo, novas informações estão sendo constantemente adicionadas ao relatório de crédito de uma pessoa. Assim, os indivíduos não devem exercer os direitos apenas uma vez para cada agência de informação ao consumidor, mas também devem fazê-lo de forma rotineira, talvez até mesmo diariamente. Esta seria uma tarefa desafiadora se as agências de informação ao consumidor fossem as únicas organizações que reuniam e utilizavam os dados das pessoas. Mas existem centenas, talvez milhares, de tais organizações. Policiar os registros de uma pessoa em todas essas organizações com freqüência seria um trabalho difícil para uma grande equipe de trabalhadores em tempo integral; não há nenhuma maneira plausível para um indivíduo solitário exercer todos os direitos proporcionados por várias leis de privacidade de uma forma sistemática significativa." (tradução nossa). (SOLOVE, 2022).

igualmente importante avaliar se normas existentes ou em elaboração preveem mecanismos para assegurar direitos dos cidadãos em relação a seus dados pessoais.

Em seguida serão abordados os contornos dos direitos assegurados aos cidadãos em relação ao seu tratamento pelo poder público. Essa análise não será realizada de forma exaustiva, mas tão somente com o objetivo de estabelecer um primeiro esforço de conectar o disposto na LGPD com a legislação vigente aplicável às atividades governamentais. Uma análise mais aprofundada no tema é urgente, e deve contar com a identificação de boas práticas adotadas nacional e internacionalmente, especialmente em países que possuem legislação específica para o tratamento de dados pelo poder público, a exemplo do México e do Canadá. De todo modo, para fins desta tese, serão primeiro abordados os direitos tradicionalmente oferecidos aos cidadãos brasileiros, alguns desde a edição da Constituição Federal e, em seguida, os direitos mais recentemente previstos na legislação brasileira.

17.1 Direitos tradicionalmente assegurados: acesso aos dados, e a correção de dados incompletos, inexatos ou desatualizados

Como mencionado, certos direitos são tradicionalmente assegurados aos cidadãos em relação aos seus dados pessoais mantidos pelo Estado. Esse é o caso dos direitos de acesso e correção a dados pessoais, que no Brasil foi assegurado após a previsão constitucional do *habeas data* e reforçado por outras normas, como a Lei de *Habeas Data*, a LAI e a Lei nº 13.460/2017.[549]

A Lei de *habeas data* (Lei nº 9.507/1997), estabelece que os cidadãos poderão apresentar requerimento administrativo perante órgão ou entidade que detenha o registro ou banco de dados para que possa solicitar acesso e retificação de suas informações pessoais.[550] De acordo com o julgamento pelo STF do Recurso Extraordinário nº 673.707, trata-se de

[549] Interessante notar que a Lei Canadense destinada a regular a proteção de dados pessoais mantidos pelo poder público, os direitos assegurados aos titulares de dados são os de acesso e retificação. Vide art. 12 em diante da Privacy Act, disponível aqui: https://laws-lois.justice.gc.ca/eng/acts/p-21/fulltext.html. Acesso em 04.09.2022.

[550] Há precedentes do Superior Tribunal de Justiça que determina o que se segue: "embora o art. 5º, XXXIII, da Carta Magna de 1988 tutele o direito à informação, de interesse particular ou coletivo, não se pode afirmar que o *habeas data* o resguarde. Deveras, o direito à informação abrange os mais variados temas, como, *in casu*, o direito de petição junto a administração pública; enquanto que o *habeas data* visa assegurar o acesso às informações pertinentes à própria pessoa do impetrante e desconhecidas pelo mesmo [...]. A pretensão do impetrante, de obter certidão para o cômputo do adicional por tempo de serviço, respeita ao direito de informação, cuja previsão encontra-se no art. 5º, XXXIII, da Carta Magna de 1.988, devendo ser pleiteada via mandado de segurança" STJ. EDcl no HD 67 – DF, Relatora Ministra DENISE ARRUDA, Primeira Seção, DJ de 02 de agosto de 2.004; HD 67 MC – SP, decisão monocrática do Ministro CELSO DE MELLO, DJ de 18 de novembro de 2004.

remédio constitucional assegurado aos cidadãos para que possam ter ciência das informações que são mantidas sobre si em registros públicos ou de caráter público, de forma a "preservar o status de seu nome, planejamento empresarial, estratégia de investimento e [...] a recuperação de tributos pagos indevidamente".[551] Por isso, o *habeas data* deve ser movido pela própria pessoa sobre quem os dados se referem e pode alcançar informações sigilosas.[552]

A entidade requerida terá um prazo de 48 horas para responder (art. 2º) e 24 horas para comunicar o requerente (art. 2º, parágrafo único). Caso o pedido de acesso aos dados seja deferido e o solicitante verificar inexatidão de registro ou informação, poderá encaminhar petição acompanhada de documentos comprobatórios para solicitar sua retificação (art. 4º). A retificação (ou anotação no cadastro do indivíduo, caso a entidade pública não diagnostique inexatidão) deverá ser realizada em até 10 dias (art. 4º, §§1º e 2º). Por outro lado, caso o pedido de acesso ou de retificação não seja apreciado ou implementado dentro do prazo, ou caso seja rejeitado, o solicitante poderá ajuizar a ação judicial de *habeas data* para fazer valer o pedido rejeitado pela via administrativa (art. 7º).

Já a Lei de Acesso à Informação assegura procedimento para que cidadãos possam solicitar acesso a informações de interesse público não divulgadas por meio de transparência ativa. Como mencionado anteriormente, a LAI impõe ao poder público o dever de garantir o acesso à informação, de forma ativa (ou seja, independente de requerimento) ou passiva (mediante solicitação), que será efetivada mediante procedimentos objetivos, ágeis, de forma transparente, clara e em linguagem de fácil compreensão (art. 5º). Para tanto, o poder público deverá oferecer aos cidadãos orientação sobre os procedimentos para o acesso às informações desejadas (art. 7º, I) e apresentar informações primárias, íntegras, autênticas e atualizadas (art. 7º, V). O procedimento de transparência passiva será gratuito[553] (art. 12) e realizado mediante requerimento, que poderá ser apresentado em canais oficiais na internet (art. 10, §2º), que indique com precisão a informação de interesse público que se deseja acessar e apresente a

---

[551] STF, Recurso Extraordinário 673.707-MG. Ministro Relator Luiz Fux, julgado em 17 de junho de 2015. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur322444/false. Acesso em 04.012023.

[552] "As informações fiscais conexas ao próprio contribuinte, se forem sigilosas, não importa em que grau, devem ser protegidas da sociedade em geral, segundo os termos da lei ou da constituição, mas não de quem a elas se referem, por força da consagração do direito à informação do art. 5o, inciso XXXIII, da Carta Magna, que traz como única ressalva o sigilo imprescindível à segurança da sociedade e do Estado, o que não se aplica no caso *sub examine"* STF, Recurso Extraordinário 673.707-MG. Ministro Relator Luiz Fux, julgado em 17 de junho de 2015. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur322444/false. Acesso em 04.01.2023.

[553] No entanto, segundo o art. 12, §1º da LAI: "O órgão ou a entidade poderá cobrar exclusivamente o valor necessário ao ressarcimento dos custos dos serviços e dos materiais utilizados, quando o serviço de busca e de fornecimento da informação exigir reprodução de documentos pelo órgão ou pela entidade pública consultada."

identificação do solicitante, sendo vedado aos órgãos ou entidades públicas a imposição de exigências que inviabilizem a realização do pedido (art. 10, §3º).

O procedimento de transparência previsto na LAI também pode ser utilizado por cidadãos para acessar seus dados pessoais mantidos pelo poder público,[554] mas não será o instrumento apto a corrigir os dados incompletos, inexatos ou desatualizados.[555] Além disso, e diferentemente do *habeas data*, o pedido de acesso à informação fundamentado na LAI não será mecanismo adequado para fornecer informações sigilosas, na medida que se destina a fornecer à sociedade informações de interesse público.

A entidade que possui os dados solicitados deverá responder imediatamente ou, não sendo possível, dentro do prazo de 20 dias, prorrogáveis por mais 10 dias (art. 11, §§1º e 2º). Se o solicitante autorizar, a informação deverá ser fornecida preferencialmente em formato digital (art. 11, §5º). Em sua resposta, o ente público consultado deverá: (i) comunicar data, local e modo de acesso à informação; (ii) indicar as razões para a recusa do pedido, que poderá ser total ou parcial; ou (iii) comunicar que não possui a informação e, se possível, indicar qual órgão ou entidade pública que poderá atender ao pedido (art. 11, §1º). Em caso de negativa, o solicitante poderá recorrer, dentro do prazo de 10 dias da ciência da decisão (art. 15), para a autoridade hierarquicamente superior à que proferiu a decisão, que deverá se manifestar dentro de 5 dias (art. 15, parágrafo único). Caso negado o acesso à informação e tratar-se de autoridade da administração pública Federal, o solicitante poderá recorrer à CGU, que terá 5 dias para se manifestar (art. 16), e, posteriormente, à Comissão Mista de Reavaliação de Informações.

O Decreto nº 7724, de 12 de maio de 2012, que regulamenta a LAI, determina que os órgãos devem disponibilizar formulário padrão para que qualquer pessoa faça pedido (art. 11,

---

554 Nesse sentido se manifestou o Ministro do Supremo Tribunal Federal, Ricardo Lewandowski, no julgamento do Recurso Extraordinário nº 589998, em 12.09.2023 "[...] inobstante a LAI não tenha substituído o *habeas data* (mesmo porque tal ato seria flagrantemente inconstitucional), inegável que o espírito dessa lei teve por espírito diminuir as ações de *habeas data* perante o judiciário, conforme declaração do próprio ministro chefe da CGU à época da análise do projeto de lei, da onde se conclui, por óbvio, que ambos os instrumentos, seja o habeas data, seja a LAI, possuem o mesmo objeto, a saber: informações de caráter público."

555 Nesse sentido, se posicionou a CGU: "Ocorre que debates sobre retificação de dados realizam-se em procedimentos diversos daquele regulamentado pela Lei de Acesso à Informação (lei 12.527/2011). Para essas situações, a Constituição Federal (tal como a lei 9.507/97) reconheceu o instituto do habeas data [...)]. Assim, orienta-se o cidadão a socorrer-se desse instrumento constitucional, porquanto os processos instaurados no âmbito da Lei 12.527/2011 visam a disponibilização de dados e de informações tal como os detém os órgãos e entidades públicos do Poder Executivo Federal." Parecer nº 23480.003273/2016-21 no Recurso contra resposta incompleta ao pedido de acesso à informação movido contra a Fundação Universidade Federal do ABC. Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/23480003273201621_CGU.pdf#search=%22habeas%20data%22. Acesso em 30.08.2022.

§2º) informando o nome do requerente, número de documento de identificação válido, especificação da informação solicitada e endereço para que recebe a resposta (art. 12). O Decreto veda qualquer forma de exigência de motivação para que os pedidos sejam atendidos (art. 14), de modo a facilitar o acesso à informação e minimizar os casos de resposta negativa por eventual alegação de falta de interesse no conteúdo solicitado. Ainda, estabelece que apenas poderá ser solicitado pagamento para acesso à informação nos casos em que, para se atender ao pedido, seja necessário reprodução de materiais. Nesses casos, o órgão disponibilizará ao requerente Guia de Recolhimento da União ou documento equivalente, para pagamento restrito dos custos dos serviços e dos materiais utilizados (art. 18).

Por sua vez, a Lei nº 13.460/2017,[556] que dispõe sobre os direitos do usuário dos serviços públicos da administração pública federal, estabelece direitos básicos do usuário, como os exemplos do acesso e obtenção de informações relativas à sua pessoa constantes de registros ou bancos de dados (art. 6º, III), da obtenção e utilização de serviços com liberdade de escolha entre os meios oferecidos e sem discriminação (art. 6º, II), do recebimento de informações precisas e de fácil acesso (art. 6º, VI), e da proteção de suas informações pessoais (art. 6º, IV). Além disso, a norma estabelece que os procedimentos administrativos referentes a esses direitos devem ser pautados pela eficiência e celeridade (art. 12), serem viabilizados por formulários simplificados e de fácil compreensão (art. 10, §6º) e serem explicados na Carta de Serviços ao Usuário (art. 7º). Assim, a lei assegura aos usuários de serviços públicos os direitos de acesso e proteção das suas informações pessoais mantidas pelo poder público, cujo exercício deve ser viabilizado, de forma eficiente e eficaz, em local de fácil acesso e com liberdade de escolha entre os mecanismos oferecidos.

A manifestação deverá ser dirigida à ouvidoria (quando existente) do órgão ou entidade responsável, por meio eletrônico, oral ou correspondência convencional (art. 10, §4º). No caso de comunicação eletrônica, a administração pública poderá desenvolver a certificação da identidade do usuário (art. 10, §5º). Além disso, o poder público não poderá impor exigências de identificação do solicitante ou motivação do pedido que possam acabar por inviabilizar sua manifestação (art. 10, §§1º e 2º), bastando a apresentação do número de inscrição no CPF.[557] Finalmente, as informações sobre identificação serão protegidas com restrição de acesso (art. 10, §7º).

---

[556] Vide: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13460.htm. Acesso em 03.09.2022.

[557] No entanto, como esclarece a CGU, sequer o requisito de apresentação do CPF pode ser uma condição ao atendimento de pedido de acesso à informação de interesse público. A seguir, segue trechoem sobre esse respeito: "Em resposta, a Fundação Universidade de Brasília - UnB alegou que o pedido de informação não

Na LGPD, o acesso a dados é relacionado ao princípio de livre acesso (art. 6º, IV)[558] e está elencado entre os direitos assegurados aos titulares de dados pessoais (art. 18, II). Esse direito poderá ser precedido de pedido de confirmação pelo controlador de que seus dados são por ele tratados (art. 18, I) e deverá ser acompanhado de informações a respeito de como o tratamento é realizado (art. 9º). O formato para atendimento desta solicitação pode ocorrer, a critério do titular, por meio eletrônico ou de forma impressa (art. 19, §2º, I e II). A resposta deverá ser fornecida de modo imediato e em formato simplificado ou por meio de declaração clara e completa, em até 15 dias da data do requerimento pelo titular (art. 19, II). Nos casos em que o controlador realiza tratamento de dados pessoais com base em consentimento ou na execução de contrato em que o titular seja parte, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais (art. 19, §3º), respeitados os segredos industriais e comerciais do controlador, que possui particularidades para o poder público ou particulares atuando em parceria com o Estado. Esse procedimento deverá ser informado pelo órgão ou entidade pública em local de fácil acesso e em formato de fácil compreensão.

A LGPD também requer que os dados pessoais sejam armazenados em formato que favoreça o exercício do direito de acesso. No caso do poder público, essa obrigação se associa ao dever de manter dados em formato interoperável e estruturado para o uso compartilhado (art. 25). Nesse sentido, a LGPD requer que a adoção de sistemas eletrônicos não somente seja direcionada a facilitar o fluxo de dados entre órgãos e entidades públicas para o fim de

---

pôde ser atendido, pois não cumpriu os requisitos de admissibilidade previstos no art. 10 da Lei no 12.527/2011 e no art. 12 do Decreto no 7.724/2012. Inicialmente, a título de esclarecimento prévio à análise de mérito, ressalte-se que a possibilidade de preservação da identidade do solicitante foi medida implementada com base na Lei no 13.460/2017 - que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da Administração Pública - com vistas à promoção e ao aprimoramento da transparência pública no Brasil. Nesse sentido, ao prever que a identificação do requerente é informação pessoal protegida com restrição de acesso nos termos da LAI, o art. 10, §7o da Lei no 13.460/2017 faculta ao requerente optar pela preservação de sua identidade, sendo este um direito que não eclipsa o seu direito de acesso à informação, nos termos da Lei de Acesso à Informação - LAI. [...]. Após análise da integralidade do processo, verifica-se que a negativa de acesso à informação pleiteada, de fato, vai de encontro à legislação vigente, porquanto não reconhece a legitimidade do pedido do solicitante pelo fato de a sua identidade não ter sido revelada, o qual encontra amparo legal na previsão constante do art. 10o, §7o da Lei no 13.460/2017, conforme explicado anteriormente. Nesse sentido, é importante salientar mais uma vez que, ao prever que a identidade do requerente se configura como informação pessoal protegida nos termos da LAI, o art. 10o, § 7o da Lei no 13.460/2017 faculta manter a identificação do solicitante sob sigilo, sem que esse fato impacte negativamente no seu direito de solicitar aos órgãos públicos informações de inegável caráter público e não protegida por nenhuma hipótese de sigilo legal." Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/23480024491201942_CGU.pdf. Acesso em: 26.11.20222.

[558] O princípio do livre acesso exige que os agentes de tratamento assegurem consulta facilitada e gratuita sobre a forma e a duração do tratamento de dados que realizam e o princípio da qualidade dos dados requer a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

execução de políticas públicas e de suas atribuições legais, mas também para operacionalizar com qualidade e rapidez os direitos de titulares de dados.

Quanto à alegação de incompletude, inexatidão ou falta de clareza, ela encontrará alguns desafios, como quando **(a)** o dado for derivado de uma decisão do controlador com base em dados corretos; **(b)** as informações forem necessárias para constituir elementos de prova em procedimentos administrativos ou processos judiciais,[559] ou **(c)** se tratar de bancos de dados que reproduzam ou guardem documentos oficiais, peças de procedimentos administrativos ou processos judiciais. De todo modo, esses desafios vêm sendo enfrentados em procedimentos administrativos e judiciais, especialmente em procedimentos de *habeas data*.[560]

A seguir consta quadro comparativo de como a legislação vigente e aplicável ao poder público regula os direitos de confirmação, acesso e correção de dados:

Quadro 9: Semelhanças e diferenças no direito de acesso a dados pessoais entre a Lei de *Habeas Data*, LAI, Lei nº 13.460/2017 e LGPD

	Lei de Habeas Data	**LAI**	**Lei nº 13.460/2017**	**LGPD**
Proponente	Cidadão ou representante legal	Cidadão	Usuário de serviço público	Titular de dados ou representante legal

559 Por outro lado, habeas data apreciado pelo Tribunal de Justiça do Paraná determinou a retificação do Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade do Conselho Nacional de Justiça, na medida em que inadequadamente inseridos. TJPR. Habeas Data 1569980-8. Impetrante: Cláudio Dirceu Eberhard. Impetrado: Presidente da 4ª Câmara Cível do Tribunal de Justiça do Estado do Paraná. Relator: Des. Leonel Cunha. Julgado em: 31/10/2017. Disponível em: https://portal.tjpr.jus.br/e-dj/publico/diario/baixar.do?tjpr.url.crypto=0816f08ecbc775d55aa4ef22398087e31772d2855b57a12ec00ed3382c4c4543#page=173. Acesso em 26.11.2022.

560 Por exemplo, decisão proferida pelo Tribunal Regional Federal da 3a Região concedeu o pedido formulado pelo solicitante de retificação de seus dados no Cadastro Nacional de Informações Sociais (CNIS) para esclarecer que não está mais empregado pelo exército. Segundo o solicitante, a inadequação das informações no CNIS estava impactando sua possibilidade de usufruir de assistência social. TRF-3. Remessa Necessária Cível 5000520-19.2019.4.03.6003. Autor: Edinaldo de Oliveira Santos. Réu: Instituto Nacional do Seguro Social. Relatora: Desembargadora Federal Mônica Nobre. Julgado em: 18.10.2021. Disponível em: https://pje2g.trf3.jus.br/pje/ConsultaPublica/DetalheProcessoConsultaPublica/documentoSemLoginHTML.seam?ca=75243bb30f32a07358b563222303ac7e5ae52db29c483490ebf92d82f4ecec655ea1978872dd3e5725ca5723b6a5fe2baac761f7c0295fc4&idProcessoDoc=203731402. Acesso em 10.12.2022. Caso similar, mas julgado pelo Superior Tribunal de Justiça. STJ. Habeas Data nº 472-DF. Impetrante: Anne Gabriela Alves Tome. Impetrado: Ministério da Cidadania. Relator: Ministro Herman Benjamin. Julgado em 09.06.2021. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=2067984&num_registro=202003443998&data=20210803&formato=PDF. Acesso em 10.10.2022.

Escopo	Confirmação, acesso e retificação de informações suas mantidas pelo governo.	Acesso a informações de interesse público (sobre o solicitante ou terceiros)	Acesso a informações suas mantidas pelo governo	Confirmação, acesso e retificação de informações suas mantidas pelo controlador
Identificação e motivação	Não esclarecido na Lei (mas solicitante deve comprovar sua identidade)	Vedadas exigências de motivação ou de identificação que inviabilizar o pedido	Vedadas exigências de motivação; Apresentação de documento com nº do CPF	Não esclarecido na Lei (mas solicitante deve comprovar sua identidade e não precisa motivar)
Forma de cumprimento	Não esclarecido na Lei	Informação armazenada em formato digital será fornecida nesse formato;	Liberdade de escolha sobre os mecanismos oferecidos: eletrônico, oral, correspondência	Por meio eletrônico ou de forma impressa, a critério do titular
Custos	Não esclarecido na Lei	Gratuito, podendo cobrar ressarcimento de serviços e materiais	Não previsto na Lei	Gratuito, conforme regulação
Prazos	48h de resposta, 24h para comunicar e 10 dias para retificação	Acesso imediato ou 20 dias que podem ser prorrogados por mais 10 dias	30 dias prorrogáveis por mais 30 dias	Se simplificado, imediatamente; se completa, em 15 dias

Como se verifica, os direitos de confirmação, acesso e retificação de dados pessoais mantidos pelo poder público são assegurados aos cidadãos brasileiros desde a vigência da Constituição Federal, com regulação pela Lei de *Habeas Data* (Lei nº 9.507/1997). No entanto, devido à ainda existente cultura de opacidade na administração pública e da exigência de recurso judicial em caso de não atendimento ao pedido formulado pelo cidadão, o exercício desses direitos pelo mecanismo do *habeas data* não foi amplamente adotado.

Alguns anos depois, com a edição da LAI e da Lei nº 13.460/2017 (que regula os direitos do usuário de serviços públicos), foram assegurados aos cidadãos outras ferramentas para acessar suas informações pessoais de forma mais célere e simplificada. Em pesquisa simples à ferramenta de pesquisa a decisões da CGU, é possível notar que essas três leis (ie.: Lei de *Habeas Data*, LAI e Lei nº 13.460/2017) vêm sendo utilizadas em conjunto para assegurar aos cidadãos o acesso a suas informações que são mantidas por governos. No entanto, como se pode notar pelo quadro acima, há diferenças de escopo e procedimento entre

essas leis, que vem sendo compatibilizadas na prática. Por exemplo, enquanto a Lei de *Habeas Data* assegura aos cidadãos o direito de confirmação, acesso e retificação de informações pessoais, a LAI e a Lei nº 13.460/2017 apenas prevêem o direito de acesso a dados pessoais. Além disso, ao passo que os procedimentos da Lei de *Habeas Data* e na Lei nº 13.460/2017 devem ser movidos pela pessoa sobre quem as informações se referem e podem alcançar informações sigilosas, o procedimento previsto pela LAI pode ser movido por qualquer interessado e só alcança informações de interesse público.

Outro ponto de divergência reside nos prazos apresentados: enquanto a Lei de *Habeas Data* exige resposta em 48 horas (com prazo de 24h para comunicar o solicitante), a LAI determina o prazo de 20 dias prorrogáveis por mais 10 dias e a Lei nº 13.460/2017 estabelece prazo de 30 dias prorrogáveis por mais 30 dias. O prazo que prevalecerá será aquele do procedimento escolhido pelo titular de dados para realizar o seu pedido. Sobre esse respeito, Laura Schertel Mendes (2014) argumenta que aplica-se a "lei de acesso para o procedimento administrativo (formas de acesso, prazos, responsabilidade) e a lei do *habeas data* para a regulamentação do instrumento processual, caso a Administração negue o acesso do cidadão às informações".

Em relação aos pontos de contato, em todas as leis há vedação de exigências de motivação ou de identificação que possam inviabilizar o pedido formulado. No entanto, especialmente nos procedimentos previstos pela Lei de *Habeas Data* e pela Lei nº 13.460/2017, os pedidos de confirmação e acesso a informações pessoais dependerá de prévia identificação do indivíduo, especialmente se o pedido envolver informações sigilosas, de forma a garantir a segurança dos dados e proteger a privacidade dos titulares de dados. Além disso, em todas essas normas o pedido será gratuito e processado preferencialmente na forma eletrônica, respeitada a liberdade de escolha diversa pelo solicitante. Segundo a LAI, a depender dos custos gerados pelo serviço e produção da resposta, o poder público poderá solicitar o ressarcimento dos custos incorridos para responder à solicitação.

Limitações ao exercício de direitos de titulares tratados pelo poder público

Controladores poderão deixar de atender, parcial ou integralmente, a solicitações de acesso à informação em certas circunstâncias, quando a solicitação for **manifestamente excessiva** ou **implicar esforço desproporcional**. A análise desses fatores dependerá de uma abordagem caso a caso e não dão ao controlador o direito de recusar solicitações com base em qualquer dificuldade ou obstáculo encontrado. Essa exceção possui respaldo tanto na lei de

proteção de dados pessoais como na legislação aplicável à divulgação de dados pelo poder público.

Em relação à LGPD, ela não estabelece referida exceção expressamente, mas prevê alguns fundamentos pelos quais controladores podem limitar ou restringir um pedido de exercício de direitos, como o exemplo da proteção ao segredo comercial ou industrial (e.g., arts. 9°, II, 18, V, 19, II, 19, §3° e 20, §1° da LGPD), a falta de razoabilidade dos recursos necessários para anonimizar dados (art. 6°, XI, 12 da LGPD) ou a impossibilidade ou desproporcionalidade dos esforços para comunicar outros controladores com os quais divulgaram dados sobre as solicitações recebidas de exercício de direitos de titulares de dados (art. 18, §6° da LGPD).

Em relação às normas que regulam a divulgação de dados pelo poder público, é possível identificar casos em que será impossível atender a solicitações do cidadão por resultarem em esforço desproporcional ou irrazoável por parte do poder público, ou por serem contrários à boa-fé ou afrontarem direitos de terceiros. Primeiramente, cumpre observar que referidos requisitos possuem respaldo na Constituição Federal, na Lei que regula o Processo Administrativo da administração pública Federal (Lei nº 9.784/1999) e no Decreto que regula a LAI no âmbito da administração pública Federal (Decreto nº 7.724/2012). Embora essas normas não sejam destinadas a regular solicitações de exercício de direitos assegurados a titulares de dados pessoais, sua regulação e prática são aplicáveis a esses pedidos.

Por sua vez, o art 13 do Decreto nº 7.724/2012 estabelece que não serão atendidos pedidos de informação que sejam **genéricos**, **desproporcionais ou desarrazoados** ou que **exijam trabalhos adicionais** de análise, interpretação ou consolidação de informações, ou serviço de produção ou tratamento de dados que não seja de competência do órgão ou entidade. Com isso, a legislação busca assegurar que pedidos de acesso à informação sejam apresentados considerando sua finalidade social - a saber, viabilizar o controle social, o acesso a informações e o exercício de direitos por cidadãos -, e evitar seu manejo para fins espúrios e contrários à boa-fé, de forma a onerar economicamente o Estado ou em prejuízo a direitos de terceiros.

Será considerado **genérico** o pedido que não descreve de forma clara e precisa (art. 12) o objeto do pedido de informação (e.g., período temporal, localização, formato), de forma a dificultar a delimitação do alcance do pedido. A falta de precisão do pedido resulta em impossibilidade fática de cumprimento por parte do poder público. Nas palavras da CGU: "O

assunto do registro solicitado deve ser indicado de modo individualizado e com suficiente particularidade quanto ao tempo, lugar e evento, de forma a permitir que o servidor do órgão ou entidade que tenha familiaridade com o assunto possa identificá-lo de maneira célere e precisa" (CGU, 2013). No entanto, o pedido de especificação não pode ser tamanho que inviabilize o exercício do direito pelo cidadão, como apontado pela Controladoria: "é desarrazoado exigir-se que do cidadão que este delimite ainda mais o escopo do seu pedido, pois isso não seria apenas dificultoso, mas simplesmente impossível do ponto de vista fático."[561]

Já o pedido **desproporcional** será aquele que significativa e comprovadamente comprometa a realização das atividades do ente público detentor da informação, inclusive podendo prejudicar a resposta a pedidos de acesso à informação realizados por outros solicitantes. Por exemplo, em pedido de acesso a ofícios e avisos assinados nos anos de 2016 e 2017 pelo Ministro do Planejamento, Desenvolvimento e Gestão e pelo Ministério dos Transportes, Portos e Aviação Civil, a Controladoria rejeitou o recurso por concordar com o órgão recorrido que o pedido seria genérico e desproporcional. A desproporcionalidade residiria na necessidade de, para cada Ministério, avaliar cerca de 500 avisos e 400 ofícios para identificar quais não poderiam ser divulgados por se enquadrarem nas hipóteses legais de restrição de acesso, de modo a comprometer as atividades regulares da unidade.[562] Em outro exemplo, o argumento de falta de proporcionalidade foi acolhido em pedido de acesso à informação que requereu informações atualizadas sobre a estrutura organizacional da Universidade Federal de Goiás (UFG), incluindo nome da unidade administrativa e competências legais. Para comprovar a desproporcionalidade, o ente requerido apresentou cálculo de horas que seriam gastas por servidores públicos para cumprir com o pedido, o que resultaria em prejuízo a outras demandas corriqueiras da instituição.[563]

---

[561] Vide: CGU, Parecer 502, de 24/02/2014, elaborado pela Auditoria Federal de Finanças e Controle Anjuli Tostes Faria Osterne.

[562] Conforme esclarece a própria CGU quando do julgamento do Recurso contra negativa de acesso à informação nsº 03950.003129/2017-85 e 50650.003930/2017-95, realizada pelo Ministério de Planejamento, Desenvolvimento e Gestão e pelo Ministério dos Transportes, Portos e Aviação Civil Disponível em: https://apublica.org/wp-content/uploads/2020/02/resposta-recurso-cgu-03950003129201785-e-50650003930201795.pdf. Acesso em 28.08.2022.

[563] Na resposta apresentada pela UFG, que foi acolhida pela CGU, argumentou-se que: "para atender a demanda de informação, dimensionamos o seguinte esforço empregado: (a) 1 servidor para execução da demanda e 1 servidor para coordenação do trabalho, tendo em vista as especificidades técnicas que precisam ser observadas; (b) Servidor de execução: 320 horas; Servidor de coordenação: 32 horas; (c) Total de horas: 352; (d) 2 meses para a conclusão da atividade. Observação: Não há servidores disponíveis para atendimento do pedido, uma vez que, no presente momento, estes estão envolvidos com outras demandas da instituição." Conforme relata a CMRI (Comissão Mista de Reavaliação de Informações) no Julgamento do Recurso contra negativa de acesso à informação nº 23546.007197/2021-89. Disponível em:

Por sua vez, o pedido **desarrazoado** será aquele que não está alinhado aos objetivos da LAI e não possui amparo na legislação vigente. Essa ausência de razoabilidade decorre do potencial lesivo da divulgação da informação (como atrasos no cumprimento de outras atividades essenciais ou o cerceamento de direitos fundamentais de terceiros), mesmo que o cidadão não deseje prejudicar o Estado ou terceiros com a informação.[564] Na jurisprudência da CGU, em poucos casos se reconheceu que seria impossível divulgar informações com base nesse argumento.[565] No entanto, a desarrazoabilidade foi reconhecida em alguns casos, como o exemplo de pedido de acesso à íntegra de toda a correspondência digital institucional trocada pelo presidente da EBC e pelo seu chefe de gabinete no ano de 2017. No caso, a CGU entendeu que o pedido seria desarrazoado por contemplar lapso temporal demasiadamente amplo, não identificar o assunto de interesse e exigir da requerida a execução de serviço catalogação de informações em e-mails. A falta de razoabilidade, no caso, estaria também conectada à apresentação de pedido genérico (ie.: não identifica assunto de interesse), desproporcional (ie.: contempla período de tempo externo) e exige dos agentes públicos trabalho adicional (ie.: catalogar emails para identificar a presença de informações pessoais, sensíveis, de tomada de decisões e de estratégia da empresa).

Finalmente, ao permitir a recusa de pedidos que **exijam trabalhos adicionais**, a legislação reconhece outra situação de impossibilidade fática de cumprimento da solicitação pela entidade requerida, seja porque exige do órgão público a elaboração de informações em

---

https://www.gov.br/acessoainformacao/pt-br/assuntos/recursos/recursos-julgados-a-cmri/decisoes/2021-1/decisao-102-2021_nup-23546007197202189_ufg.pdf. Acesso em 28.08.2022.

564 "A avaliação acerca da razoabilidade demanda uma reflexão qualitativa a respeito da plausibilidade do pedido, ou seja, se este se encontra dentro dos limites impostos pelos princípios gerais do direito e pelo meio social com que o direito de acesso a informação dialoga. Trata-se de pedidos que vão de encontro ao espírito da própria Lei, e, em última instância, do interesse público, não constituindo manifestações legítimas do direito de acesso à informação. Exemplificando, pedidos que solicitem a planta de um presídio ou do Banco Central são desarrazoados, pois ultrapassarem os limites do que poderia ser considerado como aceitável num contexto social, beirando o absurdo. Para facilitar a compreensão, expomos abaixo algumas categorias/situações em que um pedido pode ser considerado como desarrazoado: a) Pedidos desrespeitosos – são aqueles pedidos que, apesar de conterem uma solicitação de informação, são redigidos em tom insultuoso, acusativo, depreciativo ou ofensivo, especialmente nos casos em que são direcionados a servidores identificados (...) b) pedidos obsessivos – têm por efeito ou intenção sobrecarregar a capacidade do órgão/entidade, com objetivo de prejudicar suas operações. Ocorre quando várias pessoas, de modo coordenado, ou uma pessoa, de forma contínua, agem de modo a desorganizar as funções do órgão ou entidade. Os pedidos obsessivos, em geral, se analisados isoladamente, poderiam ser considerados razoáveis; no entanto, postos em contexto, caracterizam-se pela ausência de razoabilidade devido a existência de várias solicitações realizadas de modo coordenado ou sucessivo. (...) c) Pedidos frívolos – trata-se de solicitações jocosas, sarcásticas ou que objetivam expor o órgão ou entidade ao ridículo. Não têm fundamentação ou propósito razoável, caracterizam-se pela falta de seriedade ou senso." CGU, recurso de acesso à informação nº 16853.007617/2012-05, julgado em 17.07.2013.

565 Conforme esclarece o próprio CGU quando do julgamento do Recurso contra negativa de acesso à informação nº 99936.000114/2017-12 realizada pela EBC (Empresa Brasil de Comunicação S.A.). Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/99936000114201712_CGU.pdf. Acesso em 28.08.2022.

formatos não existentes ou porque o processamento de dados necessários ao cumprimento do pedido e fogem sua competência do órgão requerido - nesse caso, a resposta ao pedido de acesso à informação deverá indicar o ente público com competência para realizar essa atividade. De fato, a lei não exige que a informação seja entregue no formato solicitado pelo cidadão, podendo ocorrer no formato existente.

Além disso, o controlador também poderá deixar de atender a pedido de exercício de direitos de titular de dados quando verificar que a solicitação pode **afetar adversamente direitos e liberdades de um terceiro**. Por exemplo, quando o atendimento a um direito do titular implicar a divulgação de dados pessoais de terceiros que não tenham consentido com essa divulgação, faz-se necessário considerar se esta solicitação pode ser atendida parcialmente, aplicando técnicas de anonimização aos dados de terceiros e disponibilizando exclusivamente os dados requisitados pelo titular. A LGPD não regula expressamente essa exceção, mas ela é fruto de uma interpretação sistemática de seus dispositivos, na medida em que: (i) seu art. 9º permite ao titular acesso facilitado às informações sobre o tratamento se seus dados (e não de terceiros), e (ii) uma lei destinada a assegurar a privacidade de um indivíduo não poderá impor limitações irrevogáveis à privacidade de terceiros (art. 2º, II e IV).

17.2 Atualização dos direitos: anonimização, bloqueio, eliminação, oposição e portabilidade

Para além dos direitos já assegurados tradicionalmente pela legislação brasileira, a LGPD apresentou novas formas para o titular de dados exercer alguma modalidade de controle sobre como seus dados pessoais são tratados. Entre elas estão a anonimização, o bloqueio, a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD (art. 18, IV), a eliminação dos dados pessoais tratados com o consentimento do titular (art. 18, VI), a oposição ao tratamento realizado com fundamento nas bases legais alternativas ao consentimento e em descumprimento com o disposto na LGPD (art. 18, § 2º), e solicitação de portabilidade de seus dados a outro fornecedor de serviço ou produto (art. 18, V).

No entanto, isso não significa que esses controles não tenham sido anteriormente assegurados na prática, por outros mecanismos existentes no ordenamento jurídico, a exemplo de decisão judicial que determine a suspensão de certa atividade de tratamento de dados

pessoais em função de sua ilegalidade ou inconstitucionalidade. Por exemplo, no julgamento das ADIs nº 6.387, 6.388, 6.389, 6.390 e 6.393, o STF declarou a constitucionalidade da Medida Provisória nº 954/2020 e a consequente suspensão do compartilhamento de dados pessoais de todos os usuários se serviços de telefonia com o IBGE.

Em relação aos direitos de **anonimização, bloqueio e eliminação dos dados pessoais**, eles se aplicarão quando o controlador possuir dados excessivos ou desnecessários ou quando o tratamento for realizado em desconformidade com a legislação. Os já mencionados direitos de confirmação, acesso e transparência assumem papel importante na eficácia desses direitos, na medida em que fornecem informações aos titulares de dados sobre quais de seus dados são tratados, para quais finalidades e em quais condições. De todo modo, quando o controlador estiver diante de solicitação de exercício de qualquer um desses direitos, ele deve primeiro se certificar se realmente: **(i)** mantém dados excessivos ou desnecessários, ou que sua atividade é realizada em desconformidade com a LGPD; **(ii)** não possui obrigação ou justificativa legal para manter os dados e seguir com a atividade de tratamento. Caso alguma dessas hipóteses se confirme, o controlador deverá cumprir com a solicitação apresentada.

Por outro lado, será possível ao controlador recusar, total ou parcialmente, a solicitação encaminhada pelo titular de dados se o tratamento for necessário para cumprir obrigação legal ou regulatória, executar políticas públicas ou para o exercício de direitos em processos judiciais, administrativos ou arbitrais. No caso do poder público, será comum a existência de justificativa legal para a manutenção dos dados e do tratamento realizado, na medida em que a maioria de suas atividades são fruto de exigência legal ou uma etapa necessária à execução de suas atribuições legais. Também será possível recusar o pedido infundado (e.g.: se o indivíduo claramente não possui a intenção de exercer seus direitos ou se o pedido possuir objetivos maliciosos) ou excessivo (e.g.: pedidos repetidos em relação a pedidos anteriores), conforme será mais detidamente detalhado adiante.

Em relação à solicitação de **bloqueio** dos dados pessoais, ele assegura ao indivíduo a possibilidade de limitar a forma como seus dados são tratados. Sua implementação poderá ser temporária ou definitiva e resultará, nos termos da LGPD, em "suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados" (art. 5º, XIII). Em outras palavras, quando o direito de bloqueio é exercido, o controlador poderá seguir armazenando os dados, mas não poderá seguir com o tratamento suspenso.

Segundo a LGPD, ele poderá ocorrer quando o tratamento for sobre dados

desnecessários ou excessivos, ou quando o tratamento estiver em desconformidade com a LGPD. Na prática, esse direito oferece uma solução emergencial contra potenciais riscos ao tratamento inadequado de dados (por exemplo, enquanto se avalia a viabilidade da retificação de dados),[566] e como alternativa à eliminação dos dados, visto que eles poderão ser necessários para outras finalidades (incluindo o fornecimento de cópia dos dados para o titular), ou como um remédio temporário enquanto o controlador avalia outras solicitações de exercício de direitos apresentadas pelo usuário, a exemplo da objeção ao tratamento.[567]

Especificamente em relação à divulgação de dados pelo poder público, o direito de bloqueio pode assumir diversas formas, como a remoção temporária de dados publicados por força de políticas de transparência e dados abertos, a pausa do compartilhamento de dados com outras entidades, ou até a suspensão ao pedido de eliminação de dados pessoais que precisam ser mantidos por força de obrigação legal. No entanto, o direito não será concedido caso o órgão ou entidade pública possua obrigação legal ou regulatória de divulgar os dados (e.g., servidor público não poderá solicitar o bloqueio da publicação de seu salário), caso esse bloqueio afronte direitos de terceiros (e.g., se o bloqueio do compartilhamento de dados impacta o acesso a outros cidadãos a direitos, serviços públicos ou benefícios sociais) e/ou se demonstre que a divulgação dos dados é necessária ao alcance do interesse público.

A **oposição** ao tratamento pode ser solicitada quanto à totalidade ou parcela de atividade de tratamento não seja fundamentada no consentimento e desde que: **(i)** verificada que a base legal que fundamentou o tratamento legítimo de dados não se aplica mais; **(ii)** o

---

[566] Esse papel emergencial do direito de bloqueio é reconhecido pela Corte Administrativa de Baden Wüttemberg, conforme se verifica: "a) Com sua reclamação principal, o requerente prossegue a reclamação para substituir a inscrição no registro de residentes do réu referente ao seu ano de nascimento ("1958") pela inscrição "1953", por meio de uma correção. Uma condenação do réu a "restringir" o processamento desta data pessoal de acordo com ou análogo ao Artigo 18.1 letra a da DPA corresponderia, no máximo em parte, a esta reivindicação. No caso presente, tal condenação também está fora de questão por razões legais. Isto porque uma "não liquidação" para a questão da exatidão de uma data pessoal inscrita em um registro de população não leva - ao contrário de uma opinião defendida na literatura - a uma reivindicação de limitação. O artigo 18 parágrafo 1 letra a FADP prevê uma regra especial caso a exatidão de uma declaração seja contestada entre a pessoa em questão e o responsável pelo tratamento dos dados. De acordo com esta disposição, o envolvido tem o direito de solicitar ao responsável pelo tratamento que "limite" o tratamento se a exatidão dos dados pessoais for contestada pelo envolvido "por um período de tempo suficiente para permitir ao responsável pelo tratamento verificar a exatidão dos dados pessoais". Se o tratamento for restrito desta forma, Art. 18 § 2 A DPA estipula que, por enquanto, os dados pessoais em questão - além de serem armazenados - só podem ser processados com o consentimento do envolvido ou com a finalidade de afirmar, exercer ou defender reivindicações legais ou proteger os direitos de outra pessoa física ou jurídica ou com base em um interesse público importante da União ou de um Estado Membro." (tradução nossa). Disponível em: https://gdprhub.eu/index.php?title=VGH_Baden-W%C3%BCrttemberg_-_1_S_397/19. Acesso em 27.11.2022.

[567] Nesse sentido se posicionou o European Data Protection Supervisor em relatório de 2014 nomeado "Guidelines on the Rights of Individuals with regard to the Processing of Personal Data." Disponível em: https://edps.europa.eu/sites/edp/files/publication/14-02-25_gl_ds_rights_en.pdf. Acesso em 04.09.2022.

tratamento esteja em desconformidade com o disposto na LGPD. Na prática, o resultado prático do pedido de oposição poderá, mas nem sempre significará, a cessação do tratamento e a eliminação dos dados. Além disso, o direito de objeção não é absoluto, podendo o controlador prosseguir com o tratamento se conseguir demonstrar que possui motivos legítimos para tanto, que devem superar os interesses e direitos dos titulares de dados.[568]

A LGPD não delimita, para além do apontado acima, as condições para o exercício do direito de oposição. Na Europa, o direito de oposição (ou "*objection rights*") está atrelado às bases legais de legítimo interesse e de execução de atividade realizada para o interesse público, não sendo previsto para casos nos quais o tratamento de dados pessoais está fundamentado no cumprimento de obrigação legal ou regulatória (GDPR, art. 21(1)). Nesse sentido se posicionou a Corte de Justiça Europeia, em julgamento realizado antes mesmo da vigência da GDPR, reforçando a impossibilidade de objeção a atividades de tratamento realizadas com fundamento na base legal de cumprimento de obrigação legal.[569] No entanto, a Corte realizou ressalva de que essa limitação não se aplica quando a base legal aplicável for a de execução de atividade para o alcance do interesse público ("*task carried out in the public interest*") ou quando a lei que justifica a base legal de cumprimento de obrigação legal possua exceções.[570]

Além disso, como apontado pela Suprema Corte Holandesa e pelo Tribunal de Apelação Holandês de Arnhem-Leeuwarden, ainda que a legislação não autorize o direito de oposição em casos de tratamento de dados realizados com fundamento em obrigação legal, os titulares de dados não deverão ficar desamparados em relação a tratamentos realizados em desconformidade com a legislação. Não somente a legislação de proteção de dados pessoais prevê outros direitos similares que se aplicam a atividades baseadas em qualquer uma das

---

[568] Os direitos de eliminação e oposição ao tratamento de dados pessoais estão previstos na Lei Mexicana de Proteção de Dados Pessoais aplicável ao poder público. Vide arts. 46 e 47, disponíveis aqui: https://www.gob.mx/indesol/documentos/ley-general-de-proteccion-de-datos-personales-en-posesion-de-sujetos-obligados. Acesso em 04.09.2022.

[569] Vide: disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0028. Acesso em 04.09.2022.

[570] Segundo o EDPS, em manifestação a respeito do julgamento do caso C-28/08 P, *Commission v Bavarian Lager*: "Há uma distinção importante com relação ao direito de objeção entre o processamento dos dados com base no Artigo 5(b) (obrigação legal) e com base no Artigo 5(a) (tarefa realizada no interesse público). Se os dados forem processados com base em uma obrigação legal, isto é excluído do escopo do direito no Artigo 18(a) do regulamento de proteção de dados, e o envolvido não tem direito de objeção. Entretanto, se a obrigação legal não for incondicional e, por exemplo, incluir a exceção mencionada no parágrafo anterior, a saber, que os dados não serão divulgados publicamente no caso de haver um motivo para supor que a divulgação prejudicaria os legítimos interesses da pessoa e a identificação da pessoa envolvida é devidamente informada com antecedência, a pessoa em questão terá a possibilidade de apresentar as razões pelas quais considera que essa exceção se aplica a ela" (tradução nossa). Disponível em: https://edps.europa.eu/sites/edp/files/publication/11-03-24_bavarian_lager_en.pdf. Acesso em 04.09.2022.

bases legais (a exemplo dos direitos de retificação, eliminação e bloqueio), como o titular de dados pode recorrer a autoridades competentes para assegurar seus direitos[571] e o controlador de dados deverá assegurar que o tratamento é necessário, adequado e proporcional.[572]

A GDPR também estabelece que o direito de objeção deverá estar embasado na situação específica do titular de dados ("*relating to his or her particular situation*") e exige que o controlador demonstre possuir motivos legítimos convincentes ("*compelling legitimate grounds*") para seguir tratando os dados mesmo após a solicitação de oposição (art. 21). Em relação ao primeiro requisito, o entendimento majoritário (mas não uníssono) consiste em que o simples desejo de cessação do tratamento não seria o suficiente para justificar um pedido de oposição, sendo necessário demonstrar a presença de risco à sua vida, propriedade ou interesse assemelhado.[573] Em relação ao segundo requisito, ele exige do controlador maior esforço para comprovar a legitimidade da atividade de tratamento que desenvolve. Isso poderá envolver demonstrar que o benefício do tratamento alcança a sociedade como um todo e não somente os seus interesses econômicos, ou que o interesse no tratamento é reconhecido

---

[571] Conforme a Suprema Corte Holandesa: "Deve-se observar que a pessoa cujos dados pessoais foram processados com base na Arte. 6 parágrafo. 1, preâmbulo e sob c GDPR não tem os direitos de apagamento e objeção de dados estabelecidos no art. 6. 17 GDPR ou no Art. 21 GDPR. Isto não significa que o envolvido seja privado de proteção legal nesse caso. Por exemplo, ele pode recorrer ao tribunal civil com base no art. 17 GDPR. 6:162 do Código Civil Holandês, seja ou não em conjunto com o art. 8 CEDH, opor-se ao tratamento de seus dados pessoais (cf. o que foi considerado acima em 3.1.2)" (tradução nossa). Vide: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2021:1814 e https://gdprhub.eu/index.php?title=Hoge_Raad_-_21/00241. Acesso em 04.09.2022.

[572] Nas palavras do Tribunal "Se o tratamento de dados pessoais, como neste caso, se basear num dever legal, o titular dos dados ([recorrente]) não tem direito ao apagamento dos dados previsto no artigo 17 da [GDPR], conforme decorre do artigo 17, cláusula 3 (b) da [GDPR]. Nesse caso, o titular dos dados também não tem o direito de oposição referido no artigo 21 da [GDPR], uma vez que esse direito está ligado ao tratamento de dados com base no artigo 6.º, n.º 1, e ou f da [GDPR]. No entanto, a proteção das pessoas singulares no tratamento de dados pessoais é um direito fundamental, segundo o Considerando 1 da [GDPR]. [...] O acima exposto implica que, mesmo que o processamento de dados pessoais seja baseado em uma obrigação legal [...], a tarefa de cumprir essa obrigação não justifica automaticamente qualquer processamento de dados. [...] qualquer tratamento de dados pessoais deve cumprir os requisitos de proporcionalidade e subsidiariedade e, tendo em conta a natureza da invasão de privacidade, é necessário ponderar os interesses caso a caso necessário." (Tradução livre) Vide: https://gdprhub.eu/index.php?title=GHAL_-_200.256.387 e https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHARL:2019:10345&showbutton=true&keyword=AVG. Acesso em 04.09.2022.

[573] "Por exemplo, não seria suficiente que um sujeito de dados simplesmente indicasse que não quer que o processamento ocorra. Ao invés disso, eles poderiam ter que afirmar uma ameaça à sua vida, propriedade, ou algo semelhante. Em contraste, outros argumentam que o limiar não deve ser interpretado de forma muito estrita. Este ponto de vista pode ser apoiado por um julgamento do Tribunal Regional de Frankfurt, que considerou suficientes as dificuldades do reclamante em procurar um apartamento devido à divulgação de dados sobre sua dívida. Outro ponto de vista menos comum é que, em vez de agir como um pré-requisito para o exercício do direito de objeção, a frase "relativo à sua situação particular" indica simplesmente que o envolvido deve ter o direito de afirmar seus interesses específicos em seus dados pessoais não processados, o que o controlador pode considerar em sua ponderação de interesses.A GDPR não concede ao envolvido um direito geral de objeção ao processamento de seus dados pessoais. Ao contrário, este direito limita-se às circunstâncias delineadas no artigo 21(1) a (6) GDPR, conforme discutido mais adiante." (tradução nossa). Vide: https://gdprhub.eu/index.php?title=Article_21_GDPR#cite_note-1. Acesso em 04.09.2022.

expressa ou tacitamente por legislação europeia.[574]

Além disso, a GDPR também prevê a possibilidade de o titular de dados exercer o direito de objeção ao tratamento de dados realizado para fins de pesquisa, histórico ou estatístico, salvo se o tratamento for necessário com fundamento na base legal de execução de atividade realizada para o interesse público. Diante dessa limitação, que também se aplica ao direito de eliminação de dados, o *Considerando* 156 da GDPR exige que a legislação de estados-membros preveja salvaguardas para o tratamento desses dados, com especial ênfase à observância do princípio da minimização (que possui contornos similares ao princípio da necessidade).[575]

Trazendo essa discussão de volta para o contexto brasileiro e ao tratamento de dados pelo poder público, verifica-se que na LGPD não há: (i) limitação à objeção quando o tratamento de dados pessoais for realizado com base no cumprimento de obrigação legal ou regulatória; (ii) exigência para que o titular de dados demonstre a relevância da oposição para evitar ou fazer cessar situações de risco às suas liberdades individuais; (iii) dispositivo que expressamente permita o controlador a seguir com o tratamento de dados quando verificar que poderá legitimamente fazê-lo; e (iv) exceção ao direito de oposição para o tratamento realizado para fins históricos, de pesquisa e estatísticos, quando fundamentado na base legal de execução de políticas públicas. No entanto, é possível argumentar que essas regras da GDPR possuem algum respaldo na LGPD.

Primeiro, quando a atividade de tratamento de dados pessoais estiver fundamentada na

---

574 "De acordo com Zanfir-Fortuna, "convincente" significa que o interesse legítimo deve ser "avassalador" e anular os interesses do sujeito dos dados "de uma forma forte e significativa". Além disso, Herbst observa que não pode haver formas alternativas de satisfazer o interesse do controlador. Este interesse será considerado convincente se for reconhecido pela legislação da eu (seja expressa ou tacitamente) ou se estiver dentro do escopo remanescente de regulamentação pela legislação nacional. Isto inclui os interesses e objetivos descritos no Artigo 23(1)(a) a (j) GDPR (por exemplo, segurança nacional e pública), bem como no Considerando 73 GDPR (por exemplo, proteção da vida humana). Em qualquer caso, o limite é certamente superior ao interesse legítimo primordial que um controlador deve demonstrar sob o Artigo 6(1)(f) GDPR, pois qualquer processamento baseado no Artigo 6(1)(f) GDPR seria, de outra forma, essencialmente imune a objeção"." (tradução nossa). Vide: https://gdprhub.eu/index.php?title=Article_21_GDPR#cite_note-1. Acesso em 04.09.2022.

575 Sobre esse tema se manifestou a Autoridade Austríaca de Proteção de Dados Pessoais: "Como fica claro, em particular, no considerando 156 da GDPR, os Estados-Membros devem ter a permissão, sob certas condições e sujeito a garantias adequadas para os sujeitos dos dados, de fornecer informações mais precisas e exceções aos direitos de eliminação e objeção ao tratamento de dados pessoais arquivados para fins de interesse público, para fins de pesquisa científica ou histórica ou para fins estatísticos. O direito de objeção de acordo com o Art. 21 (6) A GDPR é um direito relativo de objeção que deve ser justificado. De acordo com o art. 21 (6) 21 Parágrafo 6, o responsável pode rejeitar a objeção se o processamento for necessário para fins científicos, históricos ou estatísticos para cumprir uma tarefa de interesse público (de acordo com äo Haidinger em Knyrim, DatKomm Art. 21 GDPR (a partir de 1º de outubro de 2018 , rdb.at), margem nos. 2 e 45 f)." (tradução nossa). Disponível em: https://gdprhub.eu/index.php?title=DSB_(Austria)_-_DSB-D124.1177/0006-DSB/2019. Acesso em 27.11.2022.

base legal de cumprimento de obrigação legal, acatar o pedido de oposição formulado pelo titular resultará em tratamento ilegítimo de dados pessoais, na medida em que contraria a legislação vigente e, para o poder público, também o princípio da legalidade (Constituição Federal, art. 5º, II). Por sua vez, a licitude do tratamento é requisito do princípio da finalidade (LGPD, art. 6º, I), que deverá guiar qualquer atividade de tratamento de dados pessoais. Por outro lado, assim como apontado pelo citado Tribunal de Apelação Holandês, caso a legislação que justificou a utilização da base legal de cumprimento de obrigação legal ou regulatória possua exceções ou permita algum nível de discricionariedade ao gestor público, nesses casos será possível legitimamente executar a oposição apresentada pelo indivíduo.

Segundo, na hipótese de oposição ao compartilhamento ou publicação de dados pessoais realizado pelo poder público, a própria legislação exige a ponderação entre a proteção dos dados pessoais (representado pelo direito de oposição) e o interesse público na divulgação da informação a terceiros ou à sociedade (LAI, art. 31, § 3º, V e LGPD, art. 23). Com isso, o atendimento automático de solicitação de oposição poderia resultar, no limite, em afronta ao interesse público. Nesse mesmo sentido se posicionou a Autoridade de Proteção de Dados Pessoais do Reino Unido ao argumentar que entidades públicas que receberem solicitação de objeção ao tratamento de dados e desejarem divulgar dados pessoais, ativa ou passivamente, deverão ponderar a objeção em relação ao interesse público na divulgação dos dados (ICO, 2020.2). No caso de preponderância do interesse público, a informação poderá ser divulgada a despeito da solicitação do indivíduo.

Já a **eliminação** dos dados requer um processo de exclusão definitivo dos dados nos bancos de dados pelo controlador. Esse direito está relacionado aos princípios da finalidade e da necessidade, visto que, se ausente uma finalidade para a manutenção dos dados ou se eles não forem mais necessários para o alcance de finalidades informadas aos titulares de dados, eles devem ser eliminados, salvo se houver outra base legal que justifique sua manutenção. Ela também poderá ser um pedido subsequente do exercício do direito de oposição, caso em que o controlador poderá avaliar a possibilidade de não cumprir com a solicitação realizada pelo titular de dados, tendo em vista seus interesses legítimos no tratamento.

Assim, para que o controlador possa cumprir com tal pedido, deverá ter ocorrido pelo menos algumas dessas situações: **(i)** encerrou-se a finalidade que justificou o tratamento dos dados e não há outra base legal que autorize a manutenção dos dados; **(ii)** o tratamento de dados pessoais se baseou no consentimento e o titular de dados revogou essa autorização; **(iii)** existência de obrigação legal que determine a exclusão dos dados; e **(iv)** o tratamento é

realizado em desconformidade com a LGPD. Em relação à primeira hipótese, o art. 16 da LGPD estabelece que dados poderão ser mantidos mesmo após o término da finalidade que justificou o tratamento em caso de seja necessário para: **(a)** o cumprimento de obrigação legal ou regulatória pelo controlador, **(b)** estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; **(c)** transferência a terceiro, desde que respeitado o disposto na LGPD; e **(d)** em caso de uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

No caso de tratamento de dados realizado pelo poder público, muitas vezes a exclusão dos dados não será o direito mais adequado, na medida em que a manutenção de dados pessoais por prazo prolongado pode ser necessária para o cumprimento de obrigações legais ou a execução de uma política pública. Nesse caso, os demais direitos ora abordados poderão ser mais apropriados, como o bloqueio ou a oposição a determinados tratamentos. De todo modo, é necessário ao poder público ter uma política de deleção de dados que deve ser informada aos titulares de dados.[576]

Além disso, caso os dados mantidos pelo poder público tenham sido divulgados por compartilhamento ou por publicação, o cumprimento desses direitos pode exigir que o controlador adote medidas para assegurar que os dados também sejam removidos das bases de dados mantidas por aqueles que receberam os dados (art. 18, §6º, LGPD). Similar obrigação é prevista no arts. 17(2) e 19 da GDPR, segundo os quais o controlador que tenha tornado públicos dados pessoais e recebe solicitação de eliminação de dados deverá adotar medidas razoáveis, levando em consideração custos e tecnologia disponível, para informar os demais controladores que tenham recebido os dados para que também cumpram com a solicitação de eliminação. Essa obrigação é dispensada caso se comprove que essa comunicação é impossível ou exige esforços desproporcionais pelo controlador (no entanto, a lei não apresenta critérios claros para essa avaliação). Além disso, ainda que a comunicação seja realizada, o outro controlador poderá ter uma justificativa legal para manter os dados por tempo prolongado, desde que possa fundamentar a atividade em uma das bases legais ou caso estejam presentes as demais exceções à eliminação.

Assim, nem sempre será possível ao poder público informar os outros controladores que tenham acesso a dados que tenha compartilhado ou publicado. De fato, é esperado que

[576] Nesse sentido se manifestou a autoridade de proteção de dados pessoais polonesa, que uma municipalidade estaria tratando dados em desconformidade com a legislação de proteção de dados pessoais porque, entre outros, não informava aos cidadãos o período que seus dados seriam divulgados a terceiros. Vide: https://gdprhub.eu/index.php?title=UODO_-_ZSPU.421.3.2019. Acesso em 27.11.2022.

essa comunicação seja menos custosa em casos de compartilhamento de dados (se comparado com a atividade de publicação de dados), visto que essa atividade geralmente é precedida de acordos estabelecidos entre as partes. No entanto, isso não significa que essa comunicação será sempre impossível em casos de publicação de dados, sendo possível ao órgão ou entidade pública adotar sistemas que, entre outras possíveis salvaguardas, permitam o envio de comunicação para aqueles que acessarem os dados. De todo modo, para que seja possível cumprir esse requisito, o órgão ou entidade pública que divulga dados pessoais deve implementar mecanismos técnicos ou jurídicos capazes de controlar ou identificar quais terceiros acessem os dados que estão compartilhando e publicando (e.g., firmar contratos, desenvolver RoPAs e adotar sistemas de gestão de acesso às bases de dados).

No caso da **anonimização**, ela possui relação direta com o direito de eliminação de dados, na medida em que ela busca remover a possibilidade de identificação do titular de dados. Como mencionado anteriormente, o direito de anonimização enfrentará dificuldade prática nos casos em que órgãos e entidades públicas reúnem grandes quantidades de dados (como na criação de cadastros unificados) ou quando são divulgados a terceiros, especialmente porque esses dados poderão ser associados a informações constantes de outras bases de dados e revelar dados pessoais. De todo modo, ele é uma alternativa para controladores continuarem tratando certos dados após pedidos válidos de eliminação dos dados, desde que seja possível efetivamente remover a capacidade de reidentificar o indivíduo.

Em relação ao direito à **portabilidade**, busca assegurar ao titular de dados maior controle sobre a transferência de dados a fornecedores de sua escolha para que possa utilizar essas informações no âmbito da prestação de seus próprios serviços. Ele também complementa o direito de acesso à informação por autorizar titulares de dados a receber uma cópia de seus dados em formato estruturado e inteligível, de modo a ser compreensível pelo titular de dados e que possa ser posteriormente utilizado por um fornecedor de sua escolha.

Não há na LGPD delimitação sobre como o direito deve ser viabilizado ao titular de dados, podendo ser disponibilizada ferramenta que o permita a baixar diretamente arquivo com seus dados, ou que envie diretamente as informações ao fornecedor de escolha do titular de dados. A expectativa é que o tema seja regulado pela ANPD e também setorialmente.

No entanto, ainda há consideráveis incertezas em relação ao exercício desse direito, especialmente quando o tratamento de dados é realizado pelo poder público. Por exemplo, há

autores que argumentam não ser o direito à portabilidade aplicável para órgãos ou entidades públicas, tendo em vista que a LGPD estabelece que ele será assegurado por fornecedor. Por isso, segundo esse entendimento, o direito à portabilidade estaria limitado às relações entre consumidor e fornecedor. Isso porque a LGPD utiliza o termo fornecedor para descrever em face de quem o titular poderia exercer esse direito e o poder público atua como fornecedor apenas quando presta serviços públicos singulares e remunerados por tarifa, o que limitaria de forma expressiva o âmbito de aplicação do direito à portabilidade (CRAVO; KESSLER; DRESCH, 2020). Por outro lado, essa interpretação não parece adequada porque a LGPD se aplica de forma relativamente homogênea sobre controladores e operadores, e não há exceção legal a esse direito para o poder público. Com isso, entende-se que qualquer controlador de dados, seja ele entidade pública ou privada, deverá cumprir com o direito à portabilidade.

De todo modo, ainda existem questões em aberto sobre a execução prática deste direito, especialmente no setor público, diante de sua complexidade técnica e operacional, além dos custos para estar em acordo com a lei (CRAVO; KESSLER; DRESCH, 2020). Além disso, é possível que seu alcance seja limitado em casos de tratamento de dados pessoais pelo poder público. Por exemplo, na Europa, o direito à portabilidade só se aplica aos casos em que a base legal usada para fundamentar o tratamento é o consentimento ou a execução de contrato (art. 20(1)a da GDPR). Caso se adote o mesmo parâmetro no Brasil, em vista da preponderância das bases legais de cumprimento de obrigação legal ou de execução de políticas públicas, o direito de portabilidade será de alcance restrito.

Finalmente, interessante notar que o direito de portabilidade previsto na LGPD não se confunde com a interoperabilidade de sistemas, tal como regulado por normas diversas, como Marco Civil da Internet e até mesmo no art. 25 da LGPD. Ainda que a interoperabilidade e o direito de portabilidade possam envolver a comunicação de sistemas para envio ou recebimento de dados, a interoperabilidade ocorre independente de solicitação do titular de dados e terá como possíveis objetivos a desburocratização e aumento de eficiência na prestação de serviços. Por outro lado, o direito de portabilidade depende de solicitação do titular e terá como objetivo central atribuir-lhe maior controle sobre seus dados por terceiros.

18 SALVAGUARDAS NA PUBLICAÇÃO E NO COMPARTILHAMENTO DE DADOS

Para além de desenvolver documentação capaz de demonstrar que o compartilhamento e a publicação de dados pessoais objetivam o alcance do interesse público e estão sendo realizados em observância ao disposto na legislação aplicável, é necessário ao órgão ou à entidade pública que divulgar dados pessoais estabelecer salvaguardas destinadas a reduzir riscos relacionados ao compartilhamentos ou à publicação de dados pessoais. A eficiência e vantagens da adoção dessas salvaguardas devem também ser avaliadas quando da realização do teste de proporcionalidade para a determinação do interesse público na divulgação de dados pessoais, visto que sua adoção permite avaliação mais precisa sobre os riscos à privacidade e proteção de dados pessoais no caso concreto, e evitar situações de restrições excessivas de acesso a dados em prejuízo ao interesse público da divulgação.

Como se demonstrará a seguir, algumas salvaguardas estão previstas em legislação, mas podem ser também soluções técnicas ou jurídicas estabelecidas pelo controlador dos dados para restringir os possíveis riscos do compartilhamento ou a publicação dos dados sobre direitos e liberdades de titulares de dados pessoais. Como se demonstrará, a escolha sobre quais salvaguardas adotar deverá considerar a efetividade da proteção assegurada em relação à limitação que ela impõe ao interesse público no acesso aos dados que se pretende divulgar.

18.1 Regulação sobre reuso de dados como primeiro elemento de proteção

Assim como ocorre no momento da decisão em torno do compartilhamento ou da publicação de dados pessoais, a divulgação e o uso posterior desses dados pessoais deverão observar o disposto na legislação vigente. Para os dados publicados em portais de transparência ou dados abertos, a LGPD impôs salvaguardas adicionais que deverão ser observadas por aqueles que receberem os dados (art. 7º, §§ 3º e 7º). Como se demonstrará a seguir, esses mesmos cuidados se aplicam ao compartilhamento de dados por entes públicos.

O art. 7º, § 3º da LGPD determina que o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificou sua divulgação. Além disso, observa-se que: **(i)** o CDC e a LGPD exigem que todas as atividades de tratamento de dados pessoais devem ser realizadas em observância à boa-fé e ao princípio da finalidade; **(ii)** o princípio constitucional da finalidade, a LAI e a LGPD exigem que as

atividades de tratamento de dados pessoais realizadas pelo poder público deverão observar o interesse público; e **(iii)** em vista do princípio da finalidade da LGPD, segundo o qual o reuso de dados pessoais deverá ser realizado para finalidades compatíveis com aquelas que justificaram a sua coleta, qualquer uso subsequente de dados pessoais mantidos pelo poder público deve observar o interesse público.

Assim, segundo a legislação vigente, todas as atividades de tratamento de dados mantidos pelo poder público deverão observar a finalidade, a boa-fé e o interesse público que justificaram sua divulgação. Por isso, para fins de tratamento de dados pessoais publicados pelo poder público, o art. 7º, §3º da LGPD apenas reforça as disposições que já seriam aplicáveis ao reuso de dados publicados pelo poder público, por força da própria LGPD, da Constituição Federal e de outras normas, como a LAI e o CDC. Mais que isso, essa leitura integrativa da legislação permite concluir que o disposto no art. 7º, §3º da LGPD, embora seja focado na reutilização de dados publicados pelo poder público, se assemelha às balizas legais do reuso de dados compartilhados por órgão ou entidade pública, respeitadas as particularidades do caso concreto.

Dito isso, cumpre destacar que a **boa-fé** é parâmetro que guia a aplicação de normas e a celebração de negócios jurídicos, pois constitui em um modelo de conduta social ou padrão ético que impõe a todos, entes públicos ou privados, que atuem com honestidade, lealdade e probidade. Segundo a boa-fé, deve sempre haver lealdade e confiança nas relações jurídicas e interpretação da lei, de forma a preservar as relações sociais. Com isso, impõe-se aos sujeitos de direito, públicos ou privados, o dever de respeito, lealdade, probidade, transparência e de agir razoavelmente. Nas palavras de Cláudia Lima Marques (2003), a boa-fé seria “uma atuação refletindo, pensando no outro, no parceiro contratual, respeitando-o, respeitando os seus interesses legítimos, suas expectativas razoáveis, seus direitos, agindo com lealdade, sem abuso, sem obstrução, sem causar lesão ou desvantagem excessiva, cooperando para atingir o bom fim das obrigações". Por sua vez, nas palavras de Carlos Ari Sundfeld (2017), a boa-fé seria um padrão de conduta, "sendo inválidos os atos que produzam fora das pautas de lealdade que os particulares dele poderiam esperar.".

Assim, para o tratamento de dados pessoais, por entes públicos ou privados, a boa-fé pode se traduzir em um compromisso com a legalidade do tratamento, ou seja, consiste em uma garantia de que dados pessoais serão sempre tratados em observância à legislação e aos direitos dos titulares de dados. Além disso, constitui um dever de agir honesta e razoavelmente, isto é, sempre dentro das expectativas legítimas do titular de dados. Segundo

Laura Schertel Mendes (2018) "[t]em especial relevância no processamento de dados pessoais do consumidor a boa-fé, na sua função limitadora, que restringe a liberdade de conduta das partes, ao considerar certas práticas e cláusulas como abusivas."

Quanto ao **interesse público**, amplamente debatido nesta tese, seria o resultado de mediação, pública e motivada, dos diferentes interesses existentes na sociedade (MARQUES NETO, 2002) que, no caso da publicação e do compartilhamento de dados pessoais por governos, busca assegurar a transparência e eficiência governamental, *accountability*, acesso à informação. Já a **finalidade**, requer que o tratamento de dados ocorra para propósitos legítimos e específicos, não sendo autorizadas atividades posteriores que se mostrem incompatíveis com as finalidades informadas ao titular no momento da coleta dos dados. No caso de tratamento de dados mantidos pelo poder público, a verificação da compatibilidade no reuso desses dados deverá observar as atribuições legais dos agentes envolvidos no tratamento e o interesse público do tratamento. Já no tratamento de dados divulgados pelo poder público, a verificação de compatibilidade deverá observar a finalidade e o interesse público da divulgação realizada (que deverá ser informada ao titular de dados). Por exemplo, se um órgão ou entidade governamental divulga dados sobre gastos públicos realizados por servidores públicos ou detentores de cargos políticos e, posteriormente, uma entidade replica essas mesmas informações em seu *website*, mas em formato diferente que facilita possíveis interessados a encontrar e analisar mais facilmente a informação, esse reuso é realizado em observância ao interesse público e à finalidade que justificaram a publicação dos dados. Isso se dá porque a replicação dos dados para viabilizar o controle social sobre gastos públicos está alinhado aos objetivos de transparência governamental e de acesso à informação que justificaram a divulgação dos dados pelo órgão público.[577]

De fato, o art 7º, §7º, incluído na LGPD pela Lei nº 13.853/2019, determina que o tratamento de dados cujo acesso é público poderá ser destinado ao alcance de outras finalidades, desde que observados propósitos legítimos e específicos e a preservação dos direitos do titular. De acordo com esse dispositivo, será necessário ao controlador observar o princípio da finalidade, mas com maior flexibilidade em relação às possíveis novas finalidades. Vê-se aqui nova semelhança entre as normas que regulam o reuso de dados pessoais publicados ou compartilhados, na medida em que o compartilhamento de dados por órgãos públicos deverá buscar propósitos legítimos (na medida em que deverão estar

[577] Exemplo extraído da Opinião 06/2014 do Working Party 29 sobre legítimo interesse. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Acesso em 06.09.2022.

respaldados pelo princípio da boa-fé e serem destinados ao alcance do interesse público), estarem respaldados em legislação que autorize esse novo tratamento e assegurar meios para que titulares de dados exerçam seus direitos.

De todo modo, foi para viabilizar a utilização de dados tornados públicos para outras finalidades não relacionadas àquela que motivou a sua coleta ou publicação, desde que observados alguns requisitos, que foi realizada a inclusão do §7º ao art 7º LGPD, segundo se verifica pelo parecer do relator da Medida Provisória nº 869/2018, Deputado Orlando Silva, que resultou na Lei nº 13.853/2019:

> Sobre a utilização de dados de uso público e daqueles tornados manifestamente públicos para fins diversos, entendemos que a redação proposta é muito ampla. Por isso, propomos para esses casos o tratamento sem necessidade de obtenção de consentimento, desde que para propósitos legítimos e específicos, assim como respeitados os fundamentos e princípios desta Lei. Assim, acredita-se que haverá um balanço saudável entre a livre iniciativa e a criação de novos serviços com o direito à privacidade e intimidade.

Essas novas finalidades de tratamento de dados são por vezes chamadas de finalidades secundárias. Segundo Bioni (2019), o elemento que definiria a legalidade do tratamento de dados de acesso público seria a compatibilidade da finalidade nova ou secundária com o interesse público que justificou a publicação do dado. Já Miriam Wimmer (2021) argumenta que o tratamento secundário poderá ocorrer quando houver compatibilidade entre as finalidades, a nova autorização pelo titular de dados ou a existência de previsão legal específica. Nesta tese se concorda com a interpretação de que a compatibilidade da finalidade secundária deve ser avaliada tendo em vista a finalidade que motivou a divulgação dos dados, e reconhece-se a relevância do uso desses dados para outras finalidades (inclusive privadas, como o desenvolvimento de novo modelo de negócios legítimo), desde que isso resulte em benefício para o interesse público e não imponha demasiadamente elevados a direitos e liberdades de titulares de dados. Do contrário, o compartilhamento e a publicação de dados teriam sua eficácia consideravelmente reduzida, impactando o interesse público na eficiência governamental, inovação no setor público e produção científica.

Além disso, é interessante notar que similares dispositivos (§§ 3º e 7º do art. 7º da LGPD) não estão presentes no art. 11 da LGPD, que regula as bases legais aplicáveis ao tratamento de dados sensíveis. Uma literal interpretação desse silêncio normativo seria que não seria autorizado o tratamento de dados sensíveis eventualmente publicados por entes públicos. Essa interpretação mais restritiva pode ser extraída da manifestação do Deputado

Orlando Silva no parecer que elaborou a respeito da Medida Provisória nº 869/2018, que resultou na Lei nº 13.853/2019:

> Já para dados sensíveis, não julgamos seguro para a proteção do titular essa extensão de possibilidade de tratamento [prevista no art art. 7º, §7º da LGPD]. Temos essa compreensão pelo fato de que na LGPD foram impostas cláusulas mais rígidas do que no instrumento europeu, por exemplo, com relação aos dados de saúde.

De fato, esses dados muitas vezes não devem ser divulgados ao público, em vista de seu maior potencial lesivo ao titular de dados em casos de uso indevido, mas não é possível supor que essas categorias de dados nunca serão tornadas públicas. Esse é o exemplo de dados sobre filiação a determinado partido político. No entanto, como se percebe pelo próprio exemplo citado, também não é possível supor que esses dados não poderão ser reutilizados. Os dados sobre filiação partidária constituem informações de interesse público por excelência (na medida em que auxiliam com investigações relacionadas ao exercício de direitos básicos à democracia, consistentes na capacidade de eleger e ser eleito), mas que permitem a extração de conclusões sobre orientação política, que é dado sensível pela LGPD.

Vale ressaltar que o Anteprojeto de Lei elaborado pelo Ministério da Justiça estabelecia que dados de acesso público irrestrito, sem distinção entre dados triviais ou sensíveis, poderiam ser tratados sem o consentimento do titular de dados.[578] Mais que isso, estudo realizado pelo InternetLab sobre as contribuições feitas a essa proposta normativa durante a consulta pública realizada pelo Ministério da Justiça, aponta que houve grande preocupação dos participantes em conceituar o que seriam dados de acesso público irrestrito e em limitar a possibilidade de uso desses dados.[579] A despeito dessas preocupações, não houve por parte dos contribuintes da consulta pública tentativa de impedir de forma definitiva a possibilidade de tratar dados sensíveis que porventura estivessem acessíveis publicamente.

De fato, por ser uma categoria de dados cujo tratamento indevido pode causar maior prejuízo aos direitos e liberdades do titular de tratados, são necessárias cautelas adicionais ao tratamento de dados sensíveis tornados públicos. No entanto, a extensão dessa cautela não deve alcançar a vedação completa desse tratamento para quaisquer finalidades secundárias.

---

[578] Pode-se encontrar a versão do projeto apresentado ao debate no seguinte link: http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/. Acesso em 22.01.2021.

[579] Associação InternetLab de pesquisa em direito e tecnologia. O que está em jogo no debate sobre dados pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais. 2016. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf. Acesso em 22.01.2021.

Nesse sentido, embora os art. 7º, §§3º e 7º estejam situados em artigo que se refere a dados triviais, eles são igualmente aplicáveis aos dados sensíveis tornados públicos. Essa leitura tem respaldo na interpretação atribuída aos §§ 5º e 6º do art 7º da LGPD, que estabelecem obrigações aos controladores que devem ser aplicáveis também ao tratamento de dados sensíveis (ie.: eventual dispensa de consentimento não afasta do controlador as demais disposições da LGPD e, quando a base legal do tratamento for o consentimento, o envio dos dados a outro controlador também dependerá de consentimento). Não seria razoável pressupor que o maior cuidado no tratamento de dados pessoais assegurado pelos §§ 5º e 6º do art 7º seriam aplicáveis apenas aos dados triviais e não a dados pessoais sensíveis.

Além disso, deve-se também ter em mente que, em vista de sua maior possibilidade de ser tratados de forma a prejudicar direitos e liberdades dos titulares de dados, maior também é o ônus do detentor das bases de dados ou arquivos em demonstrar o interesse público e a necessidade de compartilhar ou publicar dados dessa natureza, assim como do receptor dos dados em fundamentar a atividade de tratamento de dados subsequente em uma base legal e adequar aos princípios da finalidade e necessidade.

Do mesmo modo, também não há em leis que inspiraram a edição da LGPD similar limitação ao tratamento de dados pessoais sensíveis. A GDPR, por exemplo, no Considerando 154 e nos arts. 14[580] e 86, apresenta orientações a respeito do reuso de dados públicos, mas não faz distinção em relação aos dados pessoais sensíveis. O Considerando 154 e o art. 186 determinam que a divulgação de dados pessoais mantidos por entes públicos deverá ser realizada com respeito às normas pertinentes à proteção de dados pessoais. Já o art. 14 impõe ao controlador que obtiver dados obtidos por meios que não sejam o fornecimento direto pelo titular dos dados, o que inclui dados de acesso público, obrigações de informação a respeito do processamento realizado. Por exemplo, o controlador deverá fornecer uma série de informações ao titular, incluindo os propósitos objetivados no tratamento, caso esses sejam diversos daqueles para os quais os dados pessoais foram obtidos inicialmente. No entanto,

[580] As exceções a essa obrigação são: (i) quando o titular dos dados já possuir as informações destacadas; (ii) quando o fornecimento de tais informações se provar impossível ou gerar um esforço desproporcional por parte do controlador - situação na qual esse deve tomar as medidas apropriadas para proteger os direitos, liberdades e legítimos interesses dos titulares de dados; (iii) quando a obtenção ou divulgação seja expressamente prevista pela União Europeia ou Estado-membro ao qual o controlador está sujeito - que deve prover medidas apropriadas para a proteção dos legítimos interesses envolvidos; e (iv) quando os dados pessoais devam permanecer confidenciais por motivos de obrigações profissionais ou outras. Desta maneira, em determinadas circunstâncias, será possível realizar o processamento de dados pessoais públicos e/ou de acesso público mesmo que esses não tenham sido obtidos diretamente com seu titular.

como mencionado, referidos dispositivos não fazem diferenciação ou limitam o reuso de dados pessoais sensíveis.[581]

Pelos motivos expostos acima, entende-se que o disposto no art. 7º, §§3º e 7º se aplicam também ao tratamento de dados pessoais sensíveis tornados públicos. Ou seja, dados pessoais sensíveis poderão ser reutilizados desde que observados propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular. No entanto, diferentemente do que ocorre com dados triviais, cujo reuso poderá ser respaldado na base legal de legítimo interesse, como se demonstrará a seguir, não será permitido utilizar essa base legal para o reuso de dados tornados públicos para extrair inferências sobre dados sensíveis. Nesse caso, será necessário justificar a atividade em outra base legal, a exemplo do consentimento.

Como se verifica, outra salvaguarda que deve ser observada no uso secundário de dados pessoais compartilhados ou publicados pelo poder público está na definição da **base legal aplicável**. Embora usos secundários possam se utilizar de bases legais diversas, destacam-se as bases legais de consentimento, legítimo interesse, realização de estudos por órgãos de pesquisa e a proteção ao crédito (essa última base legal não possui um bom equivalente na legislação europeia). A definição de qual base legal será aplicável está relacionada às particularidades do caso concreto, como a definição da finalidade específica de reuso e a natureza dos dados pessoais (como mencionado, são mais restritas as bases legais aplicáveis ao tratamento de dados pessoais sensíveis).

Entre as bases legais mais debatidas no direito comparado para fins de tratamento secundário estão o cumprimento de obrigação legal ou regulatória, a execução de políticas públicas, o legítimo interesse e o consentimento. A fundamentação do reuso de dados publicados ou compartilhados pelo poder público nas bases legais de execução de políticas públicas ou no cumprimento de obrigação legal ou regulatória geralmente será permitida para entes públicos ou para particulares enquanto delegatários de atividades públicas. Por exemplo, o uso de dados coletados pelos Centros de Referência de Assistência Social (CRAS), quando

[581] Nas regras específicas sobre dados pessoais sensíveis (art. 9º), a GDPR determina que quando dados pessoais sensíveis forem tornados manifestamente públicos por seu titular, seu processamento é permitido sem da obtenção de consentimento. Além desta razão, cabe ressaltar aqui que esses também poderão ser processados em casos de interesse público. Na situação mencionada acima, no entanto, é importante mencionar que o processamento de dados pessoais sensíveis manifestamente tornadas públicas só pode ocorrer caso haja um indicativo de que o objetivo de tal ação pelo titular era justamente promover e permitir que tais dados fossem posteriormente processados. As salvaguardas previstas na GDPR acerca da proteção de dados pessoais, ademais, seguem em observância. No entanto, essa situação não equivale ao tratamento de dados tornados públicos pelo poder público.

do cadastro de potenciais beneficiários do Bolsa Família, pela Caixa Econômica Federal (CEF) para a atribuição de um Número de Identificação Social àqueles selecionados para participar do programa, é parte essencial para a realização da política pública (FRAGOSO *et al.*, 2021). Essa atividade de reuso dos dados pela CEF poderá ser fundamentada no cumprimento de obrigação regulatória, na medida em que está expressamente prevista em ato normativo que regula o funcionamento do Programa Bolsa Família. Outro exemplo consiste no compartilhamento de dados biométricos de cidadãos, realizado entre o Denatran e o TSE para finalidades de desburocratização de processos eleitorais (na medida em que cidadãos não precisam se deslocar para uma repartição pública para registrar sua biometria para fins eleitorais), que poderá ser fundamentado na base legal de execução de políticas públicas.

Por outro lado, nos casos em que a atividade de reuso de dados não esteja diretamente atrelado a uma obrigação legal ou regulatória, as bases legais mais recorrentes serão o consentimento ou o legítimo interesse. A escolha por uma ou outra base legal impõe a adoção de cuidados distintos pelo controlador. No caso do legítimo interesse (conforme abordado mais detidamente em capítulo anterior desta tese), será necessário ao controlador: **(i)** promover transparência capaz de assegurar a legítima expectativa dos titulares de dados sobre esses novos usos atribuídos aos seus dados; **(ii)** elaboração de teste de adequação que comprove que os interesses legítimos do controlador devem prevalecer sobre os direitos e liberdades dos titulares de dados (que, por sua vez, exige a demonstração da adequação, necessidade e proporcionalidade em sentido estrito do novo tratamento); e **(iii)** adoção de mecanismos para que titulares de dados possam facilmente exercer seu direito de oposição ao tratamento. Por outro lado, o consentimento será a base legal apropriada caso outras bases legais não possam ser utilizadas, especialmente em vista das legítimas expectativas do titular de dados em relação às novas finalidades de uso de seus dados. Para a utilização dessa base legal, será necessário solicitar uma autorização específica para esse novo uso dos dados, que deverá ser expressa e obtida de forma livre e informada.

18.2 Pseudonimização e anonimização como possíveis soluções

Havendo o interesse público na divulgação dos dados, outra salvaguarda recorrentemente utilizada consiste na adoção de medidas técnicas que assegurem a pseudonimização ou anonimização de dados pessoais. Como mencionado, a anonimização consiste na adoção de medida técnica capaz de impossibilitar, mediante a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento, a sua posterior associação direta ou

indireta a um indivíduo. Por outro lado, se estará diante procedimento pseudonimização caso a técnica utilizada possa ser revertida (e o indivíduo identificado) mediante a utilização exclusiva de meios próprios ou pelo emprego de esforços razoáveis.

Entre as técnicas de anonimização ou pseudonimização que o gestor público poderá adotar estão a **(i)** remoção (deletar ou destruir) de dados constantes de documentos ou bases de dados, **(ii)** não publicação ou compartilhamento de documentos que apresentem dados sensíveis ou cuja divulgação possa infringir grande risco aos titulares de dados, **(iii)** divulgação de apenas dados previamente agregados,[582] ou **(iv)** promoção da generalização ou a modificação de certos dados para impedir a identificação de indivíduos.

Similares práticas já vêm sendo realizadas por certos órgãos e entidades públicas de forma a alcançar o interesse público em respeito à proteção de dados pessoais de cidadãos, como os exemplos de **(a)** processos judiciais protegidos por segredo de justiça ou documentos que contêm informações consideradas sensíveis não são publicados para consulta ao público; **(b)** informações sigilosas em petições de inquéritos administrativos do Conselho Administrativo de Defesa Econômica são tarjados; **(c)** o IBGE possui uma API com dados agregados de pesquisas e censos.

No entanto, em certos casos, é possível que haja interesse público na publicação ou no compartilhamento do próprio dado pessoal. Nesses casos, é possível adotar medidas de parcial remoção ou a tarja de dados, ou outras técnicas ou tecnologias que mitigam riscos à privacidade, enquanto viabilizam o interesse público da divulgação do dado. Por exemplo: **(i)** na divulgação de informações sobre salários de servidores públicos do governo federal, os dados não são divulgados em formato aberto (e.g., o interessado deverá procurar por categoria, como "servidores da Secretaria Nacional de Defesa do Consumidor" ou incluir alguma informação para que o sistema possa localizar a informação desejada, como o sobrenome) e o CPF é parcialmente tarjado (e.g., 358.***.***-26); e **(ii)** para garantir a publicidade de processos judiciais, em ações não protegidas por segredo de justiça, Tribunais restringem o acesso a determinados arquivos (ex.: documento contendo a foto da carteira de

[582] Cumpre observar que o dado agregado poderá não ser anonimizado. Nesse sentido se posicionou a EDPS "Os dados agregados não são necessariamente dados não pessoais, uma vez que os dados agregados ainda podem estar relacionados a um indivíduo identificado ou identificável. A este respeito, a EDPS lembra que, de acordo com o considerando 26 do GDPR e a jurisprudência do TJUE, devem ser levados em devida consideração todos os fatores objetivos, incluindo os custos e o tempo necessário para a identificação, a tecnologia disponível, bem como os meios legais e outros meios para acessar dados adicionais sobre a pessoa". (tradução nossa). Trecho extraído em Opinião de 2020, disponível em: https://edps.europa.eu/sites/default/files/publication/20-06-16_opinion_data_strategy_en.pdf. Acesso em 05.03.2021.

motorista das partes) ou divulgam o andamento processual ou peças processuais com apenas as iniciais das partes (e.g., Recorrente: I.C.S.F. e Recorrida: B.P.L).

No entanto, quanto mais dados são removidos ou mais barulho se insere em determinada base de dados, menor poderá ser a utilidade dos documentos e bases de dados divulgados, visto que haverá restrição nos tipos de análise possíveis e/ou os dados publicados e/ou suas possíveis análises estarão mais distantes da realidade dos dados originais (OBSERSKI; KREUTER, 2020).[583] Esse é um dos principais dilemas na proteção de dados pessoais quando do compartilhamento e publicação de dados pelo governo: **(i)** quanto mais granularidade e acessibilidade, maior a exposição de dados sobre indivíduos; e **(ii)** quanto menor a granularidade e acessibilidade dos dados, igualmente menor será a utilidade dos dados (GREEN *et al.*, 2017). Assim, mesmo a utilização de soluções técnicas de anonimização e pseudonimização destinadas a assegurar a privacidade de dados não remove do gestor público a escolha entre interesse público no acesso e privacidade, na medida em que ele que deverá escolher qual a intensidade de mudanças que deverá ser realizada nos documentos e bases de dados divulgadas - e, consequentemente, aumentar ou reduzir a privacidade ou as possibilidades analíticas das informações divulgadas.

Isso não significa que técnicas de anonimização não devam ser adotadas, visto que elas efetivamente reduzem as chances de exposição de indivíduos. O que se argumenta aqui é que mesmo nos casos nos quais são anonimizadas ou pseudonimizadas bases de dados ou arquivos, é necessário ao poder público avaliar o interesse e os riscos da publicação de determinadas bases de dados. Além disso, essas medidas deverão ser acompanhadas de outras salvaguardas, como as já mencionadas, adotadas em todos os momentos do ciclo de vida dos dados, destinadas a proteger os direitos dos titulares de dados.

Limites da anonimização e pseudonimização

Além disso, ainda que fossem adotadas todas as técnicas citadas, a literatura especializada sustenta que não existe técnica capaz de assegurar a impossibilidade de posterior identificação de indivíduos em bases de dados anonimizadas. Com o avanço das tecnologias e com a quantidade de dados disponíveis *online* - divulgados por indivíduos em

[583] Nesse sentido se manifestou o EDPB: "Além disso, os processos de anonimização não são simples. Quanto mais variados os dados, mais difícil é ser anonimizado, reduzindo o risco de reidentificação a um limite aceitável. As dificuldades práticas associadas a um processo de anonimização robusto podem impedir que os controladores de dados, e especialmente as PMEs, compartilhem dados valiosos." (tradução nossa).Vide: https://edps.europa.eu/sites/default/files/publication/20-06-16_opinion_data_strategy_en.pdf. Acesso em 04.03.2021.

redes sociais ou constantes de bases de dados públicas ou privadas -, é cada vez mais fácil realizar associações e re-identificações de, pelo menos, parte dos dados divulgados.

Assim, embora a adoção de técnicas de anonimização ou pseudonimização em determinadas bases de dados busquem reduzir a possibilidade de serem estabelecidas relações entre dados de fontes distintas, a re-identificação é cada vez mais frequente. Esse é, inclusive, um ponto de embate em relação às normas de proteção de dados pessoais, visto que o conceito legal de anonimização gera uma falsa sensação de privacidade, na medida em que remove do dado sua qualificação jurídica de dado pessoal (PCAST, 2014), mas reconhece que essa proteção poderá ser superada pela ação de agentes com capacidade computacional superior à média do mercado ou pela simples e natural evolução da tecnologia.

Há casos diversos que demonstram a possibilidade de re-identificar dados que se imaginou estarem desidentificados. Por exemplo, pesquisadores do MIT e da Universidade de Louvin demonstraram que a análise de dados anonimizados de geolocalização de celulares permite grande sucesso na re-identificação dos indivíduos aos quais os dados se referem - fato esse bastante relevante em época de pandemia de COVID-19, em que governos realizaram parceria com empresas de telefonia para obter dados de geolocalização para promover políticas de distanciamento social.[584]

Outro exemplo, embora do setor privado, foi a re-identificação de base de dados divulgada pela empresa Netflix de forma anonimizada. A empresa divulgou lista com o ranqueamento de filmes realizada por seus consumidores, com vistas a estimular a sociedade a encontrar sistemas de recomendação diferentes daqueles utilizados pela empresa. Na lista, nomes e outros identificadores pessoais foram removidos e substituídos por números aleatórios, de forma a assegurar a privacidade de indivíduos. No entanto, pesquisadores da Universidade do Texas associaram esses dados com informações de *ranking* público de filmes (*Internet Movie Database*), no qual indivíduos podem realizar avaliações identificadas.[585]

No Brasil, um exemplo de re-identificação, conforme mencionado, foi a conduzida pela agência de notícias The Intercept Brasil em base de dados divulgada no *website* da Secretaria de Turismo do Espírito Santo ("Setur").[586] A base de dados foi produzida pela empresa Telefônica-Vivo, com a ciência da Anatel, e possui dados de localização de usuários

---

584 Vide: https://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data. Acesso em 30.12.2023

585 Vide: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf. Acesso em 04.01.2023.

586 DIAS, Tatiana. Vigiar e Lucrar: nós identificamos dois clientes dos dados de localização 'anônimos' vendidos pela Vivo. Disponível em: https://theintercept.com/2020/04/13/vivo-venda-localizacao-anonima/. Acesso em 14.03.2021.

dos serviços de telecomunicações oferecidos pela empresa, que foram desidentificados pela utilização de tecnologia denominada de *Smart Steps*. Ela é comercializada para interessados diversos, como a Setur, que a divulgou em seu *website* e utilizou suas informações para compreender como ocorre a circulação de turistas no Estado. O The Intercept cruzou essa base de dados com outras bases de dados e conseguiu identificar alguns titulares de dados, demonstrando a ineficácia das medidas técnicas adotadas para a proteção dos dados.

Entre as soluções técnicas mais tradicionais de anonimização ou pseudonimização de dados estão a exclusão de identificadores ou de outros dados que, quando associado a outros, permitem a identificação de seus titulares. Outras técnicas consistem na substituição de dados pessoais por números ou pseudônimos, na agregação de dados ou na realização de mudanças no conteúdo da base de dados. No entanto, a literatura afirma que cada uma dessas técnicas apresenta fragilidade específica.

De fato, dados podem ser mais ou menos facilmente associados a uma pessoa natural (LUBARSKY, 2010). Os identificadores pessoais (*direct identifier*)[587] como o nome, o CPF ou número de telefone possuem a capacidade de mais facilmente identificar um indivíduo. Há outros dados, como gênero, data de nascimento e código postal (*indirect identifier*), que, embora não sejam diretamente associados a indivíduos, permitem sua fácil identificação quando combinados entre si (GOLLE, 2006). Há também dados que poderão ser associados a diversos indivíduos, como suas preferências musicais ou restaurante de predileção, ou dados que não podem ser associados a indivíduos específicos porque são anonimizados.

Embora seja frequente a anonimização ou pseudonimização pela mera remoção de identificadores diretos ou indiretos, exemplos diversos (inclusive os apresentados acima) demonstram que essa técnica é uma das mais facilmente reversíveis. Isso pode ocorrer por fatores como a avaliação do contexto de um documento (e.g., em decisões judiciais, mesmo que os nomes das partes sejam tarjados, a narrativa dos fatos do caso poderá permitir a identificação dos envolvidos) ou da combinação de dados comuns entre as bases de dados.

Por exemplo, a ocultação de dados pessoais em peças processuais, por padrão *(by default)* ou mediante solicitação, é prática comum em alguns países. No entanto, questiona-se

[587] Segundo consta no relatório publicado pela cidade de Seattle: "Identificadores diretos: Estes são pontos de dados que identificam uma pessoa sem informações adicionais ou ligando-se a outras informações prontamente disponíveis. "Informações Pessoais Identificáveis", ou PII, freqüentemente se enquadram nesta categoria. Por exemplo, eles podem ser nomes, números de previdência social ou um número de identificação de funcionário." (tradução nossa). Vide: https://privacytools.seas.harvard.edu/files/privacytools/files/fpf.pdf. Acesso em 14.03.2021.

a efetividade e o interesse público dessa solução, na medida em que **(i)** a despeito do elevado custo em implementar técnicas de pseudonimização aos documentos, dados constantes dos autos processuais poderão permitir a identificação das partes, e **(ii)** a divulgação das partes em determinado processo pode ser essencial à devida compreensão do caso ou ser de interesse público, especialmente quando se trata de pessoas públicas.

Na divulgação de dados agregados não há identificadores diretos ou indiretos - exceto quando os números apresentados não representam um conjunto maior de indivíduos, caso em que é possível identificar a(s) pessoa(s) natural(is) em questão. Por exemplo, se uma empresa possui apenas uma mulher em seus cargos de diretoria, análises associadas ao gênero poderão permitir a associação a uma pessoa específica (e.g., um dos diretores poderá se ausentar por tempo prolongado em função de licença maternidade).

Finalmente, dentre as técnicas que envolvem a modificação das bases de dados está a privacidade diferencial (há outras, como o k-anonimato), consistente em fórmula matemática que indica quando a divulgação de bases de dados poderá ocorrer de forma matematicamente segura para a privacidade. Essa verificação é realizada pela adoção de mecanismos diversos (em inglês, *noise*) que dificultam a posterior identificação dos indivíduos em técnicas de reversão de dados, como a reconstrução de bases de dados (OBSERSKI; KREUTER, 2020).

Diante desse cenário, a reflexão sobre as chances de reidentificação de dados divulgados é particularmente importante, em um contexto no qual as bases de dados públicos são cada vez mais divulgadas por governos e exploradas por atores diversos para finalidade inúmeras, inclusive para a produção de categorias analíticas que permitirão a realização de inferências sobre outros indivíduos. Em outras palavras, a preocupação com dados pessoais na divulgação de bases de dados mantidas pelo poder público não se restringe a casos como a divulgação de salários de servidores públicos ou dos beneficiários de programas sociais, nos quais o governo divulga dados pessoais considerados de interesse público. Alcança também a divulgação de dados originalmente desidentificados, mas que poderão ser posteriormente associados a uma pessoa física por meio da integração entre bases de dados diversas ou da utilização de novas e mais avançadas técnicas a essas bases de dados.

18.3 Divulgação de dados com restrição de acesso e de usos secundários

Além das salvaguardas estabelecidas pela legislação e da possibilidade de anonimizar ou pseudonimizar dados constantes de documentos e bases de dados mantidos pelo poder

público, é também possível adotar salvaguardas técnicas e/ou jurídicas ao reuso de dados. Entre as possíveis salvaguardas estão: **(i)** a adoção de restrições técnicas à coleta e reuso de dados publicados ou compartilhados, como os exemplos da utilização de ferramentas que impeçam práticas maliciosas de *web scraping* ou *download* de arquivos, **(ii)** quando houver riscos mais elevados na publicação de dados, compartilhar com entidades específicas para finalidades previamente autorizadas, e **(iii)** a limitação ao reuso dos dados por intermédio de cláusulas em contratos ou constantes de Termos de Serviço (ToS) e Políticas de Privacidade.

A seguir serão apresentadas brevemente algumas das possíveis salvaguardas que vem sendo utilizadas por órgãos ou entidades públicas (ou seja, não se deseja abordar exaustivamente as soluções e tampouco aprofundar nos seus benefícios e limitações).[588]

Em relação às **soluções técnicas**, elas não serão abordadas em profundidade nesta tese, mas são tais como a inclusão de ferramentas (e.g., *capcha*) em *websites* ou APIs para impedir a extração em larga escala de informações por robôs e outras tecnologias (e.g., *web scraping*). Há também a possibilidade de utilizar as denominadas *Privacy Enhancing Technologies* (PETs), consistentes em tecnologias que estão sendo desenvolvidas para promover a privacidade em atividades de tratamento de dados pessoais (esse conceito amplo é objeto de divergência). Por exemplo, há PETs que, ao transformar, encriptar ou armazenar dados em outros sistemas, limitam seu acesso enquanto estão sendo analisados por terceiros - como a técnica de aprendizado federado (*federated learning*), que permite o desenvolvimento de modelos de *machine learning* sem a coleta de dados em uma base centralizada. No entanto, elas são destinadas a alcançar objetivos específicos, de forma que não se propõem a eliminar integralmente os riscos à privacidade, devendo ser utilizadas segundo as particularidades do caso concreto e combinadas com outras salvaguardas existentes.

Uma outra salvaguarda consiste em, a depender dos contornos do interesse público no caso concreto, **substituir a publicação de dados pessoais pelo compartilhamento** com aqueles interessados que desejam utilizar os dados para finalidades legítimas e que sejam capazes de demonstrar a adequação de suas práticas à legislação pertinente e às exigências estabelecidas pelo órgão custodiante dos dados. Nesse sentido se manifestou Hayden Dahm

[588] Como mencionado, nos casos em que há interesse público na divulgação de documentos ou bases de dados contendo dados pessoais, a adoção de salvaguardas que limitam o acesso e reuso a dados pessoais poderá significar limitação ao interesse público. Por isso, será necessário ao gestor público entender como a adoção dessas salvaguardas impactará o interesse público na divulgação dos dados. Para tanto, deverá identificar no caso concreto se o interesse público: **(a)** alcança todos os dados de uma base de dados ou arquivos ou se é possível remover os dados pessoais antes da divulgação, ou **(b)** exige a divulgação de documentos e arquivos com restrições de acesso e reuso. Após identificar os contornos do interesse público, é possível avaliar no caso concreto a adequação das salvaguardas que se pretende utilizar no compartilhamento ou na publicação.

(2020): "Quando não for possível tornar os dados gratuitos e abertos ao público, estender o acesso a terceiros no caso-a-caso pode ser uma opção. Nessa situação, o fornecedor de dados geralmente é obrigado a fornecer aprovação prévia" (tradução livre).

Por exemplo, como já mencionado nesta tese, o Denatran estabeleceu procedimentos para viabilizar que certos interessados que cumprem determinados requisitos possam acessar dados constantes de seus sistemas e subsistemas. Segundo a Portaria Denatran nº 15/201, que apresenta como um de seus fundamentos legais o dever de transparência regulado pela LAI, será necessário aos interessados: (i) demonstrar que exercem atividades relacionadas ao trânsito, transporte, ou que precisem dos dados para a validação de Carteira Nacional de Habilitação ou de Certificação de Registro de Veículo; (ii) identificar a finalidade para a qual desejam utilizar os dados e a necessidade de acesso dos dados mantidos pelo Denatran para alcançar essas finalidades; e (iii) comprovar que cumprem com determinados requisitos técnicos para acesso aos dados, por meio da indicação de informações como quais equipamentos serão utilizados no acesso. Nesse caso, em vista da natureza dos dados mantidos pelo Denatran, o interesse público não resulta na publicação dos dados ao público, mas permite que certos interessados possam acessar certos dados para finalidades específicas. Todavia, é importante destacar certos pedidos de acesso a esses dados também não atenderão o interesse público, motivo pelo qual devem ser rejeitados, a exemplo do compartilhamento com a Abin, que foi declarado inconstitucional pelo Supremo Tribunal Federal.

Outro exemplo seria o estabelecimento de parcerias entre o ente público detentor de dados e instituições acadêmicas. Com isso, é possível assegurar o interesse acadêmico no uso de dados pessoais que não poderão ser publicados em portais de transparência e dados abertos em função dos elevados riscos à privacidade e proteção de dados pessoais decorrentes dessa divulgação. Para tanto, entidades públicas podem estabelecer normas ou editais contendo: (a) qualificações mínimas daqueles que desejam acessar e reutilizar os dados; (b) orientação sobre possíveis finalidades para as quais os dados poderão ser utilizados; (c) cuidados que devem ser assegurados no tratamento dos dados; (d) periodicidade do acesso aos dados; e (e) possibilidade ou limites à subsequente divulgação dos dados acessados. Caso a entidade acadêmica solicitante de acesso demonstre cumprir os requisitos mínimos estabelecidos na norma ou edital, será possível estabelecer contrato formalizando as condições de uso, após o qual pode-se dar efeito ao compartilhamento de dados pessoais.

Outra relevante salvaguarda consiste no estabelecimento de **balizas jurídicas à utilização dos dados**, cuja materialização ocorre em cláusulas de contratos (e.g., contratos

destinados a regular o compartilhamento de dados ou contratos de concessão com cláusulas sobre o uso de dados dos usuários do serviço público) ou de Termos de Serviço ou Política de Privacidade do *website* do ente público. Essas cláusulas delimitam os contornos do compartilhamento e da publicação de dados pelo ente público, assim como dos possíveis novos tratamentos que serão realizados com os dados. Tanto no compartilhamento quanto na publicação de dados, é possível estabelecer cláusulas que limitem quem poderá acessar os dados (é inclusive possível haver vedação à utilização de ferramentas de varredura de dados), para quais finalidades e de qual forma. Mais do que uma boa prática, a previsão de cláusulas que regulam a divulgação de dados pessoais é essencial para fins de *accountability* e confiança cidadã sobre o uso de seus dados pessoais (DAHM, 2020). No entanto, tais cláusulas contratuais devem ser construídas de forma a efetivamente assegurar a observância à legislação de proteção de dados pessoais. Do contrário, estarão apenas limitando o interesse público ou facilitando a prática de afronta a direitos de titulares de dados.

Por exemplo, a portaria CNPQ nº 976/2022,[589] que institui os Termos de Uso (ToU) e a Política de Privacidade da Plataforma *Lattes*, possui cláusula (art. 8º, XIII, dos ToU) impedindo o usuário de usar "robôs, sistemas de varredura e armazenamento de dados (como "spiders" ou "scraper"), links escondidos ou qualquer outro recurso escuso, ferramenta, programa, algoritmo ou método coletor/extrator de dados automático para acessar, adquirir, copiar ou monitorar o serviço, sem permissão expressa por escrito do órgão". Além disso, a Política de Privacidade informa que o CNPQ compartilha em formato XML, por meio do sistema "Extrator Lattes" e por meios físicos, dados com entidades científicas para a promoção da ciência e melhoria dos instrumentos de aferição da atividade científica no país.

De um lado, trata-se de interessante forma de restringir o uso secundário de dados pessoais divulgados no sistema *Lattes*, na medida em que impede a varredura de dados pessoais e informa que o compartilhamento de dados será realizado apenas para finalidades atreladas ao desenvolvimento da ciência no país. De outro lado, essa limitação de coleta dos dados poderá ser considerada excessiva, na medida em que **(i)** estudantes, professores e pesquisadores estão cientes de que determinados dados incluídos no sistema lattes serão tornados públicos, para fins de divulgação do próprio conhecimento científico e para viabilizar a medição de eficiência da ciência brasileira; **(ii)** a política de privacidade do sistema lattes informa que determinados dados pessoais com maior potencial lesivo à

[589] Disponível em: https://in.gov.br/en/web/dou/-/portaria-cnpq-n-976-de-4-de-agosto-de-2022-420668836. Acesso em 23.10.2022.

privacidade não serão divulgados ao público, a exemplo de dados que revelam a origem racial ou étnica da pessoa; e **(iii)** exigir a utilização do sistema oferecido pelo CNPQ (Extrator *Lattes*) pode limitar o alcance dos próprios objetivos da divulgação de informações realizada pelo lattes (divulgação e medição de eficiência científica), visto que eventuais restrições técnicas do sistema disponibilizados podem ser superadas pela adoção outras tecnologias oferecidas por atores privados.

Como a publicação e o compartilhamento de informações sobre conhecimento científico brasileiro é de interesse público, beneficia o próprio pesquisador, estudante ou professor (na medida em que auxilia na divulgação de sua produção científica), e os potenciais riscos à privacidade decorrentes da utilização inadequada são mais restritos (em verdade, o próprio titular de dados possui interesse que suas informações biográficas sejam tornadas públicas), a restrição imposta pelo sistema lattes é excessiva e acaba por restringir tratamentos destinados a alcançar as finalidades que justificam a divulgação de currículos no portal lattes. Uma alternativa mais eficaz seria a previsão de cláusulas nos Termos de Uso ou Política de Privacidade do Lattes para delimitar quais finalidades de reuso são consideradas compatíveis com a publicação ou compartilhamento dos dados. Com isso, se estimula o reuso legítimo dos dados e impede tratamentos para finalidades indesejadas, visto que não serão realizados em observância ao princípio da finalidade e com fundamento em uma base legal.

Diante da centralidade de cláusulas contratuais na delimitação sobre como dados pessoais divulgados pelo poder público poderão ser legitimamente reutilizados, e também reconhecendo que a negociação ou aprovação de cláusulas contratuais pode ser morosa, certas entidades vêm elaborando modelos de cláusulas que regulam diferentes práticas de compartilhamento e publicação de dados pessoais. Por exemplo, o projeto *Contracts for Data Collaboration* (C4CD),[590] desenvolvido por entidades como o *Governance Lab* da Universidade de Nova York e a Universidade de Washington,[591] reuniu diferentes formatos de cláusulas de compartilhamento de dados estabelecidas para finalidades de interesse público e categorizou perguntas que devem ser respondidas no caso concreto para identificar quais os contornos mais apropriados de cláusula de divulgação de dados pessoais.

Essas perguntas são similares àquelas que perpassam a análise realizada nesta tese, a saber: (i) por que os dados estão sendo divulgados? Qual o contexto e finalidade dessa divulgação?; (ii) quais tipos de dados estão sendo divulgados? Quais as origens, formatos, e

[590] Vide: https://contractsfordatacollaboration.org/our-framework/. Acesso em 23.10.2022.
[591] Vide: https://www.sdsntrends.org/research/2019/4/24/partnerships-trust-c4dc#read. Acesso em 23.10.2022.

outros requisitos técnicos?; (iii) quem são as partes no contrato? Quem irá divulgar e receber os dados? Sobre quem recaem quais direitos e obrigações?; (iv) Como os dados são divulgados? Como serão regulados aspectos como segurança, privacidade e riscos?; (v) Quando a divulgação irá ocorrer? Quando ela se inicia e encerra?; (vi) Para onde dados são divulgados e para onde? Há aspectos jurisdicionais que devem ser considerados?[592] A depender da resposta para cada uma das perguntas, as cláusulas deverão assumir formatos distintos. Quanto mais específicas forem as cláusulas à situação concreta, maior será sua efetividade.

No entanto, ainda que seja necessário avaliar, no caso concreto, as particularidades da divulgação que se pretende realizar, é possível encontrar alguns parâmetros para auxiliar o gestor público na formulação de cláusulas contratuais, como a delimitação de quais dados podem ser tratados, para quais finalidades, por quanto tempo, em quais condições, e possibilidade de o receptor dos dados divulgá-los a terceiros. Especificamente, entre as possíveis exigências para o consumidor de dados que podem (ou devem) estar previstas em Termos de Uso ou Contratos estão: (a) limitar determinadas práticas de varredura e certas finalidades de usos secundários, (b) somente coletar os dados essenciais à realização de atividades secundárias lícitas e legítimas; (c) obter dos titulares de dados a autorização necessária para o tratamento dos dados, que envolve informá-los sobre a origem e finalidades do tratamento e fundamentar em uma base legal compatível com o tratamento secundário; (d) viabilizar mecanismos para que titulares de dados possam exercer seus direitos, especialmente os direitos de oposição e remoção de consentimento, quando aplicáveis; (e) sempre que a atividade de tratamento for qualificada como de elevado risco, elaborar um relatório de impacto; e (f) se possível, tratar dados de forma anonimizada ou pseudonimizada. Além disso, quando os dados forem protegidos por normas de sigilo, se o compartilhamento for autorizado por lei (essa hipótese não se aplica à publicação de dados), o contrato deverá também prever restrições ao uso e compartilhamento subsequente de dados que seja compatível com o racional e limites impostos pela norma de sigilo.

Assim, ao restringir o reuso dos dados (mesmo que na publicação de dados) àqueles que cumprem com alguns requisitos mínimos e que se comprometem a utilizar os dados para finalidades autorizadas e por período específico,[593] limita-se a possibilidade de práticas de

---

[592] Vide: https://medium.com/data-stewards-network/introducing-the-contractual-wheel-of-data-collaboration-ca4c55938e7a. Acesso em 25.10.2022.

[593] "Os colaboradores precisarão considerar como lidar com os dados a longo prazo e se os dados devem ser retidos para uso futuro ou apagados. O Centro de Dados Humanitários forneceu orientações sobre esta

abuso viabilizadas pela divulgação de dados.[594] De fato, a limitação jurídica de reuso de dados pessoais não evita que agentes maliciosos utilizem os dados de forma incompatível com a legislação. No entanto, assim como as soluções técnicas, as cláusulas contratuais constituem uma dentre as possíveis medidas que devem ser adotadas para assegurar a privacidade e proteger os dados pessoais. Inclusive, como abordado extensamente nesta tese, em algumas situações será recomendado sequer publicar ou compartilhar os dados. As soluções que se discutem aqui, no entanto, visam a expandir a possibilidade de divulgar dados para finalidades lícitas e legítimas. Nesse sentido, impor balizas jurídicas para o acesso e reuso de dados por agentes que atuam em conformidade com a legislação possui a capacidade de promover e incentivar o interesse público.

Para além disso, as cláusulas de compartilhamento e publicação de dados pessoais pelo poder público devem ser disponibilizados ao público, por força das obrigações de transparência previstas tanto na LGPD como na LAI, de forma a viabilizar o controle social da adequação dos limites jurídicos impostos ao reuso pretendido aos dados pessoais de cidadãos. Por exemplo, o já mencionado Termo de Cooperação nº 07/2020, firmado entre Denatran e Abin, foi declarado como inconstitucional pelo STF por não ter estabelecido com precisão quais dados seriam compartilhados, para quais finalidades e de qual forma, e por tampouco ter demonstrado a necessidade desse compartilhamento.

Mais uma possível salvaguarda consiste na instituição de **Conselhos e Códigos de Ética** para guiar e avaliar se o compartilhamento e a publicação de dados para determinadas

---

questão sob uma perspectiva humanitária e aconselha que "seguindo o princípio de retenção, os dados humanitários devem ser retidos enquanto seu valor potencial previsível superar os riscos associados à retenção. Os dados sensíveis só devem ser retidos pelo tempo necessário para a finalidade especificada" (OHA, 2019). Se o equilíbrio entre risco dos dados e utilidade favorecer a eliminação, então os dados devem ser completamente removidos de todos os dispositivos.". (DAHMM, 2020, tradução nossa).

[594] "Para evitar abusos ou consequências imprevistas, muitos acordos delinearão limitações. Muitas vezes, isto envolve a declaração de limitações específicas sobre que tipos de dados não podem ser compartilhados e a explicação de como os dados podem e não podem ser usados. Alguns acordos podem assumir uma forma geral, permitindo que os dados sejam utilizados de várias maneiras com restrições apenas seletivas, enquanto outros colocam restrições mais extremas. [...]. Ao mesmo tempo, não definir o que é "incompatível com a finalidade" poderia criar riscos ou incertezas desnecessárias. Alguns outros acordos esclarecem limitações muito explícitas. Isto é especialmente comum quando a das se relaciona com pessoas em situações vulneráveis. Por exemplo, um acordo entre o Samoa Bureau of Statistics (SBS) e a UNICEF que faz referência a dados sobre crianças e deficientes elucida cuidadosamente as restrições sobre o uso potencial de dados individuais. Primeiro, o texto do acordo afirma que os dados só podem ser usados para determinar informações sobre grupos de pessoas, e especifica que os dados não podem ser usados para identificar indivíduos, famílias ou empresas. Depois vai um passo além e exige que, se tal identificação ocorrer por acidente, a informação não possa ser usada, e o evento deve ser relatado ao S"S." (DAHMM, 2020, tradução nossa).

finalidades são considerados éticos e em benefício do interesse público.[595] Mais que isso, essas práticas são particularmente relevantes para delimitar parâmetros para identificar atividades que, embora juridicamente viáveis, não são aceitáveis socialmente e, se praticadas, acabam por reduzir a confiança social no aparato Estatal (OCDE, 2019).[596] Na experiência estrangeira (embora também existam exemplos na experiência nacional, especialmente na área médica), é possível identificar **Conselhos de Ética** relacionados à utilização de dados para finalidades de pesquisa e elaboração de estatísticas. Inclusive, em Opinião Editada pelo EDPS em 2020, a autoridade europeia ressaltou a importância de pesquisas científicas serem rigorosamente revisadas por Conselhos de Ética e de estas entidades dialogarem com Autoridades de Proteção de Dados Pessoais, de tal forma a garantir a em observância a direitos humanos quando do desenvolvimento de estudos destinados a contribuir com interesse público.

Já em relação aos **Códigos de Ética**, um exemplo internacionalmente reconhecido consiste no *Data Ethics Framework*[597] do governo do Reino Unido (publicado em 2018 e revisado em 2020), que prevê princípios e ações destinados a auxiliar o poder público em decisões sobre a utilização legítima de dados pessoais. Na mais recente versão do documento, os princípios previstos são os de transparência, *accountability* e legitimidade[598] e as ações consistem em: (i) definir o benefício público almejado pelo projeto e entender as necessidades do usuário do projeto e como ele será impactado pelas ações adotadas; (ii) elaborar e desenvolver o projeto com profissionais com expertises diferentes; (iii) cumprir com o determinado em legislação aplicável; (iv) rever a qualidade (e.g., acurácia e

---

[595] Interessante notar que a Comissão Europeia elaborou relatório informando que análises sobre ética em pesquisas devem também observar procedimentos destinados à proteção de dados pessoais. Vide: https://ec.europa.eu/info/sites/default/files/5._h2020_ethics_and_data_protection_0.pdf. Acesso em 26.10.2022.

[596] Segundo o relatório do OCDE (2019): "Os setores e organizações de política têm sido encorajados a desenvolver seus próprios princípios de dados a fim de tornar suas práticas mais éticas e transparentes e, portanto, mais confiáveis. De fato, construir práticas claras de dados é fundamental para manter a confiança dos cidadãos. O tratamento correto dos dados pode equilibrar a inovação com as práticas de dados éticos, colocando os usuários no centro do processo de projeto de produtos e serviços. Para que isso aconteça, os cidadãos precisam entender como os dados sobre eles estão sendo coletados, analisados e armazenados e por quanto tempo eles serão mantidos, para que eles vejam o valor criado a partir de sua contribuição, bem como os valores e a cultura do governo que lida com os dados. Consequentemente, equipar o público para entender e participar da confiança pública é fundamental, pois a voz dos cidadãos e o empoderamento é um elemento significativo para alimentar a confiança e a confiança, ao mesmo tempo em que contribui para a inclusão digital." (tradução nossa).

[597] Disponível em: https://www.gov.uk/government/publications/data-ethics-framework. Acesso em 24.10.2022

[598] Enquanto o princípio da transparência exige que informações sobre projetos envolvendo o uso de dados sejam divulgados de forma completa e de fácil compreensão, o princípio de *accountability* recomenda a implementação de estrutura de governança com clara distribuição de responsabilidades, incluindo a de fiscalização, e o princípio de legitimidade ("*fairness*") exige a adoção de medidas destinadas a remover o potencial discriminatório do tratamento sobre grupos e indivíduos.

representatividade) e limitação dos dados; e (v) avaliar e monitorar a utilização de dados de forma responsável.

De forma similar, a OCDE (2021) desenvolveu dez princípios para o uso de dados pelo poder público segundo parâmetros éticos, entre os quais estão: (a) gestão de dados com integridade; (b) observância ao determinado em legislação aplicável; (c) inclusão de considerações éticas em processos de tomada de decisão governamentais, (d) monitoramento e fiscalização sobre a entradas de dados, especialmente as usadas para informar o desenvolvimento e treinamento de sistemas de inteligência artificial, e adotar uma abordagem baseada em risco na automação de decisões; (e) estabelecer finalidade específica de uso de dados; (f) definir limites para acesso, compartilhamento e uso de dados; (g) ampliar o controle de indivíduos e grupos sobre seus dados pessoais; e (h) responsabilidade e proatividade na gestão de riscos.

19 CONCLUSÃO PARCIAL: DIÁLOGO ENTRE LGPD E NORMAS APLICÁVEIS AO PODER PÚBLICO PARA A CONCRETIZAÇÃO DA PUBLICAÇÃO E DO COMPARTILHAMENTO DE DADOS EM OBSERVÂNCIA À PRIVACIDADE

Nos casos em que o compartilhamento ou a publicação de dados pessoais atender o interesse público, será necessário adotar cuidados adicionais para assegurar a privacidade e a proteção de dados pessoais dos cidadãos. Diante das incertezas decorrentes da abertura (ou falta de clareza) no texto legal, e da ainda incipiente literatura nacional que promova diálogo entre a LGPD e normas aplicáveis às atividades do poder público, este capítulo buscou apresentar interpretações e soluções possíveis para a divulgação de dados pessoais em observância à privacidade e proteção de dados pessoais. O objetivo não foi esgotar todos os pontos de interface entre a LGPD e demais normas que regulam a atuação governamental (e tampouco de realizar teoria de direito administrativo), mas tão somente apresentar balizas para serem consideradas na efetivação do compartilhamento e da publicação de dados pelo governo. Além disso, as conclusões desta Parte se limitam às atividades do poder público, não podendo ser replicadas para a divulgação de dados realizados exclusivamente por entes privados. Além disso, as conclusões desta Parte se limitam às atividades do poder público, não podendo ser replicadas para a divulgação de dados realizados exclusivamente por entes privados.

Os temas debatidos nesta Parte foram selecionados com base nos aprendizados decorrentes da experiência estrangeira avaliada, que possui paralelo com o procedimento legal estabelecido pela LGPD. Além disso, cumpre ressalvar que certos aspectos centrais à devida divulgação de dados pelo poder público foram analisados em capítulo anterior, como etapa do procedimento para a determinação sobre a divulgação de dados pessoais pelo poder público, motivo pelo qual não foram novamente enfrentados nesse momento (e.g., princípios da necessidade e da finalidade). Outros aspectos da LGPD que também dizem respeito ao tratamento de dados pelo poder público não foram enfrentados por não serem centrais na determinação e efetivação da publicação ou do compartilhamento de dados (e.g, regras pertinentes sobre incidentes de segurança da informação).

Tal como as leis de proteção de dados pessoais adotadas em outros locais (e.g., a GDPR ou as leis de proteção de dados pessoais do Canadá, Colômbia e México), a LGPD

possui princípios fundantes que conduzem toda a interpretação de suas disposições e permitem que a lei se mantenha atual mesmo diante da rápida evolução da tecnologia. Entre esses princípios, para fins de discussão sobre a divulgação de dados por governos, destacam-se os princípios da finalidade, necessidade, transparência e prestação de contas e responsabilização.[599] Nesta Parte da tese foram abordados os últimos dois princípios, visto que os demais já foram enfrentados em outro momento desta tese.

Em relação ao **princípio da prestação de contas**, ele requer aos agentes de tratamento de dados pessoais adotar medidas e registros que demonstrem a adequação de suas atividades às exigências da legislação de proteção de dados pessoais. Trata-se de uma exigência legal aos controladores, mas que busca assegurar maior flexibilidade e autonomia sobre como eles podem executar as determinações da LGPD. Essa maior maleabilidade inclui aspectos como a formatação da documentação exigida (i.e., RoPA, LIA e RIPD), a metodologia de análise de risco adotada e quais medidas de mitigação implementar (e.g., cláusulas contratuais e *privacy enhancing technologies*). Já o princípio da responsabilização é a outra face do princípio da prestação de contas, na medida em que diz respeito à possibilidade de fiscalização sobre o cumprimento das normas de proteção de dados.

De todo modo, entre as obrigações decorrentes do princípio da prestação de contas, esta tese se preocupou particularmente com a elaboração de **relatório de impacto** à proteção de dados pessoais, na medida em que constitui procedimento no qual o agente público poderá, nos casos de divulgação de alto risco, descrever o contexto do tratamento, avaliar sua necessidade, proporcionalidade e interesse público, identificar seus riscos e benefícios, e apontar as salvaguardas propostas para mitigar esses riscos. O RIPD elaborado pelo poder público poderá depois ser publicado, total ou parcialmente, respeitadas normas de sigilo e segredos comerciais ou industriais, como uma forma de cumprir com o princípio de transparência e de assegurar meios para *accountability* social sobre como dados pessoais são tratados por determinados órgãos ou entidades públicas. No entanto, é importante notar que a elaboração de relatório de impacto (que envolve algum nível de complexidade) não poderá atuar como uma barreira ou motivo de atraso na divulgação de informações de interesse público.

[599] Outros princípios são cruciais a qualquer atividade de tratamento de dados realizado pelo poder público, como os princípios da segurança e não discriminação, mas não foram abordados nesta tese por necessidade de recorte temático ao procedimento de divulgação de dados pelo poder público.

Em relação à **avaliação de risco**, entende-se que ela deverá ser contextual e considerar elementos como a natureza dos dados, quem são os titulares de dados, as condições em que eles foram coletados e a finalidade do tratamento. Em vista da ausência de parâmetros claros na LGPD sobre como avaliar riscos, a ANPD submeteu o tema a consulta pública, tendo elaborado proposta segundo a qual o tratamento de dados pessoais será considerado como de alto risco ao cumular critérios gerais (e.g., tratamento em larga escala) com critérios específicos (e.g., tratamento de dados pessoais de crianças e idosos). No entanto, os critérios estabelecidos pela ANPD impõem consideráveis dificuldades, especialmente para o tratamento de dados pessoais pelo poder público (porque muitos de seus tratamentos cumprem com o critério de larga escala).

De todo modo, caso esse seja efetivamente o critério a ser adotado pela legislação brasileira, a eventual qualificação de uma atividade como sendo de elevado risco **não** leva o resultado do teste de proporcionalidade a concluir que o interesse público resulta necessariamente na restrição de acesso a dados pessoais. Assim, é possível publicar ou compartilhar dados pessoais em casos de tratamento de dados qualificado pela ANPD como de alto risco, desde que presente o interesse público e adotadas salvaguardas efetivas. Além disso, o teste de proporcionalidade deverá considerar também outros fatores em sua análise de riscos, como a efetividade da técnica de anonimização adotada, se o titular se encontra em situação de vulnerabilidade e se o tratamento pode produzir efeitos discriminatórios ilícitos ou abusivos.

Quanto ao **princípio da transparência**, ele exige aos controladores e operadores oferecer, em local de fácil acesso, informações completas, claras e adequadas sobre as atividades de tratamento de dados que realizam. Com isso, referido princípio assegura informações para que os titulares de dados possam exercer sua autodeterminação informativa (ou seja, para que possam compreender, escolher e até questionar os possíveis usos que são atribuídos a seus dados pessoais) e para a prestação de contas do controlador em relação a outros agentes interessados, como reguladores, pesquisadores e parceiros comerciais.

No caso do poder público, esse princípio é reforçado pelo direito fundamental de acesso à informação e pelo princípio da publicidade dos atos administrativos, que asseguram a todo cidadão o direito de obter informações provenientes de órgãos públicos, salvo em hipóteses prescritas em lei, e que os órgãos públicos possuem o dever de ativamente publicizar dados e informações a respeito de sua atuação. Por isso, determinações sobre transparência constantes de leis como a LAI se aplicam igualmente às atividades realizadas

que envolvem o tratamento de dados pessoais mantidos pelo poder público. Esse esforço poderá ser efetivado de múltiplas formas, como a publicação de política de privacidade que explique quais dados o órgão ou entidade trata e em quais condições (ou seja, a política de privacidade não pode se limitar a descrever como são tratados os dados coletados durante a navegação do *webiste* do ente público), a divulgação de trechos relevantes do RoPA, LIA e/ou RIPD que não estejam protegidos por sigilo ou segredos comercial e industrial, o fornecimento de informações durante a utilização do serviço público, e a listagem dos terceiros com quem o ente público divulga ou recebe dados pessoais.

Em seguida, como mencionado anteriormente, um dos meios pelos quais as leis de proteção de dados pessoais asseguram autodeterminação informativa aos titulares de dados constitui o estabelecimento de **bases legais**, ou seja, situações nas quais o tratamento de dados pessoais será considerado legítimo. Para o poder público, a existência de balizas legais à prática de suas atividades não é novidade, na medida em que órgãos e entidades públicos estão adstritos aos princípios constitucionais da legalidade e da impessoalidade, segundo os quais as condutas dos agentes públicos devem ser autorizadas pela ordem constitucional e pela lei. O art. 23 da LGPD reforça essa exigência ao determinar que o poder público trate dados pessoais sempre com vistas ao atendimento de suas funções públicas, no atendimento do interesse público e com o objetivo de executar competências ou atribuições legais.

Na LGPD, as bases legais são delimitadas nos arts. 7º e 11, que preveem base legal específica para atividades de tratamento que sejam necessárias à execução de políticas públicas. Essa base legal, no entanto, não é a única que pode ser utilizada por órgãos e entidades públicas. De fato, esta tese defende que as bases legais previstas nos arts. 7º e 11 são taxativas e que todas podem ser utilizadas para justificar atividades de tratamento realizadas pelo poder público, desde que observados os requisitos do art. 23 (i.e., ser realizada em atendimento ao interesse público e nos limites das suas atribuições legais). Nesse cenário, as bases legais de execução de políticas públicas e de cumprimento de obrigação legal são geralmente as mais apropriadas para justificar o tratamento de dados pessoais pelo poder público, visto que exigem que a atividade seja embasada em legislação. Interessante notar que, justamente por estarem atreladas à existência de uma obrigação legal ou regulatória prévia, elas apresentam grande semelhança entre si. No entanto, elas possuem diferenças importantes e que impactam no dever de os agentes públicos justificarem o interesse público e a necessidade da atividade.

A base legal de cumprimento de obrigação legal ou regulatória se aplica quando a legislação exigir a realização de certa atividade de tratamento de dados (e.g., envio de dados por um órgão ou entidade público a outro ente público). O tratamento deverá ser resultado de uma obrigação clara, precisa e previsível pelo titular de dados, não podendo ser uma dentre as possíveis formas de executar essa obrigação. Nesse caso, a ponderação sobre o interesse público na publicação ou no compartilhamento de dados pessoais é realizada pelo legislador ou pelo administrador em sua capacidade legislativa, cabendo ao agente público menor grau de discricionariedade em relação às condições de tratamento dos dados.

Já a base legal de execução de políticas públicas poderá estar prevista em obrigação legal ou regulatória ampla, mas o tratamento deverá ser realizado dentro das atribuições legais do órgão ou entidade pública e ser necessário para o alcance do interesse público. Se o fim estabelecido em lei ou regulamento for alcançável de outra forma razoável e menos intrusiva, essa base legal não será aplicável. Diante disso, caberá ao agente público demonstrar a razoabilidade e a necessidade do tratamento pretendido, avaliar os riscos que a atividade impõe aos titulares de dados, ponderar sobre o interesse público envolvido no uso dos dados, e apontar quais salvaguardas adotar para proteger os titulares. Na prática, essa tarefa poderá ser realizada em documento de *accountability*, como o relatório de impacto nos casos em que a atividade de tratamento imponha elevado risco às liberdades e direitos dos cidadãos.

Por sua vez, ainda que o consentimento e o legítimo interesse não sejam as bases legais mais apropriadas para fundamentar atividades praticadas pelo poder público, elas muitas vezes serão as mais apropriadas para justificar o reuso de dados publicados ou compartilhados. O consentimento é a base legal mais conhecida por ter sido, nas primeiras leis de proteção de dados, a materialização da autodeterminação informativa. No entanto, o consentimento como única base legal impõe dificuldades em sua implementação, especialmente em casos de tratamento de dados pelo poder público, em que muitas vezes o titular de dados não possui uma opção real quanto ao tratamento de seus dados, visto que atividades governamentais decorrem de obrigações legais e regulatórias e são destinadas ao alcance do interesse público.

É por isso que as mais modernas leis de proteção de dados pessoais preveem outras bases legais e fortalecem outros mecanismos para a garantia da autodeterminação informativa, a exemplo da previsão de novos direitos aos titulares de dados. Nesse desenho, também se destacam os requisitos do consentimento que permitem ao titular de dados oferecer e remover a qualquer momento a sua autorização para determinada atividade de tratamento e sem afetar

seu uso dos serviços. Assim, a legislação moderna de proteção de dados ressalta que o consentimento deverá ser livre, informado, inequívoco, não sendo permitida a obtenção de autorizações genéricas, enganosas ou abusivas.

No tratamento de dados pelo poder público, é particularmente desafiador obter consentimento livre (ou seja, ser uma escolha genuína e desimpedida de pressões externas), diante da disparidade de poder entre governos e cidadãos e da necessidade do tratamento de dados para o desempenho pelo poder público de suas atribuições legais, que acabam por remover a autonomia do cidadão em decidir se deseja consentir. Além disso, a exigência de que o consentimento seja obtido para finalidades determinadas (ou seja, deverá ser obtida autorização autônoma para cada uma das diferentes finalidades de tratamento) impõe desafios práticos para sua utilização em casos de compartilhamento e para a publicação de dados pelo poder público, na medida em que a obtenção e gestão dessas múltiplas autorizações adiciona complexidade à burocracia estatal, que atualmente conta com sistemas de interoperabilidade para atribuir efetividade à suas atividades.

De todo modo, nos casos em que for adequada a utilização do consentimento pelo poder público, seu requisito informacional exerce papel importante na redução dessa disparidade de poder entre governos e cidadãos. Com isso, o cidadão terá condições de compreender e confiar que sua decisão sobre o consentimento não irá impactar seu acesso a direitos, serviços públicos ou políticas públicas. Essa tarefa deverá ser feita em consideração ao segmento da população impactado, o que poderá abranger pessoas de diferentes origens e níveis de escolaridade, e também populações em situação de vulnerabilidade. Entre as situações em que o consentimento poderá ser utilizado para fins de divulgação de dados pelo poder público estão: (i) situações em que não há significativa disparidade de poder na relação entre cidadão e governo, e quando a atividade realizada não é fruto de obrigação legal ou regulatória, ou quando não necessária para o exercício de políticas públicas; e (ii) certos tipos de reuso de dados recebidos por consequência de práticas de divulgação de dados pelo poder público.

Já a base legal de legítimo interesse pode ser utilizada quando o tratamento de dados for necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso em que prevaleçam direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. Como é uma base legal mais flexível, a legislação restringe seu uso para o tratamento de dados sensíveis e estabelece algumas condições para que possa ser utilizada. Por exemplo, o controlador deverá demonstrar no caso concreto, a presença de interesse

legítimo que não gere impactos significativos a direitos e liberdades de titulares, que exige a verificação da legitimidade do interesse, da identificação da necessidade do tratamento, o balanceamento dos interesses envolvidos, e a implementação de salvaguardas para mitigar os riscos decorrentes do tratamento. Esse teste se assemelha com o teste de proporcionalidade, o que é em alguma medida esperado, pois as bases legais são uma dentre as medidas destinadas a assegurar aos indivíduos mais autonomia sobre como seus dados são tratados, e a base legal de legítimo interesse é mais flexível que as demais bases legais. Assim, como o legítimo interesse, em tese, permite maior flexibilização a direitos e liberdades de titulares de dados, o sopesamento de interesses é recomendado.

Esse é também um dos motivos pelos quais, na Europa, a base legal do legítimo interesse não seria aplicável ao tratamento de dados pelo poder público. A LGPD silencia sobre o tema, de tal forma que seria possível ao poder público utilizar-se da base legal de legítimo interesse, desde que: (i) superado o teste do legítimo interesse; e (ii) não aplicáveis outras bases legais como as de cumprimento de obrigação legal e regulatória, e execução de políticas públicas. No entanto, a combinação dessas duas condições é desafiadora, especialmente porque as bases legais de cumprimento de obrigação legal e de execução de políticas públicas são atreladas ao princípio da finalidade, incidente aos atos da administração pública. Além disso, a base legal de execução de políticas públicas já oferece ao poder público maior flexibilidade para o tratamento de dados pessoais e exige a adoção de medidas similares àquelas necessárias para a utilização da base legal do legítimo interesse.

Por outro lado, o legítimo interesse poderá ser utilizado por particulares receptores de dados compartilhados ou publicados pelo poder público, desde que permitido pelo teste de legítimo interesse e observados o princípio da finalidade, a boa-fé e o interesse público que justifiquem a publicação e o compartilhamento de dados. Para tanto, o interessado em reutilizar os dados com a base legal do legítimo interesse deverá tomar maior cuidado com as seguintes etapas do teste de legítimo interesse: (a) a legitimidade do reuso de dados que deseja realizar, cuja finalidade deverá ser compatível com as finalidades que justificaram a divulgação; e (b) a avaliação das legítimas expectativas dos titulares de dados, visto que os dados foram coletados pelo poder público por força de legislação ou como condição para o exercício de direitos, utilização de serviços públicos ou obtenção de benefícios sociais.

Após observados os princípios da prestação de contas e da transparência, e assegurado que o tratamento está devidamente fundamentado em uma das bases legais previstas na LGPD, será necessário ao órgão ou ente público viabilizar meios para que os titulares de

dados possam exercer seus **direitos relacionados à publicação ou compartilhamento de seus dados**. Esses direitos surgem como mais uma forma de garantir a autodeterminação informativa a titulares de dados, ao lado, por exemplo, do consentimento.

Os primeiros direitos assegurados estavam relacionados à confirmação sobre a existência do tratamento de dados pessoais, o acesso aos dados, e a correção de dados incompletos, inexatos ou desatualizados. No Brasil esses direitos são assegurados na LGPD e em normas específicas ao poder público, como a Lei de *Habeas Data*, a LAI e a Lei sobre direitos do usuário dos serviços públicos da administração pública federal. Elas delimitam o escopo, estabelecem o procedimento e preveem exceções ao exercício desses direitos. Ainda que com diferenças, essas leis vêm sendo compatibilizadas na prática. Já as mais recentes leis globais de proteção de dados pessoais, incluindo a LGPD, preveem meios adicionais para que os titulares possam exercer controle sobre como seus dados pessoais são tratados, como os exemplos dos direitos de anonimização, portabilidade e oposição ao tratamento de dados.

No entanto, para o tratamento de dados pelo poder público, alguns desses direitos serão de difícil execução, como o exemplo dos direitos de oposição e de anonimização, tendo em vista que muitas vezes haverá justificativa legal para a manutenção dos dados e do tratamento. Por motivos como esse (além de as soluções serem focadas em indivíduos para problemas que muitas vezes alcançam toda uma coletividade), tais direitos não podem ser entendidos como a única ou a principal ferramenta para que titulares possam exercer controle sobre como seus dados pessoais são usados. Isso se faz particularmente importante porque (i) como o tratamento é muitas vezes exigido para que o poder público exerça suas atribuições legais, haverá limitação no alcance do exercício de direitos; e (ii) a possível inadequação no tratamento pode não ocorrer em relação a uma única pessoa, afetando toda a sociedade. Por isso, são igualmente importantes iniciativas de *accountability* e transparência.

Finalmente, outra etapa essencial para que a publicação e o compartilhamento de dados sejam acompanhadas de **salvaguardas destinadas a reduzir os riscos** oferecidos a direitos e liberdades de cidadãos em decorrência dessas atividades de tratamento de dados. A eficiência dessas salvaguardas deve também ser avaliada quando da realização do teste de proporcionalidade para a determinação do interesse público na divulgação de dados pessoais, visto que permite avaliação mais precisa sobre os riscos efetivos à privacidade e proteção de dados pessoais no caso concreto, e evitar situações de restrições excessivas de acesso a dados em prejuízo ao interesse público da divulgação. Determinadas salvaguardas estão previstas

em legislação, mas podem ser também soluções técnicas ou jurídicas estabelecidas pelo controlador dos dados, como abordado.

Em relação a salvaguardas estabelecidas em lei está a regulação sobre as possibilidades e limites do reuso de dados pessoais. A leitura integrativa da legislação vigente (e.g., LGPD, CDC e Constituição Federal) estabelece que todas as atividades de tratamento de dados mantidos pelo poder público deverão observar a finalidade, a boa-fé e o interesse público que justificaram sua divulgação. Esses parâmetros se aplicam tanto à publicação quanto ao compartilhamento de dados pessoais. Ainda que a LGPD possua dispositivo específico sobre o reuso de dados publicados pelo poder público (art. 7º, §3º), seu conteúdo se aplica aos dados compartilhados, por força dos princípios da legalidade e da finalidade do ato administrativo e do disposto nos arts. 6º e 23 da LGPD. A exigência de boa-fé no tratamento de dados pessoais pode se traduzir em um compromisso de agir honesta e razoavelmente e em observância à legalidade do tratamento, ou seja, em uma garantia de que dados pessoais serão sempre tratados em observância à legislação, aos direitos dos titulares de dados, e dentro das expectativas legítimas do titular de dados. Já o interesse público seria o resultado de mediação, pública e motivada, dos diferentes interesses existentes na sociedade, que, na divulgação de dados por governos, busca a transparência e eficiência governamental, *accountability*, acesso à informação. Por sua vez, a finalidade estabelece que o tratamento de dados deverá ser realizado para propósitos legítimos e específicos, não sendo autorizadas atividades posteriores que se mostrem incompatíveis com as finalidades informadas ao titular no momento da coleta dos dados - no reuso de dados divulgados pelo poder público, a compatibilidade no reuso observa as atribuições legais dos agentes envolvidos no tratamento e o interesse público da divulgação realizada. A avaliação dessa compatibilidade deverá levar em consideração a relevância do uso desses dados para outras finalidades, desde que isso resulte em benefício para o interesse público e não imponha riscos demasiadamente elevados a direitos e liberdades de titulares de dados. Do contrário, medidas de transparência e eficiência governamental teriam sua eficácia consideravelmente reduzida.

Outra modalidade de salvaguarda prevista em lei (ainda que sua execução seja técnica) consiste na anonimização na ou pseudonimização de dados, que podem assumir formatos distintos, como a remoção de dados, a não divulgação de documentos, a divulgação de apenas dados previamente agregados, ou a promoção da generalização ou a modificação de certos dados para impedir a identificação de indivíduos. Todavia, em certos casos: (i) o interesse público reside na publicação ou no compartilhamento do próprio dado pessoal, podendo, para

tanto, adotar medidas de parcial remoção ou tarja de dados, ou outras medidas similares, e (ii) quanto mais dados são removidos, ou mais barulho se insere em determinada base de dados, menor poderá ser a utilidade dos documentos e bases de dados divulgados. Assim, a adoção de salvaguardas tecnológicas apresenta o seguinte dilema: de um lado, quanto mais granulares e acessíveis forem os dados, maior a exposição da privacidade de indivíduos, e, de outro lado, quanto menor a granularidade e acessibilidade dos dados, igualmente menor será a utilidade dos dados. Assim, mesmo a utilização de soluções técnicas destinadas a assegurar a privacidade de dados não remove do gestor público a ponderação sobre o conteúdo do interesse no caso concreto, devendo escolher qual a intensidade de mudanças que deverá ser realizada nos documentos e bases de dados divulgadas, de forma a aumentar ou reduzir a privacidade ou as possibilidades analíticas das informações divulgadas.

Além disso, a anonimização ou a pseudonimização não assegura a total impossibilidade de posterior identificação de indivíduos em bases de dados anonimizadas. Diante do avanço das tecnologias e com a quantidade de dados disponíveis, é cada vez mais fácil aos receptores de dados reidentificá-los. Isso ocorre especialmente com técnicas que meramente removem identificadores diretos ou indiretos, mas também pode ocorrer com outras técnicas, como a divulgação de dados agregados ou técnicas de privacidade diferencial. Assim, quando da anonimização ou pseudonimização de dados, é crucial a reflexão sobre a possibilidade de reidentificação de dados divulgados, especialmente diante do contexto no qual dados são cada vez mais disponíveis online ou mediante parcerias.

Há ainda outras possíveis salvaguardas técnicas e jurídicas para mitigar os riscos decorrentes da publicação ou do compartilhamento de dados mantidos pelo poder público, que poderão ser técnicas ou jurídicas. De fato, a limitação jurídica de reuso de dados pessoais não evita completamente que agentes maliciosos utilizem os dados de forma incompatível com a legislação, mas visam a expandir a possibilidade de divulgar dados para finalidades lícitas e legítimas. Entre essas possíveis salvaguardas estão: (i) a adoção de restrições técnicas à coleta e reuso de dados publicados ou compartilhados, como os exemplos da utilização de ferramentas que impeçam práticas maliciosas de *web scraping* ou *download* de arquivos, (ii) em situações de riscos mais elevados na publicação de dados, compartilhar com entidades específicas para finalidades previamente autorizadas, (iii) a adoção de cláusulas em contratos ou constantes de Termos de Serviço e Políticas de Privacidade; e (iv) a instituição de Conselhos e Códigos de Ética destinadas a guiar e avaliar se estão sendo realizadas segundo parâmetros éticos e em benefício do interesse público.

Especificamente em relação à adoção de cláusulas em contratos, ToS ou Políticas de Privacidade, elas delimitam os contornos do compartilhamento e da publicação de dados pelo ente público, assim como dos possíveis novos tratamentos que serão realizados com os dados. Essas cláusulas são essenciais para fins de *accountability* e confiança cidadã sobre o uso de seus dados pessoais, mas devem ser elaboradas de forma a efetivamente assegurar a observância à legislação de proteção de dados pessoais. Caso contrário, apenas limitam o interesse público ou facilitam a afronta a direitos de titulares de dados. Por isso, entre as possíveis exigências que podem ser feitas aos receptores dos dados estão: **(a)** evitar certas atividades de varredura e/ou finalidades de usos secundários, **(b)** somente coletar os dados necessários à realização de atividades secundárias lícitas e legítimas; **(c)** obter dos titulares de dados a autorização para o tratamento dos dados, incluindo informações sobre a origem e finalidades do tratamento e a fundamentação em uma base legal compatível com o tratamento secundário; e **(d)** viabilizar mecanismos para o exercício de direitos por titulares de dados. Se os dados forem protegidos por normas de sigilo, mas a sua divulgação for autorizada por lei, a cláusula deverá também prever restrições ao tratamento subsequente de dados que seja compatível com os limites da norma de sigilo. Essas cláusulas devem ser disponibilizadas ao público, de forma a viabilizar o controle social da adequação dos limites jurídicos impostos ao reuso de dados pessoais de cidadãos que tenham sido divulgados pelo governo.

CONCLUSÃO

Esta tese buscou equacionar a eficiência e a transparência governamental com a privacidade e a proteção de dados pessoais na publicação e no compartilhamento de dados por governos.

A publicação e o compartilhamento de dados são considerados nesta tese como modalidades de divulgação de dados, visto que promovem a sua circulação e permitem seu reuso por terceiros. Dito de forma diferente, são modalidades de interação entre governos e outras entidades, públicas ou privadas, por meio do envio ou recebimento de dados para finalidades como a eficiência e a transparência governamental. Especificamente, a publicação resulta em viabilizar acesso e uso posterior de dados de interesse público para, entre outros, promover a transparência e o acesso à informação, e o compartilhamento envolve o acesso de dados a terceiros específicos, para finalidades como a eficiência e a desburocratização estatal. Diante dessas semelhanças (e considerando que muitas vezes buscam alcançar objetivos similares), esta tese defende que o compartilhamento e a publicação são passíveis de serem comparados e submetidos a soluções jurídicas harmônicas, respeitadas as suas diferenças (e.g., quem são os receptores dos dados, as finalidades de divulgação, e os riscos oferecidos aos cidadãos).

Assim, a publicação e o compartilhamento de dados pelo poder público auxiliam o Estado a alcançar objetivos diversos, dentre os quais esta tese destaca a prestação de serviços públicos, o desenvolvimento de políticas públicas, a desburocratização do aparato governamental, a promoção de transparência governamental, a viabilização de *accountability* e a participação social no governo, e a colaboração com práticas de inovação governamental ou privada. Por outro lado, essas atividades podem envolver dados pessoais, cujo tratamento irregular oferece riscos aos direitos e liberdades dos cidadãos (e.g., permite práticas de vigilância, o reforço de vieses discriminatórios, e a remoção de autonomia individual sobre como seus dados são usados).

Como se verificou nesta tese, esforços de equacionar a privacidade com a circulação de dados pessoais pelo governo não são novidade e motivaram as primeiras iniciativas de regulação do tratamento de dados pessoais. A despeito disso, as literaturas recentes sobre modernização e abertura governamental e sobre privacidade e proteção de dados pessoais ainda possuem diálogo escasso. Enquanto a literatura sobre novos modelos de governo está

dedicada à promoção de transparência e eficiência governamental, a literatura sobre privacidade e proteção de dados têm se preocupado mais com o uso de dados pessoais por agentes privados ou com atividades governamentais de persecução penal e segurança do Estado. Para tanto, faz-se necessário ampliar o diálogo entre estas literaturas, com o propósito de encontrar soluções para garantir os benefícios da divulgação de dados pelo poder público com o menor prejuízo possível a direitos e liberdades de cidadãos.

De forma similar, a análise da legislação nacional aplicável ao tema permite concluir que, a despeito dos avanços legislativos ocorridos desde a década de 1990, e que culminaram com a edição da LGPD em 2018, ainda há considerável incerteza sobre como harmonizar na prática a publicação e o compartilhamento de dados mantidos pelo poder público com a proteção de dados pessoais. De um lado, a legislação pertinente à divulgação de dados por governos está centrada em romper com paradigmas de burocracia e sigilo governamentais, e, de outro lado, a legislação que regula a privacidade e proteção de dados pessoais é principiológica e conta com problemas de técnica legislativa que dificultam a sua aplicação para fins de tratamento de dados pelo poder público.

Especificamente, tanto a publicação como o compartilhamento de dados pelo poder público podem ser apoiados nos bens jurídicos constitucionalmente assegurados da transparência, acesso à informação ou na eficiência governamental. A LAI permite a publicação de dados pessoais em situações específicas, como a presença de interesse público ou o consentimento do titular de dados, e as normas que regulam o compartilhamento de dados por órgãos da administração pública federal apenas preveem obrigações genéricas de observar o disposto nas normas de privacidade e proteção de dados pessoais. Por sua vez, a privacidade e a proteção de dados pessoais são direitos fundamentais protegidos pela constituição, cuja proteção alcança não somente indivíduos, constituindo um interesse coletivo. Embora a LGPD seja destinada a atribuir concretude a tais direitos, suas disposições específicas para o poder público possuem imprecisões que dificultam sua aplicação no caso concreto.

Diante dessa falsa percepção de que a divulgação de dados pelo poder público é incompatível com a privacidade e a proteção de dados pessoais, e da carência de parâmetros legislativos claros sobre como harmonizar esses interesses, é possível observar inconsistência prática na publicação e no compartilhamento de dados por governos. Enquanto a LGPD tem sido utilizada para restringir o alcance de políticas de transparência, foram editadas regras

para viabilizar o compartilhamento de dados pelo poder público sem similares cuidados com a privacidade e a proteção de dados pessoais de cidadãos.

No entanto, não somente esses interesses são compatíveis entre si, como sua harmonização é necessária. Isso se dá principalmente porque, de um lado, o uso inadequado de dados poderá provocar prejuízos a liberdades e direitos individuais, e, de outro lado, a priorização da privacidade e proteção de dados pessoais pode levar à generalização do sigilo governamental e à redução de práticas de inovação e de controle social sobre a gestão pública. Além disso, não é desejável a uma democracia garantir a privacidade e proteção de dados pessoais de formas distintas em situações similares. Ainda que o compartilhamento e a publicação de dados por governos possuam diferenças entre si, elas devem ocorrer em observância a um procedimento similar, destinado à garantia da privacidade e proteção de dados pessoais. Assim, ela deve observar as particularidades da situação concreta, mas não seguir lógicas distintas para avaliar quando o uso de dados poderá ser restrito em favor da privacidade (ou quando a privacidade poderá ser limitada em favor do uso de dados).

Em linha com esse entendimento, em julgamento realizado em setembro de 2022, o STF concluiu pela inconstitucionalidade de normas ou interpretações legais que permitam a ampla e irrestrita divulgação de dados pessoais pelo poder público, sendo necessário haver procedimentos capazes de garantir a divulgação e o reuso de dados para finalidades legítimas, informadas aos titulares de dados, e limitadas ao mínimo necessário. Para tanto, considerando esse cenário, esta tese buscou apresentar proposta dogmático-jurídica capaz de contribuir com a promoção de diálogo teórico e prático sobre a divulgação de dados por governos em observância à privacidade e proteção de dados pessoais.

Considerando exemplos da experiência estrangeira e tendo em vista a legislação nacional, esta tese apresenta procedimento para auxiliar o agente público a divulgar dados pessoais em observância à privacidade e proteção de dados pessoais. Esse procedimento pode ser utilizado tanto para a publicação quanto para o compartilhamento, respeitadas suas particularidades, e conta com três etapas que se relacionam: delimitação do escopo do compartilhamento ou da publicação, identificação do conteúdo do interesse público no caso concreto, e adoção de medidas para a divulgação em observância à privacidade e proteção de dados pessoais.

Quanto à **delimitação do escopo** da divulgação pretendida, o agente público deverá primeiro identificar se ela envolve dados que permitam a identificação da pessoa natural sobre

quem se referem. Essa tarefa não será simples em casos de publicação ou compartilhamento de dados por governos, visto que o conceito de dados pessoais é amplo e o receptor dos dados poderá associá-los a outros dados ou empregar recursos tecnológicos que permitam a reidentificação do titular. Diante disso, a divulgação de dados pelo poder público muitas vezes envolve dados pessoais e deve ocorrer segundo a LGPD; isso não significa que não deve haver a divulgação, mas que deve-se observar cuidados adicionais. Nesse momento, é preciso ter em mente que a publicação ou o compartilhamento, assim como a incidência de sigilo ou confidencialidade sobre a informação, não remove do dado a sua qualidade de dado pessoal. Em verdade, se o dado puder ser razoavelmente associado a uma pessoa natural, ele será qualificado como dado pessoal. Assim, os fatos de o dado ser controlado pelo governo, estar disponível publicamente, ser divulgado a terceiros ou ser protegido por norma de sigilo ou cláusula de confidencialidade não afastam a incidência da LGPD.

Em seguida, o controlador deverá especificar quais os objetivos almejados com a divulgação, de modo a observar os princípios da finalidade e da necessidade. Segundo as normas de proteção de dados pessoais e de direito administrativo, o princípio da finalidade exige que o compartilhamento e a publicação de dados pelo poder público não somente atendam um objetivo específico, legítimo e informado ao titular de dados, como estejam previstos no ordenamento jurídico, sejam realizados conforme as atribuições legais do órgão ou entidade pública, e almejem o alcance do interesse público. Além disso, a divulgação de dados será realizada para finalidades compatíveis com as informadas aos titulares no momento da coleta dos dados. Para fins da divulgação do dado pelo poder público, deve levar em consideração a competência do ente público e o interesse público nessa divulgação, em linha com o conceito de separação informacional dos poderes, segundo o qual o Estado não deve ser considerado uma entidade única para fins de uso de dados pessoais. Com isso, garante-se que, mesmo para dados coletados no contexto da execução de serviços públicos e de políticas públicas, o novo tratamento esteja razoavelmente dentro das legítimas expectativas do titular de dados. Em relação ao princípio da necessidade, a divulgação de dados pessoais deve ser limitada ao estritamente relevante para alcançar a finalidade informada, não podendo haver outros meios de alcançar os mesmos objetivos de forma menos lesiva a direitos dos titulares.

Após, o controlador deverá identificar quem são os receptores dos dados. Em práticas de governos eletrônicos, digitais ou abertos, há um complexo de arranjo de *stakeholders* que podem se envolver. Sua identificação permite uma melhor compreensão das possíveis

finalidades e riscos no reuso de dados divulgados pelo poder público, assim como auxilia na distribuição de responsabilidades a serem observadas, assim como na resolução de casos de descumprimento do disposto na legislação. Na literatura referente ao reuso de dados, esses agentes podem ser os detentores das bases de dados, intermediários de dados e os consumidores deles. Os detentores das bases de dados são geralmente órgão ou entidade público que coleta o dado diretamente do cidadão ou o recebe de terceiros. Os intermediários de dados atuam na localização de bases de dados, conexão e estruturação das informações, e produção de valor às bases de dados. Já o consumidor de dados será o destinatário final dos dados, que poderá atuar de forma independente, cooperativa ou direcionada a parcerias com outros agentes. Por sua vez, na literatura de dados pessoais, os agentes são qualificados como controladores ou operadores, a depender do seu envolvimento na atividade de tratamento. O controlador será o agente responsável por estabelecer as finalidades de uso e os meios essenciais do tratamento, e o operador atuará em conformidade com a legislação e as orientações do controlador. Por isso, a responsabilidade do tratamento inadequado de dados pessoais recai principalmente no controlador, e apenas residualmente no operador. Assim, os detentores de bases de dados, intermediários e consumidores de dados poderão atuar como operadores ou controladores, a depender do seu envolvimento na divulgação de dados pessoais mantidos pelo poder público.

Constatada a presença de dados pessoais, será necessário identificar a presença de **interesse público** na publicação ou no compartilhamento pretendido. Essa é decorrente de previsão legal da LAI e da LGPD, e se aplica a qualquer atividade de tratamento de dados pessoais realizada pelo poder público, incluindo a publicação e o compartilhamento de dados pessoais. Segundo a moderna teoria de direito administrativo, essa tarefa requer o reconhecimento da existência de uma pluralidade de interesses sociais heterogêneos que deverão ser mediados por uma decisão pública motivada. No caso de compartilhamento ou publicação de dados, os interesses em conflito são os direitos fundamentais à privacidade e proteção de dados pessoais (que são interesses da coletividade, e não somente do indivíduo) em relação ao direito à informação e aos princípios da eficiência e transparência governamental. Ainda que objeto de críticas teóricas, entre outros motivos, por considerar que direitos fundamentais podem ser limitados, o método mais utilizado pela jurisprudência nacional e internacional para mediar princípios no caso concreto consiste no teste de proporcionalidade. Assim, o interesse público consistirá no resultado do teste de

proporcionalidade e poderá consistir na divulgação de dados ou na restrição de acesso a esses dados.

Desde que superadas as duas primeiras etapas do teste de proporcionalidade (i.e., demonstrar que a divulgação contribui para fomentar a transparência e a eficiência governamental e que isso não seria razoavelmente viabilizado de outra forma), e adotadas salvaguardas capazes de mitigar os riscos à privacidade e proteção de dados pessoais, o teste de balanceamento poderá pender em favor da divulgação de acesso aos dados. Além disso, para identificar elementos que auxiliem na realização do teste de proporcionalidade para fins de divulgação de dados pessoais pelo poder público, esta tese realizou análise não exaustiva das experiências Europeia e Canadense e de decisões do STF e da CGU a respeito do conflito entre transparência e/ou eficiência governamental e os direitos de privacidade e proteção de dados pessoais.

De imediato, foi possível diagnosticar que as decisões brasileiras apresentam semelhança em relação aos entendimentos de autoridades do Canadá e do Reino Unido, segundo os quais geralmente haverá interesse público na publicação e no compartilhamento de dados pessoais por governos em casos de fomento ao *accountability*, à participação social e proteção do processo democrático, à tomada qualificada de decisão por órgãos públicos, e à garantia do melhor uso de dinheiro público. Essas situações não são exaustivas, podendo incluir, por exemplo, a promoção de saúde pública ou o apoio à administração da justiça. Por outro lado, segundo a experiência estrangeira e as decisões nacionais, não será de interesse público a informação obtida para fins de curiosidade ou para benefícios estritamente privados.

Nas decisões brasileiras também foi possível identificar que, se a divulgação resultar em afronta a norma ou a determinações contratuais de confidencialidade, em riscos elevados à privacidade e/ou as salvaguardas propostas não forem consideradas satisfatórias, o teste de proporcionalidade pende em favor da restrição de acesso aos dados. Nesses casos, o sigilo ou confidencialidade estariam assegurando confiança aos cidadãos sobre a privacidade de suas informações, de modo que a sua inobservância afrontaria a legítima expectativa dos titulares sobre como seus dados seriam utilizados. No entanto, é possível que regras de sigilo ou de confidencialidade sejam irregulares, podendo ser afastadas por autoridade competente.

Outros aspectos identificados nas decisões brasileiras consistem na: (i) avaliação não aprofundada sobre a presença de dados pessoais no caso concreto; (ii) qualificação equivocada de certos dados pessoais como sensíveis e o questionável entendimento de que

não deverá haver divulgação de dados dessa natureza; (iii) pouca reflexão sobre a necessidade dos dados para o alcance da finalidade almejada ou sobre formas de concretizar a publicação ou o compartilhamento, em observância à privacidade e proteção de dados pessoais. Especificamente em relação ao segundo aspecto, a LGPD estabelece situações taxativas que serão consideradas como tratamento de dados pessoais sensíveis (e.g., raça e orientação sexual) e não impede a publicação ou o compartilhamento desses dados. Embora o tratamento de dados sensíveis tenha o potencial de gerar maiores danos aos titulares de dados, nem toda atividade de tratamento envolvendo tais dados resultará em elevado risco a seus direitos e liberdades. Assim, a divulgação de certos dados pessoais sensíveis, a depender das particularidades do caso concreto, poderá ser qualificada como de interesse público.

Determinado que o interesse público consiste na divulgação de dados pessoais, deverá o controlador adotar procedimentos destinados a assegurar que os dados sejam divulgados e subsequentemente tratados em observância às normas de proteção de dados pessoais.

Havendo interesse público na publicação ou no compartilhamento de dados pessoais, devem ser adotadas **medidas** para garantir que a divulgação de dados pelo poder público ocorra em observância à privacidade e proteção de dados pessoais de cidadãos. Para tanto, esta tese buscou promover o diálogo entre a LGPD e normas aplicáveis às atividades do poder público, apresentando interpretações e soluções possíveis para esse esforço.

Note que essas conclusões são focadas no poder público e não podem ser replicadas de forma irrefletida para atividades de divulgação de dados realizadas exclusivamente por entidades privadas. Além disso, elas abordam somente aspectos legais centrais para divulgação de dados pelo poder público.

Primeiro, deverão ser observados os princípios de prestação de contas e transparência. Em relação ao primeiro princípio, ele requer aos agentes de tratamento de dados pessoais registrar e demonstrar a efetividade de medidas que adotam para que o tratamento seja realizado em observância às exigências da legislação de proteção de dados pessoais, a exemplo da elaboração de RoPAs e Relatórios de Impacto. Nos casos em que a divulgação for considerada de alto risco, a ANPD poderá exigir a elaboração de RIPD que contenha a descrição do contexto do tratamento, avaliação da sua necessidade, proporcionalidade e interesse público, identificação dos riscos e benefícios do tratamento, e sugestão de salvaguardas para mitigar esses riscos. Esse documento elaborado pelo órgão ou entidade público poderá depois ser publicado, total ou parcialmente, respeitadas normas de sigilo e

segredos comerciais ou industriais, como uma forma de cumprir com o princípio de transparência, e de assegurar meios para *accountability* social sobre como dados pessoais são tratados.

Por sua vez, a identificação do risco da divulgação é um esforço contextual que deve considerar elementos como a natureza dos dados, quem são os titulares de dados, as condições em que os dados foram coletados e a finalidade do tratamento. Nesta tese se argumenta que a metodologia de análise de risco proposta pela ANPD resulta em muitas atividades de tratamento realizadas pelo poder público serem consideradas como de alto risco, na medida em que apresenta como um dos principais critérios para essa análise a presença de tratamento de larga escala. Considerando que governos reúnem dados de todos os residentes no país, em muitas situações haverá o tratamento em larga escala, bastando a utilização de tecnologias inovadoras ou o tratamento de dados sensíveis, por exemplo, para o tratamento ser qualificado como de alto risco. Diante disso, em muitos casos de publicação ou de compartilhamento de dados pelo poder público, será necessário elaborar RIPD, o que poderá impactar o tempo necessário para que se possa divulgar os dados. De todo modo, o fato de o tratamento ser qualificado, segundo os parâmetros da ANPD, como de alto risco não impede que haja presença de interesse público na publicação ou no compartilhamento de dados, desde que não produzam impactos significativos a direitos e liberdades de titulares de dados, e que salvaguardas efetivas sejam adotadas.

Além disso, não é possível presumir que a publicação de dados pessoais pelo poder público promove maiores riscos que o compartilhamento. Embora as políticas de transparência e dados abertos envolvem o acesso de dados por uma quantidade maior de destinatários, é possível haver maior risco no compartilhamento de dados a depender de fatores como a natureza do tratamento a ser realizado, quem são os titulares de dados ou a efetividade das salvaguardas adotadas. O mesmo se aplica à divulgação de dados pessoais sensíveis - não é possível presumir que a divulgação de dados sensíveis será sempre de maior risco do que a divulgação de dados triviais (e tampouco que não haverá interesse público nessa divulgação).

Em relação ao princípio da transparência, ele exige ao controlador divulgar informações completas de fácil compreensão sobre as atividades de tratamento que realiza em local de fácil acesso. Para o poder público, esse princípio é reforçado pelo direito fundamental de acesso à informação, pelo princípio da publicidade governamental e pelo disposto em normas infraconstitucionais, como a LAI e a Lei de Governo Digital. Essa obrigação poderá

ser efetivada de múltiplas formas, como a publicação de política de privacidade que explique quais dados o órgão ou entidade trata, e em quais condições, a divulgação de trechos relevantes do RoPA, LIA e/ou RIPD que não estejam protegidos por sigilo ou segredos comercial e industrial, o fornecimento de informações durante a utilização do serviço público, e a listagem dos terceiros com quem o ente público divulga ou recebe dados pessoais.

Em relação às bases legais, embora aquelas previstas nos arts. 7º e 11 da LGPD se apliquem às atividades de tratamento de dados pelo poder público, desde que observados os requisitos do art. 23 da LGPD, muitas vezes as mais apropriadas para o caso concreto serão cumprimento de execução de políticas públicas ou obrigação legal ou regulatória, na medida em que o poder público pauta suas atividades no princípio da legalidade. Inclusive, por estarem associadas à existência de obrigações legais, essas bases legais possuem grande similaridade. De todo modo, a base legal de cumprimento de obrigação legal ou regulatória se aplica quando a legislação exigir a realização de certa atividade de tratamento de dados - ou seja, há uma obrigação clara, precisa e previsível de tratamento de dados, não podendo ser uma dentre as possíveis formas de executar essa obrigação -, e a base legal de execução de políticas públicas poderá estar prevista em obrigação legal ou regulatória ampla, desde que seja necessária para o alcance do interesse público e esteja dentro das atribuições legais do órgão ou entidade pública.

Por sua vez, as bases legais do consentimento e do legítimo interesse, ainda que genericamente aplicáveis, não são as mais adequadas para o tratamento de dados pelo poder público. De todo modo, elas poderão embasar o reuso de dados pessoais pelo seu receptor. Em relação ao consentimento, a disparidade de poder entre Estado e cidadão, e a necessidade do tratamento de dados pessoais para que o poder público possa exercer suas atribuições legais, remove a capacidade do titular de dados de exercer uma escolha genuína e desimpedida de pressões externas. Quanto ao legítimo interesse, embora sua utilização pelo poder público não seja impedida pela legislação, dificilmente será a base legal mais apropriada, em vista da existência de outras bases legais mais pertinentes, inclusive com alguma flexibilidade de aplicação (i.e., execução de políticas públicas).

Em seguida, o órgão ou entidade público deverá assegurar meios para que titulares de dados possam exercer seus direitos. Certos direitos são assegurados desde a edição da Constituição Federal de 1988, e são regulados por normas como a Lei de *Habeas Data*, a LAI e a LGPD, a exemplo dos direitos de confirmação do tratamento, acesso aos dados, e a correção de dados incompletos, inexatos ou desatualizados. Outros meios para que cidadãos

possam exercer controle sobre como seus dados são tratados foram previstos na LGPD, como os exemplos dos direitos de anonimização, portabilidade e oposição ao tratamento de dados. Todavia, sua garantia pelo poder público possui limitações, a exemplo da oposição a certas atividades de tratamento ou a anonimização de dados, pois muitas vezes haverá justificativa legal para a manutenção dos dados e do tratamento. Por esse motivo, medidas de *accountability* e transparência assumem ainda mais importância.

Finalmente, para que o poder público possa divulgar dados pessoais em observância à privacidade e proteção de dados pessoais, deverá adotar salvaguardas capazes de mitigar os riscos decorrentes desse tratamento. Em verdade, a existência e a eficácia das salvaguardas devem ser consideradas desde o momento de avaliação do interesse público, de forma a permitir um balanceamento mais apurado dos riscos e benefícios da divulgação pretendida. Determinadas salvaguardas estão previstas em legislação, mas podem ser também soluções técnicas ou jurídicas estabelecidas pelo controlador dos dados, como abordado.

Em relação a salvaguardas estabelecidas em lei está a regulação sobre o reuso de dados pessoais. A leitura integrativa da legislação vigente (e.g., LGPD, CDC e Constituição Federal) estabelece que a divulgação de dados pelo poder público deve observar a finalidade, a boa-fé e o interesse público que justificaram sua divulgação. Esses parâmetros se aplicam tanto à publicação quanto ao compartilhamento de dados pessoais. Isso significa que o reuso de dados compartilhados ou publicados pelo poder público deverá ocorrer em observância à legislação, segundo expectativas legítimas dos titulares de dados, e para propósitos legítimos, específicos, informados aos titulares de dados e compatíveis com a finalidade que justificou sua divulgação pelo poder público. A avaliação da compatibilidade poderá contar com alguma flexibilidade, desde que beneficie o interesse público e não imponha riscos demasiadamente elevados a direitos e liberdades de titulares de dados.

Outras possíveis salvaguardas para a publicação e o compartilhamento de dados pessoais pelo poder público são: (i) a anonimização e na pseudonimização de dados; (ii) a adoção de restrições técnicas à coleta e reuso de dados publicados ou compartilhados, como os exemplos da utilização de ferramentas que impeçam práticas maliciosas de *web scraping* ou *download* de arquivos, (ii) em situações de riscos mais elevados na publicação de dados, compartilhar com entidades específicas para finalidades previamente autorizadas, (iii) a adoção de cláusulas em contratos ou constantes de Termos de Serviço e Políticas de Privacidade; e (iv) a instituição de Conselhos e Códigos de Ética destinadas a guiar e avaliar se estão sendo realizadas segundo parâmetros éticos e em benefício do interesse público.

Outra salvaguarda prevista na legislação consiste na anonimização e na pseudonimização de dados. Em relação às práticas de anonimização, elas não garantem totalmente que os dados não poderão ser posteriormente identificados e impõem ao agente público o dilema entre: (a) divulgar dados granulares e aumentar a exposição da privacidade de indivíduos; e (b) divulgar dados com menor a granularidade, mas com menor utilidade. Já a adoção de cláusulas contratuais ou em políticas contribuem para fins de *accountability* e confiança cidadã sobre o uso de seus dados pessoais, mas devem ser elaboradas de forma a efetivamente assegurar a observância à legislação de proteção de dados pessoais.

REFERÊNCIAS

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. **Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais.** São Paulo: InternetLab, 2017.

ADAMI, Mateus Piva *et. al*. Tratamento de dados pessoais pela administração pública: análise do Serpro. *In*: BRANCHER, P. M. R.; BEPPU, A. C. (coord.). **Proteção de Dados Pessoais do Brasil: Uma Nova Visão a partir da Lei Nº 13.709/2018**. Editora Fórum, 2019.

ADAMI, Mateus Piva; LANGENEGGER, Natalia. Proteção de Impacto da LGPD em parcerias privadas no contexto de governos eletrônicos e digitalização. **Revista do Advogado**, São Paulo, n. 144, 2019.

AFONSO DA SILVA, Virgílio. O proporcional e o razoável. **Revista dos Tribunais**, São Paulo, 798, p. 23-50, 2002.. Disponível em: https://constituicao.direito.usp.br/wp-content/uploads/2002-RT798-Proporcionalidade.pdf. Acesso em: 11.10.2022.

AGRE, Philip; ROTENBERG, Marc (ed). **Technology and Privacy: The New Landscape**. Cambridge: MIT Press, 1997.

AITKEN, Mhairi *et al*. Establishing a social licence for Financial Technology: Reflections on the role of the private sector in pursuing ethical data practices. **Big Data & Society**, p. 1-15, jan./jun. 2020.

ALIZADEH, Tooran. **Global Trends of Smart Cities**: A Comparative Analysis of Geography, City Size, Governance, and Urban Planning. [*S. l.*]: Elsevier, 2021.

ALTMAN, Micah *et. al*. Towards a modern approach to privacy-aware government data releases. **Berkeley Technology Law Journal**, v. 30, n. 3, p. 1967-2072, 2015.

ANTHOPOULOS, L. G. Understanding the smart city domain: A literature review. *In*: **Transforming city governments for successful smart cities**. Springer, 2015. Cham, p. 9-21.

ANTHOPOULOS, Leonidas G.; REDDICK, Christopher G. Understanding electronic government research and smart city: A framework and empirical evidence. **Information Polity**, v. 21, n. 1, p. 99-117, 2016.

ANTHOPOULOS, Leonidas G.; REDDICK, Christopher G. Understanding electronic government research and smart city: A framework and empirical evidence. **Information Polity**, v. 21, n. 1, p. 99-117, 2016.

ANTHOPOULOS, Leonidas. G. Understanding the smart city domain: A literature review. In: **Transforming city governments for successful smart cities**. Springer, Cham, p. 9-21, 2015.

ARAÚJO, Ana Carolina *et al*. Do Transparency and Open Data Walk Together? An Analysis of Initiatives in Five Brazilian Capitals. **Medijske studije**, v. 7, n. 14, p. 65-82, 2016.

ARTIGO 19. **Balanço de 1 ano da Lei de Acesso à Informação Pública.** O direito à informação no Brasil. Resultados e recomendações do primeiro monitoramento de acesso à

informação da ARTIGO 19 a partir de experiências de organizações da sociedade civil. . Disponível em: https://artigo19.org/wp-content/uploads/2013/05/Relatorio-Monitoramento-LAI.20131.pdf. Acesso em: 30.11.2022.

ARTIGO 19. **Caminhos da transparência: a Lei de Acesso à Informação e os Tribunais de Justiça**. São Paulo: Artigo 19, 2016.

ASSAR, S.; BOUGHZALA, I.; ISCKIA, T. eGovernment Trends in the Web 2.0 Era and the Open Innovation Perspective: An Exploratory Field Study. In: JANSSEN, M.; SCHOLL, H. J.; WIMMER, M. A. et al. (org.). Electronic Government, Berlin, p. 210–222, Springer 2011.

BANDEIRA DE MELLO, C. A. Curso de Direito Administrativo. 32. ed. São Paulo: Malheiros, 2015.

BANDEIRA DE MELLO, Celso Antônio. Curso de Direito Administrativo. 32ª ed.. São Paulo: Malheiros, 2015.

BANDEIRA DE MELLO. Discricionariedade e controle jurisdicional. 8. ed. São Paulo: Malheiros, 2007. cap. 2.

BARBER, Grayson. Personal information in government records: protecting the public interest in privacy. **Louis U. Pub. L. Rev.**, v. 25, 2006.

BARGH, Mortaza S. et. al. On design and deployment of two privacy-preserving procedures for judicial-data dissemination. **Government Information Quarterly**, v. 33, n. 3, p. 481-493, 2016.

BARROS, Gabriel da Silva; SILVA, Lorena Santos; SCHMIDT, Clarissa. **Documentos públicos e dados pessoais**: o acesso sob a ótica da Lei Geral de Proteção de Dados Pessoais e da Lei de Acesso à Informação. Revista do Arquivo, São Paulo, n. 9, p. 22-39, out. 2019. Disponível em: http://www.arquivoestado.sp.gov.br/revista_do_arquivo/09/artigo_01.php.

BARUH, Lemi; POPESCU, Mihaela. Big data analytics and the limits of privacy self-management. **New Media & Society**, v. 2, p. 1–18, 2015.

BATTY, Michael et. al. Smart cities of the future. **The European Physical Journal Special Topics**, n. 214, p. 481–518, 2012.

BAWDEN, David et. al. Perspectives on information overload. **Aslib proceedings**, v. 51, n. 8, p. 249-255, 1999.

BAWDEN, David; ROBINSON, Lyn. The dark side of information: overload, anxiety and other paradoxes and pathologies. **Journal of information science**, v. 35, n. 2, p. 180-191, 2009.

BELENGUER, Lorenzo. **Citizens' Assembly: a Complementary Tool to Develop Legislative Guidelines and Raise Public Awareness on Data Privacy and Artificial Intelligence**. 2021. Disponível em: https://medium.com/escapadasuk/citizens-assemblies-for-a-more-democratically-engaged-and-informed-society-on-ai-data-privacy-4d22e1c5b585. Acesso em: 29.11.2022.

BEPKO, Arminda Bradford. Public availability or practical obscurity: the debate over public access to court records on the Internet. **NYL Sch. L. Rev**., v. 49, p. 967,2004.

BHATTACHARJEE, Kaustav; CHEN, Min; DASGUPTA, Aritra. Privacy-Preserving Data Visualization: Reflections on the State of the Art and Research Opportunities. **Computer Graphics Forum**, v. 39, n. 3, p. 675-692, jul. 2020.

BIONI, Bruno Ricardo. **Accountability na regulação de dados pessoais**: virtudes e vicissitudes. 2021. 353 p. Tese (Doutorado em Direito Comercial) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. *In*: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (coord.). **Lei geral de proteção de dados (Lei nº 13.709/2018)**: a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020.

BIONI, Bruno Ricardo. Expansão do Wi-Fi público às "custas" de dados pessoais. **Jota**. 2017. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/expansao-do-wi-fi-publico-as-custas-de-dados-pessoais-17072017. Acesso em: 28.11.2022

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BLACK, Gillian; STEVENS, Leslie. Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest. **SCRIPTed**, v. 10, n. 1, p. 93–122, 2013.

BLAKLEY, Alan. The Sedona Guidelines: Best Practices Addressing Protective Orders, Confidentiality and Public Access in Civil Cases. **The Sedona Conference Journal**, v. 8, p. 141-188, 2007.

BOERSMA, Martijn. **Paradox of the social license to operate**. 2020. Disponível em: https://www.uts.edu.au/about/uts-business-school/management-department/news/paradox-social-license-operate. Acesso em: 29.11.2022.

BORGESIUS, Frederik Zuiderveen; GRAY, Jonathan; VAN EECHOUD, Mireille. Open data, privacy, and fair information principles: Towards a balancing framework. **Berkeley Technology Law Journal**, v. 30, n. 3, p. 2073-2131, 2015.

BOYD, Danah. **Privacy and publicity in the context of big data**. 2010. Disponível em: https://www.danah.org/papers/talks/2010/WWW2010.html. Acesso em: 30.11.2022.

BRANDEIS, Louis; WARREN, Samuel. Right to Privacy. **Harvard Law Review**, v. 4, n. 5, dez. 1890.

BRASIL. Câmara dos Deputados. **Projeto de Lei n. 219, de 2003**. Regulamenta o inciso XXXIII do art. 5º, da Constituição Federal, dispondo sobre prestação de informações detidas pelos

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4060, de 2012**. Brasília, DF: [*S. n.*], 2018. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em:

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename. Acesso em: 13 set. 2022.

BROWN, Mary M.; BRUDNEY, Jeffrey L. Achieving advanced electronic government services: An examination of obstacles and implications from an international perspective. *In*: NATIONAL PUBLIC MANAGEMENT RESEARCH CONFERENCE, [2001?] Bloomington. Anais […]. Bloomington: [*S. n.*], [20001?]. p. 143-49, out. 2001.

BURLE, Caroline *et. al*. Os degraus da implementação efetiva no Brasil: como as regulamentações locais de acesso à informação impactam na implementação de portais de dados abertos e transparência. *In*: OPEN DATA RESEARCH SYMPOSIUM, 2015, Ottawa. **Anais** […]. Ottawa: [*S. n.*], 2015.

BYGRAVE, Lee A. **Data privacy law**: an international perspective. Oxford: Oxford University Press, 2014.

CÂMARA DOS DEPUTADOS. **Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei nº 4060, de 2012.** 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename. Acesso em: 13 set. 2022.

CÂMARA DOS DEPUTADOS. **Comissão Especial Informações detidas pela Administração Pública, Projeto de Lei nº 219, de 2003.** 2010. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=736307&filename=PRL+2+PL021903+%3D%3E+PL+219/2003. Acesso em: 26.11.2022.

CARTER, Megan; BOURIS, Andrew. **Freedom of information**: balancing the public interest. 2. ed. London: The Constitution Unit School of Public Policy, 2006.

CARVALHO FILHO, José dos Santos. **Manual de direito administrativo**. 28. ed. São Paulo: Atlas, 2015.

CATE, Fred H. *et al*. The right to privacy and the public's right to know: The central purpose of the Freedom of Information Act. **Admin. L. Rev.**, v. 46, p. 41, 1994.

CATE, Fred H. Government data mining: The need for a legal framework. **Articles by Maurer Faculty**, v. 43, p. 435-489. 2008.

CATE, Fred H. The failure of fair information practice principles. *In*: WINN, Jane K. **Consumer protection in the age of the information economy**, 2006.

CAVALLO, Sara *et al*. The digital divide in citizen-initiated government contacts: A GIS approach. **Journal of Urban Technology**, v. 21, n. 4, p. 77-93, 2014.

CERRILLO-I-MARTÍNEZ, Agustí. The reuse of public sector information in Europe and its impact on transparency. **European Law Journal**, v. 18, n. 6, p. 770-792, 2012

CHAMBERS, Simone. Behind closed doors: publicity, secrecy, and the quality of deliberation. **The Journal of Political Philosophy**, v. 12, n. 4, p. 389-410, 2004.

CHAMBERS, Simone. Behind closed doors: publicity, secrecy, and the quality of deliberation. **The Journal of Political Philosophy**, v. 12, n. 4, p. 389-410, 2004.

CHEN, Daniel L. *et al*. **Early predictability of asylum court decisions.** Proceedings of the ACM Conference on AI and the Law, 2017.

CHESBROUGH, Henry William. **Open Innovation**: The New Imperative for Creating and Profiting from Technology. Boston: Harvard Business Press, 2003.

CHOENNI, Sunil *et al*. Preserving privacy whilst integrating data: Applied to criminal justice. **Information Polity**, v. 15, n. 1, 2, p. 125-138, 2010.

CHOO, Mabel; FINDLAY, Mark. Data Reuse and its Impacts on Digital Labour Platforms. **SMU Centre for AI & Data Governance Research Paper,** n. 13. 2021.

CITRON, Danielle Keats; SOLOVE, Daniel J. Privacy Harms. **GWU Legal Studies Research Paper No. 2021-11**, GWU Law School Public Law Research Paper No. 2021-11, 102 Boston University Law Review 793. 2022.

CLARKE, Amanda. **Opening the Government of Canada**: The Federal Bureaucracy in the Digital Age. Chicago: UBC Press, 2019.

COHEN, Julie E. What Privacy is For. **Harvard Law Review**, v. 126, p. 1931, 2013.

CONRADIE, Peter; CHOENNI, Sunil. Exploring process barriers to release public sector information in local government. *In*: ICEGOV. **Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance**. ACM, p. 5-13, 2012.

CONROY, Amy; SCASSA, Teresa. Promoting Transparency While Protecting Privacy in Open Government in Canada. **Alberta Law Review**, v. 53, n.1, p. 175-204, 2015.

CRAVO, Daniela Copetti; KESSLER, Daniela Seadi; DRESCH, Rafael de Freitas Valle. **Direito à Portabilidade na Lei Geral de Proteção de Dados**. São Paulo: Editora Foco, 2020.

CRAWFORD, Kate; SCHULTZ, Jason. Big data and due process: Toward a framework to redress predictive privacy harms. **BCL Rev.**, v. 55, 2014.

CUEVA, Ricardo Vilas Boas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo**, São Paulo, n. 13, p. 59-67, 2017.

CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord). **Compliance e política de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021.

DAHMM, Hayden. **Laying the foundation for effective partnerships**: an examination of data sharing agreements. 2020. Disponível em: https://static1.squarespace.com/static/5b4f63e14eddec374f416232/t/5ee3e249b07a7d49fa6da34e/1591992905052/Laying+the+Foundation+for+Effective+Partnerships-+An+Examination+of+Data+Sharing+Agreements.pdf. Acesso em: 11 nov. 2022.

DAVIES, Tim. **Open data, democracy and public sector reform**: A look at open government data use from data. gov. uk. Practical Participation, 2010.

DAVIES, Tim. **Open data, democracy and public sector reform**: A look at open government data use from data. gov. uk. Practical Participation, 2010.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo**. 28. ed. São Paulo: Atlas, 2015.

DIFRANZO, Dominic *et al*. The Web is My Back-end: Creating Mashups with Linked Open Government Data. *In*: WOOD, D. (e) **Linking Government Data.** New York: Springer, 2011.

DING, Li; LEBO, Timothy; ERICKSON, John S. *et al*. TWC LOGD: A portal for linked open government data ecosystems. **Journal of Web Semantics**, v. 9, n. 3, p. 325–333, 2011.

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

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2019.

DONEDA, Danilo. Iguais mas Separados: o Habeas Data no Ordenamento Brasileiro e a proteção de dados pessoais. **Cadernos da Escola de Direito**, v. 2, n. 9, 2008.

DONEDA, Danilo. O registro único de identidade civil entre a cidadania e o controle. *In*: FIRMINO, Rodrigo, BRUNO, Fernanda, KANASHIRO, Marta. **Surveillance in latin america**: vigilância, segurança e controle social. Curitiba: Editora Universitária Champagnat, 2009. p. 246-255.

DONEDA, Danilo. **Privacidade e transparência no acesso à informação** pública. Zaragoza: Prenssas Universitárias de Zaragoza, 2010.

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

DONEDA, Danilo; ZANATTA, Rafael A. F. Personality rights in Brazilian data protection law: a historical perspective. *In*: ALBERS (ed.). **Personality and Data Protection Rights on the Internet**: Brazilian and German Approaches. Suíça: Springer Nature Switzerland, 2022. No prelo.

DOS SANTOS CARVALHO FILHO, José. **Manual de direito administrativo**. 28. ed. São Paulo: Atlas, 2015.

DROR, Yebezkel. Transparency and openness of quality democracy. *In*: KELLY, Michael. **Openness and transparency in governance**: Challenges and opportunities. p. 25-43, 1999.

DUMPAWAR, Suruchi. **Open government data intermediaries**: Mediating data to drive changes in the built environment. 2015. Tese (Doutorado) - Massachusetts Institute of Technology, Massachusetts, 2015.

DUNLEAVY, Patrick *et al*. **Policy learning and public sector information technology: Contractual and e-government changes in the UK, Australia, and New Zealand**. American Political Science Association's Annual Conference, American Political Science Association, 2001.

DUNLEAVY, Patrick *et al*. The Advent of a Digital State and Government-Business Relations. **Paper to the Annual Conference of the UK Political Science Association**, 2000.

Disponível em: https://ora.ox.ac.uk/objects/uuid:8d34e103-1f98-4183-9c11-9cce866405fd/download_file?file_format=pdf&safe_filename=PSA_2000.pdf&type_of_work=Report. Acesso em: 30.11.2022.

DUNLEAVY, Patrick *et. al*. **Policy learning and public sector information technology**: Contractual and e-government changes in the UK, Australia, and New Zealand. American Political Science Association's Annual Conference, American Political Science Association, 2001.

DUNLEAVY, Patrick *et. al*. The Advent of a Digital State and Government-Business Relations. **Paper to the Annual Conference of the UK Political Science Association**, 2000. Disponível em: https://ora.ox.ac.uk/objects/uuid:8d34e103-1f98-4183-9c11-9cce866405fd/download_file?file_format=pdf&safe_filename=PSA_2000.pdf&type_of_work=Report. Acesso em: 30.11.2022.

DUNLEAVY, Patrick; MARGETTS, Helen Z. The advent of digital government: Public bureaucracy and the state in the Internet age. **Paper to the Annual Conference of the American Political Science Association**, Omni Shoreham Hotel, Washington, 2000.

DUNLEAVY, Patrick; MARGETTS, Helen Z. The second wave of digital era governance. *In*: **APSA 2010 Annual Meeting Paper**. 2010.

ESTEFAM, Felipe Faiwichow. A discricionariedade administrativa à luz da reconfiguração do princípio da legalidade. **Revista de Interesse Público.** Belo Horizonte, ano 15, n. 79, mai/jun. 2013.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.** 2017. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF. Acesso em: 16.09.2022.

EUROPEAN COMMISSION. **Public sector information: a key resource for Europe - Green Paper on public sector information in the information society**. 1999. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/599834ce-7a43-44fe-8cd8-334b3c19feba. Acesso em: 12.11.2022.

FEDOROWICZ, Jane *et al*. Barriers to interorganizational information sharing in e-government: A stakeholder analysis. **The Information Society**, v. 26, n. 5, p. 315-329, 2010.

FEINTUCK, Mike. **The Public Interest in Regulation**. Oxford: Oxford University Press, 2004

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites da função fiscalizadora do estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 88, p. 430-459, jan./dez. 1993.

FILGUEIRAS, Fernando. Além da transparência: accountability e política da publicidade. **Lua Nova**, n. 84, 2011.

FLORINI, Ann. Behind closed doors: Governmental transparency gives way to secrecy. **Research Collection School of Social Sciences**, v. 26, n. 1, p. 18-21, 2004.

FLORINI, Ann. Does the invisible hand need a transparent glove? **Research Collection School of Social Sciences**, 2000.

FORST, Martin; WECKLER, David. Research Access into Automated Criminal Justice Information Systems and the Right to Privacy. **U. San Fernando Valley L. Rev.**, v. 5, p. 321, 1976.

FRAGOSO, Nathalie et. al. **Proteção de dados pessoais em políticas de proteção social**: contribuições a partir do estudo sobre o Programa Bolsa Família. 2021. Disponível em: https://internetlab.org.br/wp-content/uploads/2021/10/Protecao-de-Dados-Pessoais-em-Politicas-de-Protecao-Social.pdf. Acesso em: 10.11.2022.

FRANCO, Ivan de *et. al*. Transparência pode aproximar o cidadão do Judiciário. **Jota**, São Paulo, 2015. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/transparencia-pode-aproximar-o-cidadao-do-judiciario-20052015. Acesso em: 30 nov. 2022.

FRANCO, Ivan de; LANGENEGGER, Natalia. Transparency and open data in the Brazilian Judiciary: a case study on the São Paulos Court of Justice. **2016 OPEN DATA RESEARCH SYMPOSIUM**, Madri, Espanha, out. 2016.

FRANCO, Ivan de; MARCHEZAN, Jonas Coelho; LANGENEGGER, Natalia. **Acesso à informação no Tribunal de Justiça de São Paulo**. 2015. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2015/11/AcessoAInf_TJSP.pdf. Acesso em: 30 nov. 2022.

FROST, Amanda. Restoring faith in government: Transparency reform in the United States and the European Union. *In*: BIRKINSHAW, Patrick (ed.). **European public law**, v. 9, n. 1, p. 87-104, 2003.

FUNG, Archon; GRAHAM, Mary; WEIL, David. **Full disclosure**: The perils and promise of transparency. Cambridge: Cambridge University Press, 2007.

GABARDO, Emerson. Princípio da eficiência. *In*: ENCICLOPÉDIA Jurídica da PUCSP, Tomo Direito Administrativo e Constitucional. 2. ed. 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/82/edicao-2/principio-da-eficiencia. Acesso em: 30 nov. 2022.

GALLIGAN, Denis. J. Legal Theory and Empirical Research. In: CANE, Peter; KRITZER, Herbert M. (ed.), **The Oxford Handbook of Empirical Legal Research**. Oxford: Oxford University Press, 2010.

GARCIA CABRAL, Flávio. O princípio da boa administração pública e a LGPD. *In*: NEVES DAL POZZO, Augusto; MARCONDES MARTINS, Ricardo. **LGPD & Administração Pública**. São Paulo: Revista dos Tribunais, 2020.

GARG, Nikhil et. al. Word embeddings quantify 100 years of gender and ethnic stereotypes. **Proceedings of the National Academy of Sciences**, v. 115, n. 16, p. E3635-E3644, 2018.

GASSER, Urs. Regulating search engines: Taking stock and looking ahead. **Yale JL & Tech**., v. 8, p. 201, 2005.

GEIGER, Christian Philipp; VON LUCKE, Jörn. Open government and (linked)(open)(government)(data). **JeDEM-eJournal of eDemocracy and open Government**, v. 4, n. 2, p. 265-278, 2012.

GELLMAN, Robert. Willis Ware's Lasting Contribution to Privacy: Fair Information Practices. **IEEE Security & Privacy**, v. 12, n. 4, p. 51-54, jul-aug, 2014.

GERRING, John. What is a case study and what is it good for? **American political science review**, v. 98, n. 2, p. 341-354, 2004.

GERRING, John. What is a case study and what is it good for? **American political science review**, v. 98, n. 2, p. 341-354, 2004.

GIBSON, James L. Institutional legitimacy, procedural justice, and compliance with Supreme Court decisions: A question of causality. **Law & Society Review**, v. 25, n. 3, p. 631-635, 1991.

GIBSON, James L. Institutional legitimacy, procedural justice, and compliance with Supreme Court decisions: A question of causality. **Law & Society Review**, v. 25, n. 3, p. 631-635, 1991.

GIL-GARCIA, J. Ramon *et al*. Information Sharing as a Dimension of Smartness: Understanding Benefits and Challenges in Two Megacities. **Urban Affairs Review**, v. 57, n.1, 2019.

GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights. **Research Publication**, v. 7641, 2015.

GILLESPIE, Tarleton. The relevance of algorithms. *In*: GILLESPIE, Tarleton; BOCKOWSKI, Pablo; FOOT, Kirsten (ed.). **Media technologies**: Essays on communication, materiality, and society. Cambridge, 2014.

GLASMEIER, Amy; CHRISTOPHERSON, Susan. Thinking about smart cities. **Cambridge Journal of Regions Economy and Society**, v. 8, n. 1, p. 3-12, fev. 2015.

GLOBAL FREEDOM OF EXPRESSION. Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland. 2017. Disponível em: https://globalfreedomofexpression.columbia.edu/?s=Satakunnan+Markkinap%C3%B6rssi+Oy+and+Satamedia+Oy+v.+Finland. Acesso em: 11.11.2020.

GOLLE, Philippe. Revisiting the uniqueness of simple demographics in the US population. **WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society**, 2006.

GOMES, Maria Cecília O. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. *In*: LIMA, Ana Paul; HISSA, Carmina; SALDANHA, Paloma Mendes (org.). **Direito digital**: debates contemporâneos. São Paulo: Revista dos Tribunais, 2019. p. 141-153.

GOMEZ-VELEZ, Natalie. Internet Access to Court Records-Balancing Public Access and Privacy. **Loy. L. Rev**., v. 51, p. 365, 2005.

GRAEF, Inge; GELLERT, Raphael; HUSOVEC, Martin. Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation (September 27, 2018). **TILEC Discussion Paper**, n. 29, 2018. Disponível em: https://ssrn.com/abstract=3256189 or http://dx.doi.org/10.2139/ssrn.3256189. Acesso em: 11 nov. 2020.

GRANKA, Laura A. The politics of search: A decade retrospective. **The Information Society**, v. 26, n. 5, p. 364-374, 2010.

GREEN, Ben et. al. Mining Administrative Data to Spur Urban Revitalization. In: ACM. **Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining**, p. 1829-1838, 2015.

GREEN, Ben *et. al*. Open Data Privacy. **Berkman Klein Center for Internet & Society Research Publication**, 2017.

GRIMMELIKHUIJSEN, Stephan G. et. al. The effect of transparency on trust in government: A cross-national comparative experiment. **Public Administration Review**, v. 73, n. 4, p. 575-586, 2013.

GRIMMELIKHUIJSEN, Stephan G.; MEIJER, Albert J. Effects of transparency on the perceived trustworthiness of a government organization: Evidence from an online experiment. **Journal of Public Administration Research and Theory**, v. 24, n. 1, p. 137-157, 2012.

GUIMARÃES, Caroline Burle dos Santos. Parceria para Governo Aberto e Relações Internacionais: oportunidades e desafios. 2014. Dissertação (Mestrado) - UNESP/UNICAMP/PUC-SP, Programa San Tiago Dantas, 2014.

HACHEM, Daniel Wunder. A dupla noção jurídica de interesse público em Direito Administrativo. A&C - **Revista de Direito Administrativo & Constitucional**, v. 11, n. 44, p. 59, 16 abr. 2011.

HAND, David J. Data mining: new challenges for statisticians. **Social Science Computer Review**, v. 18, n. 4, p. 442-449, 2000.

HARRISON, Teresa M.; SAYOGO, Djoko Sigit. Transparency, participation, and

HARRISON, Teresa M.; SAYOGO, Djoko Sigit. Transparency, participation, and accountability practices in open government: A comparative study. **Government information quarterly**, v. 31, n. 4, p. 513-525, 2014.

HEALD, David. **Transparency as an instrumental value**. Oxford: Oxford University Press for The British Academy, 2006.

HEALD, David. **Varieties of transparency**. Oxford: Oxford University Press for The British Academy, 2006.

HILLER, Janine S.; BÉLANGER, France. Privacy strategies for electronic government. **E-government**, v. 200, p. 162-198, 2001.

HIRSCHEY, Jeffrey Kenneth. Symbiotic relationships: Pragmatic acceptance of data scraping. **Berkeley Tech. LJ**, v. 29, 2014.

HUSCROFT, Grant; MILLER, Bradley W.; WEBBER, Grégoire, *et al*. Proportionality and the Rule of Law – Rights, Justification, Reasoning. **Cambridge University Press**, New York, 2014.

IEEE. The Authoritative Dictionary of IEEE Standards Terms. 7th e. **IEEE Std 100-2000**, p. 1–1362, 2000.

IGO, Sarah E. **The Known Citizen**: A History of Privacy in Modern America. Cambridge: Harvard University Press, 2018.

INSTITUTO IGARAPÉ. **Reconhecimento Facial no Brasil. 2019**. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 28 nov. 2022.

INTERNETLAB. **O que está em jogo no debate sobre dados pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais**. 2016. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf. Acesso em: 11 nov. 2022.

INTRONA, Lucas D.; NISSENBAUM, Helen. Shaping the Web: Why the politics of search engines matters. **The information society**, v. 16, n. 3, p. 169-185, 2000.

IPEA; TJSP; Secretaria de Reforma do Judiciário. **Desburocratização dos cartórios judiciais:** Análise dos juizados especiais do Tribunal de Justiça de São Paulo. Relatório de pesquisa. Brasília, 2015.

ITS RIO. **Carta aberta por um governo digital que fomente (e não obste) o uso de Dados Públicos Abertos.** 2021. Disponível em: https://itsrio.org/pt/comunicados/carta-aberta-dados-publicos-abertos/. Acesso em: 22.08.2022.

JAATINEN, Tanja. The relationship between open data initiatives, privacy, and government transparency: a love triangle? **International Data Privacy Law**, v. 6, n. 1, 2016.

JACOBS, James B.; LARRAURI, Elena. Are criminal convictions a public matter? The USA and Spain. **Punishment & Society**, v. 14, n. 1, p. 3-28, 2012.

JAEGER, Paul T. The endless wire: E-government as global phenomenon. **Government Information Quarterly**, v. 20, n. 4, p. 323-331, 2003.

JANSSEN, Marijn *et al*. Benefits, adoption barriers and myths of open data and open government. **Information systems management**, v. 29, n. 4, 2012.

JANSSEN, Marijn *et al*. Big and open linked data (BOLD) to create smart cities and citizens: Insights from smart energy and mobility cases. In: Electronic Government. EGOV 2015. **Lecture Notes in Computer Science**, Cham, v. 9248, 2015

JANSSEN, Marijn; VAN DEN HOVEN, Jeroen. Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy?. **Government Information Quarterly**, v. 32, n. 4, p. 363-368, out. 2015.

JANSSEN, Marijn; VAN DEN HOVEN, Jeroen. Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy?. **Government Information Quarterly**, v. 32, n. 4, p. 363-368, out. 2015.

JELENIC, Michael. From Theory to Practice: Open Government Data, Accountability, and Service Delivery in Sub-Saharan Africa. **Policy Research Working Paper**, jun. 2019.

JOHNSON, Peter A.; SIEBER, Renee E. Situating the adoption of VGI by government. *In*: SUI, Daniel; ELWOOD, Sarah; GOODCHILD, Michael (ed.). **Crowdsourcing geographic knowledge**. Dordrecht: Springer, 2013. p. 65-81.

KASSEN, Maxat. Open Data Politics: Building a Research Framework. *In*: KASSEN, Maxat. **Open Data Politics**. SpringerBriefs in Political Science. Springer, Cham, p. 1-18, 2019.

KENYON, Andrew T.; RICHARDSON, Megan (Ed.). **New Dimensions in Privacy Law: International and Comparative Perspectives**. Cambridge: Cambridge University Press, 2006.

KHATOUN, Rida; ZEADALLY, Sherali. Smart Cities: Concepts, Architectures, Research Opportunities. **Communications of the ACM**, v. 59, n. 8, p. 46-57, ago. 2016.

KHATOUN, Rida; ZEADALLY, Sherali. Smart Cities: Concepts, Architectures, Research Opportunities. **Communications of the ACM**, v. 59, n. 8, p. 46-57, ago. 2016.

KIM, Gang-Hoon; TRIMI, Silvana; CHUNG, Ji-Hyong. Big-data applications in the government sector. **Communications of the ACM**, v. 57, n. 3, p. 78-85, 2014.

KITCHIN, Rob. Big Data, new epistemologies and paradigm shifts. **Big Data & Society**, v. 1, n. 1, 2014.

KORFF, Douwe; GEORGES, Marie. **The DPO Handbook:** Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation. 2019. Disponível em: https://www.ipvz.cz/seznam-souboru/5028-2019-korff-the-dpo-handbook.pdf. Acesso em: 12.12.2022.

KOSTA, Eleni. **Consent in European data protection law.** [*S. l.*]: Martinus Nijhoff Publishers, 2013.

KRAEMER, Kenneth L.; KING, John Leslie. Information technology and administrative reform: Will the time after e-government be different? Paper prepared for the Heinrich Reinermann Schrift fest, Post Graduate School of Administration, Speyer, Alemanha, set. 2003.

LAGOS, Yianni. Taking the personal out of data: Making sense of de-identification. **Ind. L. Rev.**, v. 48, n. 187, p. 187-203, 2014.

LANEY, Doug. **3D data management**: Controlling data volume, velocity, and variety. Technical report, META Group, 2001.

LANIUS, Danielle; GICO JUNIOR, Ivo; STRAIOTTO, Raquel Maia. O princípio da eficiência na jurisprudência do STF. **Rev**. **Direito Adm**., Rio de Janeiro, v. 277, n. 2, p. 107-148, maio/ago. 2018.

LAYNE, Karen; LEE, Jungwoo. Developing fully functional E-government: A four stage model. **Government information quarterly**, v. 18, n. 2, p. 122-136, 2001.

LEMOS, Ronaldo *et al*. A criação da Autoridade Nacional de Proteção de Dados pela MP nº 869/2018. **Jota**. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-criacao-da-autoridade-nacional-de-protecao-de-dados-pela-mp-no-869-2018-29122018. Aceso em 21 jul. 2021.

LEMOS, Ronaldo *et al*. GovTech e computação em nuvem: o Brasil precisa de uma agenda digital. **Jota**, São Paulo, 12 abr., 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/govtech-e-computacao-em-nuvem-o-brasil-precisa-de-uma-agenda-digital-12042019. Acesso em: 21 jul. 2019.

LEONARDI, Marcel. Responsabilidade civil pela violação do sigilo e privacidade na internet. *In*: SILVA, Regina Beatriz Tavares da; SANTOS, Manoel J. Pereira dos (coord.). **Responsabilidade civil na internet e nos demais meios de comunicação**. Rio de Janeiro: Saraiva, 2012

LEONARDI, Marcel. **Tutela da privacidade na internet**. 2009. Tese (Doutorado) - Universidade de São Paulo, São Paulo, 2009.

LESSIG, Lawrence. The Architecture of Privacy. Artigo apresentado na Conferência Taiwan Net '98, Taipei, mar. 1998. Disponível em: http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf. Acesso em: 21.07.2019.

LIMA, Stephane. **Educação, Dados e Plataformas – análise descritiva dos termos de uso dos serviços educacionais Google e Microsoft**. São Paulo: Iniciativa Educação Aberta, 2020. Disponível em: https://www.aberta.org.br. Acesso em: 22 ago. 2022.

LIMBERGER, Têmis; RITTER, Renée Cristina Herlin. A Lei de Acesso à Informação Pública e a decisão do STF na Repercussão Geral nº 483: o desencontro entre interesse público e vida privada dos servidores públicos. **Int. Públ**., Belo Horizonte, v. 19, n. 103, p. 79-98, maio/jun. 2017.

LUBARSKY, Boris. Re-identification of "anonymized" data. **Georgetown Law Technology Review**, 2010. Disponível em: https://www. georgetownlawtechreview. org/re-identification-of-anonymized-data/GLTR-04-2017. Acesso em: 10.09.2021.

MAIER-RABLER, Ursula; HUBER, Stefan. "Open": the changing relation between citizens, public administration, and political authority. **Jedem - Ejournal Of Edemocracy And Open Government**, v. 3, n.2, 182-191, 2012.

MARDER, Nancy S. From Practical Obscurity to Web Disclosure: A New Understanding of Public Information. **Syracuse Law Review**, v. 59, 2008.

MARGETTS, Helen; DUNLEAVY, Patrick. **Better Public Services through e-government**: Academic Article in support of Better Public Services through e-government. Report by the

Comptroller and Auditor General, HC 704-III, Session 2001-2002, National Audit Office. 2002.

MAROUBO, Felipe Pereira. Transparência, acesso à informação e Administração Pública: Êxitos e obstáculos do Poder Executivo Federal nos 30 anos da Constituição de 1988. *In*: HACHEM, Daniel Wunder; LEAL, Fernando Angelo Ribeiro; MENDONÇA, José Vicente Santos de. **Transformações do direito administrativo**: o estado administrativo 30 anos depois da Constituição de 1988. Rio de Janeiro Rio: ed. FGV, 2018. p. 233-270.

MARQUES NETO, Floriano de Azevedo. **Regulação Estatal e interesses públicos**. São Paulo: Malheiros, 2002. cap. 4, p. 144-170.

MARQUES, Cláudia Lima *et al*. **Comentários ao Código de Defesa do Consumidor**: arts. 1º à 74: aspectos materiais. São Paulo: Revista dos Tribunais, 2003.

MARRARA, Thiago. A boa-fé do administrado e do administrador como fator limitador da discricionariedade administrativa. **Revista de Direito Administrativo**, v. 259, p. 207-247, 2012.

MARTIN, Peter W. Online Access to Court Records-from Documents to Data, Particulars to Patterns. **Villanova Law Review.** Cornell Law Faculty Publications, v. 53, p. 854-888, 2008.

MARTIN, Roger; OSBERG, Sally. Social Entrepreneurship: The Case for Definition. **Stanford Social Innovation Review**, v. 5, p. 28-39, 2007.

MARTINS CARDOZO, José Eduardo; LOPES QUEIROZ, João Eduardo; WALQUÍRIA BATISTA DOS SANTOS, Márcia. **Curso de Direito Administrativo Econômico**. São Paulo: Malheiros, 2006. v. 1.

MARTINS, Paula Ligia. Acesso à Informação: Um direito fundamental e instrumental. **Acervo - Revista do Arquivo Nacional**, v. 24, n. 1, p. 233–244, jan./jun. 2012.

MATHEUS, Ricardo; JANSSEN, Marijn. Transparency dimensions of big and open linked data. *In*: **Open and Big Data Management and Innovation**. I3E 2015. Lecture Notes in Computer Science, v. 9373. Springer, Cham, p. 236-246, 2015.

MATHEUS, Ricardo; RIBEIRO, Manuella Maia; VAZ, José Carlos. New perspectives for electronic government in Brazil: the adoption of open government data in national and subnational governments of Brazil. In: ACM. **Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance**. ACM, p. 22-29, 2012

MATHEWS, Jud; SWEET, Alec S. All Things in Proportion? American Rights Review and the Problem of Balancing. **Emory Law Journal**, v. 60, p.797-875, 2010.

MATHEWS, Jud; SWEET, Alec S. **Proportionality balancing and constitutional governance**: A comparative and global **approach.** Oxford: Oxford University Press, 2019.

MATTIUZZO, Marcela; PONCE, Paula Pedigoni. O legítimo interesse e o teste da proporcionalidade: uma proposta interpretativa. **Revista InternetLab**, v. 1, n. 2, dez. 2020. Disponível em: https://revista.internetlab.org.br/o-legitimo-interesse-e-o-teste-da-proporcionalidade-uma-proposta-interpretativa/. Acesso. em: 25.10.2022.

MAYER-SCHONEBERGER, Viktor. Generational development of data protection in Europe. *In*: AGRE, Phillip E.; ROTENBERG Marc (org.). **Technology and privacy: the new landscape**. Cambridge: The MIT Press, 1997.

MAYER-SCHONEBERGER, Viktor; CUKIER, K. **Big data: A revolution that will transform how we live, work, and think**. [S. l.]: Houghton Mifflin Harcourt, 2013.

MCDERMOTT, Yvonne. Conceptualising the right to data protection in an era of Big Data. **Big Data & Society**, v. 4, n. 1, 2017.

MEDAUAR, Odete. **Direito administrativo moderno**. 20. ed. São Paulo: Revista dos Tribunais, 2016.

MEDAUAR, Odete. **O Direito Administrativo em Evolução**. Brasília: Gazeta Jurídica, 2017.

MEIJER, Albert. Understanding modern transparency. **International Review of Administrative Sciences**, v. 75, n. 2, p. 255-269, 2009.

MEIJER, Albert. Understanding modern transparency. **International Review of Administrative Sciences**, v. 75, n. 2, p. 255-269, 2009.

MEIJER, Ronald *et al*. Bridging the contradictions of open data. In: **13th European Conference on E-government**, p. 329-336, 2013.

MEIJER, Ronald *et al*. Reconciling contradictions of open data regarding transparency, privacy, security and trust. **Journal of theoretical and applied electronic commerce research**, v. 9, n. 3, p. 32-44, 2014.

MEIJER, Ronald et. al. Bridging the contradictions of open data. In: **13th European Conference on E-government**, p. 329-336, 2013.

MEIRELLES, Hely Lopes. **Direito Administrativo Brasileiro.** 41. ed. São Paulo: Malheiros 2015.

MEJÍA, Juan Carlos Upegui. **Transparencia estatal y datos personales: el problema de la publicidad de la información personal en poder del Estado: estudio comparado México-Colombia**. Bogotá: Universidad Externado, 2020.

MEJIAS, Ulises A.; COULDRY, Nick. Datafication. **Internet Policy Review**, v. 8, n. 4, 2019.

MENDES, Conrado Hubner. **Direitos fundamentais, separação de poderes e deliberação**. 2011. Tese (Doutorado) - Universidade de São Paulo, 2011.

MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, p. 37-69, 2018.

MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, p. 37-69, 2018.

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

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. 2008. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, 2008.

MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, Brasília, DF, 2008.

MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. **Revista de Direito Civil Contemporâneo-RDCC**, v. 9, p. 35-48, 2017.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **REI-Revista Estudos Institucionais**, v. 6, n. 2, p. 507-533, 2020.

MENDES, Laura Schertel; GASIOLA, Gustavo Gil. **Inconstitucionalidade do Decreto 10.046: limites do compartilhamento de dados.** 2022. Disponível em: https://www.conjur.com.br/2022-set-14/schertel-gasiola-compartilhamento-dados-setor-publico. Acesso em: 10.10.22022.

MILLER, Arthur R. Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society. **Michigan Law Review**, v. 67, n. 6, 1969.

MILLER, Daniel; SLATER, Don. Etnografia on e off-line: cibercafés em Trinidad. **Horizontes antropológicos**, v. 10, n. 21, p. 41-65, 2004.

MORAIS, Dalton Santos. Os custos da atividade administrativa e o princípio da eficiência. **Revista de Direito Administrativo**, v. 237, p. 165–196, 2004.

MOREIRA NETO, Diogo de Figueiredo. **Curso de direito administrativo**. 14. ed. São Paulo: Forense, 2015.

MORIBE, Gabriela Tiemi. **A proteção de dados pessoais na Secretaria Nacional do Consumidor (2019- 2021)**. Dissertação (Mestrado em Direito) - Fundação Getulio Vargas, Escola de Direito de São Paulo, São Paulo, 2022.

MOROZOV, Evgeny, BRIA, Francesca. **A cidade inteligente: tecnologias urbanas e democracia**. [S. l.]: Ubu Editora, 2020.

MORRISON, Caren Myers. Privacy, accountability, and the cooperating defendant: Towards a new role for internet access to court records. **Vanderbilt Law Review**, v. 62, p. 919-978, 2009.

MOTA ALVES, Fabrício da. Desafios da adequação do Poder Público à LGPD. In: PALHARES, Felipe (org.). **Temas Atuais de Proteção de Dados**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

MOTA ALVES, Fabrício da. Desafios da adequação do Poder Público à LGPD. In: PALHARES, Felipe (org.). **Temas Atuais de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2020.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado**, São Paulo, n. 144, 2019.

MULLER, Sam et. al. The social licence for data-intensive health research: towards co-creation, public value and trust. **BMC Med Ethics**, v. 22, n. 110, 2021

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust de-anonymization of large datasets (how to break anonymity of the Netflix prize dataset). **University of Texas at Austin**, 2008.

NEAMTU, Florentina; ZAIT, Luminita. The Coordinates And Typology Of Relationship Between The Public System And The Different Categories Of Stakeholders. **Studies and Scientific Researches. Economics Edition**, n. 18, 2013.

NISSENBAUM, Helen. Symposium, Privacy as Contextual Integrity, **79 Wash. L. Rev.** n. 119, 2004. Disponível em: https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10. Acesso em: 10.11.2022.

NOBREGA, Camila. **Os 5 anos da Lei de Acesso à Informação**: uma análise de casos de transparência. São Paulo: Artigo 19 Brasil, 2017.

O'DONNELL, Guillermo. Accountability horizontal e novas poliarquias. **Lua nova**, v. 44, n. 98, p. 27-54, 1998.

O'DONNELL, Guillermo. Accountability horizontal e novas poliarquias. **Lua nova**, v. 44, n. 98, p. 27-54, 1998.

OBERSKI, Daniel; KREUTER, Frauke. Differential Privacy and Social Science: An Urgent Puzzle. **Harvard Data Science Review**, n. 2.1, Winter 2020.

OCDE. **Goode Practice Principles for Data Ethics in the Public Sector.** 2021. Disponível em: https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.pdf. Acesso em: 23.12.2021.

OCDE. **Recommendation of the Council on Digital Government Strategies**. Public Governance and Territorial Development Directorate. 2014. Disponível em: https://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf. Acesso em: 10 nov. 2022.

OCDE. **The Path to Becoming a Data-Driven Public Sector, OECD Digital Government Studie**s. Paris: OECD Publishing, 2019.

OGDEN, Patti. Mastering the lawless science of our law: a story of legal citation indexes. **Law Libr. J.**, v. 85, p. 1-48, 1993.

O'HARA, Kieron. **Transparent government, not transparent citizens: a report on privacy and transparency for the Cabinet Office**, 2011. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61279/transparency-and-privacy-review-annex-a.pdf. Acesso em: 30.11.2022.

OHM, Paul. **Broken promises of privacy: Responding to the surprising failure of anonymization**. UCLA Law Review, v. 57, p. 1701-1777, 2010.

órgãos da Administração Pública. Brasília, DF: [*S. n.*], 2010. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=736307&filename=PRL+2+PL021903+%3D%3E+PL+219/2003. Acesso em: 26 nov. 2022.

OTJACQUES, Benoît et. al. Interoperability of e-government information systems: Issues of identification and data sharing. **Journal of Management Information Systems**, v. 23, n. 4, p. 29-51, 2007.

PALMA, Juliana. **Sanção e acordo na administração pública**. São Paulo: Malheiros, 2015.

PATERSON, Moira; MCDONAGH, Maeve. Freedom of information and the public interest: the Commonwealth experience. **Oxford University Commonwealth Law Journal**, v. 17, n. 2, p. 189-210, 2017.

PATERSON, Moira; MCDONAGH, Maeve. Freedom of information and the public interest: the Commonwealth experience. **Oxford University Commonwealth Law Journal**, v. 17, n. 2, p. 189-210, 2017.

PCAST. **Report to the president Big Data and Privacy: a technological perspective**. 2014. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf. Acesso em: 20.12.2021.

PIRES, Álvaro P. Amostragem e pesquisa qualitativa: ensaio teórico e metodológico. In: POUPART, Jean et. al. **A pesquisa Qualitativa**. Enfoques Epistemológicos e Metodológicos. Petrópolis: Editora Vozes, 2008a.

PIRES, Álvaro P. Sobre algumas questões epistemológicas de uma metodologia geral para as Ciências Sociais. In: POUPART, Jean et. al. **A pesquisa qualitativa: enfoques epistemológicos e metodológicos**. Petrópolis: Vozes, p. 43-94, 2008b.

POSSAMAI, Ana Júlia. Portal brasileiro de dados abertos: Novas práticas para o fortalecimento da democracia e da gestão pública na Era Digital. In: SILVA, Sivaldo Pereira da; BRAGATTO, Rachel Callai; SAMPAIO, Rafael Cardoso. **Democracia digital, comunicação política e redes: Teoria e prática**. Rio de Janeiro: Letra e Imagem, 2016.

POSSAMAI, Ana Júlia. Portal brasileiro de dados abertos: Novas práticas para o fortalecimento da democracia e da gestão pública na Era Digital. In: SILVA, Sivaldo Pereira da; BRAGATTO, Rachel Callai; SAMPAIO, Rafael Cardoso. **Democracia digital, comunicação política e redes: Teoria e prática**. Rio de Janeiro: Letra e Imagem, 2016.

PRIVACY INTERNACIONAL. **Privacy International's submission on digital technology, social protection and human rights**. 2019. Disponível em: https://privacyinternational.org/sites/default/files/2019-05/PI%20submissions%20to%20UNSR%20Extreme%20Poverty_May%202019.pdf. Acesso em: 22.08.2022.

PRIVACY INTERNACIONAL. **Privacy International's submission on digital technology, social protection and human rights**. 2019. Disponível em: https://privacyinternational.org/sites/default/files/2019-05/PI%20submissions%20to%20UNSR%20Extreme%20Poverty_May%202019.pdf. Acesso em: 22 ago. 2022.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. **Law, Innovation and Technology**, v. 10, n. 1, p. 40-81, 2018.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. **Law, Innovation and Technology**, v. 10, n. 1, p. 40-81, 2018.

QUIGLEY, Andrew S. *et al*. Combining tensile testing and structural analysis at the single collagen fibril level. **Scientific data**, v. 5, n. 1, p. 1-8, 2018.

QUIGLEY, Andrew S. et. al. Combining tensile testing and structural analysis at the single collagen fibril level. **Scientific data**, v. 5, n. 1, p. 1-8, 2018.

RAAB, Charles D. Privacy, social values and the public interest. in **A. Busch and J. Hofmann (eds), Politik und die Regulierung von Information** (2012).

RAAB, Charles D. Privacy, social values and the public interest. in **A. Busch and J. Hofmann (eds), Politik und die Regulierung von Information** (2012).

RAJAMÄKI, Jyri *et al*. How transparency improves the control of law enforcement authorities' activities?. In: IEEE. **Intelligence and Security Informatics Conference (EISIC), 2012 European**, p. 14-21, 2012.

RAJAMÄKI, Jyri et. al. How transparency improves the control of law enforcement authorities' activities?. In: IEEE. **Intelligence and Security Informatics Conference (EISIC), 2012 European**, p. 14-21, 2012.

RAUB, McKenzie. Bots, bias and big data: artificial intelligence, algorithmic bias and disparate impact liability in hiring practices. **Arkansas Law Review**, v. 71, n. 2, 2018.

RAUB, McKenzie. Bots, bias and big data: artificial intelligence, algorithmic bias and disparate impact liability in hiring practices. **Arkansas Law Review**, v. 71, n. 2, 2018.

RAUL, Alan Charles. **Privacy and the digital state: balancing public information and personal privacy**. Boston: Kluwer Academic Publishers, 2002.

RAUL, Alan Charles. **Privacy and the digital state: balancing public information and personal privacy**. Boston: Kluwer Academic Publishers, 2002.

RICHARDS, Neil M. The dangers of surveillance. **Harvard Law Review**, v. 126, n. 7, p. 1934-1965, 2013.

RICHARDS, Neil M.; HARTZOG, Woodrow. A Duty of Loyalty for Privacy Law. **Washington University Law Review**, v. 99, n. 961, 2021.

RICHARDS, Neil M.; HARTZOG, Woodrow. A Duty of Loyalty for Privacy Law. **Washington University Law Review**, v. 99, n. 961, 2021.

ROBERTS, Alasdair. Transparency in the Security Sector. *In*: FLORINI, Ann (ed.). **The Right to Know**. Columbia: Columbia University Press, 2007. p. 309-336.

ROBINSON, David et. al. Government data and the invisible hand. **Yale JL & Tech.**, v. 11, 2008.

RODRIGUES, Jõao Gaspar. Publicidade, transparência e abertura na administração pública. **Revista de Direito Administrativo**, v. 266, ago. 2014.

ROWLEY, Jennifer. e-Government stakeholders—Who are they and what do they want?. **International journal of Information management**, v. 31, n. 1, p. 53-62, 2011.

RUGER, Theodore W. *et al*. The Supreme Court forecasting project: Legal and political science approaches to predicting Supreme Court decision making. **Columbia Law Review**, p. 1150-1210, 2004.

RUIJER, Erna *et al*. Open data for democracy: Developing a theoretical framework for open data use. **Government Information Quarterly**, v. 34, n. 1, p. 45-52, 2017.

SABO, Isabela Cristina *et al*. Entraves ao governo aberto na Justiça Federal brasileira. **Rev. direito GV**, v. 16, n. 1, 2020.THE ROYAL SOCIETY. Protecting privacy in practice: **The current use, development and limits of Privacy Enhancing Technologies in data analysis**. 2019. Disponível em: https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf. Acesso em: 30.22.2022.

SABO, Isabela Cristina et. al. Entraves ao governo aberto na Justiça Federal brasileira. **Rev. direito GV**, v. 16, n. 1, 2020.

SANTOS, Bruna; ANASTÁCIO, Kimberly; VARON, Joana. **Cadastro base do cidadão**: a megabases de dados. 2020. Disponível em: https://www.codingrights.org/docs/megabase.pdf. Acesso em: 10 nov. 2022.

SCASSA, Teresa. Privacy and open government. **Future Internet**, v. 6, n. 2, p. 397-413, 2014.

ŞCHIOPU, Silviu-Dorin. Some Considerations On The Lawfulness Of Personal Data Processing By Public Administration Authorities Under Regulation (EU) 2016/679. **Bulletin of the Transilvania University of Brasov**. Series VII, Social Sciences and Law, v. 11, n. 2, 2018.

SCHLANGER, Margo; LIEBERMAN, Denise. Using Court Records for Research, Teaching, and Policymaking: The Civil Rights Litigation Clearinghouse. **UMKC Law Review**, v. 75, 2006.

SCHWARTZ, Paul M. Internet privacy and the state. **Conn. L. Rev.**, v. 32, 1999a.

SCHWARTZ, Paul M. Privacy and democracy in cyberspace. **Vand. L. Rev.**, v. 52, 1999b.

SCHWARTZ, Paul M. The EU-US privacy collision: a turn to institutions and procedures. **Harv. L. Rev**. 2012.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. Reconciling personal information in the United States and European Union. **Calif. L. Rev.**, v. 102, 2014.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII problem: Privacy and a new concept of personally identifiable information. **NYUL rev.**, v. 86, 2011.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII problem: Privacy and a new concept of personally identifiable information. **NYUL rev.**, v. 86, 2011.

SEVIGNANI, Sebastian. The commodification of privacy on the Internet. **Science and Public Policy**, v. 40, n. 6, p. 733-739, 2013.

SHOAE, Mortanza Bargh; CHOENNI, Sunil. On preserving privacy whilst integrating data in connected information systems. In: ENDICOTT-POPOVSKY, B. **Proceedings of the International Conference on Cloud Security Management (ICCSM'13)**. Seattle: University of Washington, 2013.

SILVA, Sivaldo Pereira da. Transparência digital em instituições democráticas: horizontes, limites e barreiras. In: MENDONÇA, Ricardo Fabrino; PEREIRA, Marcus Abílio; FILGEIRAS, Fernando (org.). **Democracia digital: Publicidade, instituições e confronto político**. Belo Horizonte: Editora UFMG, p. 27-54, 2016.

SILVA, Virgílio Afonso da. O proporcional e o razoável. **Revista dos Tribunais**, São Paulo, n. 798, p. 23-50, 2002. Disponível em: https://constituicao.direito.usp.br/wp-content/uploads/2002-RT798-Proporcionalidade.pdf. Acesso em: 11 out. 2022.

SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico. **Reconhecimento Facial e o Setor Privado**: Guia para a adoção de boas práticas. São Paulo: InternetLab/IDEC, 2020.

SKEEM, Jennifer L.; LOWENKAMP, Christopher T. Risk, race, and recidivism: Predictive bias and disparate impact. **Criminology**, v. 54, n. 4, p. 680-712, 2016.

SMITH, Matthew et al. Big data privacy issues in public social media. **Digital Ecosystems Technologies (DEST), 2012 6th IEEE International Conference**. 2012.

SMITH, Matthew *et al*. Big data privacy issues in public social media. **Digital Ecosystems Technologies (DEST), 2012 6th IEEE International Conference**. 2012

SOLOVE, Daniel J. A taxonomy of privacy. **University of Pennsylvania Law Review**, v. 154, 2005.

SOLOVE, Daniel J. Identity Theft, Privacy, and the Architecture of Vulnerability. **Hastings Law Journal**, v. 54, p. 1-46, 2003.

SOLOVE, Daniel J. Identity Theft, Privacy, and the Architecture of Vulnerability. **Hastings Law Journal**, v. 54, p. 1-46, 2003.

SOLOVE, Daniel J. The Limitations of Privacy Rights. **Notre Dame Law Review**, v. 98, 2022.

SOLOVE, Daniel J. The Myth of the Privacy Paradox. **George Washington Law Review,** v. 89, n. 1, p. 1-51, 2021.

SOUZA, Carlos Affonso de; VIOLA, Mario; PADRÃO, Vinícius. Considerações iniciais sobre os interesses legítimos do controlador na Lei Geral de Proteção de Dados Pessoais. **RDU**, Porto Alegre, v. 16, n. 90, 2019, 109-131, nov-dez 2019.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet**: construção e aplicação. Juiz de Fora: Editora Associada, 2016.

STALLA-BOURDILLON, Sophie et. al. **Privacy vs. security**. Springer, 2014.

STIGLITZ, Joseph E. On Liberty, the Right to Know, and Public Discourse: The Role. **Globalizing Rights**: The Oxford Amnesty Lectures. 1999. Disponível em: https://internationalbudget.org/wp-content/uploads/On-Liberty-the-Right-to-Know-and-Public-Discourse-The-Role-of-Transparency-in-Public-Life.pdf. Acesso em: 30 nov. 2022.

STOKES, Elen. "Mike Feintuck, the Public Interest in Regulation." (2007): 154.

SULEA, Octavia-Maria et. al. Predicting the law area and decisions of french supreme court cases. **Proceedings of the International Conference Recent Advances in Natural Language Processing, RANLP 2017**, p. 716-722, 2017.

SUNDFELD, Carlos Ari. **Fundamentos de direito público**. 5. ed. São Paulo: Malheiros, 2017.

SURDEN, Harry. Machine learning and law. **Washington Law Review**, v. 89, p. 87-115, 2014.

TAVARES, Giovanna Milanez. **O tratamento de dados pessoais disponíveis publicamente e os limites impostos pela LGPD**. Rio de Janeiro: Editora Processo, 2021.

TAYLOR, John.; LIPS, Miriam; ORGAN, Joe. Identification practices in government: Citizen surveillance and the quest for public service improvement. **Identity in the Information Society**, v. 1, n. 1, p. 135-154, nov. 2008.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **civilistica.com**, v. 9, n. 1, p. 1-38, maio, 2020.

TEIXEIRA, Pedro Eurico de Souza Cruz. **Lei de Acesso à Informação nos Tribunais Brasileiros**. São Paulo: Artigo 19 Brasil, 2017.

TENE, Omer. Privacy law's midlife crisis: a critical assessment of the second wave of global privacy laws. **Ohio State Journal**, v. 74, n. 6, p. 1217-1261, 2013.

TENE, Omer; POLONETSKY, Jules. Big Data for All: Privacy and User Control in the Age of Analytics. **Northwestern Journal of Technology and Intellectual Property**, v. 11, n. 5, p. 204-273, 2013.

TENE, Omer; POLONETSKY, Jules. Privacy in the age of big data: a time for big decisions. **Stan. L. Rev. Online**, v. 64, p. 63-69, 2011.

THE ROYAL SOCIETY. Protecting privacy in practice: **The current use, development and limits of Privacy Enhancing Technologies in data analysis**. 2019. Disponível em: https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf. Acesso em: 30.22.2022.

TITAH, Ryad; BARKI, Henri. E-government adoption and acceptance: A literature review. **International Journal of Electronic Government Research (IJEGR)**, v. 2, n. 3, 2006.

TOMASEVICIUS FILHO, Eduardo. Informação assimétrica, custos de transação, princípio da boa-fé. 2007. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2007. Acesso em: 29.11.2022.

TSAKYRAKIS, Stavros. Proportionality: An assault on human rights?, **International Journal of Constitutional Law**, v. 7, n. 3, p. 468–493, jul. 2009.

TYLER, Tom R.; RASINSKI, Kenneth. Procedural justice, institutional legitimacy, and the acceptance of unpopular US Supreme Court decisions: A reply to Gibson. **Law and Society Review**, n. 25, p. 621-630, 1991.

UBALDI, Barbara. Open government data: Towards empirical analysis of open government data initiatives. **OECD Working Papers on Public Governance**, Paris, n. 22, 2013.

UE; ASPA. **Benchmarking e-government**: A global perspective. New York: U.N. Publications, 2002.

URBINA, Francisco J. A critique of proportionality. **The American Journal of Jurisprudence**, v. 57, p. 49-80, 2012.

VAN BASTELAER, Béatrice. Digital cities and transferability of results. *In*: **4th EDC Conference on digital citie**s, Salzburg. 1998. p. 61-70.

VAN DEN BRAAK, Susan W. et. al. Trusted third parties for secure and privacy-preserving data integration and sharing in the public sector. *In*: ACM. **Proceedings of the 13th Annual International Conference on Digital Government Research**. ACM, p. 135-144, jun. 2012.

VAN SCHALKWYK, Francois *et al*. **Open data intermediaries in developing countries**. 2015. Disponível em: https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56288/IDL-56288.PDF?sequence=1&isAllowed=y. Acesso em: 11 nov. 2022.

VERHULST, Stefaan G. *et al*. Data & Policy: A new venue to study and explore policy–data interaction. **Data & Policy**, v. 1, 2019.1.

VERHULST, Stefaan G. *et al*. Data & Policy: A new venue to study and explore policy–data interaction. **Data & Policy**, v. 1, 2019.1.

VERHULST, Stefaan G. *et al*. **Leveraging Private Data for Public Good.** 2019.2. Disponível em: https://datacollaboratives.org/static/files/existing-practices-report.pdf. Acesso em: 11.11.2022.

VERHULST, Stefaan G. *et al*. **Wanted: data stewards.(Re-) defining the roles and responsibilities of data stewards for an age of data collaboration**, v. 7. New York: The GovLab, 2020.

VERHULST, Stefaan G.; SANGOKOYA, David. **Data collaboratives**: Exchanging data to improve people's lives. 2015. Disponível em: https://sverhulst.medium.com/data-collaboratives-exchanging-data-to-improve-people-s-lives-d0fcfc1bdd9a#:~:text=The%20term%20data%20collaborative%20refers,to%20help%20solve%20public%20problems. Acesso em: 12 nov. 2022.

VERHULST, Stefaan G.; YOUNG, Andrew. **How the Data That Internet Companies Collect Can Be Used for the Public Good**. 2018. Disponível em: https://hbr.org/2018/01/how-the-data-that-internet-companies-collect-can-be-used-for-the-public-good#:~:text=Shared%20(often%20aggregated)%20corporate%20data,support%20public%20or%20humanitarian%20objectives. Acesso em: 11 nov. 2022.

VERMA, Neeta; GUPTA, M. P. Open government data: beyond policy & portal, a study in Indian context. In: ACM. **Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance**. ACM, p. 338-341, 2013.

VERNADAT, François B., Technical, semantic and organizational issues of enterprise interoperability and networking, **Annual Reviews in Control**, v. 34, n. 1, p. 139–144, 2010.

VYDRA, Simon; KLIEVINK, Bram. Techno-optimism and policy-pessimism in the public sector big data debate. **Government Information Quarterly**, v. 36, n. 4, out. 2019.

VYDRA, Simon; KLIEVINK, Bram. Techno-optimism and policy-pessimism in the public sector big data debate. **Government Information Quarterly**, v. 36, n. 4, out. 2019.

WANG, Xiushi *et al*. A survey on the status of open data and its future. In: IEEE. **2018 4th International Conference on Universal Village (UV)**. IEEE, p. 1-4, 2018.

WANG, Xiushi et. al. A survey on the status of open data and its future. In: IEEE. **2018 4th International Conference on Universal Village (UV)**. IEEE, p. 1-4, 2018.

WESTIN, Alan. **Privacy and Freedom.** New York: Athenum, 1967.

WESTIN, Alan. Social and political dimensions of privacy**. Journal of Social and Political Dimensions**, v. 59, n. 2, 2003.

WILSON, Susan Copeland; LINDERS, Dennis. The open government directive: a preliminary assessment. In: ACM. **Proceedings of the 2011 iConference**. ACM, p. 387-394, 2011.

WIMMER, Miriam. Cidadania, tecnologia e governo digital: proteção de dados pessoais no estado movido a dados. In: MARTINHÃO, Maximiliano Salvadori (coord). **TIC Governo Eletrônico Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro**. São Paulo, Comitê Gestor da Internet no Brasil, 2020.

WIMMER, Miriam. Cidadania, tecnologia e governo digital: proteção de dados pessoais no estado movido a dados. *In*: MARTINHÃO, Maximiliano Salvadori (coord). **TIC Governo**

Eletrônico Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro. São Paulo: Comitê Gestor da Internet no Brasil, 2020.

WIMMER, Miriam. Limites e possibilidade para o uso secundário de dados pessoais no poder público: lições da pandemia. **Revista Brasileira de Políticas Públicas** 11, n. 1. 2021.

WIRTZ, Bernd W.; BIRKMEYER, Steven. Open government: Origin, development, and conceptual perspectives. **International Journal of Public Administration**, v. 38, n. 5, p. 381-396, 2015.

WOO, Jisuk. The right not to be identified: privacy and anonymity in the interactive media environment. **New media & society**, v. 8, n. 6, p. 949-967, 2006.

WU, Yuehua. Protecting personal data in e-government: A cross-country study. **Government Information Quarterly**, v. 31, n. 1, p. 150-15, 2014.

YANG, Longzhi; ELISA, Noe; ELIOT, Neil. Privacy and security aspects of E-government in smart cities. **Smart cities cybersecurity and privacy**, p. 89-102, 2019.

YANG, Zhenbin; KANKANHALLI, Atreyi. Innovation in government services: The case of open data. *In*: **International Working Conference on Transfer and Diffusion of IT**. Berlin: Springer, Heidelberg, p. 644-651, 2013.

YILDIZ, Mete. E-government research: Reviewing the literature, limitations, and ways forward. **Government information quarterly**, v. 24, n. 3, p. 646-665, 2007.

YU, Harlan; ROBINSON, David G. The new ambiguity of open government. **UCLA L. Rev. Discourse**, v. 59, 2011.

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica? *In*: ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, 1, nov. 2017. Disponível em: http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf. Acesso em: 12 nov. 2022.

ZANELLA DI PIETRO, Maria Sylvia. **Direito Administrativo**. 28. ed. São Paulo: Atlas, 2015.

ZHANG, Sheldon X.; ROBERTS, Robert EL; FARABEE, David. An analysis of prisoner reentry and parole risk using COMPAS and traditional criminal history measures. **Crime & Delinquency**, v. 60, n. 2, p. 167-192, 2014.

ZUBOFF, Shoshana. **The age of surveillance capitalism**: The fight for a human future at the new frontier of **power.** [*S. l.*]: Profile Books, 2019.

ZUIDERWIJK, Annaeke; JANSSEN, Marijn. Open data policies, their implementation and impact: A framework for comparison. **Government Information Quarterly**, v. 31, n. 1, 2014.

ZUIDERWIJK, Anneke *et al*. Issues and guiding principles for opening governmental judicial research data. In: **International Conference on Electronic Government**. Berlin: Springer, Heidelberg, p. 90-101, 2012a.

ZUIDERWIJK, Anneke *et al*. Issues and guiding principles for opening governmental judicial research data. In: **International Conference on Electronic Government**. Berlin: Springer, Heidelberg, p. 90-101, 2012a.

ZUIDERWIJK, Anneke *et al*. Open data for competitive advantage: insights from open data use by companies. *In*: ANNUAL INTERNATIONAL CONFERENCE ON DIGITAL GOVERNMENT RESEARCH, 16, 2015. **Proceedings** […]. [S. l.]: ACM, 2015. p. 79-88.

ZUIDERWIJK, Anneke *et al*. Socio-technical Impediments of Open Data. **Electronic Journal of e-Government**, v. 10, n. 2, 2012b.

ZUIDERWIJK, Anneke *et al*.. Design principles for improving the process of publishing open data. **Transforming Government: People, Process and Policy**, v. 8, n. 2, 2014.

ZUIDERWIJK, Anneke *et al*.. Open data for competitive advantage: insights from open data use by companies. In: ACM, **Proceedings of the 16th Annual International Conference on Digital Government Research**. ACM, p. 79-88, 2015.

ZUIDERWIJK, Anneke *et al*. Design principles for improving the process of publishing open data. **Transforming Government: People, Process and Policy**, v. 8, n. 2, 2014.

ZUIDERWIJK, Anneke *et al*. Socio-technical Impediments of Open Data. **Electronic Journal of e-Government**, v. 10, n. 2, 2012b.

DECISÕES JUDICIAIS E ADMINISTRATIVAS

Bundesverwaltungsgericht (BVwG). W211 2210458-1/10. 2019. Disponível em: https://gdprhub.eu/index.php?title=BVwG_-_W211_2210458-1/10. Acesso em: 12.11.2022.

Corte de Justiça da União Europeia (CJUE). Acórdão do Tribunal de Justiça C-465/00, C-138/01 e C-139/01. 2003. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=48331&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=8829097. Acesso em: 30 ago. 2022.

Controladoria-Geral da União (CGU). Recursos contra negativa de acesso à informação nsº 16853.0076172012-05, 16853.0076152012-16, 16853.0076182012-41, 16853.0076162012-52. 17 de jul. de 2013. Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/16853007617201205_CGU.pdf. Acesso em 28.08.2022.

Controladoria-Geral da União (CGU). Processo 23480.027986/2013-38. 27 de ago. de 2014. Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/23480027986201338_CGU.pdf#search=%22privacidade%22. Acesso em: 30.08.2022.

Controladoria-Geral da União (CGU). Processo 60502.001286/2014-25. 20 de mar. de 2015.1. Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/60502001286201425_CGU.pdf#search=%22privacidade%22. Acesso em: 30.08.2022.

Controladoria-Geral da União (CGU). Processo 01590.000162/2015-01. 09 de jun. de 2015.2. Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/01590000162201501_CGU.pdf#search=ALL%28%22carta%22%20%22vinicius%22%29. Acesso em: 30.08.2022.

Controladoria-Geral da União (CGU). Processo 23480.013438/2016-73. 09 de set. de 2016. Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/23480013438201673_CGU.pdf. Acesso em: 30.08.2022.

Controladoria-Geral da União (CGU). Processo 46800.001705/2016-03. 18 de dez. de 2017. Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/46800001705201603_CGU.pdf#search=%22privacidade%22. Acesso em: 30.08.2022.

Controladoria-Geral da União (CGU). Processo 99936.000114/2017-12. 14 de maio de 2018. Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/99936000114201712_CGU.pdf. Acesso em: 30.08.2022.

Controladoria-Geral da União (CGU). Processo 09002.001842/2021-76. 20 de out. de 2021. Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/09002001842202176_CGU.pdf#search=%22privacidade%22. Acesso em: 30.08.2022.

European Court of Human Rights. Case of Satakunnan Markkinapörssi oy and Satamedia Oy v. Finland. Strasbourg, 27 de junho de 2017. Disponível em: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2017/07/CASE-OF-SATAKUNNAN-MARKKINAP-RSSI-OY-AND-SATAMEDIA-OY-v.-FINLAND.pdf. Acesso em: 30.08.2022.

Ministério Público Federal (MPF). Processo 0083673-69.2018.1.00.0000. Mandado de Segurança 36.150/DF. Relator: Ministro Roberto Barroso. Brasília, 30 de jan. de 2020. Disponível em: https://www.mpf.mp.br/pgr/documentos/MS_36150.pdf. Acesso em: 12.11.2022.

Raad van State (RvS). 201906880/1/A3. Julgado em: 30.06.2021. Disponível em: https://gdprhub.eu/index.php?title=RvS_-_201906880/1/A3. Acesso em: 12.12.2022.

Supreme Court of Canada. RJR -- MacDonald Inc. v. Canada (Attorney General). Julgado em 03.03.1994. Disponível em: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1111/index.do. Acesso em: 13.11.2022.

Superior Tribunal de Justiça (STJ). Habeas Data nº 472-DF. Impetrante: Anne Gabriela Alves Tome. Impetrado: Ministério da Cidadania. Relator: Ministro Herman Benjamin. Julgado em: 09.06.2021. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=2067984&num_registro=202003443998&data=20210803&formato=PDF. Acesso em: 10.10.2022.

Supremo Tribunal Federal (STF). Agravo Regimental no Recurso Extraordinário 631.104 Santa Catarina. Agravante: Centrais Elétricas de Santa Catarina. Agravado: Ministério Público Federal. Relator: Ministro Roberto Barroso. Brasília, 24 de mar. 2017. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=311612174&ext=.pdf. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Arguição de Descumprimento de Preceito Fundamental 129. Requerente: Partido Popular Socialista. Intimado: Presidente da República. Relator: Ministro Edson Fachin. Brasília, 05 de outubro de 2019. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=751580083. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Arguição de Descumprimento de Preceito Fundamental 153. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Intimado: Presidente da República e Congresso Nacional. Relator: Ministro Eros Grau. Brasília, 29 de abril de 2010. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=612960. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Arguição de Descumprimento de Preceito Fundamental 403. Requerente: Partido Popular Socialista. Intimado: Juiz de Direito da Vara Criminal da Comarca de Lagarto. Relator: Ministro Edson Fachin. Brasília, 13 de maio de 2020. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15343104252&ext=.pdf. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Arguição de Descumprimento de Preceito Fundamental 690. Requerente: Rede de Sustentabilidade e outros. Intimado: Presidente da República e Ministro de Estado da Saúde. Relator: Ministro Alexandre de Moraes. Brasília, 15 de março de 2021. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755586015. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Referendo Segunda em Tutela Provisória Incidental na Arguição de Descumprimento de Preceito Fundamental 754. Requerente: Rede Sustentabilidade. Intimado: Presidente da República. Relator: Ministro Ricardo Lewandowski. Brasília, 01 de março de 2021. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755295024. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental 695. Requerente: Partido Socialista Brasileiro. Intimado: União. Relator: Ministro Gilmar Mendes. Brasília, 24 de junho de 2020. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15343579920&ext=.pdf. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Medida Cautelar na Ação Direta de Inconstitucionalidade 6390. Requerente: Partido Socialismo e Liberdade. Intimado: Presidente da República. Relatora: Ministra Rosa Weber. Brasília, 07 de maio de 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358567. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Mandado de Segurança 28.177. Impetrante: Folha da Manhã. Impetrado: Mesa da Câmara dos Deputados. Relator: Ministro Marco Aurélio. Brasília, 19 de agosto de 2009. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stf/14760496. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Mandado de Segurança 28.178. Impetrante: Empresa Folha da Manhã. Impetrado: Presidente do Senado Federal. Relator: Ministro Roberto Barroso. Brasília, 04 de mar. de 2015. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=8399320. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Mandado de Segurança 33.340. Impetrante: Banco Nacional de Desenvolvimento Econômico e Social. Impetrado: Tribunal de Contas da União. Relator: Ministro Luiz Fux. Brasília, 26 de maio de 2015. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=8978494. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Mandado de Segurança 36.150. Impetrante: Instituto Nacional de Estudos e Pesquisas Educacionais Anisio Teixeira. Impetrado: Tribunal de Contas da União. Relator: Ministro Roberto Barroso. Brasília, 10 de dez. de 2018. Disponível em: https://www.conjur.com.br/dl/stf-garante-sigilo-informacoes.pdf. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Mandado de Segurança 24.725. Impetrante: Folha da Manhã. Impetrado: Presidente da Mesa da Câmara dos Deputados. Relator: Ministro Celso de

Mello. Brasília, 17 de dez. de 2003. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2184937. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Recurso Extraordinário 631.240 Minas Gerais. Reclamante: Instituto Nacional do Seguro Social. Reclamado: Marlene de Araújo Santos. Relator: Ministro Roberto Barroso. Brasília, 03 de setembro de 2014. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=7168938. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Recurso Extraordinário 673.707 Minas Gerais. Reclamante: Rigliminas Distribuidora Ltda. Reclamado: União. Relator: Ministro Luiz Fux. Brasília, 17 de jun. de 2015. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=9487405. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Recurso Extraordinário 586.424 Rio de Janeiro. Reclamante: Assembléia Legislativa do Estado do Rio de Janeiro. Reclamado: Alan Onofre Gripp. Relator: Ministro Roberto Barroso. Brasília, 19 de jan. de 2015. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=293883709&ext=.pdf. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Ação Direta de Inconstitucionalidade 2.859 Distrito Federal. Requerente: Partido Trabalhista Brasileiro. Intimado: Presidente da República e Congresso Nacional. Relator: Ministro Dias Toffoli. Brasília, 24 de fevereiro de 2016. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11899965. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Ação Direta de Inconstitucionalidade 5.394 Distrito Federal. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Intimado: Presidente da República, Câmara dos Deputados, Senado Federal. Relator: Ministro Alexandre de Moraes. Brasília, 22 de mar. de 2018. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15339527374&ext=.pdf. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Ação Direta de Inconstitucionalidade 6649 Distrito Federal. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Intimado: Presidente da República. Relator: Ministro Gilmar Mendes. Brasília, 15 de set. de 2022. Disponível em: https://portal.stf.jus.br/processos/downloadTexto.asp?id=5641150&ext=RTF. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Ação Direta de Inconstitucionalidade 6.529 Distrito Federal. Requerente: Rede Sustentabilidade. Intimado: Presidente da República e Congresso Nacional. Relatora: Ministra Cármen Lúcia. Brasília, 11 de out. de 2022. Disponível em:https://portal.stf.jus.br/processos/downloadPeca.asp?id=15348384228&ext=.pdf. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Medida Cautelar na Ação Direta de Inconstitucionalidade 6387, 6388, 6389, 6390 e 6393. Julgamento conjunto. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Intimado: Presidente da República. Relatora: Ministra Rosa Weber. Brasília, 07 de maio de 2020. Disponível em:

https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 31 ago. 2022.

Supremo Tribunal Federal (STF). Medida Cautelar na Ação Direta de Inconstitucionalidade 5394 Distrito Federal. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Intimado: Presidente da República, Câmara dos Deputados, Senado Federal. Relator: Ministro Teori Zavascki. Brasília, 12 de nov. de 2015. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11999509. Acesso em: 31 ago. 2022.

Tribunal de Contas (TCU). TC 032.908/2017-2. Relator: Walton Alencar Rodrigues. Brasília, 14 de nov. 2018. Disponível em: https://contas.tcu.gov.br/egestao/ObterDocumentoSisdoc?codPapelTramitavel=60225650. Acesso em: 10.10.2022.

Tribunal de Justiça da União Europeia (TJUE). Case C-28/08. Julgado em: 29.06.2010. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0028. Acesso em: 12.12.2022.

Tribunal de Justiça da União Europeia (TJUE). Case C-175/20. Julgado em: 01.04.2022. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=245557&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2607038. Acesso em: 12.08.2022.

Tribunal de Justiça do Distrito Federal e Territórios (TJDFT). Apelação 0006457-60.2016.8.07.0020. Segredo de Justiça. Relator: Rômulo de Araújo Mendes. Brasília, 24 de outubro de 2018. Disponível em: https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj. Acesso em: 30 ago. 2022.

Tribunal de Justiça do Estado do Paraná (TJPR). Habeas Data 1569980-8. Impetrante: Cláudio Dirceu Eberhard. Impetrado: Presidente da 4ª Câmara Cível do Tribunal de Justiça do Estado do Paraná. Relator: Des. Leonel Cunha. Julgado em: 31.10.2017. Disponível em: https://portal.tjpr.jus.br/e-dj/publico/diario/baixar.do?tjpr.url.crypto=0816f08ecbc775d55aa4ef22398087e31772d2855b57a12ec00ed3382c4c4543#page=173. Acesso em: 12.09.2022.

Tribunal de Justiça do Estado de São Paulo (TJSP). Sentença em Ação de Procedimento Comum 1013430-56.2015.8.26.0008. Autor: Gilberto Trama. Réu: Google Brasil Internet Ltda e outros. Juizo: Mariana Dalla Bernardina. São Paulo, 20 de julho de 2016. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/1276416323/inteiro-teor-1276416325. Acesso em: 30 ago. 2022.

Tribunal de Justiça do Estado de São Paulo (TJSP). Agravo de Instrumento 2017.0000005262. Agravante: Charles Berbare. Agravado: Google Brasil Internet Ltda. Relator: Rui Cascaldi. São Paulo, 12 de janeiro de 2017. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/418745447/inteiro-teor-418745466. Acesso em: 30 ago. 2022.

Tribunal de Justiça do Estado de Rondônia (TJRO). Ação Direta de Inconstitucionalidade 0802559-78.2018.822.0000 Recurso Ordinário 0802559-78.2018.822.0000, Des.Rel. Eurico Montenegro, Julgado em 01.04.2019. Disponível em: https://tj-

ro.jusbrasil.com.br/jurisprudencia/699366137/direta-de-inconstitucionalidade-adi-80255978201882200000-ro-0802559-7820188220000/inteiro-teor-699366139 Acesso em 13.09.2020.

Tribunal de Justiça do Estado do Rio Grande do Sul (TJRS). Ação Direta de Inconstitucionalidade 70075503433 RS, Des.Rel. Marilene Bonzanini, Julgado em 24.09.2012. Disponível em: https://tj-rs.jusbrasil.com.br/jurisprudencia/759485066/direta-de-inconstitucionalidade-adi-70075503433-rs/inteiro-teor-759485067. Acesso em: 13.09.2020.

Tribunal Regional Federal da 3ª Região (TRF-3). Remessa Necessária Cível 5000520-19.2019.4.03.6003. Autor: Edinaldo de Oliveira Santos. Réu: Instituto Nacional do Seguro Social. Relatora: Desembargadora Federal Mônica Nobre. Julgado em: 18.10.2021. Disponível em: https://pje2g.trf3.jus.br/pje/ConsultaPublica/DetalheProcessoConsultaPublica/documentoSemLoginHTML.seam?ca=75243bb30f32a07358b563222303ac7e5ae52db29c483490ebf92d82f4ecec655ea1978872dd3e5725ca5723b6a5fe2baac761f7c0295fc4&idProcessoDoc=203731402. Acesso em: 10.12.2022.

VGH Munchen. 5 CS 19.2087. Julgado em: 15.04.2020. Disponível em: https://gdprhub.eu/index.php?title=VGH_M%C3%BCnchen_%E2%80%93_5_CS_19.2087. Acesso em 14.12.2022.

GUIA DE AUTORIDADES DE PROTEÇÃO DE DADOS PESSOAIS

ARTICLE 29 WORKING PARTY (WP 29). Opinion nº 3/99 on Public sector information and the protection of personal data. 1999. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp20_en.pdf. Acesso em: 30 ago. 2022.

ARTICLE 29 WORKING PARTY (WP 29). Opinion 5/2001 On the European Ombudsman Special Report to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH. 2001. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp44_en.pdf. Acesso em 04.03.2021.

ARTICLE 29 WORKING PARTY (WP 29). Opinion 7/2003 on the re-use of public sector information and the protection of personal data. 2003. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp83_en.pdf. Acesso em: 30 ago. 2022.

ARTICLE 29 WORKING PARTY (WP 29). Opinião 4/2007 sobre o conceito de dados pessoais. 2007. Disponível em https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf. Acesso em 17.07.2022.

ARTICLE 29 DATA PROTECTION WORKING PARTY (WP 29). Opinion 1/2010 on the concepts of “controller” and “processor”. 2010. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. Acesso em 10.04.2021.

ARTICLE 29 WORKING PARTY (WP 29). Opinion 03/2013 on purpose limitation. 2013. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em 04.03.2021.

ARTICLE 29 WORKING PARTY (WP 29). Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Acesso em 04.03.2021.

ARTICLE 29 WORKING PARTY (WP 29). Opinion 02/2016 on the publication of Personal Data for Transparency purposes in the Public Sector. 2016. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp239_en.pdf. Acesso em 04.03.2021.

ARTICLE 29 DATA PROTECTION WORKING PARTY (WP 29). Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Bruxelas: adotado em 09 de abril de 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Acesso em 03.10.2020.

ARTICLE 29 DATA PROTECTION WORKING PARTY (WP 29). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01. Disponível em

https://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=611236. Acesso em 12.11.2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Agentes de Tratamentos de Dados Pessoais e do Encarregado. 2022.1. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 30 ago. 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo sobre Segurança da informação para Agentes de Tratamento de Pequeno Porte**.** 2022.2. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf. Acesso em: 30 ago. 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público. 2022.3. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico___defeso_eleitoral.pdf. Acesso em: 30 ago. 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Estudo Técnico: A LGPD e o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos por órgão de pesquisa. Texto para discussão. 2022.4. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000810_2022_17.pdf. Acesso em: 30 ago. 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Nota Técnica nº 46/2022/CGF/ANPD - Manifestação técnica da Coordenação-Geral de Fiscalização acerca da divulgação dos microdados do Enem e de censos escolares pelo INEP à luz da Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD). 2022.5. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000730_2022_53-nt-46.pdf. Acesso em: 30 ago. 2022

BRITISH COLUMBIA. Privacy Management and Accountability Policy. 2022. Disponível em: https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/resources/policies-guidelines/pmap_version_4.pdf. Acesso em: 10.11.2022.

EUROPEAN DATA PROTECTION BOARD (EDPB). Statement 05/2021 on the Data Governance Act in light of the legislative developments. 2021.1. Disponível em: https://edpb.europa.eu/system/files/2021-05/edpb_statementondga_19052021_en_0.pdf. Acesso em: 10.11.2022.

EUROPEAN DATA PROTECTION BOARD (EDPB). Statement on the Digital Services Package and Data Strategy. 2021.2. Disponível em: https://edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf. Acesso em: 10.11.2022.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS). Opinion of the European Data Protection Supervisor on the 'Open-Data Package' of the European Commission including a

Proposal for a Directive amending Directive 2003/98/EC on re-use of public sector information (PSI), a Communication on Open Data and Commission Decision 2011/833/EU on the reuse of Commission documents. 2012. Disponível em: https://edps.europa.eu/sites/default/files/publication/12-04-18_open_data_en.pdf. Acesso em: 30 ago. 2022.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS). Comments of the EDPS on a Proposal for a Regulation of the European Parliament and of the Council on a framework for the free-flow of non-personal data in the European Union.. 2018. Disponível em: https://edps.europa.eu/sites/default/files/publication/18-06-08-edps_formal_comments_freeflow_non_personal_data_en.pdf. Acesso em: 11.12.2021.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS). Opinion 3/2020 on the European strategy for data. 2020. Disponível em: https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf. Acesso em: 10.11.2022.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS). A Preliminary Opinion on data protection and scientific research. 2020. Disponível em: https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf. Acesso em: 10.11.2022.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS); EUROPEAN DATA PROTECTION BOARD (EDPB). EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act). 2021. Disponível em: https://edpb.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf. Acesso em: 30.08.2021.

INFORMATION COMMISSIONER'S OFFICE (ICO). The Guide to Freedom of Information. 2017. Disponível em: https://ico.org.uk/media/for-organisations/guide-to-freedom-of-information-4-9.pdf. Acesso em: 11.11.2022.

INFORMATION COMMISSIONER'S OFFICE (ICO). What are the substantial public interest conditions?. 2020.1. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-substantial-public-interest-conditions/. Acesso em: 11.11.2022.

INFORMATION COMMISSIONER'S OFFICE (ICO). Personal information (section 40 and regulation 13) Freedom of Information Act Environmental information Regulations. 2020.2. Disponível em: https://ico.org.uk/media/for-organisations/documents/2619056/s40-personal-information-section-40-regulation-13.pdf. Acesso em: 11.11.2022.

INFORMATION COMMISSIONER'S OFFICE (ICO). The Public Interest Test. 2022. Disponível em: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf. Acesso em: 11.11.2022.

OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER (OAIC). Privacy Code Checklist. 2017. Disponível em: https://www.oaic.gov.au/privacy/privacy-for-government-agencies/privacy-code-checklist. Acesso em: 30.08.2022.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (OPC). Public Consultation on Modernization of the Privacy Act. 2021. Disponível em: https://priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_jus_pa_2103/. Acesso em: 30.08.2021.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (OPC). Public interest disclosures by federal institutions under the Privacy Act. 2022. Disponível em: https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/02_05_d_29/. Acesso em: 30.08.2022.