



Escola Nacional de Administração Pública

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA
PROGRAMA DE MESTRADO PROFISSIONAL EM GOVERNANÇA
E DESENVOLVIMENTO

COMPARTILHAMENTO DE DADOS PESSOAIS
NO PODER PÚBLICO

DISSERTAÇÃO DE MESTRADO

NATÁLIA BREZOLIN VUORI

BRASÍLIA – DF

2024

COMPARTILHAMENTO DE DADOS PESSOAIS NO PODER PÚBLICO

Dissertação apresentada ao Programa de Mestrado em Governança e Desenvolvimento da Escola Nacional de Administração Pública - ENAP como requisito para obtenção do título de Mestre em Governança e Desenvolvimento.

Aluno: Natália Brezolin Vuori

Orientador: Prof. Dr. Maurício Ebling

Brasília - DF

2024

V994c Vuori, Natália Brezolin

Compartilhamento de dados pessoais no poder público /
Natália Brezolin Vuori. -- Brasília: Enap, 2024.
97 f. : il.

Dissertação (Mestrado – Programa de Mestrado
Profissional em Governança e Desenvolvimento) -- Escola
Nacional de Administração Pública, 2024.

Orientação: Prof. Dr. Maurício Ebling
1. Proteção de dados. 2. Sigilo de dados. 3. Poder
público. 4. Interesse público. I. Título. II. Ebling, Maurício
orient.

CDD 343.09995

Bibliotecária: Kelly Lemos da Silva – CRB1/1880



Mestrado Profissional em Governança e Desenvolvimento

ATA DA BANCA DE DEFESA DE TRABALHO DE CONCLUSÃO DO CURSO DE MESTRADO PROFISSIONAL EM GOVERNANÇA E DESENVOLVIMENTO

Aluno (a): Natália Brezolin Vuori

Ano de Ingresso: 2022

Título da Dissertação: Compartilhamento de dados pessoais no poder público

Orientador: Prof. Dr. Maurício Ebling

Avaliador: Prof. Dr. Clóvis Henrique Leite de Souza
Profa. Dra. Miriam Wimmer

Avaliação:

- [☒] Aprovada
[☐] Aprovada com ressalvas
[☐] Reprovada

Brasília, 8 de outubro de 2024

DocuSigned by:

Clóvis Henrique Leite de Souza

CE1C2FDFBED74B5...

Avaliador

Assinado por:

Miriam Wimmer

527063B30EF7463...

Avaliadora

DocuSigned by:

Mauricio Ebling

FC433A5BFE7E45B...

Orientador

ENAP

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS
PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO
IV

GOVERNO FEDERAL



AGRADECIMENTOS

Agradeço, primeiramente, sempre a Deus e à minha Santa Teresinha, que me abençoam diariamente e me deram forças para enfrentar todos os desafios dessa etapa do mestrado.

Aos meus pais, Alberto e Maristela, à minha sobrinha, Gabriella, à minha irmã, Lisiane, e aos meus amigos, pela paciência e apoio incondicional para me acompanhar nesse complexo desenvolvimento da dissertação. A meus avós, especialmente a meu saudoso avô Valdir Nelson Brezolin, que partiu durante esses últimos meses, pela inspiração aos estudos e à leitura, exemplo profissional e pessoal. Sempre te levarei comigo e tenho orgulho pelo tempo de convivência e aprendizado.

Ao meu orientador Maurício Ebling, que pacientemente me acompanhou nesse processo, sempre com total disponibilização para os debates e as dúvidas, me dando apoio em todas as etapas.

Aos integrantes da banca de qualificação, Clóvis Henrique Leite de Souza e Miriam Wimmer, que foram fundamentais para alinhamento e direcionamento da minha pesquisa e fizeram da minha qualificação um momento tranquilo e muito proveitoso, muito obrigada pela disponibilidade e pelos ensinamentos durante esse período.

LISTA DE SIGLAS E ABREVIATURAS

ABIN	- Agência Brasileira de Inteligência
ADI	- Ação Direta de Inconstitucionalidade
ADPF	- Arguição de Descumprimento de Preceito Fundamental
AGU	- Advocacia-Geral da União
ANATEL	- Agência Nacional de Telecomunicações
ANPD	- Autoridade Nacional de Proteção de Dados
BPC/AGU	- Manual de Boas Práticas Consultivas da Advocacia-Geral da União
CadÚnico	- Cadastro Único para Programas Sociais
CNH	- Carteira Nacional de Habilitação
CRFB	- Constituição da República Federativa do Brasil
DF	- Distrito Federal
EC	- Emenda Constitucional
GDPR	- General Data Protection Regulation
IBGE	- Fundação Instituto Brasileiro de Geografia e Estatística
LGPD	- Lei Geral de Proteção de Dados Pessoais
PGDF	- Procuradoria-Geral do Distrito Federal
PGE	- Procuradoria-Geral do Estado
SERPRO	- Serviço Federal de Processamento de Dados
STF	- Supremo Tribunal Federal
TCU	- Tribunal de Contas da União

LISTA DE TABELAS

Tabela 1: Requisitos exigidos e correção com os princípios da LGPD

Tabela 2: Comparação entre requisitos STF e ANPD

Tabela 3: Lista de documentos jurídicos das advocacias públicas

Tabela 4: Compartilhamento de dados pessoais e dados pessoais sensíveis

Tabela 5: Lista de Estados que dispensam formalização de acordo para compartilhamento de dados pessoais

LISTA DE GRAFICOS

Gráfico 1: Base Legal

Gráfico 2: Formalização e Registro

Gráfico 3: Objeto

Gráfico 4: Finalidade

Gráfico 5: Duração do Tratamento

Gráfico 6: Transparência e Direitos dos Titulares

Gráfico 7: Prevenção e Segurança

Gráfico 8: Outros Requisitos

Gráfico 9: Critérios para definição de tratamento de alto risco

Gráfico 10: Novos Requisitos

LISTA DE DIAGRAMA

Diagrama: Possibilidade de conservação ou eliminação de dados pessoais após o tratamento

RESUMO

A Lei Geral de Proteção de Dados Pessoais (LGPD) trouxe um sistema específico de proteção de dados pessoais, conceituados como aqueles relacionados às pessoas naturais identificadas ou identificáveis. O Poder Público, para o desenvolvimento de suas atividades, por vezes compartilha dados pessoais constantes de suas bases de dados, o que é disciplinado pela LGPD. Com base nas determinações legais em torno do compartilhamento de dados pessoais pelo Poder Público, o presente estudo interpretou a LGPD para se aferir como o compartilhamento de dados pessoais deve ser realizado para observar as prescrições legais. Para tanto, em busca de orientações interpretativas, analisou-se como a questão vem sendo tratada por três atores, quais sejam: a Autoridade Nacional de Proteção de Dados (ANPD); Supremo Tribunal Federal (STF); e as advocacias públicas da União, dos Estados e do DF. Realizou-se pesquisa bibliográfica e análise dos documentos expedidos por essas instituições com o auxílio da ferramenta *Atlas.ti*. Ao final, foram apresentados todos os parâmetros e orientações que devem ser observados para o regular compartilhamento de dados pessoais no Poder Público.

Palavras-chave: LGPD. Parâmetros e orientações. Compartilhamento. Dados pessoais. Poder Público.

ABSTRACT

The General Personal Data Protection Law (GPDPL) introduced a specific system for the protection of personal data, defined as those related to identified or identifiable natural persons. Public authorities, in order to carry out their activities, sometimes share personal data contained in their databases, which is regulated by the GPDPL. Based on the legal determinations surrounding the sharing of personal data by the Public Authorities, the present study interpreted the GPDPL how the sharing of personal data should be carried out to comply with legal requirements. To this end, in search of interpretative guidance, we analyzed how the issue has been handled with by three actors, namely: the National Data Protection Authority; the Federal Supreme Court; and the public lawyers of the Union, the States and the Federal District. Bibliographical research and analysis of ocuments issued by these institutions were carried out with the help of the Atlas.ti tool. At the end, all the parameters and guidelines that must be observed for the regular sharing of personal data within the Public Authorities were presented.

Keywords: GPDPL. Parameters and guidelines. Sharing. Personal data. Public Authorities.

SUMÁRIO

1	INTRODUÇÃO	1
2	PROTEÇÃO DE DADOS	4
2.1	Proteção de dados pessoais no Brasil	4
2.2	Direito fundamental à proteção de dados e interesse público	7
2.3	Governança de dados	11
3	LGPD	13
3.1	Âmbito de aplicação	13
3.2	Dados pessoais e dados pessoais sensíveis	15
3.3	Tratamento de dados pessoais	17
4	COMPARTILHAMENTO	18
4.1	O papel dos atores envolvidos na definição dos requisitos de compartilhamento de dados pessoais sensíveis	18
4.1.1	A Autoridade Nacional de Proteção de Dados – ANPD	18
4.1.2	O Supremo Tribunal Federal – STF	21
4.1.3	As advocacias públicas	22
5	ABORDAGEM METODOLÓGICA	25
5.1	Dados analisados	26
6	REQUISITOS PARA O COMPARTILHAMENTO DE DADOS PESSOAIS NO PODER PÚBLICO	33
6.1	Base legal	35
6.2	Formalização e registro	43
6.2.1	Ato formal: instrumentos utilizados pela União, DF e Estados	46
6.2.2	Formalização em atenção às normas gerais que regem o procedimento administrativo	51
6.2.3	Formalização em atenção à obrigatoriedade de registro	54
6.3	Objeto	55
6.4	Finalidade	57
6.5	Duração do tratamento	60
6.6	Transparência e direitos dos titulares	64
6.7	Prevenção e segurança	67
6.8	Outros requisitos	71
6.8.1	Funções e responsabilidades dos agentes de tratamento	72
6.8.2	Ônus financeiro	75
6.8.3	Relatório de impacto à proteção de dados pessoais	75

6.8.4	Vedação ou autorização de novo compartilhamento	78
6.9	Novos requisitos	78
6.9.1	Vedação ou autorização para transferência internacional.....	79
6.9.2	Princípios da qualidade do dado e da não discriminação	81
6.9.3	Indicação do encarregado de dados	81
6.10	Considerações finais sobre os dados analisados.....	82
7	CONSIDERAÇÕES FINAIS	84
	REFERÊNCIAS BIBLIOGRÁFICAS	89
	ANEXO: Guia de Boas Práticas: Lei Geral de Proteção de Dados (LGPD) – Guia de Boas Práticas para Implementação na Administração Pública Federal (p. 29):.....	97

1 INTRODUÇÃO

Com o desenvolvimento da sociedade da informação, cada vez mais os cidadãos preenchem cadastros em sistemas de entidades privadas e públicas, disponibilizando seus dados pessoais. Diante desse cenário de ampla disponibilização de dados, é necessário conciliar interesses. No caso do Poder Público, de um lado, tem-se o interesse público em se utilizar os dados pessoais para concretização de suas funções e atividades públicas, de interesse de toda a sociedade. De outro lado, a necessidade de se pensar em formas de proteção aos detentores de dados pessoais, que são também destinatários do interesse público.

No Brasil, a publicação da Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709, de 14 de agosto de 2018, trouxe um sistema específico de proteção de dados pessoais, conceituados como aqueles relacionados às pessoas naturais identificadas ou identificáveis. A LGPD não traz proteção aos dados das pessoas jurídicas. Os dados pessoais podem receber o adjetivo de sensíveis, quando referentes à origem racial ou étnica, saúde ou vida sexual, convicção religiosa, opinião política, filiação a sindicato ou organização religiosa, filosófica ou política, dado genético ou biométrico. Nesse caso, a LGPD seleciona algumas características da pessoa natural e as insere em um nível de proteção maior.

A LGPD é aplicável tanto à pessoa natural e pessoa jurídica de direito privado como à pessoa jurídica de direito público. A aplicabilidade às pessoas jurídicas de direito público é reforçada pelo parágrafo único do art. 1º ao afirmar que a norma se aplica à União, aos Estados, ao Distrito Federal e aos Municípios. Nesse sentido, é dever do Poder Público proteger os dados pessoais que recebe em seus diversos sistemas, sendo que a Lei dedica um capítulo específico para o Tratamento de Dados Pessoais pelo Poder Público - Capítulo IV, além de previsões em artigos esparsos, como o art. 7º, III e § 3º, art. 11, II, b e § 3º, art. 55-J, XI e XVI.

O tratamento de dados pessoais consiste em toda operação realizada com dados pessoais. Especificamente quanto ao Poder Público, a LGPD criou a figura do uso compartilhado de dados para tratar do acesso a banco de dados pessoais entre órgãos e entidades públicas ou entre esses e entidades privadas para as hipóteses permitidas pela Lei. Dentre essas hipóteses, insere-se o cumprimento de obrigação legal ou regulatória, o cumprimento de atribuições legais do serviço público e a execução de políticas públicas.

Com base nas determinações legais em torno do compartilhamento de dados pessoais pelo Poder Público, cabe interpretar a LGPD para se aferir como o compartilhamento de dados

peçoais deve ser realizado para observar as prescrições legais. Para tanto, em busca de orientaões interpretativas, o presente estudo analisará como a questão vem sendo tratada por três atores, quais sejam: a Autoridade Nacional de Proteção de Dados (ANPD); o Supremo Tribunal Federal (STF); e as advocacias públicas da União, dos Estados e do DF.

A ANPD, autarquia de natureza especial, tem como competência primordial a interpretação da LGPD com a definição de diretrizes para sua implementação. Com o fim de estabelecer as principais diretrizes a serem observadas pelo Poder Público, a ANPD publicou, em 2023, o Guia Orientativo - Tratamento de dados peçoais pelo Poder Público, com capítulo específico para o compartilhamento de dados peçoais pelo Poder Público.

O STF, guardião da Constituição da República e última instância do Poder Judiciário, teve relevante papel na definição da proteção de dados peçoais como direito fundamental, tendo, em 2020, reconhecido, por meio do referendo na Medida Cautelar na ADI nº 6.387/DF, a proteção de dados peçoais como um direito fundamental autônomo. Também teve papel emblemático sobre o tema ao indicar os principais requisitos para o compartilhamento de dados peçoais na decisão no julgamento conjunto da ADI 6649 e da ADPF 695 do STF.

As advocacias públicas da União, do DF e dos Estados têm a função primordial de auxiliar seus respectivos entes no exercício de suas atribuições legais e execução de políticas públicas, apresentando soluções para resolução de dúvidas jurídicas relacionadas às funções do Poder Executivo. Como atores, desenvolvem análise jurídica dos processos administrativos que objetivam o compartilhamento de dados peçoais.

Diante desse cenário, o presente estudo busca responder à seguinte pergunta de pesquisa: quais parâmetros e orientaões, que decorrem da interpretação da lei, da jurisprudência do STF e dos entendimentos administrativos, devem ser observados para o compartilhamento de dados peçoais no Poder Público?

É relevante elucidar que parâmetros e orientaões abarcam todas as informações e exigências que serão tratadas ao longo do presente estudo. Por vezes, o estudo adotará a nomenclatura requisitos para abarcar aquelas condições que devem ser adotadas para o regular compartilhamento de dados peçoais. Veja-se, o que se busca, com o presente estudo, não é apenas citar um requisito, mas aprofundar os subtemas com base em cada parâmetro e cada orientação a ser observada. Assim, apesar de, em algumas oportunidades, haver prevalência da nomenclatura requisitos, isso não simplifica o processo de estudo para sua inteira compreensão.

Com o objetivo de elucidar a questão, será realizada pesquisa bibliográfica, analisando os aspectos relevantes à compreensão e aprofundamento do tema, seguida de análise dos documentos coletados com auxílio da ferramenta de análise de dados qualitativos *Atlas.ti*. Os documentos coletados referem-se ao Guia Orientativo da ANPD, à citada decisão do STF e às manifestações jurídicas das advocacias públicas da União, dos Estados e do DF. Nesse sentido, a abordagem metodológica será apresentada no capítulo cinco da dissertação. O subcapítulo 5.1 apresentará, de forma pormenorizada, os dados coletados, bem como as sequências de análises realizadas.

Os capítulos dois, três e quatro serão dedicados aos aspectos relevantes para compreensão do tema. O capítulo dois apresenta o contexto da proteção de dados pessoais no Brasil, bem como aprofunda o estudo sobre o direito fundamental à proteção de dados pessoais, fazendo correlação com a nova vertente sobre o princípio da supremacia do interesse público, que entende e acolhe o interesse público também na proteção dos direitos fundamentais.

O capítulo três descreve aspectos relevantes da LGPD. No subcapítulo 3.1, apresenta-se o âmbito de aplicação da LGPD, exemplificando-se com casos analisados pelas advocacias públicas. Após, no subcapítulo 3.2, apresenta-se o conceito e a diferenciação entre dados pessoais e dados pessoais sensíveis. Por fim, o subcapítulo 3.3 define o tratamento de dados pessoais.

O capítulo quatro tratará o compartilhamento sob o viés do papel dos atores envolvidos na definição das orientações para o compartilhamento de dados pessoais no Poder Público, com um subcapítulo dedicado a cada um desses atores: ANPD, STF e advocacias públicas da União, dos Estados e do DF.

Após a exposição desses aspectos para compreensão do tema e a abordagem metodológica, a dissertação adentrará no campo da pesquisa dos dados coletados no capítulo seis, que tratará especificamente dos requisitos para o compartilhamento de dados pessoais no Poder Público, analisando e aprofundando cada um dos parâmetros e orientações que devem ser observados. Cada requisito será analisado de forma aprofundada em um subcapítulo, expondo-se o conceito, a base principiológica da LGPD, os princípios de governança pública aplicáveis, as abordagens e as formas de observá-lo.

Por fim, para encerramento do tema, serão traçadas as considerações finais com as principais questões apreendidas ao longo do estudo, formulando-se eventuais perspectivas que ainda permeiam o tema.

2 PROTEÇÃO DE DADOS

2.1 Proteção de dados pessoais no Brasil

Com o desenvolvimento da sociedade da informação, cada vez mais os cidadãos preenchem cadastros em sistemas de entidades privadas e públicas, disponibilizando seus dados pessoais. Stéfano Rodotà há muito já demonstra sua preocupação com essas repercussões, comparando a transparência a que os cidadãos atualmente são submetidos com o homem de vidro de matriz nazista. Em suas palavras, “os cidadãos da sociedade da informação correm o risco de parecer homens de vidro: uma sociedade que a informática e a telemática estão tornando totalmente transparente” (Rodotà, 2008, p. 8).

Diante desse cenário de disponibilização de dados, os debates envolvendo a livre circulação de dados pessoais (*free data flow*) iniciaram na União Europeia há mais de cinco décadas (Doneda, 2023a, p. 3), sendo que as principais regras consolidadas, denominadas por Doneda como “núcleo duro” (2023a, p. 5), originam-se da interrelação entre diversos sistemas, especialmente da Europa e dos Estados Unidos. Como marco regulatório, cita-se a lei de proteção de dados do Estado alemão de Hesse, de 1970, “por ter operado uma mudança de perspectiva que trouxe consigo o desenvolvimento de um modelo normativo autônomo, o da proteção de dados pessoais” (Doneda, 2023a, p. 8).

No âmbito da consolidação das normas europeias, em 1995 foi adotada a Diretiva 95/46/CE, que foi substituída, em 2016, pelo Regulamento Geral de Proteção de Dados, *General Data Protection Regulation - Regulation (EU) 2016/679* (União Europeia, 2016), aprovado em 27 de abril de 2016 e aplicável a partir de 25 de maio de 2018 (Doneda, 2023a, p. 9).

No Brasil, antes mesmo da edição do Regulamento da União Europeia, já havia amplos debates sobre o tema. O primeiro projeto de lei que fez referência direta à proteção de dados foi o nº 2.796 de 1980, que “assegura aos cidadãos acesso às suas informações constantes de bancos de dados e dá outras providências”, tendo sido arquivado ao final da legislatura. Os debates se intensificaram e ressoavam com o processo de redemocratização da década de 1980, resultando, por exemplo, na ação de *habeas data* na Constituição de 1988 (Doneda, 2023a, p. 11-12).

Além do *habeas data*, dentre as disposições trazidas pela Constituição da República de 1988 que tangenciam o tema, tem-se também o direito à privacidade e à intimidade e o segredo das comunicações telefônicas, telegráficas e telemáticas.

Em 1990, o Código de Defesa do Consumidor trouxe “um volume considerável das demandas relacionadas a dados pessoais” (Doneda, 2023a, p. 14). O art. 43 da seção de banco de dados e cadastros de consumidores, abordou o direito ao acesso às informações constantes em cadastros, fichas, registros e dados pessoais e de consumo arquivados.

Em 2011, duas normas abordaram o tema: a Lei do Cadastro Positivo e a Lei de Acesso à Informação. A Lei do Cadastro Positivo – Lei nº 12.414/2011 (Brasil, 2011a), disciplinou a formação e consulta a bancos de dados com informações de adimplemento para formação de histórico de crédito.

Por sua vez, a Lei de Acesso à Informação – Lei nº 12.527/2011 (Brasil, 2011b), buscou regulamentar o direito à transparência, trazendo uma seção própria para as informações pessoais. Aqui já houve previsão expressa sobre o tratamento de informações pessoais pelo Poder Público, deixando claro que as informações pessoais relativas à intimidade, vida privada, honra e imagem terão acesso restrito a agentes públicos legalmente autorizados e à pessoa a que eles se referirem, pelo prazo máximo de cem anos.

De acordo com a Lei de Acesso à Informação (Brasil, 2011b), a divulgação ou acesso por terceiros depende de previsão legal ou consentimento expresso da pessoa titular das informações, dispensando-se o consentimento em hipóteses expressamente definidas:

Art. 31. (...)

§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:

I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;

II - à 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 - ao cumprimento de ordem judicial;

IV - à defesa de direitos humanos; ou

V - à proteção do interesse público e geral preponderante (Brasil, 2011b).

O cenário legislativo anterior à LGPD conta ainda com o Marco Civil da Internet – Lei nº 12.965/2014 (Brasil, 2014), que traz no seu rol de princípios a proteção dos dados pessoais,

na forma da lei. Conforme Doneda (2023a, p. 15), o texto legal “já acenava para legislação própria sobre proteção de dados, que lhe seria posterior”.

Entremeando essas normas, especialmente se considerarmos o Código de Defesa do Consumidor de 1990 e a Lei do Cadastro Positivo de 2011, pode-se dizer que o debate sobre proteção de dados pessoais se intensifica no Brasil em decorrência dos debates e propostas encaminhados pelo Subgrupo de Trabalho de número 13 do Mercosul, que resultou no documento “Medidas para a proteção de dados pessoais e sua livre circulação”, endossado pelos países-membros em 2010 (Doneda, 2023a, p. 15-16).

Em decorrência dos debates originados após o endosso do documento formulado pelo Mercosul, após várias versões de anteprojeto de lei, foi consolidado e protocolado o Projeto de Lei 5.276/2016. À época, o tema já estava sendo debatido também na Câmara dos Deputados com o Projeto de Lei 4.060/2012 e no Senado Federal com os Projetos de Lei 330/2013, 131/2014 e 181/2014.

Assim, após todos os debates e tramitações legislativas, o PL 4.060/2012 foi transformado na Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento de dados pessoais. A LGPD se inspirou, em sua maior parte, no modelo europeu de proteção de dados pessoais, como as normas que exigem base legal para o tratamento de dados, os princípios gerais, as regras específicas para os dados sensíveis, bem como a criação de uma autoridade nacional para a aplicação da Lei (Mendes; Doneda, 2018, p. 470). Também abrange regras do modelo americano, como a prevista no art. 48 da LGPD, que determina a necessidade de notificar à ANPD os incidentes de segurança, bem como “dialoga com a legislação e cultura jurídica brasileira, tendo as suas normas obtido influências de inúmeras leis do nosso ordenamento” (Mendes; Doneda, 2018, p. 470).

Posteriormente à publicação da LGPD, o STF, em 2020, reconheceu, por meio do referendo na Medida Cautelar na ADI nº 6.387/DF, a proteção de dados pessoais como um direito fundamental autônomo. Em 2022, foi publicada a Emenda Constitucional nº 115, que inseriu, no inciso LXXIX do art. 5º da Constituição da República, o direito fundamental à proteção de dados pessoais.

2.2 Direito fundamental à proteção de dados e interesse público

Anteriormente ao reconhecimento constitucional da proteção de dados pessoais como direito fundamental, a doutrina debatia o tema inserto no conceito de privacidade. Alguns autores diferenciam a privacidade da proteção de dados pessoais. Ao discorrer sobre a privacidade digital, que assim como a privacidade física, é um valor essencial, Garcia *et al.* (2020, p. 13) defendem que a “privacidade se distingue de proteção de dados, e que mesmo um dado público deve ser protegido”.

Outros autores tratam a proteção de dados pessoais como “uma dimensão da privacidade” (Da Silva, 2019, p. 798). Entende-se que “a Constituição Federal de 1988 protege, de maneira esparsa, o direito à privacidade, englobando, segundo a doutrina, a proteção de dados pessoais, tanto no meio físico como digital” (Magrani, 2019, p. 56). Rodotà, em 2008 (p. 92), já afirmava que a privacidade passara a abranger “o direito de manter o controle das próprias informações”.

Nesse cenário anterior à promulgação da Emenda Constitucional n. 115/2022, “a percepção da proteção dos dados pessoais como um direito fundamental autônomo era fruto da constatação da insuficiência de outros institutos para abrigar a tutela integral do indivíduo” (Miranda; Doria; Barbosa, 2022, pp. 330-331). De acordo com a justificativa apresentada ao Senado, a privacidade é o ponto de partida dos debates, mas “já se vislumbra, dadas as suas peculiaridades, uma autonomia valorativa em torno da proteção de dados pessoais, de maneira, inclusive, a merecer tornar-se um direito constitucionalmente assegurado” (Brasil, 2019).

O cenário traçado antes da aprovação da Emenda Constitucional n. 115/2022, portanto, demonstrou a relevância e a utilidade do reconhecimento de um direito fundamental autônomo à proteção de dados no contexto da sociedade contemporânea, tendo em vista sua especificidade face a outros direitos, bem como a atribuição de características que majoram a efetividade da tutela do indivíduo (Miranda; Doria; Barbosa, 2022, p. 332).

Merece previsão específica, eis que o direito à privacidade não é eficaz para resolver todas as lides envolvendo o tratamento de dados pessoais (Miranda; Doria; Barbosa, 2022, pp. 330-331).

Com a publicação da Emenda Constitucional nº 115, de 2022, a proteção de dados pessoais passou a ter status de direito fundamental expressamente previsto na Constituição da

República. Está inserido no rol dos direitos fundamentais previstos no seu art. 5º “o direito à proteção dos dados pessoais, inclusive nos meios digitais” (Brasil, 2022), ao lado dos demais direitos fundamentais.

A proteção de dados pessoais pode ser compreendida sob três teorias diversas: a) a teoria personalista, pela qual os dados pessoais são extensão da personalidade, sendo que o seu uso e compartilhamento interferem no desenvolvimento da personalidade do indivíduo; b) a visão realista, pela qual os dados são passíveis de serem apropriados, sendo objeto de propriedade; e c) uma terceira vertente que entende pela possibilidade de se “aplicar a ideia de patrimonialização gradativa à proteção de dados pessoais, criando uma gradação entre os dados para determinar quando as pessoas podem aceitar a patrimonialização de seus dados e sob quais condições (mais ou menos exigentes)” (Da Silva, 2019, p. 798).

A LGPD prevê, no capítulo IV, que o tratamento de dados pessoais pelas pessoas jurídicas de direito público “deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público” (Brasil, 2018a). Todo o tratamento de dados pessoais realizado pelo Poder Público deverá se pautar no interesse público.

Concomitantemente, a LGPD, já em seu art. 1º, estabelece “o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural” (Brasil, 2018a). O art. 2º prevê, dentre outros, como fundamentos o respeito à privacidade, a inviolabilidade da intimidade, da honra e da imagem, a autodeterminação informativa, os direitos humanos, o livre desenvolvimento da personalidade e a dignidade e exercício da cidadania (Brasil, 2018a).

Consoante se observa dos dispositivos legais, objetiva-se conciliar as normas protetoras do cidadão individualmente considerado, dentre elas o direito fundamental à proteção de dados pessoais, e o interesse público do Poder Público em utilizar dados pessoais para realização de suas atribuições legais. O debate cria duas perspectivas sobre o compartilhamento de dados. “De um lado, aquela que afirma que o amplo compartilhamento de dados no Poder Público propicia a oferta de melhores serviços públicos, a eficiência e a desburocratização; de outro, aquela que chama atenção para os riscos decorrentes de tais iniciativas” (Wimmer, 2021b, p. 132).

Com o objetivo de conciliar a proteção de dados pessoais com o interesse público, é inviável que o Poder Público trate os dados pessoais de forma indiscriminada sob a justificativa do interesse público. Apesar do número crescente de atividades públicas que demandam acesso

a dados pessoais, “alegar o atendimento ao interesse público não é circunstância suficiente para legitimar a transação de dados pessoais” (Silva; Tarter, 2021, p. 461).

Ao contrário, essa interpretação seria razoável para a parte da doutrina que interpreta a supremacia do interesse público como superioridade sobre os demais interesses existentes na sociedade. Contudo, essa visão encontra-se ultrapassada de acordo com a doutrina mais moderna do direito administrativo.

Marçal Justen Filho (2018), apresenta diversas objeções para superar essa interpretação. Primeiro, destaca a dificuldade de definir interesse público. Segundo, refere-se à pluralidade de princípios jurídicos, admitir a supremacia do interesse público não exclui os demais princípios, sendo que todos os princípios têm matriz constitucional com mesmo nível hierárquico, devendo ser aplicados com ponderação para a mais intensa realização de todos eles. Como terceira objeção, descreve a ausência de um único interesse público, os interesses públicos também se colidem e devem ser interpretados com ponderação. Em verdade, o interesse público é o resultado de uma decisão que concilia diversos interesses. A quarta objeção trata da contraposição entre direitos e interesses, devendo-se preservar os direitos subjetivos privados, limitando-os em face do interesse público.

O autor ainda destaca que proteger os direitos fundamentais indisponíveis também é um interesse público, cabendo ao Estado o dever de proteção. Para a proteção, considerando a pluralidade de interesses e direitos fundamentais, não há solução predeterminada e abstrata para todos os conflitos. O processo de concretização das normas “conduzirá à prevalência de interesses, mas sem que a Constituição autorize a solução pura e simples de prevalência de um ‘interesse público’ indeterminado e incerto”, devendo buscar a “solução mais compatível com o ordenamento jurídico e represente o modo mais adequado e satisfatório da realização dos direitos fundamentais protegidos constitucionalmente” (Justen Filho, 2018).

No mesmo sentido, Gustavo Binenbojm (2020, p. 45) sobre a redefinição do princípio da supremacia do interesse público sobre os interesses particulares, destacando a preferência reconhecida aos direitos fundamentais e o dever de ponderação proporcional que preside a atuação estatal no balanceamento entre interesses individuais e objetivos coletivos nos Estados democráticos de direito. Tem-se de dois pilares estruturantes: o sistema democrático e o sistema de direitos fundamentais:

Enquanto o sistema de direitos fundamentais viabiliza a autodeterminação individual, o sistema democrático viabiliza a autodeterminação coletiva, sendo ambas manifestações da autonomia privada e pública dos cidadãos. Todo o debate em torno da legitimidade da autoridade do Estado e do direito converge, hodiernamente, para as relações de interdependência entre esses dois elementos, essenciais para o respeito, proteção e promoção da dignidade da pessoa humana.

(...)

De fato, os direitos fundamentais, em suas múltiplas dimensões, vinculam a atuação e conformam a organização da Administração Pública. Como se sabe, tais direitos podem ser concebidos, sob o ângulo subjetivo, como direitos de defesa e direitos a prestações, apresentando-se, ainda, como direitos à organização e ao procedimento. Ao ângulo objetivo, eles carregam para o Poder Público deveres de proteção e servem como diretriz norteadora da ação administrativa (Bienebojm, 2020, p. 46)

Com isso, cabe à administração pública observar tanto os direitos fundamentais como os objetivos transindividuais, conciliando e ponderando os interesses. Permite-se “um juízo de ponderação, baseado em parâmetros como necessidade e proporcionalidade, para modelar e contrabalançar o interesse privado e o interesse público, estabelecendo a possibilidade de ingerência do Estado sobre direitos fundamentais e liberdades civis, limitando-os” (Vainzof, 2022, RL-1.2).

Especificamente, voltando-se ao direito fundamental à proteção de dados pessoais, Xavier, Xavier e Spaler (2023, RB-18.4) afirmam que, apesar de ser crível que determinada atividade ficaria comprometida sem os dados necessários, permitir o compartilhamento de forma livre e discricionária significa retirar a efetividade da LGPD. Os autores demonstram que as hipóteses de tratamento de dados são amplas e de difícil fiscalização:

Assim, ao permitir que o Estado realize o tratamento de dados sem o consentimento, e até mesmo sem o conhecimento, de seus titulares, sob argumento de que o faz em prol do interesse público, a legislação falha inclusive com os próprios direitos fundamentais de primeira dimensão, que são justamente os direitos relacionados à liberdade, palavra esta que, paradoxalmente, aparece diversas vezes na nova legislação. Igualmente podem ocorrer violações aos direitos fundamentais de quarta dimensão, os quais estão relacionados à sociedade de informação.

Entre avanços e contradições, verifica-se que a nova legislação acabou por conferir amplos poderes à Administração Pública em relação às possibilidades de tratamento de dados com fundamento na execução de políticas públicas, fato que pode, ao menos em hipótese, permitir arbitrariedades e abusos por parte do próprio Estado. É fundamental, portanto, que o assunto seja enfrentado com responsabilidade pelas instituições públicas e privadas (Xavier; Xavier; Spaler, 2023, RB-18.5).

De fato, o poder de compartilhamento de dados pessoais deve ser usado com cautelas pelo Poder Público. A LGPD, ao longo de seu texto, prevê os parâmetros a serem observados para que o compartilhamento de dados pessoais seja legal. Nesse sentido, a ANPD entende que “o uso compartilhado de dados pessoais deve ser realizado em conformidade com a LGPD, notadamente com os princípios, as bases legais, garantia dos direitos dos titulares e outras regras específicas aplicáveis ao Poder Público” (Brasil, 2023a, p. 30). Ou seja, o objetivo da LGPD não é inviabilizar o compartilhamento de dados pessoais, mas permitir esse compartilhamento com proteção aos dados pessoais.

Assim, no compartilhamento de dados pessoais pelo Poder Público, “o interesse público subjacente e inafastável é a preservação dos direitos e garantias fundamentais do administrado, pessoa natural, por ser essa a demanda do bem comum da coletividade” (Tasso, 2022, RL-1.8).

2.3 Governança de dados

A governança de dados é um conceito amplo, que aborda várias áreas do conhecimento com foco na qualidade dos dados. Busca-se uma maturidade na gerência desses recursos – os dados, “melhoria na valoração e produção dos dados, monitoração de seu uso, além de aspectos críticos de segurança, privacidade, ética e aderência a regras de compliance, associadas a eles” (Barbieri, 2019, p. 36).

Para a governança, dados transpassam o domínio da tecnologia para se inserir como ativo organizacional.

Além dos aspectos de volume, velocidade e variedade com que são produzidos, os dados passam a ter outras dimensões na sua análise: a qualidade irrestrita do seu conteúdo, os aspectos legais que os envolvem, a ética com que deverão ser tratados e a capacidade de sua transformação em valores diretos, dentro do conceito de monetização e transformação digital (Barbieri, 2019, p. 33).

Uma Política de Governança de Dados estabelece meios e mecanismos para a resolução bem-sucedida de problemas relacionados a dados, considerando a necessidade das partes interessadas. Para isso, deve-se observar, conforme Barbieri (2019, pp. 161-165):

- a) Levantar e analisar os processos de negócios que tratam dos dados pessoais;

- b) Identificar e catalogar os dados, com detalhamento sobre ciclo de vida;

Nesse ponto, deve-se responder quais dados estão armazenados e qual sua origem, quais são as áreas e os responsáveis por esses dados, quais dados são compartilhados, devendo-se providenciar uma análise desses dados sob o aspecto legal com a demonstração de atendimento à LGPD, definindo, por exemplo, a base legal que sustenta o uso daquele dado.

- c) Definir estratégia de privacidade, segurança e risco;

A análise desse ponto deve ser pautada no questionamento sobre os impactos de um eventual vazamento de dados.

- d) Definir as áreas responsáveis por cada etapa, atribuindo responsabilidade para os envolvidos;

- e) Definir Políticas, Padrões, Processos e Procedimentos;

As Políticas podem ser conceituadas como os objetivos e intenções para resolver determinado problema. Como exemplo, quais políticas serão adotadas para atendimento de solicitações dos cidadãos em relação a seus dados.

Os Padrões são as medidas para se estabelecer e enquadrar o controle desejado. Como exemplo, categorizar os dados, dados pessoais, dados pessoais sensíveis, dados de menores de idade, dados indefinidos.

Os Processos/Procedimentos são o passo-a-passo detalhado para alcançar os objetivos definidos nas Políticas e expressos nos Padrões. Como exemplo, para atendimento de solicitações de cidadãos, além de se estipular em qual formato os dados serão entregues, pode-se exigir a identificação do solicitante e a identificação de quais dados pretende ter acesso.

- f) Considerar, na Metodologia de Desenvolvimento de Sistemas, os aspectos de Privacidade por Design;

- g) Definir a Performance de acordo com medidas e indicadores de controle e de conformidade com as normas;

- h) Considerar a integração da segurança e privacidade dos dados com outras áreas como qualidade dos dados – dados atualizados e precisos; gerência de metadados – dados plenamente descritos com todos seus elementos identificadores; gerência do ciclo de vida dos dados – dados em todo o seu processo e fluxo; e gerência de risco de dados com controle sobre os cenários de riscos.

3 LGPD

O capítulo aborda os principais aspectos da LGPD, trazendo os conceitos necessários à compreensão do tema de compartilhamento de dados pessoais no Poder Público.

3.1 Âmbito de aplicação

Nos termos do art. 1º da LGPD, tem-se que a Lei é aplicável à pessoa natural ou jurídica de direito público ou privado, que realize o tratamento de dados pessoais, sendo aplicável à União, Estados, DF e Municípios (Brasil, 2018a). Ressalta-se que, embora aplicável ao setor público e privado, o legislador reconhece as particularidades de cada setor estabelecendo-se normas gerais e específicas para os diferentes agentes que realizem tratamento de dados pessoais (Miranda; Doria; Barbosa, 2022, p. 335).

Em relação ao Poder Público, recorte do presente estudo, a LGPD dedica o Capítulo IV exclusivamente ao tema para tratar das suas especificidades. Estão inseridas neste Capítulo, as seções “Das Regras” e “Da Responsabilidade”.

Para melhor delimitação do objeto de pesquisa, é relevante entender quais entidades são abrangidas pelo conceito “Poder Público”, à luz da LGPD. De acordo com o art. 23, o capítulo do Poder Público é destinado às pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527/2011. Esse, por sua vez, determina a aplicação aos órgãos públicos integrantes da Administração Direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público, bem como às autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, DF e Municípios (Brasil, 2011b).

Consoante se observa, a norma se aplica tanto à Administração Direta como Indireta dos três Poderes de todas as esferas federativas, União, Estados, DF e Municípios. Como bem anotado no Guia Orientativo, “ao lado de suas funções típicas, tais como as de legislar e aplicar a lei, órgãos dos Poderes Legislativo e Judiciário também exercem atividades administrativas” (Brasil, 2023a, p. 19).

Nos termos do § 4º do art. 23 da LGPD, a disciplina referente ao Poder Público também se estende aos serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público.

Em relação às empresas públicas e sociedades de economia mista, necessário diferenciar o regime de acordo com suas características.

Para aquelas que exercem atividade econômica em regime concorrencial, sujeitas ao art. 173, § 1º da Constituição da República, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado. Admitir o contrário seria conferir tratamento privilegiado às estatais desequilibrando a livre concorrência, princípio da ordem econômica (Tasso, 2022, RL-1.8). Considerando esse regime, estarão sujeitas “a sofrer sanções previstas para empresas privadas nos casos de eventual violação daquilo que estiver estabelecido na LGPD” (Zenkner; Spinelli, 2021, p. 294).

Por sua vez, as empresas públicas e sociedades de economia mista que atuam em regime de monopólio ou que prestam serviço público terão o mesmo tratamento destinado ao Poder Público (Tasso, 2022, RL-1.8).

Tendo em vista o âmbito de aplicação, interessa citar alguns dos destinatários abordados nos documentos analisados pelo presente estudo para exemplificar as diversas hipóteses de âmbito de aplicação:

- a) Diversos destinatários (Parecer nº 00295/2020/CONJUR-CGU/CGU/AGU: a consulta foi realizada pela Corregedoria-Geral da União sobre a possibilidade de compartilhamento com outros órgãos e entidades da administração pública direta, autárquica e fundacional e os demais Poderes da União, dos Estados, Distrito Federal e Municípios. A consulta foi formulada de forma generalizada para englobar os diversos destinatários da norma.);
- b) Órgão Estadual e União (Despacho PGE/PPE Nº 00067/2023 da PGEES: Secretaria de Estado de Segurança Pública e Defesa Social – SESP, órgão do Estado do Espírito Santo, e União, por intermédio da Superintendência Regional da Polícia Federal no Espírito Santo – SR/PF/ES);
- c) Duas entidades da Administração Indireta do mesmo ente (Despacho no Processo E:05101.0000004897/2022 da PGEAL: Departamento de Trânsito do Estado de Alagoas – DETRAN/AL e Departamento de Estradas de Rodagem do Estado de Alagoas – DER/AL, entidades da Administração Indireta do Estado de Alagoas. Como informado no próprio

Despacho, são “entes integrantes da mesma estrutura estatal, ainda que vinculados à Administração Indireta” (Alagoas, 2020, p. 1));

d) Administração Direta e Indireta do mesmo ente (Despacho nº 567/2020 – GAB da PGEGO: Agência Goiana de Defesa Agropecuária – Agrodefesa, entidade da Administração Indireta do Estado de Goiás, e Secretaria de Estado de Agricultura, Pecuária e Abastecimento – Seapa, órgão do Estado de Goiás) e (Parecer nº 258/2021-PGCONS/PGDF: Procuradoria-Geral do Distrito Federal, órgão do DF, e Companhia de Saneamento Ambiental do Distrito Federal – Caesb, entidade da Administração Indireta do DF);

e) Administração Indireta do Estado e Administração Direta dos Municípios (Parecer PGE/MS/CJUR-RESIDUAL/nº 0002/2022 da PGEMS: Junta Comercial de Mato Grosso do Sul – Jucems, entidade da Administração Indireta do Estado do Mato Grosso do Sul, e Municípios do Estado do Mato Grosso do Sul);

f) Órgãos de um mesmo ente federado (Parecer nº 000961/2020 da PGEPA: Procuradoria-Geral do Estado do Pará e Secretaria de Estado da Fazenda – Sefa, órgãos do Estado do Pará);

g) Poderes diferentes (Parecer PGE/PG-02/ASS/PARECER/RCG nº 35/2022 da PGERJ: Procuradoria-Geral do Estado do Rio de Janeiro, órgão do Poder Executivo, e Corregedoria Geral da Justiça do Tribunal de Justiça do Estado do Rio de Janeiro, órgão do Poder Judiciário); e (Parecer nº 090/21-PGE da PGESC: Tribunal de Contas do Estado de Santa Catarina, órgão do Poder Legislativo, e Secretaria de Estado de Saúde do Estado de Santa Catarina, órgão do Poder Executivo).

Consoante se observa dos exemplos citados, diversas são as possibilidades de acordos firmados pelo Poder Público envolvendo os diversos destinatários da LGPD.

3.2 Dados pessoais e dados pessoais sensíveis

A LGPD protege os dados pessoais, aplicando-se “ao tratamento de dados em estado físico ou *off-line*, migrando ou não, posteriormente, para o meio digital ou *on-line*” (Vainzof, 2022, RL-1.2).

O dado pessoal pode ser conceituado sob duas orientações principais, reducionista e expansionista. A primeira delimita o dado pessoal àquele associado a uma pessoa específica, permitindo “estabelecer de forma imediata ou direta um vínculo com o seu titular,

individualizando-o de forma precisa” (Bioni, 2015, p. 17). Para a orientação expansionista, dado pessoal “pode ser qualquer tipo de informação que permita a sua identificação, ainda que o vínculo entre o dado e um indivíduo não seja estabelecido de prontidão, mas de forma mediata ou indireta” (Bioni, 2015, p. 17).

De acordo com a letra da Lei, adotando-se uma visão expansionista, dado pessoal é a “informação relacionada a pessoa natural identificada ou identificável” (Brasil, 2018), ou seja, o dado protegido pela LGPD “é aquele dado que individualiza uma pessoa natural ou indica características que propiciam sua individualização” (Pironti; Tesseroli, 2021, p. 397).

O primeiro ponto é que a LGPD protege os dados das pessoas naturais e não das pessoas jurídicas. Dado pessoal é a identificação de uma pessoa natural, referindo-se a “identificadores únicos das pessoas” (Da Silva, 2019, p. 800), “como o nome da pessoa física, o número do seu RG ou outro documento, ou algo que possa levar à identificação de uma pessoa (capaz de identificar uma pessoa), por exemplo, a data de nascimento, o endereço, a geolocalização ou até mesmo a soma de informações” (Teixeira, 2021, p. 222).

Nem todos os dados pessoais são protegidos pela LGPD, não estando sujeitos a ela “os dados tratados por uma pessoa natural sem qualquer finalidade econômica, ou aqueles utilizados para fins artísticos, jornalísticos e acadêmicos” (Garcia *et al.*, 2020, p. 16), bem como os realizados para segurança pública e segurança do Estado, defesa nacional, atividades de investigação e repressão de infrações penais. Também se excluem da aplicação da LGPD o tratamento de dados pessoais que tenham origem fora do território nacional, que não sejam objeto de comunicação, uso compartilhado ou transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD (Brasil, 2018a).

Para além do conceito de dado pessoal, a LGPD traz também o dado pessoal sensível, que é aquele “sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (Brasil, 2018a). São dados “que podem acarretar discriminações, caso se tornem públicos” (Da Silva, 2019, p. 801) e, por essa razão, merecem um nível de proteção maior. Nas palavras de Doneda (2021, RB-2.3), “a diferenciação conceitual dos dados sensíveis atende a uma necessidade de estabelecer uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior”.

Consoante se analisará no Capítulo cinco, o tratamento de dados pessoais e de dados pessoais sensíveis é abordado em artigos diferentes da LGPD, eis que cada caso demanda um tipo de proteção, sendo a do dado pessoal sensível mais restrita.

3.3 Tratamento de dados pessoais

O tratamento de dados pessoais é toda operação realizada com dados pessoais. A LGPD apresentou um rol de operações de tratamento, constando as atividades de “coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (Brasil, 2018a).

Trata-se de um rol exemplificativo, podendo “haver outras hipóteses não previstas pela lei relacionadas com dados pessoais que serão tidas por tratamento de dados” (Teixeira, 2021, p. 223). Nesse conceito se insere o compartilhamento de dados pessoais ou a sua transferência ou, ainda, a concessão de acesso a sistemas. Os cidadãos cadastram seus dados pessoais em sistemas ou banco de dados de pessoas naturais ou jurídicas. Estes, por sua vez, compartilham ou transferem esses dados ou concedem acesso a terceiros.

Tangencia esse conceito o uso secundário de dados pessoais que consiste na “utilização de dados pessoais para finalidades distintas daquelas que justificaram originalmente sua coleta” (Wimmer, 2021b, p. 124), que também deve ser debatido no presente estudo.

Especificamente quanto ao Poder Público, a LGPD criou, ainda, a figura do uso compartilhado de dados, que é um tipo de tratamento, mas com características específicas relacionadas ao Poder Público. O uso compartilhado de dados é entendido como “comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos [...] ou entre esses e entes privados” (Brasil, 2018a).

De acordo com a ANPD, o compartilhamento de dados pessoais é “a operação de tratamento pela qual órgãos e entidades públicos conferem permissão de acesso ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas visando ao atendimento de uma finalidade pública” (Brasil, 2023a, p. 29).

4 COMPARTILHAMENTO

Com o objetivo de encontrar os parâmetros utilizados pelo Poder Público para o compartilhamento de dados pessoais entre seus órgãos e entidades, buscou-se estudar como os principais atores responsáveis pela definição desses parâmetros têm tratado o tema, sendo a ANPD, o STF e as advocacias públicas da União, do DF e de todos os Estados da Federação. Cada um desses atores será apresentado em subcapítulo próprio.

4.1 O papel dos atores envolvidos na definição dos requisitos de compartilhamento de dados pessoais sensíveis

Antes de se adentrar no papel de cada ator envolvido na definição dos requisitos de compartilhamento de dados pessoais no Poder Público, é necessário registrar que há outros atores relevantes no processo de compartilhamento de dados pessoais. A título de exemplo, cita-se os órgãos de controle da União, do DF e dos Estados, tais como as Controladorias-Gerais e os Tribunais de Contas.

Nada obstante, como recorte necessário ao desenvolvimento do presente estudo, considerou-se aqueles atores que participam do processo inicial do compartilhamento de dados pessoais. Quer dizer, os atores que atuam na definição de requisitos gerais, como a ANPD e o STF, e os atores que atuam desde a instauração do procedimento para o compartilhamento até sua efetiva formalização, como as advocacias públicas.

Passa-se então ao papel desenvolvido por cada um desses atores.

4.1.1 A Autoridade Nacional de Proteção de Dados – ANPD

A ANPD foi criada, na redação original da LGPD, como órgão da administração pública federal integrante da Presidência da República. Considerando a necessidade de independência na atuação fiscalizatória, a Lei nº 13.853/2019 introduziu, no § 1º do art. 55-A, a possibilidade de a ANPD ser transformada pelo Poder Executivo em entidade com regime autárquico especial (Brasil, 2018a).

A independência da autoridade, “atributo intrínseco à própria razão de ser de uma autoridade de proteção de dados, pode ser garantida por meio de mecanismos que busquem isolar sua atuação da influência dos poderes estatais constituídos na administração pública direta” (Doneda, 2023b, p. 466). Está relacionada a que suas atividades fiscalizatórias, sancionatórias e de decisão não estejam subordinadas a outros órgãos, devendo contar com mandato fixo de seus dirigentes, para que as funções sejam executadas de forma autônoma (Doneda, 2023b, p. 468).

Como exemplo de normas que propiciam a independência, Doneda cita gerência sobre o orçamento e estrutura, limitação da discricionariedade para escolha de seus membros, incompatibilidade de atuação dos membros com outras atividades, atuais e futuras, entre outras (Doneda, 2023b, pp. 466-467).

Em 2022, a mera possibilidade de transformação em autarquia foi alterada para criação de autarquia por determinação legal. A Medida Provisória nº 1.124/2022, convertida na Lei nº 14.460/2022, alterou a redação do art. 55-A da LGPD para determinar a criação da ANPD como autarquia de natureza especial, dotada de autonomia técnica e decisória.

Assim, além do regime autárquico de natureza especial, a LGPG adotou diversas medidas com o objetivo de prestigiar a independência da ANPD. Visando impor limites à discricionariedade na escolha de seus membros, estruturou-se o Conselho Diretor, órgão máximo de direção. Seus membros devem ser escolhidos dentre brasileiros com reputação ilibada, nível superior de educação e elevado conceito na área do cargo que será ocupado. São escolhidos e nomeados pelo Presidente da República após aprovação do Senado Federal, desempenham mandato de 4 anos e somente perderão seus cargos em razão de renúncia, condenação judicial transitada em julgado ou demissão decorrente de processo administrativo disciplinar (Brasil, 2018a).

Também restou determinada a incompatibilidade de atuação dos seus membros com outras atividades, eis que são a eles aplicáveis as disposições do art. 6º da Lei nº 12.813/2013, denominado período de quarentena:

Art. 6º Configura conflito de interesses após o exercício de cargo ou emprego no âmbito do Poder Executivo federal:

I - a qualquer tempo, divulgar ou fazer uso de informação privilegiada obtida em razão das atividades exercidas; e

II - no período de 6 (seis) meses, contado da data da dispensa, exoneração, destituição, demissão ou aposentadoria, salvo quando expressamente autorizado, conforme o caso, pela Comissão de Ética Pública ou pela Controladoria-Geral da União:

a) prestar, direta ou indiretamente, qualquer tipo de serviço a pessoa física ou jurídica com quem tenha estabelecido relacionamento relevante em razão do exercício do cargo ou emprego;

b) aceitar cargo de administrador ou conselheiro ou estabelecer vínculo profissional com pessoa física ou jurídica que desempenhe atividade relacionada à área de competência do cargo ou emprego ocupado;

c) celebrar com órgãos ou entidades do Poder Executivo federal contratos de serviço, consultoria, assessoramento ou atividades similares, vinculados, ainda que indiretamente, ao órgão ou entidade em que tenha ocupado o cargo ou emprego; ou

d) intervir, direta ou indiretamente, em favor de interesse privado perante órgão ou entidade em que haja ocupado cargo ou emprego ou com o qual tenha estabelecido relacionamento relevante em razão do exercício do cargo ou emprego (Brasil, 2013b).

Em relação à gerência sobre seu patrimônio e estrutura, a LGPD determinou que a ANPD tem patrimônio próprio e autonomia técnica e decisória. Ou seja, a Lei criou mecanismos para efetivar a independência da ANPD.

A ANPD, elemento substancial para a garantia da eficácia da LGPD (Doneda, 2023b, p. 461), tem sua competência definida no art. 55-J da LGPD. No tocante ao Poder Público, há funções normativas da ANPD relacionadas à elaboração de diretrizes para observância da LGPD, bem como normas de fiscalização das atividades desempenhadas com dados pessoais pelo Poder Público.

Nas atribuições normativas, cabe à ANPD elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, editar regulamentos e procedimentos sobre proteção de dados pessoais, deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da LGPD (Brasil, 2018a). A função regulamentar “é fundamental, tanto para viabilizar o cumprimento da nova lei quanto para uniformizar a interpretação desses dispositivos e evitar que a lei chegue ao Judiciário e comece a gerar entendimentos conflitantes” (Reis; Chede, 2021, p. 369).

Nas atribuições fiscalizatórias, cabe à ANPD solicitar às entidades do Poder Público que realizem operações de tratamento de dados pessoais informações sobre o âmbito, a natureza dos dados e os detalhes do tratamento realizado, bem como realizar auditorias ou determinar a sua realização sobre o tratamento de dados pessoais (Brasil, 2018a).

Consoante se observa, a ANPD desempenha papel normativo e fiscalizatório sobre o tratamento de dados pessoais realizado pelo Poder Público. A LGPD ainda determina que a ANPD tem prevalência sobre as competências de outras entidades e órgãos da administração pública.

Com base nessa competência, bem como considerando que muitos órgãos e entidades já vinham questionando a ANPD sobre questões afetas à interpretação da LGPD em relação ao setor público (Brasil, 2023a, p. 5), foi publicado, em janeiro de 2022, o Guia Orientativo – Tratamento de dados pessoais pelo Poder Público – versão 1.0, sendo revisado e republicado em junho de 2023 na versão 2.0.

O Guia Orientativo bem sintetizou o papel da ANPD, “órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para sua implementação” (Brasil, 2023a, p. 8), com competência originária, específica e uniformizadora quanto à proteção de dados pessoais e à aplicação da LGPD. Destacou, ainda, a competência exclusiva da ANPD “para aplicar as sanções administrativas previstas na LGPD” (Brasil, 2023a, p. 8).

4.1.2 O Supremo Tribunal Federal – STF

O papel do STF, guardião da Constituição da República, é relevante para o presente estudo 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” (Langenegger, 2023, p. 28).

Como já afirmado em capítulos anteriores, a Constituição da República passou a disciplinar, no inciso LXXIX do art. 5º, com a publicação da Emenda Constitucional nº 115/2022, o direito fundamental à proteção de dados pessoais.

Antes mesmo da previsão expressa como direito fundamental, o STF, em maio de 2020, “proferiu uma decisão histórica para o desenvolvimento da disciplina jurídica relativa à proteção de dados pessoais no Brasil” (Mendes; Rodrigues Jr.; Da Fonseca, 2023, pp. 61-62). Trata-se do referendo na Medida Cautelar na ADI nº 6.387/DF, que suspendeu a eficácia da Medida Provisória nº 954/2020, que determinava o compartilhamento de dados por empresas de telecomunicações prestadoras de serviços telefônicos com o IBGE para fins de produção estatística durante a situação de emergência de saúde pública decorrente do coronavírus (covid-19).

A decisão trouxe o “reconhecimento de um direito fundamental à proteção de dados pessoais como direito autônomo, extraído a partir de leitura sistemática do texto constitucional brasileiro” (Mendes; Rodrigues Jr.; Da Fonseca, 2023, p. 62). A promulgação posterior da EC nº 115/2022 validou a orientação jurisprudencial do STF, sendo que a positivação de um novo direito fundamental demanda um processo de aprimoramento jurisprudencial (Mendes; Rodrigues Jr.; Da Fonseca, 2023, p. 70).

Em relação às interpretações jurisprudenciais sobre o tema específico do presente estudo, o STF novamente se manifestou de forma específica desenvolvendo um papel primordial na determinação dos requisitos mínimos para o compartilhamento de dados pessoais pelo Poder Público.

Trata-se da decisão no julgamento conjunto da ADI 6649 e da ADPF 695 do STF. O julgamento abordou o Decreto nº 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados, que teve sua constitucionalidade questionada na Ação Direta de Inconstitucionalidade nº 6649. Em decorrência do referido Decreto, foi noticiado ato de compartilhamento de dados pessoais, constantes da Carteira Nacional de Habilitação (CNH), para a Agência Brasileira de Inteligência (ABIN) e o Serviço Federal de Processamento de Dados (Serpro), questionado na Arguição de Descumprimento de Preceito Fundamental nº 695. No acórdão, o STF, em julgamento conjunto, indicou os requisitos pertinentes ao compartilhamento de dados pessoais.

Como afirmado pelo Ministro Relator Gilmar Mendes, o julgamento permitiu que o STF se debruce sobre o regime jurídico de compartilhamento de dados pessoais no Poder Público, colocando em perspectiva “uma questão de crucial importância para qualquer sociedade democrática contemporânea, qual seja, o alcance, os limites e a fisionomia do direito à autodeterminação informativa” (Brasil, 2023b, p. 7).

4.1.3 As advocacias públicas

A advocacia pública, com status constitucional de função essencial à Justiça, tem como objetivo exercer a consultoria e assessoramento jurídico do Poder Executivo (Brasil, 1998). Dessa forma, as advocacias públicas da União, do DF e dos Estados têm a função primordial de auxiliar seus respectivos entes no exercício de suas atribuições legais e execução de políticas

públicas, apresentando soluções para resolução de dúvidas jurídicas relacionadas às funções do Poder Executivo.

Sobre o papel das advocacias públicas nos processos de compartilhamento de dados pessoais, inicialmente, é relevante registrar que, nos termos do Guia Orientativo, a própria ANPD destaca que sua atuação deve ocorrer de forma coordenada e articulada com outros órgãos e entidades.

Para melhor compreensão, é necessário adentrar, de forma sucinta, em um dos requisitos expostos no Guia Orientativo. A ANPD recomenda “a instauração de processo administrativo, do qual constem os documentos e as informações pertinentes, incluindo análise técnica e jurídica, conforme o caso, que exponham a motivação para a realização do compartilhamento e a sua aderência à legislação em vigor” (Brasil, 2023a, p. 30).

Consoante se observa, há recomendação para análise jurídica em cada processo administrativo instaurado para o compartilhamento de dados pessoais, sendo que esta análise jurídica é formulada justamente pelas advocacias públicas da União, do DF e dos Estados da Federação. Cada ente federado possui, em sua estrutura, um órgão jurídico com competência para analisar todos os ajustes formalizados pelo respectivo ente à luz do ordenamento jurídico, inclusive em relação à LGPD.

Além do mais, a ANPD recomenda que o compartilhamento seja formalizado por ato formal, como contratos, convênios ou instrumentos congêneres, ou decisão administrativa ou mesmo ato normativo interno (Brasil, 2023a, pp. 30-31). Esses ajustes, antes de serem celebrados pelos órgãos e entidades da administração pública, são encaminhados às advocacias públicas para análise de sua viabilidade e determinação dos requisitos necessários a sua formalização.

Assim, as advocacias públicas, ao analisar os ajustes encaminhados e demais dúvidas jurídicas referentes à aplicação da LGPD pelo Poder Público, têm emitido manifestações jurídicas sobre o tema. Segundo o Enunciado nº 3 do Manual de Boas Práticas Consultivas da Advocacia Geral da União – BPC/AGU, o exame e a aprovação das minutas de acordos, convênios, ajustes e instrumentos congêneres “devem ser realizados sempre por meio de Parecer, visto ser necessário que o Órgão Consultivo demonstre a apreciação de todos os elementos indispensáveis à contratação” (Brasil, 2016, p. 24).

Ainda que citado Manual tenha sido editado à luz da Lei nº 8.666/93, a Nova Lei de Licitações tratou do tema de forma similar. No seu art. 184 previu que suas disposições se

aplicam, no que couber, aos convênios, acordos, ajustes e instrumentos congêneres, tendo o art. 53 determinado a análise pelo órgão de assessoramento jurídico da Administração, que realizará controle prévio de legalidade mediante análise jurídica (Brasil, 2021).

Na análise jurídica a ser elaborada pelas advocacias públicas está inserida a conformidade com a LGPD dos ajustes firmados entre órgãos e entidades do Poder Público para o compartilhamento de dados pessoais. Esses ajustes preveem as cláusulas necessárias ao objeto pactuado dispondo sobre as obrigações do órgão/entidade cedente e do órgão/entidade recebedor de dados pessoais.

Nesse sentido, o Guia da Política de Governança Pública, da Presidência da República, inseriu as assessorias jurídicas no Capítulo VI – O papel dos demais atores e estruturas de governança. As assessorias jurídicas desempenham um papel primordial, que extrapola o mero controle de legalidade. Desenvolve-se por meio da atuação conjunta aos gestores públicos, da proposta de soluções jurídicas para a legalidade dos atos administrativos e do monitoramento de padrões de judicialização das atividades da organização (Brasil, 2018b, p. 77).

Sobre a relevância das assessorias jurídicas na governança pública:

Os advogados públicos podem ser partes ativas na construção de soluções jurídicas mais adequadas ao cumprimento dos objetivos da organização, em constante cooperação com os gestores públicos. Logo, a boa governança requer uma advocacia pública estável e permanente, que compreenda profundamente as atividades desempenhadas pela organização e os resultados por ela pretendidos.

[...] as assessorias jurídicas desempenham papel relevante para o sucesso da política de governança, por auxiliarem a administração pública no desenvolvimento de políticas mais efetivas a partir de uma constante melhoria regulatória (Brasil, 2018b, p. 77)

Na União, conforme o Manual de Boas Práticas Consultivas da Advocacia Geral da União – BPC/AGU, destaca-se que a sua atuação consultiva se dá por meio do assessoramento e orientação às autoridades e dirigentes do Poder Executivo “mediante exteriorização de manifestação voltada a conferir segurança jurídica à atuação administrativa, visando à efetivação das políticas públicas” (Brasil, 2016, p. 78), devendo-se observar os direitos e garantias fundamentais do cidadão, dentre os quais se enquadra a proteção de dados pessoais.

Da mesma forma, o DF e os Estados trazem normas orientadoras sobre a atuação de seus órgãos de assessoramento jurídico. A título de exemplo, para melhor compreensão da estrutura dos órgãos de assessoramento jurídico, cita-se a Procuradoria-Geral do Distrito

Federal, que tem a função constitucional de “prestar orientação jurídico-normativa para a administração pública direta, indireta e fundacional” (Distrito Federal, 1993), de acordo com o art. 111, inciso VI, da Lei Orgânica do Distrito Federal.

De acordo com o Plano Estratégico PGDF 2020-2025, 1º versionamento, como processos primários finalísticos do órgão, encontra-se o apoio jurídico ao Governo do Distrito Federal e a colaboração para a implementação de políticas públicas (Distrito Federal, 2021b, p. 15).

Na Procuradoria-Geral do Distrito Federal, a Procuradoria-Geral do Consultivo da Procuradoria-Geral do Distrito Federal, órgão central do Sistema Jurídico do Distrito Federal, tem atribuição de responder os questionamentos jurídicos formulados por todos os órgãos, autarquias e fundações do Distrito Federal (Distrito Federal, 2021a).

5 ABORDAGEM METODOLÓGICA

Com o objetivo de elucidar a pergunta de pesquisa proposta, foi realizada pesquisa bibliográfica, analisando os aspectos relevantes à compreensão e aprofundamento do tema. A pesquisa bibliográfica perpassou todos os capítulos do presente estudo. Para aprofundamento sobre os parâmetros e orientações para o compartilhamento de dados pessoais no Poder Público, foi realizada análise documental do Guia Orientativo da ANPD, da decisão no julgamento conjunto da ADI 6649 e da ADPF 695 do STF e de manifestações jurídicas das advocacias públicas.

A análise dos documentos contou com o auxílio da ferramenta *Atlas.ti*. Inicialmente, foram criados códigos embasados nos parâmetros do Guia Orientativo da ANPD e da decisão no julgamento conjunto da ADI 6649 e da ADPF 695 do STF. Com esses códigos, os demais documentos foram analisados por meio de processo dedutivo para entender quais parâmetros se repetem e se há novos parâmetros expostos pelas advocacias públicas.

Além do mais, o estudo bibliográfico contou com uma abordagem das normas de governança incidentes sobre o tema, constantes no Guia da Política de Governança Pública, da Presidência da República, e no Referencial Básico de Governança Organizacional para organizações públicas e outros entes jurisdicionados ao TCU, do Tribunal de Contas da União.

5.1 Dados analisados

Com a finalidade de compreender o tema sobre o compartilhamento de dados pessoais na Administração Pública, a pesquisa foi desenvolvida nas seguintes etapas:

a) Primeira etapa: análise da LGPD e do Guia Orientativo para formulação de tabela com os requisitos exigidos e correlação com os princípios da LGPD (Tabela 1).

Tabela 1: Requisitos exigidos e correção com os princípios da LGPD

REQUISITOS	DESDOBRAMENTOS	DEFINIÇÃO	ARTIGO DA LGPD	PRINCÍPIO
Geral	Conformidade à LGPD.	-	-	-
Formalização e Registro	Instauração de processo administrativo, com documentos, análise técnica e jurídica, motivação e aderência à legislação.	Formalizado em atenção às normas gerais que regem os procedimentos administrativos e em atenção à obrigatoriedade de registro das operações de tratamento.	Art. 37.	-
	Estabelecido em ato formal (recomendação).	Contratos, convênios ou instrumentos congêneres.		
		Decisão administrativa.		
		Ato normativo interno (padronização e celeridade).		
Objeto	-	Indicação dos dados de forma objetiva e detalhada, limitando-se ao que for estritamente necessário às finalidades do tratamento.	Art. 6º, III.	Princípio da necessidade.

REQUISITOS	DESDOBRAMENTOS	DEFINIÇÃO	ARTIGO DA LGPD	PRINCÍPIO
Finalidade	Deve ser específica com indicação precisa de qual iniciativa, ação ou programa será executado ou, ainda, de qual atribuição legal será cumprida mediante o compartilhamento dos dados pessoais: deixar claro por que e para que os dados serão compartilhados.	“Propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”.	Arts. 6º, I, e 26.	Princípio da finalidade.
	Compatibilidade entre a finalidade original da coleta e a finalidade do compartilhamento dos dados.	-	Art. 6º, II.	Princípio da adequação.
Base legal	Ato formal deve indicar a base legal (recomendação).	-	Arts. 7º, 11 e 26.	Princípio da finalidade: finalidade pública legítima, ou seja, amparada em uma base legal.
Duração do tratamento	Estabelecer, de forma expressa, o período de duração do uso compartilhado dos dados.	Processo com duração definida, após o qual, em regra, os dados pessoais devem ser eliminados.	Art. 6º, IV.	Princípio do livre acesso.
	Possibilidade de conservação ou se os dados devem ser eliminados após o término do tratamento.			
	Reavaliação periódica do instrumento que autorizou o compartilhamento.			
Transparência e direito dos titulares	Divulgar, na página eletrônica dos órgãos e das entidades responsáveis, as informações pertinentes (boa prática).	Disponibilização de informações claras, precisas e facilmente acessíveis aos titulares sobre a realização do compartilhamento e sobre como exercer seus direitos.	Arts. 6º, VI, e 23, I.	Princípio da transparência.
	Obrigações das partes delimitadas para divulgar as informações exigidas pela LGPD (recomendação).			
	Obrigações das partes no que se refere às responsabilidades e aos procedimentos a serem observados visando ao atendimento de solicitações apresentadas pelos titulares (recomendação).			

REQUISITOS	DESDOBRAMENTOS	DEFINIÇÃO	ARTIGO DA LGPD	PRINCÍPIO
Prevenção e segurança	Devem ser proporcionais aos riscos às liberdades civis e aos direitos fundamentais dos cidadãos envolvidos no caso concreto.	Estabelecer as medidas de segurança, técnicas e administrativas, que serão adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.	Arts. 6º, VII e VIII, e 46.	Princípio da prevenção e da segurança.
	Devem estar previstas nos atos que autorizam o compartilhamento.			
Outros requisitos	Novo compartilhamento ou transferência posterior dos dados: pode vedar a realização de novo compartilhamento ou autorizá-lo sob determinadas condições.	-	-	-
	Ônus financeiro: indicar a remuneração a ser paga ou prever que não haverá transferência de recursos financeiros na hipótese.	-	-	-
	Elaboração de relatório de impacto à proteção de dados pessoais, caso necessário.	-	Art. 5º, XVII.	-
	Identificar as funções e responsabilidades dos agentes de tratamento envolvidos no uso compartilhado de dados pessoais.	-	-	-

Fonte: elaboração própria.

b) Segunda etapa: Com base nos requisitos, formulou-se a devida codificação, inserindo na ferramenta *Atlas.ti* um grupo de códigos por requisito apresentado no Guia Orientativo. Dentro de cada grupo de código, foram inseridos códigos para os desdobramentos, definições e artigos citados da LGPD. Dentro da ferramenta, os códigos foram criados com cor igual do grupo de código para melhor análise e visualização dos requisitos.

c) Terceira etapa: Análise da decisão no julgamento conjunto da ADI 6649 e da ADPF 695 do STF para complementação dos requisitos apresentados no Guia Orientativo. Dessa análise, percebe-se uma uniformidade de tratamento do tema, com requisitos, em sua maioria,

convergentes na Decisão e no Guia Orientativo da ANPD. Formulou-se a seguinte tabela (Tabela 2):

Tabela 2: Comparação entre requisitos STF e ANPD

STF	ANPD
Eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados.	Requisito presente no Guia Orientativo em Finalidade.
Compatibilidade do tratamento com as finalidades informadas.	Requisito presente no Guia Orientativo em Finalidade.
Limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada.	Requisito presente no Guia Orientativo em Objeto.
Cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na LGPD, no que for compatível com o setor público.	Requisito presente no Guia Orientativo sob a forma de “Conformidade à LGPD”.
Publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais com informações claras e atualizadas, preferencialmente em seus sítios eletrônicos.	Requisito presente no Guia Orientativo em Transparência e direitos dos titulares.
Adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público.	Requisito presente no Guia Orientativo em Objeto.
Instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário.	Requisito presente no Guia Orientativo em Formalização e registro.
Utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso.	No Guia Orientativo, há previsão de registro das operações de tratamento em Formalização e registro. O STF exige não só o registro da operação que foi realizada, mas o registro de acesso de cada pessoa que acessar o dado pessoal.

Fonte: elaboração própria.

Consoante se observa, há como correlacionar os requisitos apontados pelo STF com aqueles dispostos no Guia Orientativo. O STF aprofundou o debate sobre cada requisito, considerando que a decisão visa justificar a exigência de cada um, diferente do contexto do Guia Orientativo, que, como Guia, apresenta uma visão mais sucinta.

Com essas informações, inseriu-se então novo código denominado como “registro de acesso” para aqueles casos em que foi exigido que o sistema apresentasse o registro de cada pessoa que acessou determinado dado pessoal dentro do grupo de código “STF”. O detalhamento do referido código será abordado no subcapítulo próprio.

d) Quarta etapa: Coleta e análise dos documentos jurídicos elaborados pelas advocacias públicas. Registra-se que foram pesquisados todos os sítios eletrônicos das advocacias públicas da União, do DF e dos Estados. Recorda-se, no ponto, que, para aqueles Estados que não têm sistemas disponíveis de pesquisa de pareceres ou que não publicam suas manifestações nos sítios eletrônicos, foi necessário entrar em contato por todos os meios legais disponíveis, tais como e-mails constantes nas páginas eletrônicas, canais de Ouvidoria e Fale Conosco, Canal Fala.BR do gov.br. Nesses casos, foi iniciado processo em cada um desses Canais para acesso às informações necessárias ao desenvolvimento da pesquisa, com as devidas reiteraões de solicitações e recursos até o atendimento da demanda. Com isso, anota-se que os dados obtidos foram aqueles encontrados nos sítios eletrônicos de pesquisa ou encaminhados pelas advocacias públicas em resposta às demandas através dos meios citados, ou seja, a pesquisa não é exaustiva, podendo haver outros documentos jurídicos não abarcados na análise.

É relevante registrar também que foi necessário realizar um recorte temporal dos documentos encontrados. Apesar de a LGPD ter entrado em vigor em setembro de 2020, considerou-se os documentos produzidos a partir de sua publicação, tendo em vista que alguns deles já traziam disposições da LGPD como sugestões. Como recorte final ficou definida a data de janeiro de 2024.

Com os dados encontrados, elaborou-se a seguinte tabela:

Tabela 3: Lista de documentos jurídicos das advocacias públicas

ADVOCA CIA PÚBLICA	FORMA DE LOCALIZAÇÃO	DOCUMENTO
AGU	https://repositorio.cgu.gov.br/	Parecer n° 00295/2020/CONJUR-CGU/CGU/AGU
		Parecer n° 00304/2023/CONJUR-CGU/CGU/AGU
AGE/MG	https://advocaciageral.mg.gov.br/legislacoes/pareceres/ e https://advocaciageral.mg.gov.br/fale-conosco/	Parecer 16.164, de 20/12/2019
		Parecer 16.393, de 15/10/2021

ADVOCA CIA PÚBLICA	FORMA DE LOCALIZAÇÃO	DOCUMENTO
PGE/AC	http://www.pge.ac.gov.br/ouvidoria/ , janete.melo@ac.gov.br e http://esic.ac.gov.br/sistema/site/index.html?ReturnUrl=%2fsistema%2fPedido%2fRegistroPedido.aspx	Sem resposta.
PGE/AL	https://e-ouv.al.gov.br/	Despacho no Processo E:05101.0000004897/2022 Despacho no Processo E:13020.0000001113/2023 Parecer Jurídico – DETRAN - CJUR nº 092/2022
PGE/AM	Formulário para Assuntos em Geral do Fale Conosco do Site da PGE/AM e https://falabr.cgu.gov.br/web/login?tipo=8&step=2&redirect=/manifestacao/criar?tipo=8%26step=2	Não se manifestou sobre o tema.
PGE/AP	https://ouvamapa.portal.ap.gov.br/login	Não se manifestou sobre o tema.
PGE/BA	https://www.ouvidoria.ba.gov.br/ e pa.pareceres@pge.ba.gov.br	Parecer nº PA-NPE-320-2023
PGE/CE	ouvidoria@pge.ce.gov.br e https://cearatransparente.ce.gov.br/portal-da-transparencia/ouvidoria?locale=pt-BR	Não se manifestou sobre o tema.
PGDF	http://parecer.pg.df.gov.br/#	Parecer nº 592/2022-PGCONS/PGDF Parecer nº 258/2021-PGCONS/PGDF Parecer nº 112/2021-PGCONS/PGDF
PGE/ES	faleconosco@pge.es.gov.br	Despacho PGE/PPE nº 00067/2023 Parecer PGE/PCA nº 00103/2022 Despacho PGE/PCA Nº 00196/2022
PGE/GO	https://goias.gov.br/procuradoria/orientacoes/	Despacho nº 2232/2020 – GAB Despacho nº 567/2020 – GAB
PGE/MA	http://www.ouvidorias.ma.gov.br/Ouvidorias/publico/Manifestacao/RegistrarManifestacao.aspx?ReturnUrl=%2fOuvidorias%2f	Não se manifestou sobre o tema.
PGE/MS	https://www.lgpd.ms.gov.br/legislacao-pareceres-minutas-2/pareceres/ e https://www.pge.ms.gov.br/pareceres-referenciais-pge-ms/	Parecer PGE/MS/PAA/nº 049/2021 Parecer PGE/MS/CJUR-RESIDUAL/nº 0002/2022
PGE/MT	https://ouvidoria.cge.mt.gov.br/falecidadao/	Parecer 695/SGACI/2021
PGE/PA	https://www.pge.pa.gov.br/publicacoes/em-ententario-geral-pareceres e Serviço de Informação ao Cidadão (sic@pge.pa.gov.br)	Parecer nº 000685/2021 Parecer nº 000961/2020 Parecer nº 010096/2019
PGE/PB	atendimentopgepb@gmail.com e https://ouvidoria.pb.gov.br/	Não se manifestou sobre o tema.

ADVOCA CIA PÚBLICA	FORMA DE LOCALIZAÇÃO	DOCUMENTO
PGE/PE	https://www.pge.pe.gov.br/ouvidoria.aspx , procuradoria.consultiva@pge.pe.gov.br e https://www2.lgpd.pe.gov.br/login	Parecer nº 0645/2023
		Parecer nº 0447/2021
PGE/PI	https://portal.pi.gov.br/pge/fale-conosco/ e https://falabr.cgu.gov.br/web/login?tipo=8&step=2&redirect=/manifestacao/criar?tipo=8%26step=2	Não se manifestou sobre o tema.
PGE/PR	https://www.pge.pr.gov.br/Pagina/Pareceres-juridicos-em-tabela-unica	Parecer Referencial nº 04/2022-PGE
PGE/RJ	https://www.gov.br/pt-br e https://documentacao.pge.rj.gov.br/bnportal/pt-BR/search?exp=%3E	Parecer PGE/PG-02/ASS/PARECER/RCG nº 35/2022
		Parecer nº 1/2023/PGE/PG02/ASS/DMM
		Parecer Conjunto PE/LOS nº 1/2023-PG-18
		Parecer nº 1/2024/SETD/ASJUR
PGE/RN	http://www.pge.rn.gov.br/Conteudo.asp?TRAN=PORTIF&TARG=914&ACT=&PAGE=0&PARM=&LBL=Fale+Conosco e https://falabr.cgu.gov.br/web/login?redirect=/manifestacao	Não se manifestou sobre o tema.
PGE/RO	pa@pge.ro.gov.br e https://falabr.cgu.gov.br/web/login?tipo=5&step=2&redirect=/manifestacao/criar?tipo=5%26step=2	Não se manifestou sobre o tema.
PGE/RR	https://sei.rr.gov.br/sei/modulos/pesquisa/md_pesq_processo_pesquisar.php?acao_externa=protocolo_pesquisar&acao_origem_externa=protocolo_pesquisar&id_orgao_acesso_externo=0	Parecer SEI/GRR – 0370507
		Parecer 376 DETRAN/PRESI/DJUR
		Parecer 317/2022/PGE/GAB/ADJ/CA
		Parecer 154/2023 PGE/GAB/ADJ/CA
		Parecer 158/2023 PGE/GAB/ADJ/CA
		Parecer 833/2023 PGE/GAB/ADJ/CA
		Parecer SEI/GRR – 11852053
PGE/RS	http://sid.pge.rs.gov.br/NXT/gateway.dll?f=templates&fn=default.htm&vid=W:OM	Parecer nº 19.851/23
		Parecer nº 18.910/21
PGE/SC	http://pgenet.pge.sc.gov.br/cto/auth/login.do	Parecer nº 090/21-PGE
		Parecer nº 150/2022-PGE
PGE/SE	http://acervo.se.gov.br/easysearch/	Parecer: 3576/2022
		Parecer: 2415/2023
PGE/SP	https://revistas.pge.sp.gov.br/index.php/boletins/article/view/227	Parecer: PA nº 16/2019

ADVOCA CIA PÚBLICA	FORMA DE LOCALIZAÇÃO	DOCUMENTO
PGE/TO	subprocuradoria@gmail.com e https://falabr.cgu.gov.br/web/login?tipo=5&step=2&redirect=/manifestacao/criar?tipo=5%26step=2	Não se manifestou sobre o tema.

Fonte: elaboração própria.

Todos os documentos foram analisados por meio do *Atlas.ti* realizando-se o processo de codificação. Assim, por meio do processo dedutivo, com os requisitos (grupos de códigos) já previamente definidos, analisou-se como a União, o DF e os Estados têm tratado o tema e em que medida têm observado os mesmos requisitos dispostos no Guia Orientativo da ANPD e na Decisão do STF.

Além do mais, para aqueles casos de requisitos não tratados no Guia Orientativo/Decisão, foi criado o grupo de código “Novos requisitos”, composto pelo código “Novo Requisito” e pelo código nomeado “Requisito específico caso concreto”, este último para aquelas situações que abarquem peculiaridades regionais ou peculiaridades do dado compartilhado em si.

6 REQUISITOS PARA O COMPARTILHAMENTO DE DADOS PESSOAIS NO PODER PÚBLICO

A LGPD disciplina em capítulo específico – Capítulo IV – o tratamento de dados pessoais pelo Poder Público. A par das disposições específicas previstas no Capítulo IV da LGPD, sabe-se que, quando não houver contrariedade com a disposição específica, deve observar as disposições gerais previstas para as pessoas naturais e as pessoas jurídicas de direito privado. Nesse sentido:

(...) todo tratamento de dados realizado pela Administração Pública precisará atender à principiologia da Lei, em especial, os princípios da finalidade, da adequação, da necessidade e da segurança do tratamento. Isso significa que o tratamento de dados precisa ser transparente quanto à sua finalidade específica, adequado para atingir essa finalidade e não excessivo para o alcance desse objetivo, além de prever medidas de garantia para a minimização de riscos, nos termos do princípio da boa-fé objetiva e da prevenção (Gasiola; Machado; Mendes, 2021, RB-3.6)

Com o intuito de auxiliar o Poder Público, a ANPD tratou dos principais requisitos a serem observados no compartilhamento de dados pessoais pelo Poder Público, que podem “ser ajustados ou complementados com parâmetros e requisitos adicionais de acordo com o contexto e as peculiaridades de cada caso concreto” (Brasil, 2023a, p. 30).

Os requisitos abordam os princípios dispostos na LGPD, em seu art. 6º, que devem ser observados no tratamento de dados pessoais, aplicáveis tanto ao setor privado como ao público:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização 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;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (Brasil, 2018a).

Como afirmado por Wimmer (2021a, p. 164), a previsão de um capítulo específico para o poder público “não foi o suficiente para solucionar as inúmeras dúvidas existentes quanto ao tema, seja em razão da complexidade do texto legal, seja em razão das diferenças intrínsecas entre as atividades de tratamento de dados realizadas pelo Estado e por agentes privados”. Os

princípios funcionam, assim, “como lentes interpretativas para as complexas regras previstas na legislação” (Wimmer, 2021a, p. 164).

Os requisitos devem ser abordados com referências aos princípios de governança pública. “A governança apoia-se em um conjunto de regras e princípios de forma a orientar a melhor gestão e alcançar os melhores resultados organizacionais, entendidos aqui como os melhores resultados do ponto de vista da sociedade” (Altounian; De Souza; Lapa, 2020, p. 267).

Esses princípios estão previstos na maioria dos modelos de governança e são entendidos como essenciais para prática da boa governança, sendo eles a transparência, a equidade, a prestação de contas e a responsabilidade corporativa (Altounian; De Souza; Lapa, 2020, p. 267 e 268).

No caso do setor público, serão utilizados, como modelos de governança no presente estudo, o Guia da Política de Governança Pública, da Presidência da República, e o Referencial Básico de Governança Organizacional para organizações públicos e outros entes jurisdicionados ao TCU, do Tribunal de Contas da União.

Conforme os requisitos para o compartilhamento de dados pessoais pelo Poder Público sejam analisados, serão explicitados os princípios e as diretrizes de governança para o setor público aplicáveis e correlacionados.

A seguir, cada requisito será analisado de forma aprofundada em um subcapítulo, expondo-se o conceito, a base principiológica da LGPD, os princípios de governança pública aplicáveis, as abordagens e as formas de observá-lo.

6.1 Base legal

A base legal se refere à hipótese que permite o compartilhamento de dados pessoais. As “atividades realizadas pelo ente ou órgão público seguem a regra de necessário atrelamento a uma base legal” (Tasso, 2022, RL-1.8). Não sendo uma das hipóteses de exclusão previstas no art. 4º¹ da LGPD, “deverá ocorrer o encaixe do tratamento realizado em pelo menos uma das hipóteses legais para que ele seja considerado legítimo e lícito” (Viola; De Teffé, 2023, p. 116).

¹ A LGPD exclui da sua aplicação o tratamento de dados pessoais realizado por pessoal natural para fins exclusivamente particulares e não econômicos, realizado para fins exclusivamente jornalísticos, artísticos ou acadêmicos, realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou

É um parâmetro relacionado diretamente ao princípio da finalidade, previsto no art. 6º, I, da LGPD. Esse princípio exige que o compartilhamento tenha uma finalidade pública legítima e, para ser legítima, a finalidade deve ser amparada em uma base legal prevista na LGPD.

Por meio do princípio da finalidade, “é garantido ao titular, mediante informação prévia, as fronteiras da legalidade do tratamento de seus dados, delimitando os propósitos do tratamento, desde que lícitos, e de terceiros que poderão ou não ter acesso aos dados” (Vainzof, 2022, RL-1.2).

A LGPD, nos artigos 7º e 11, define a base legal de acordo com o tipo de dado pessoal. O art. 7º prevê as hipóteses de tratamento de dados pessoais e o art. 11 as hipóteses concernentes a dados pessoais sensíveis. Relevante registrar que as bases legais de tratamento previstas nos artigos 7º e 11 são taxativas. Esse entendimento, inclusive, foi defendido no Parecer nº 0447/2021-PGEPE.

O compartilhamento de dados pessoais pelo Poder Público pode ser legitimado em três opções de base legal: a) cumprimento de obrigação legal ou regulatória pelo controlador, prevista nos artigos 7º, II, e 11, II, “a”; b) execução de competências legais ou cumprimento de atribuições legais do serviço público, prevista no art. 23 da LGPD; e c) execução de políticas públicas, prevista nos artigos 7º, III, e 11, II, “b”.

Isso não significa dizer que o Poder Público não possa utilizar as demais bases legais previstas na LGPD, entretanto adota-se o posicionamento de Wimmer (2023, p. 283) no sentido de que “o tratamento de dados pessoais pelo Poder Público deve, em regra, se dar ao abrigo de suas competências legais, ficando as demais hipóteses legais relegadas à condição de exceções”.

O presente trabalho deu enfoque às bases legais de execução de políticas públicas e cumprimento de obrigação legal, considerando que “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 na legislação” (Langenegger, 2023, p. 346).

O cumprimento de obrigação legal ou regulatória pelo controlador está relacionado às normas de conduta e de organização a que o Poder Público se submete. Normas de conduta “estabelecem obrigações de forma direta e expressa, prevendo uma consequência específica em caso de descumprimento” (Brasil, 2023a, p. 16). Por sua vez, normas de organização

atividades de investigação e repressão de infrações penais, ou provenientes de fora do território nacional que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (Brasil, 2018a).

“estabelecem obrigações que estão associadas, de forma mais geral, ao cumprimento e à execução de atribuições legais típicas da entidade ou órgão público responsável pelo tratamento de dados pessoais” (Brasil, 2023a, p. 16).

Veja-se que, na parte das normas de organização, essa base legal está relacionada à base legal de execução de competências legais ou cumprimento de atribuições legais do serviço público, prevista no art. 23 da LGPD. Há autores, contudo, que defendem que o art. 23 da LGPD “traz requisitos adicionais para o tratamento de dados pessoais por parte da Administração Pública, seja com base no art. 7º, seja com base no art. 11 da LGPD” (Viola; De Teffé, 2023, p. 116). Neste trabalho, adota-se a posição defendida por Wimmer (2023, p. 282), pela qual o art. 23 da LGPD possui linguagem mais ampla para incluir o objetivo de “executar as competências legais ou cumprir as atribuições legais do serviço público”.

No que concerne à execução de políticas públicas, inicialmente, é relevante discorrer sobre o conceito de políticas públicas, que não foi definido na LGPD. A ANPD, no Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público, sugere a adoção das definições usuais do termo (Brasil, 2023a, p. 20). No presente estudo, adotar-se-á a definição trazida por Bouldosa e Secchi, que a conceituam como os instrumentos para resolução de problemas públicos.

Bouldosa (2019, p. 92) entende políticas públicas como instrumentos, práticas e argumentos trazidos por multiatores na definição dos problemas públicos e apresentação de suas soluções. Compreende política pública “como fluxo axiológico de uma multiatorialidade ativada em experiências públicas/contextos de governo de problemas considerados de pública relevância ou em contextos de preservação de bens públicos” (Bouldosa, 2019, p. 93).

Política pública é um conceito abstrato que se materializa por meio dos instrumentos, que são a forma de se transformar as intenções de uma política pública em ação para o enfrentamento do problema público, o instrumento “é um resultado das interações entre os diversos atores, nas diversas arenas e nas fases de formulação da política pública, decisão e implementação” (Secchi, 2014, p. 104).

A ANPD, no Guia Orientativo para Tratamento de Dados Pessoais pelo Poder Público, exemplifica política pública da seguinte forma:

Exemplo 7. Política de controle do tabagismo

Secretaria de Saúde realiza tratamento de dados pessoais de pessoas fumantes, atendidas em hospitais públicos, para fins de planejamento e execução de política pública de controle do tabagismo e prevenção e tratamento do câncer de pulmão. A política foi estabelecida em norma infralegal, da qual constam, entre outros elementos, objetivos, competências e meios de financiamento. Os dados pessoais são tratados pela própria Secretaria de Saúde e, eventualmente, compartilhados com a autarquia responsável por executar programa de orientação e auxílio a pessoas que desejam parar de fumar. Por envolver dados sensíveis, o tratamento dos dados pessoais é realizado com base no art. 11, II, b, da LGPD. A finalidade é específica de execução de política pública, estabelecida em regulamento, em conformidade com a LGPD (Brasil, 2023a, p. 21).

Mais relevante que a definição de política pública, é saber se esse instrumento, programa ou ação governamental está previsto em algum ato formal, que pode ser ato normativo (lei ou regulamento) ou ajuste contratual (contrato, convênio ou instrumento congênere). Essa previsão em ato formal é o que permite o compartilhamento de dados pessoais para execução de políticas públicas.

No caso, são duas hipóteses diversas para dados pessoais e dados pessoais sensíveis. O art. 7º da LGPD entende viável o compartilhamento de dados pessoais pela administração pública para a “execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres” (Brasil, 2018a). Em relação aos instrumentos congêneres, a expressão requer cautela, sendo que a “melhor interpretação demanda restringi-la ao termo imediatamente anterior, entendendo-a como congênere de convênios e desde que tenha previsão legal” (Tasso, 2022, RL-1.8).

Para os dados pessoais sensíveis, é admissível o seu compartilhamento pela administração pública para execução de políticas públicas previstas em leis ou regulamentos (Brasil, 2018a).

Para aclarar o tema e entender as diferenças entre as hipóteses de viabilidade de compartilhamento de dados, elaborou-se a seguinte tabela:

Tabela 4: Compartilhamento de dados pessoais e dados pessoais sensíveis

Tipo de dado	Execução de política pública prevista em leis ou regulamentos	Execução de política pública respaldada em contrato, convênio ou instrumento congênere	Execução de política pública não prevista em diploma normativo ou contratual ou em instrumento congênere
Dado pessoal	Pode compartilhar*.	Pode compartilhar*.	Não é hipótese de compartilhamento.
Dado pessoal sensível	Pode compartilhar*.	Não é hipótese de compartilhamento.	Não é hipótese de compartilhamento.

*desde que observados requisitos.

Fonte: elaboração própria.

A tabela é relevante para demonstrar como a LGPD tratou a matéria. Tem-se permissão para compartilhar dados pessoais para execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. Para o compartilhamento de dados pessoais sensíveis exige-se que as políticas públicas estejam previstas em leis ou regulamentos.

Consoante se observa, a hipótese de compartilhamento dos dados pessoais sensíveis para execução de políticas públicas é mais restrita que a hipótese de compartilhamento dos dados pessoais, porque exigem a previsão em instrumentos normativos, leis ou regulamentos.

A base legal de execução de políticas públicas “se aplica em hipóteses específicas e atrai para o poder público a necessidade de justificar a necessidade e proporcionalidade do tratamento de dados pretendido” (Langenegger, 2023, p. 355)

Diferentemente da base legal de execução de políticas públicas, que apresenta diferenças para os dados pessoais e os dados pessoais sensíveis, a hipótese de cumprimento de obrigação legal não diferencia o tratamento para os dados pessoais e os dados pessoais sensíveis.

Em uma interpretação superficial, quer parecer que o cumprimento de obrigação legal abriria um amplo leque de possibilidades para o Poder Público, eis que, “no limite, sempre deverá ser possível relacionar a atividade a uma determinação legal – especialmente em vista da moderna leitura administrativa sobre os contornos do princípio da legalidade e do conceito de discricionariedade administrativa” (Langenegger, 2023, p. 349). Em sequência, a autora ressalva que “essa base legal não foi prevista para assumir tamanha amplitude” e “não poderá ser interpretada como uma autorização abrangente para qualquer atividade de tratamento de dados pessoais” (Langenegger, 2023, p. 349). A previsão de base legal tão ampla, apta a

justificar todas as atividades do Poder Público, “seria contrária à própria lógica da legislação de proteção de dados pessoais” (Langenegger, 2023, p. 349).

Diante dessa problemática, Langenegger entende que:

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 (2023, p. 415).

Por sua vez, “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” (Langenegger, 2023, p. 415).

A par dos debates sobre a escolha da base legal aplicável, é imprescindível que o compartilhamento de dados pessoais pelo Poder Público se enquadre em uma dessas bases legais citadas. “É justamente por estar jungido inexoravelmente ao princípio da legalidade que o Poder Público necessita de autorização legal para o tratamento de dados pessoais dos administrados” (Tasso, 2022, RL-1.8).

Caso seja inviável o enquadramento em uma base legal, “outra modalidade de salvaguarda prevista em lei (ainda que sua execução seja técnica) consiste na anonimização ou pseudonimização de dados” (Langenegger, 2023, 419). No mesmo sentido, a ANPD, no Guia Orientativo, sugere que, “entre outras medidas, sempre que possível, os dados pessoais devem ser pseudonimizados² ou anonimizados³” (Brasil, 2023a, p. 40).

Ocorre que, em diversos casos, a anonimização ou pseudonimização dos dados pessoais não pode ser a única solução viável, eis que, para sua viabilização, há necessidade justamente de compartilhamento dos dados pessoais da forma como registrados nos sistemas.

² Segundo o art. 13, § 4º, da LGPD, “a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro” (Brasil, 2018).

³ Nos termos do art. 5º, inciso XI, da LGPD, a anonimização consiste na “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo”, sendo, portanto, o dado anonimizado aquele “relativo a titular que não possa ser identificado” (Brasil, 2018).

A título de exemplo, cita-se o estudo sobre a política pública Programa Bolsa Família no documento “Proteção de dados pessoais em Políticas de Proteção Social: Contribuições a partir do Programa Bolsa Família, Diagnósticos e Recomendações nº 6”. Nesse estudo, vê-se que os dados do Cadastro Único para Programas Sociais - CadÚnico, com a finalidade de instituição do programa, são compartilhados com a Caixa Econômica Federal, os Municípios, a Secretaria Nacional de Renda de Cidadania, a Secretaria Nacional do Cadastro Único⁴, organizações da sociedade civil, concessionárias e permissionárias de serviços públicos ou empresas privadas que prestam serviços. Os dados são utilizados para “a identificação, seleção e exclusão de beneficiários, pagamento do benefício, acompanhamento de condicionalidades, fiscalização, e também para a formação de diagnósticos e desenvolvimento de novas políticas” (Fragoso *et al.*, 2021, p. 6). Entre os dados compartilhados é fundamental a renda per capita familiar, que é utilizada para selecionar as famílias que receberão o benefício.

Outro exemplo foi trazido pelo Despacho Jurídico PGE-PASUBGER 19829293, no qual foi sugerida a verificação da possibilidade de anonimização dos dados, ressaltando-se, contudo, em seguida, que “tal situação de anonimização pode vir a ser comprometida diante do objetivo almejado pela SEADES que é abarcar os indivíduos órfãos em decorrência do COVID-19” (Alagoas, 2023, p. 5).

A referência aos exemplos serve para destacar e justificar que a anonimização ou pseudonimização dos dados não é cabível para toda e qualquer atividade que o Poder Público necessite realizar.

Para além da base legal, que deve ser apresentada e justificada no processo de compartilhamento de dados pessoais, deve ser exposta a justificativa do interesse público no compartilhamento (Miranda; Doria; Barbosa, 2022, p. 337). Isso decorre, inclusive, da previsão do art. 23 da LGPD, que determina que o compartilhamento deve ser realizado “para o atendimento de sua finalidade pública, na persecução do interesse público” (Brasil, 2018a).

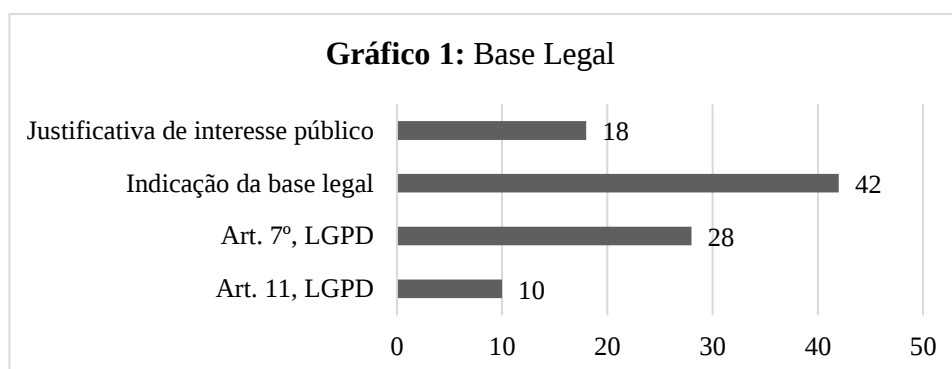
É dizer que, “em relação ao Poder Público, por sê-lo o maior agente de tratamento de dados do mundo, detendo informações dos cidadãos desde seu nascimento até seu óbito, há ainda mais requisitos, além do enquadramento na base legal (art. 7º), estando a persecução do interesse público em seu centro (art. 23 da LGPD)” (Pernambuco, 2021).

⁴ O caso do compartilhamento dos dados pessoais do Cadastro Único para Programas Sociais do Governo Federal – CadÚnico foi regulamentado pela Portaria MDS nº 10/2012, sendo que, conforme Fragoso *et al.* (2021, p. 16), “o acesso a esses dados pode ocorrer para a gestão e formulação de políticas públicas (art. 4º, I) e para a realização de estudos e pesquisas (art. 4º, II)”.

Com base nesses fundamentos, na codificação realizada na ferramenta *Atlas.ti*, foram criados os seguintes códigos para identificar o grupo de códigos “Base Legal”:

- a) Art. 7º, LGPD;
- b) Art. 11, LGPD;
- c) Indicação da base legal;
- d) Justificativa de interesse público.

Por meio do processo dedutivo, fazendo a identificação desses códigos nos documentos analisados, chegou-se ao seguinte:



Fonte: elaboração própria com dados da ferramenta *Atlas.ti*.

Com base no gráfico de barras, demonstra-se o número de recorrências que cada código apresentou dentro do grupo de códigos “Base Legal”. De uma forma geral, ainda que apenas citando o enquadramento nos artigos 7º ou 11 da LGPD, os dados analisados abordaram a questão da base legal.

Considerando esse o primeiro requisito com análise por meio de códigos dentro da ferramenta *Atlas.ti*, é relevante distinguir o número de recorrências do número de documentos analisados. A pesquisa analisou 43 documentos. Ocorre que, dentro de cada documento, pode haver uma ou mais recorrências sobre determinado código, significa que um mesmo documento pode tratar do requisito por diversas vezes. Todos os gráficos elaborados com base nos dados coletados na ferramenta *Atlas.ti* consideraram o número de recorrências de cada código.

Dos relevantes dados, constatou-se que a Procuradoria-Geral do Rio Grande do Sul, em seus pareceres, exige a pertinência temática do pedido de compartilhamento de dados pessoais

com as atribuições legais do órgão, o que, em última análise, significa o devido enquadramento na base legal.

Destaca-se que é suficiente o atendimento de uma base legal para o compartilhamento ser legítimo. Nos termos do Parecer nº 00304/2023/CONJUR-CGU/CGU/AGU, “caso se verifique a ocorrência de apenas um dos requisitos para o tratamento, ele será autorizado”, requisitos aqui se referindo aos incisos do art. 7º da LGPD.

O enquadramento em base legal e a justificativa de interesse público estão relacionados à diretriz para a boa governança, prevista no Referencial Básico de Governança Organizacional para organizações públicas e outros entes jurisdicionados ao TCU, referente a “estabelecer processos decisórios transparentes, baseados em evidências e orientados a riscos, motivados pela equidade e pelo compromisso de atender ao interesse público” (Brasil, 2020c, p. 48).

Portanto, para que o compartilhamento de dados pessoais pelo Poder Público seja legítimo, o primeiro parâmetro a ser cumprido é a base legal, que se desdobra na obrigatoriedade de se observar dois pressupostos, quais sejam, indicação e enquadramento em uma das bases legais previstas na LGPD, art. 7º, art. 11 ou art. 23, e justificativa de interesse público.

6.2 Formalização e registro

A formalização significa que o processo de compartilhamento de dados pessoais deve ser formalizado de acordo com as normas do processo administrativo. A ANPD recomenda “a instauração de processo administrativo, do qual constem os documentos e as informações pertinentes, incluindo análise técnica e jurídica, conforme o caso, que exponham a motivação para a realização do compartilhamento e a sua aderência à legislação em vigor” (Brasil, 2023a, p. 30).

Em relação ao registro, diz respeito ao art. 37 da LGPD, que exige a manutenção de registro das operações de tratamento de dados pessoais (Brasil, 2018a). O STF, para além do registro das operações de tratamento, passou a exigir, com a publicação da decisão no julgamento conjunto da ADI 6649 e da ADPF 695 do STF, o registro de acesso ao dado pessoal, ou seja, criar mecanismos dentro dos sistemas que contém dados pessoais de quem acessou determinado dado.

Veja-se que essa medida de registro de acesso é relevante medida de proteção dos dados pessoais e repercute como medidas de proteção e segurança e para apuração de eventuais responsabilidades em caso de abuso na utilização dos dados pessoais, tal como afirmado pelo STF.

Dentro do grupo de código “Formalização e registro”, foram criados os seguintes códigos:

- a) Art. 37, LGPD;
- b) Ato formal (contratos, instrumentos congêneres, decisão administrativa, ato normativo interno);
- c) Formalizado em atenção à obrigatoriedade de registro;
- d) Formalizado em atenção às normas gerais que regem os procedimentos administrativos;
- e) Instauração de processo administrativo;
- f) Lei 8.666/93.

Explica-se cada código.

O código “Art. 37, LGPD” é determinante por prever a necessidade de manutenção de registro das operações de tratamento de dados pessoais. Da mesma forma, o código “Formalizado em atenção à obrigatoriedade de registro”, que abordará tanto o registro das operações de tratamento como o registro de quem acessou determinado dado, nos moldes traçados pelo STF.

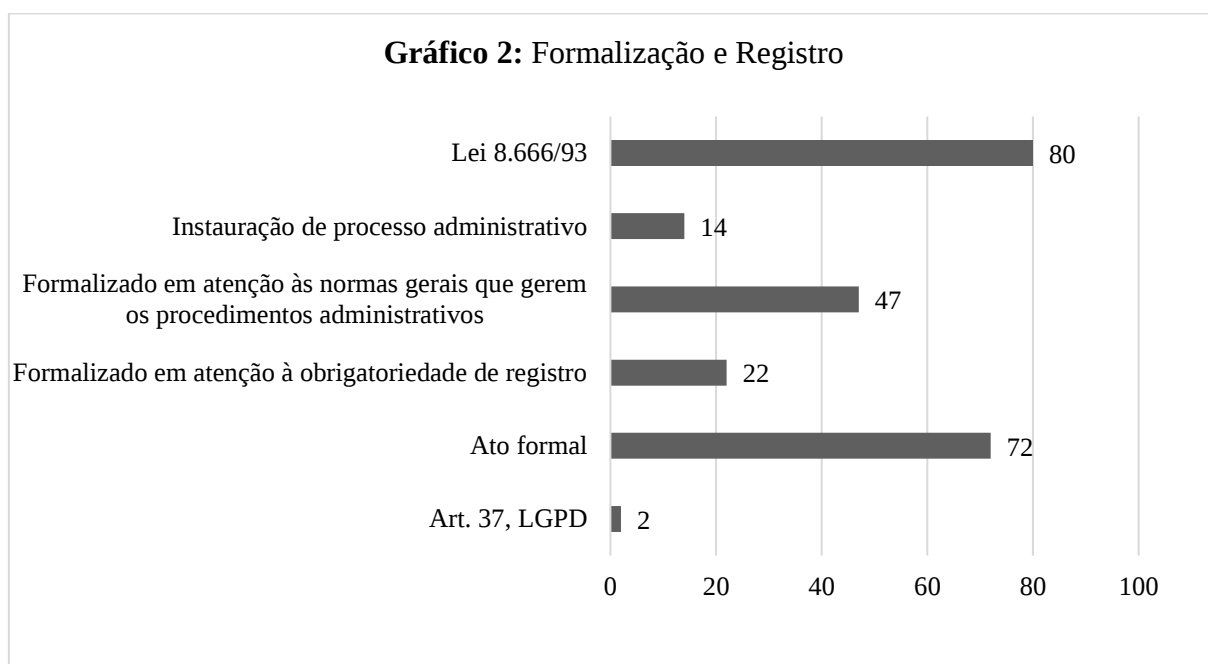
A ANPD recomenda que o compartilhamento seja formalizado por ato formal, como contratos, convênios ou instrumentos congêneres, ou decisão administrativa ou mesmo ato normativo interno (Brasil, 2023a, p. 30-31), por isso a criação do respectivo código.

O código “Instauração de processo administrativo” decorre da recomendação da ANPD de que o compartilhamento esteja formalizado em processo administrativo, com todas as informações necessárias a um devido processo administrativo.

Ainda em relação ao devido processo administrativo, foi criado o código “Formalizado em atenção às normas gerais que regem os procedimentos administrativos”. Considerando que a ANPD recomenda a instauração de um processo administrativo, devem ser observadas as normas sobre o processo administrativo.

Neste ponto, é relevante citar que muitos dos documentos analisados são anteriores à publicação da Nova Lei de Licitações, ou seja, as normas de processo administrativo observadas até então eram aquelas previstas na Lei nº 8.666, de 21 de junho de 1993. Por isso a criação do código “Lei 8.666/93”. A Lei nº 8.666/93 foi revogada pela Lei nº 14.133, de 1º de abril de 2021.

Na análise dos documentos citados, têm-se os seguintes números:



Fonte: elaboração própria com dados da ferramenta *Atlas.ti*.

Considerando que a Lei nº 8.666/93 encontra-se revogada, não é necessário que o presente estudo aprofunde o tema, bastando apontar que os documentos analisados buscavam, em sua maioria, à égide da Lei nº 8.666/93, adequar os instrumentos de compartilhamento de dados pessoais à legislação regente, especialmente o art. 116⁵.

Quanto aos demais códigos, veja-se que repercutem nos documentos analisados, especialmente o ato formal, ou seja, a celebração de um instrumento que formalize o compartilhamento de dados pessoais com as obrigações delimitadas tanto do órgão que concede o acesso como daquele que recebe o acesso ao sistema que possui dados pessoais.

⁵ Art. 116. Aplicam-se as disposições desta Lei, no que couber, aos convênios, acordos, ajustes e outros instrumentos congêneres celebrados por órgãos e entidades da Administração.

Por isso, cabe aprofundar o estudo sobre o ato formal, a formalização em atenção às normas gerais que regem os procedimentos administrativos, que abarca também a instauração de processo administrativo, e a formalização em atenção à obrigatoriedade de registro, que engloba o art. 37 da LGPD.

6.2.1 Ato formal: instrumentos utilizados pela União, DF e Estados

Este subcapítulo abordará quais instrumentos o Poder Público tem utilizado para a formalização do compartilhamento de dados pessoais entre seus órgãos e entidades da Administração Direta e Indireta. A ANPD recomenda que o compartilhamento seja formalizado por ato formal, como contratos, convênios ou instrumentos congêneres, ou decisão administrativa ou mesmo ato normativo interno (Brasil, 2023a, pp. 30-31).

Comprovada a necessidade de compartilhamento de dados pessoais pelo Poder Público, enquadrando-se em uma das bases legais previstas na LGPD, observa-se que a maioria dos documentos analisados trouxe como instrumentos de formalização o acordo ou termo de cooperação técnica, também denominado por convênio de cooperação técnica.

O acordo de cooperação técnica pode ser conceituado, de acordo com o Parecer nº 15/2013/CÂMARA PERMANENTE CONVÊNIOS/DEP CONSU/PGF/AGU,

como o instrumento jurídico formalizado entre órgãos e entidades da Administração Pública ou entre estes e entidades privadas sem fins lucrativos, com o objetivo de firmar interesse de mútua cooperação técnica, visando à execução de programas de trabalho, projeto/atividade ou evento de interesse recíproco, da qual não decorra obrigação de repasse de recursos entre os partícipes (Brasil, 2013).

Como se observa do gráfico anteriormente exposto, há alta recorrência da exigência de ato formal para o compartilhamento de dados pessoais, especificamente foram encontradas 72 recorrências para o código ato formal. Contudo, é relevante questionar e analisar se é sempre necessário que haja a formalização de um acordo de cooperação técnica para permitir o compartilhamento de dados pessoais ou se há outras formas de compartilhar os dados.

A ANPD traz outras duas possibilidades para o compartilhamento. A decisão administrativa “que autorize o acesso aos dados e estabeleça os requisitos definidos como

condição para o compartilhamento” ou, naqueles casos de compartilhamento recorrente, a emissão de “ato normativo interno, a exemplo de portarias e instruções normativas, com o objetivo de, além de proporcionar o devido formalismo, conferir maior padronização e celeridade a essas operações” (Brasil, 2023a, p. 31).

Dos dados analisados, além do acordo de cooperação técnica, encontrou-se importantes achados sobre termo de adesão para formalizar o compartilhamento de dados pessoais.

A Procuradoria-Geral do Estado do Rio de Janeiro, no Parecer 1/2023/PGE/PG02/ASS/DMM, analisa o Termo de Adesão supondo que seja um modelo estabelecido pela Secretaria Nacional de Segurança Pública - Senasp, com uma menor possibilidade de alterações na minuta proposta. Entendeu que o Termo de Adesão “se afigura como instrumento hábil à formalização da parceria” (Rio de Janeiro, 2023, p. 4). De forma semelhante, a Procuradoria-Geral do Estado do Rio Grande do Sul, no Parecer nº 19.851/23, opinou de forma favorável à formalização de Convênio de Adesão (Rio Grande do Sul, 2023).

Considerando que o Termo de Adesão ou Convênio de Adesão são instrumentos que já apresentam suas cláusulas pré-definidas, entende-se que podem ser instrumentos adequados para compartilhar dados pessoais de forma mais célere. Ou seja, o órgão que possui os dados pessoais apresenta um modelo de termo de adesão e o órgão que receberá os dados pessoais assina o termo com as exigências propostas.

Ainda assim, mesmo na adesão, é necessário a observância do procedimento administrativo, como a identificação da base legal e os demais requisitos. A adesão serve para agilizar e conferir celeridade ao procedimento, já que não há debate sobre as cláusulas ali estipuladas, ou seja, se o órgão recebedor deseja acesso a determinados dados, deve se sujeitar às cláusulas ali previstas.

Além dessa possibilidade, é necessário pensar em outras formas de compartilhar dados pessoais de forma mais célere. Sobre o ponto, chamou atenção a recomendação da Procuradoria-Geral do Estado de Santa Catarina, no Parecer nº 090/21-PGE, que sugeriu que “a entrega das informações seja feita pessoalmente à autoridade solicitante, mediante recibo, que formalize a transferência e assegure a preservação do sigilo” (Santa Catarina, 2021, p. 37). A ideia de simplificar o compartilhamento com um recibo que apenas discipline a obrigação de preservação do sigilo parece não condizer exatamente com o procedimento recomendado pela ANPD e pelo STF. Além do mais, a entrega pessoal de informações pode se demonstrar como

um instrumento precário atualmente, já que a maior parte do Poder Público trabalha com sistemas eletrônicos.

Buscando-se, então, mecanismos de conferência de celeridade para o compartilhamento de dados pessoais, a fim de complementar o estudo, foi realizada pesquisa em todos os Estados sobre eventuais normas que inovassem sobre o tema ou o previssem de forma diferenciada. O estudo utilizou o mesmo recorte temporal da coleta de documentos jurídicos das advocacias públicas.

Como achados relevantes, foram encontrados alguns Estados que dispensam a formalização de acordo de cooperação para compartilhamento de dados pessoais. Elaborou-se a seguinte tabela:

Tabela 5: Lista de Estados que dispensam formalização de acordo para compartilhamento de dados pessoais

ESTADO	NORMA	EMENTA	ARTIGO DA DISPENSA
ES	Decreto nº 4922-R, de 09 de julho de 2021	Institui a Política Estadual de Proteção de Dados Pessoais e da Privacidade do Poder Executivo Estadual em consonância com a Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).	Art. 8º (...) Parágrafo único. Fica dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres quando o compartilhamento de dados ocorrer entre os órgãos, autarquias e fundações do Poder Executivo Estadual, observados os princípios e diretrizes desta Política e as demais normas da LGPD.

ESTADO	NORMA	EMENTA	ARTIGO DA DISPENSA
MS	Decreto Estadual nº 15.572/2020.	Dispõe sobre a adoção de medidas destinadas à aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei de Proteção de Dados Pessoais (LGPD), no âmbito do Poder Executivo Estadual.	Art. 13 (...) Parágrafo único. Fica dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres quando o compartilhamento de dados ocorrer entre os órgãos da Administração Direta, as autarquias e as fundações do Poder Executivo Estadual, observadas as diretrizes previstas no caput deste artigo e o disposto na Lei Federal nº 13.709, de 2018.
PE	Decreto nº 50.474, de 29 de março de 2021.	Dispõe sobre a Política Estadual de Compartilhamento de Dados e cria a Plataforma de Compartilhamento e Análise de Dados dos órgãos e entidades da administração direta e indireta do Poder Executivo Estadual.	Art. 6º Fica dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a efetivação do compartilhamento de dados entre as instituições de que trata o art. 1º, observadas as diretrizes do art. 3º e o disposto na Lei Geral de Proteção de Dados Pessoais - LGPD.
RS	Decreto nº 56.528, de 25 de maio de 2022.	Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública estadual.	Art. 1º (...) §1º Fica dispensada a celebração de convênio, de acordo de cooperação técnica ou de ajustes congêneres para a efetivação do compartilhamento de dados, para os órgãos e as entidades referidos no “caput” deste artigo.

ESTADO	NORMA	EMENTA	ARTIGO DA DISPENSA
SC	Decreto nº 282, de 27 de setembro de 2019.	Dispõe sobre a disponibilização e compartilhamento de bases de dados no âmbito da Administração Pública Estadual.	Art. 4º Fica dispensada a celebração de convênio, acordo de cooperação técnica ou ajustes congêneres para a efetivação da disponibilização e do compartilhamento das bases de dados dos órgãos e das entidades de que trata o caput do art. 1º deste Decreto.

Fonte: elaboração própria.

Consoante se observa, cinco Estados dispensam ato formal para compartilhamento de dados pessoais. Contudo, isso não significa que não deverão ser observados os demais requisitos para o compartilhamento de dados pessoais. A propósito, as legislações estaduais citadas trazem uma dinâmica de dispensa de celebração de ato formal, observadas as diretrizes da LGPD. Ou seja, o fato de ser permitida a simplificação do processo com a dispensa do ato formal não afasta os deveres impostos ao órgão e aos servidores que terão acesso aos dados pessoais.

A dispensa condicionada às diretrizes da LGPD para formalização de instrumento de compartilhamento de dados pessoais, bem como a utilização de instrumentos de adesão estão intimamente ligados à diretriz para a boa governança de “promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico”, prevista no Referencial Básico de Governança Organizacional para organizações públicas e outros entes jurisdicionados ao TCU (Brasil, 2020c, p. 49).

Também está relacionado ao princípio da melhoria regulatória, na sua diretriz de “manter processo decisório orientado pelas evidências, pela conformidade legal, pela qualidade regulatória, pela desburocratização e pelo apoio à participação da sociedade” (Brasil, 2018b, p. 48).

Como se observa, além da desburocratização e da conformidade legal, que são trazidas pelas normas estaduais citadas, o princípio aborda a questão das políticas públicas baseadas em evidências, que têm relação com o requisito da base legal execução de políticas públicas.

Perpassa pela ideia de utilizar os dados pessoais como evidências no processo de decisão de políticas públicas, ou seja, a criação de um sistema de construção de evidências no âmbito da administração pública, “que permita destravar as amarras de acesso aos dados sem olvidar práticas adequadas de privacidade e que desenvolva a capacidade de gerar evidências de qualidade para orientar o processo decisório” (Brasil, 2018b, pp. 48-49).

Ainda sobre o ponto, destaca-se que a decisão baseada em evidência, que engloba a decisão de compartilhar os dados pessoais para execução de uma política pública ou até mesmo de uma competência legal, é uma das mais constantes recomendações em governança pública (Brasil, 2018b, p. 48).

6.2.2 Formalização em atenção às normas gerais que regem o procedimento administrativo

Consoante já abordado, a maior parte dos documentos analisados foi elaborada anteriormente à Nova Lei de Licitações, sob a égide da Lei nº 8.666/93, que tratava do tema de acordo de cooperação e instrumentos congêneres em seu art. 116. De acordo com a Lei, exigia-se para a celebração do acordo a identificação do objeto a ser executado, metas a serem atingidas, etapas ou fases de execução, plano de aplicação dos recursos financeiros e cronograma de desembolso, para casos que envolvam repasse de recursos financeiros, e previsão de início e fim da execução do objeto e da conclusão das etapas ou fases programadas (Brasil, 1993).

De acordo com os documentos analisados sob a égide da Lei nº 8.666/93, o acordo era formalizado então com normas semelhantes a um contrato administrativo, com cláusula de publicidade na imprensa oficial, juntada de certidões de regularidade, cláusulas de alteração e rescisão do acordo, eleição de foro para dirimir controvérsias.

A Nova Lei de Licitações passou a prever essa modalidade de acordos em seu art. 184⁶. Dos documentos analisados, três deles se aprofundaram sobre o tema do procedimento administrativo para formalização do acordo de cooperação. São eles:

⁶ Art. 184. Aplicam-se as disposições desta Lei, no que couber e na ausência de norma específica, aos convênios, acordos, ajustes e outros instrumentos congêneres celebrados por órgãos e entidades da Administração Pública, na forma estabelecida em regulamento do Poder Executivo federal.

a) Parecer nº 1/2024/SETD/ASSJUR da Procuradoria-Geral do Estado do Rio de Janeiro;

b) Parecer nº 00304/2023/CONJUR-CGU/CGU/AGU da Advocacia-Geral da União;

c) Parecer Referencial nº 04/2022-PGE da Procuradoria-Geral do Estado do Paraná.

O citado Parecer Referencial, a fim de conferir celeridade à formalização do ajuste, apresenta como anexo minuta padronizada de convênio de cooperação técnica e respectivo plano de trabalho, com cláusulas pré-definidas. Relevante registrar que os pareceres referenciais são instrumentos utilizados pelas diversas advocacias públicas para padronizar o seu entendimento administrativo, conferindo, assim, maior celeridade à tramitação do processo, dispensando-se a análise jurídica pela advocacia pública. Eis aqui outro mecanismo de conferência de celeridade ao processo administrativo, que confere observância à diretriz de boa governança da simplificação administrativa e da desburocratização.

Sobre o ponto, é relevante lembrar que a ANPD determina a instauração de processo administrativo, com documentos, análise técnica e jurídica. Assim, havendo parecer referencial sobre determinado tema, está cumprida a etapa de análise jurídica determinada pela ANPD.

De acordo com o Parecer Referencial nº 04/2022-PGE, o Plano de Trabalho deve conter as seguintes cláusulas: a) dados cadastrais dos partícipes; b) objeto a ser executado; c) justificativa; d) metas; e) especificações das ações; f) etapas e fases de execução; g) vigência; h) denúncia; e i) gratuidade.

A minuta de convênio apresenta as seguintes cláusulas: a) objeto; b) formas de cooperação; c) obrigações dos partícipes; d) sigilo, utilização e divulgação; e) responsabilidades financeiras; f) gerenciamento e fiscalização; g) vigência, alteração e rescisão; h) denúncia; i) legislação aplicável aos casos omissos; j) publicação; e k) foro.

No Parecer nº 1/2024/SETD/ASSJUR, o Procurador-Chefe da Coordenadoria do Sistema Jurídico, em interpretação da Nova Lei de Licitações e seus procedimentos, entendeu que

os regulamentos estaduais que tratavam de convênios e instrumentos congêneres, editados sob a baliza do art. 116 da Lei nº 8.666/1993, não foram automaticamente revogados com o fim da vigência dessa lei, devendo-se perquirir a compatibilidade desses atos pretéritos com os ditames da nova lei de licitações e contratos administrativos (Rio de Janeiro, 2024).

Assim, caberá a cada Estado verificar a regulamentação sobre a matéria. Caso já haja regulamentação posterior, a Nova Lei de Licitações deve ser aplicada. Contudo, em não havendo regulamentação posterior, mas havendo decreto ou regulamento estadual anterior à Nova Lei, que seja com esta compatível, deve ser aplicado para determinar o procedimento administrativo para a formalização dos acordos de cooperação técnica.

De toda forma, entende-se que a formalização em atenção às normas gerais do procedimento administrativo deve ser pautada por um instrumento que formalize todos os requisitos que devem ser observados para o legítimo compartilhamento de dados pessoais.

Como sugestão para celeridade do processo de compartilhamento de dados pessoais e observância das boas práticas de governança, tem-se duas opções.

A primeira refere-se à utilização de instrumentos de adesão, termo ou convênio de adesão, que disciplinem todas as cláusulas necessárias ao compartilhamento de dados pessoais.

A segunda opção é a elaboração de parecer referencial pela advocacia pública do Poder Público com a respectiva aprovação de uma minuta padronizada de acordo de cooperação técnica ou de termo ou convênio de adesão.

As opções não são excludentes, podendo-se adotar as duas medidas, e, tal como no item anterior, estão adequadas à diretriz para a boa governança de promover a simplificação administrativa e a modernização da gestão pública.

Em relação à própria estrutura das organizações, no tocante à estrutura das advocacias públicas, a instituição desses documentos de padronização está alinhada às diretrizes de desempenho do seu papel institucional de forma efetiva, de desenvolvimento continuado da capacidade da organização, assegurando eficácia e eficiência na gestão dos recursos, bem como de utilização de resultados para identificar oportunidades de melhoria e avaliação de estratégias organizacionais.

Além do mais, todos os instrumentos de padronização estão relacionados ao princípio da capacidade de resposta, que “representa a competência de uma instituição pública de atender de forma eficiente e eficaz às necessidades dos cidadãos, inclusive antevendo interesses e antecipando aspirações” (Brasil, 2018b, p. 40). Como a função do compartilhamento de dados pessoais está vinculado a um interesse público, que deve ser demonstrado e justificado, a padronização, em última análise, permite que o interesse público seja atendido de forma mais eficiente.

6.2.3 Formalização em atenção à obrigatoriedade de registro

A obrigatoriedade de registro engloba tanto o registro das operações que serão efetuadas com os dados pessoais, de acordo com o art. 37 da LGPD, bem como o controle de acesso com identificação de todos os agentes públicos que terão acesso aos dados pessoais.

Consoante o gráfico de barras, foram encontradas 22 ocorrências sobre a obrigatoriedade de registro. Considerando a relevância do tema, eis que é justamente o registro que auxiliará a apuração de eventuais responsabilidades por vazamento de dados, parece que o número de ocorrências deveria ser mais elevado. Aliás, dos documentos analisados, apenas 10 abordaram o requisito.

Veremos, contudo, no subcapítulo de medidas de segurança, que há elevado número de ocorrências desse requisito, demonstrando sim a preocupação dos entes federados com a segurança dos dados pessoais.

Da análise dos documentos, é relevante para o estudo citar os seguintes parâmetros:

- a) viabilidade de fornecimento dos registros sempre que for solicitado;
- b) os registros devem ser mantidos com condições de rastreabilidade e de prova eletrônica a qualquer tempo,
- c) indicação das pessoas que serão encarregadas das operações de tratamento dos dados pessoais.

Essas teses estão de acordo com a decisão no julgamento conjunto da ADI 6649 e da ADPF 695 do STF, que recomendou a utilização de sistemas eletrônicos de registro de acessos. Apesar de a tese do STF ser direcionada, no ponto, às atividades de inteligência e ao Cadastro Base do Cidadão, a recomendação de registro de acesso pode ser estendida a todas as atividades, considerando a sua relação com os princípios da segurança e da responsabilização e prestação de contas, previstos na LGPD.

Conforme afirmado pelo Ministro Alexandre de Moraes, a medida é essencial por possibilitar graduar quem tem acesso a todas as informações e quem tem acesso a algumas informações, “toda vez que a pessoa acessar, fica marcado quem acessou, a senha de quem acessou, para futura responsabilização” (Brasil, 2023b).

O registro das operações que serão realizadas com os dados pessoais, bem como o registro de acesso aos dados pessoais se relacionam com o princípio da boa governança da prestação de contas e responsabilidade (*accountability*), que pode ser conceituado como o processo pelo qual o Poder Público e seus agentes são responsáveis por suas decisões e ações, incluindo não só questões relacionadas aos recursos públicos mas ao desempenho geral do Poder Público (Altounian; De Souza; Lapa, 2020, p. 270).

Como afirmado por Langenegger, a documentação de prestação de contas, denominada Registro de Operação de Tratamento, nos termos do art. 37 da LGPD, atua não somente “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” (Langenegger, 2023, p. 311).

Sobre o ponto, registra-se que o tema está relacionado com as diretrizes de boa governança, consubstanciadas na definição de forma clara dos papéis e responsabilidades dos agentes envolvidos, no estabelecimento de sistema eficaz de gestão de riscos e controles internos, na implementação de mecanismos eficazes de responsabilização dos agentes e na modernização da gestão pública.

6.3 Objeto

O objeto diz respeito à apresentação, de forma clara e expressa, sobre quais dados pessoais serão compartilhados, devendo-se limitar ao estritamente necessário às finalidades do tratamento. Trata-se do princípio da necessidade, que “impõe que o tratamento recaia apenas sobre a quantidade mínima de dados que garanta o atingimento da finalidade almejada e previamente informada pelo agente, sendo vedados excessos injustificáveis” (Miranda; Doria; Barbosa, 2022, p. 335).

Nos termos da decisão no julgamento conjunto da ADI 6649 e da ADPF 695 do STF, trata-se da minimização do uso de dados, devendo o compartilhamento ocorrer apenas quando necessário e indispensável para alguma finalidade indicada.

Para este requisito, foi criado o grupo de código “Objeto” com os seguintes códigos:

- a) Art. 6º, III, LGPD: conceitua o princípio da necessidade;

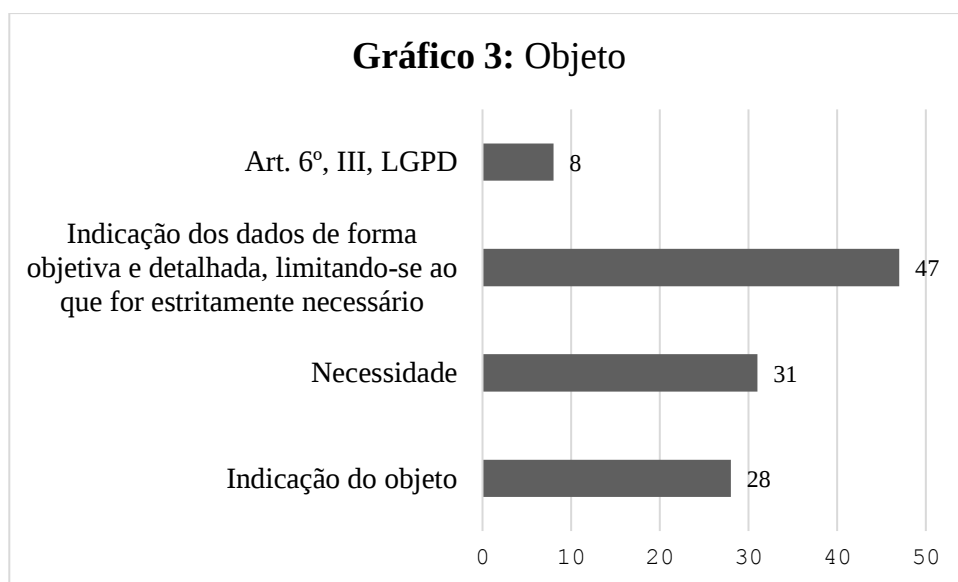
b) Indicação dos dados de forma objetiva e detalhada, limitando-se ao que for estritamente necessário;

c) Necessidade;

d) Indicação do objeto.

Consoante se observa, todos os códigos criados fazem referência à indicação dos dados pessoais que serão compartilhados e ao princípio da necessidade. As divisões são necessárias porque ora os documentos trazem apenas a citação do artigo da LGPD, ora aprofundam o tema e detalham o seu significado.

Dos dados analisados, tem-se o seguinte gráfico:



Fonte: elaboração própria com dados da ferramenta *Atlas.ti*.

Consoante se observa, há elevada recorrência sobre o grupo de código “Objeto”. Mais especificamente, 28 documentos analisados abordaram o tema do objeto.

No objeto, é imprescindível a indicação detalhada de quais dados pessoais serão compartilhados. De acordo com o Parecer Jurídico nº 592/2022-PGDF/PGCONS, recomenda-se que haja um rol, ao menos exemplificativo, dos dados pessoais que serão acessados, “como, por exemplo, endereços atualizados, dados pessoais, pesquisa de herdeiros, estado civil, à filiação, à idade, ao nome, etc” (Distrito Federal, 2022). No mesmo documento, destaca-se que “deve ficar claro, em suma, quais dados pessoais serão compartilhados, bem como por que e para que serão compartilhados” (Distrito Federal, 2022). A resposta a esses três

questionamentos, quais, por que e para que, bem resumem o atendimento do objeto, da base legal e da finalidade do compartilhamento de dados pessoais.

No caso do objeto, é necessário identificar a natureza dos dados que serão compartilhados (Rio Grande do Sul, 2021, p. 3). A indicação dos dados de forma detalhada permitirá distinguir se o compartilhamento será apenas de dados pessoais ou se englobará também dados pessoais sensíveis, o que, nesse último caso, se pautado na base legal de execução de políticas públicas, exige previsão em ato normativo como já afirmado.

Além de possibilitar a distinção entre dados pessoais e dados pessoais sensíveis, a indicação detalhada dos dados permite a identificação de dados que atraem a aplicação de regra específica de compartilhamento, tais como os dados acobertados pelo sigilo fiscal, e dados que não possam ser transferidos por proteção de sigilo, como dados bancários (Distrito Federal, 2022). Assim, nos termos do Parecer n. 00295/2020/CONJUR-CGU/CGU/AGU, “informações protegidas por sigilo seguem protegidas e sujeitas a normativos e regras específicas”.

Além da indicação detalhada dos dados, deve ser observado o princípio da necessidade, o compartilhamento deve se limitar ao mínimo necessário para a realização de suas finalidades, ou seja, os dados “apenas podem ser tratados na medida de sua imprescindibilidade à finalidade legal” (Pernambuco, 2021). Objetiva-se “preservar o cidadão do fornecimento de dados excessivos e que exponham sua privacidade de forma desnecessária, insegura ou para objetivos não adequados” (Pernambuco, 2021).

Veja-se a relação do tema com o princípio da confiabilidade, pelo qual “uma instituição confiável tem que se manter o mais fiel possível aos objetivos e diretrizes previamente definidos, passar segurança à sociedade em relação a sua atuação e, por fim, manter ações consistentes com a sua missão institucional” (Brasil, 2018b, p. 44).

6.4 Finalidade

O grupo de código “Finalidade” abarca tanto o princípio da finalidade como o princípio da adequação. O princípio da finalidade, previsto no art. 6º, I, da LGPD, é conceituado como a “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades” (Brasil, 2018a). Por sua vez, o princípio da adequação, previsto no art. 6º, II, da LGPD, é

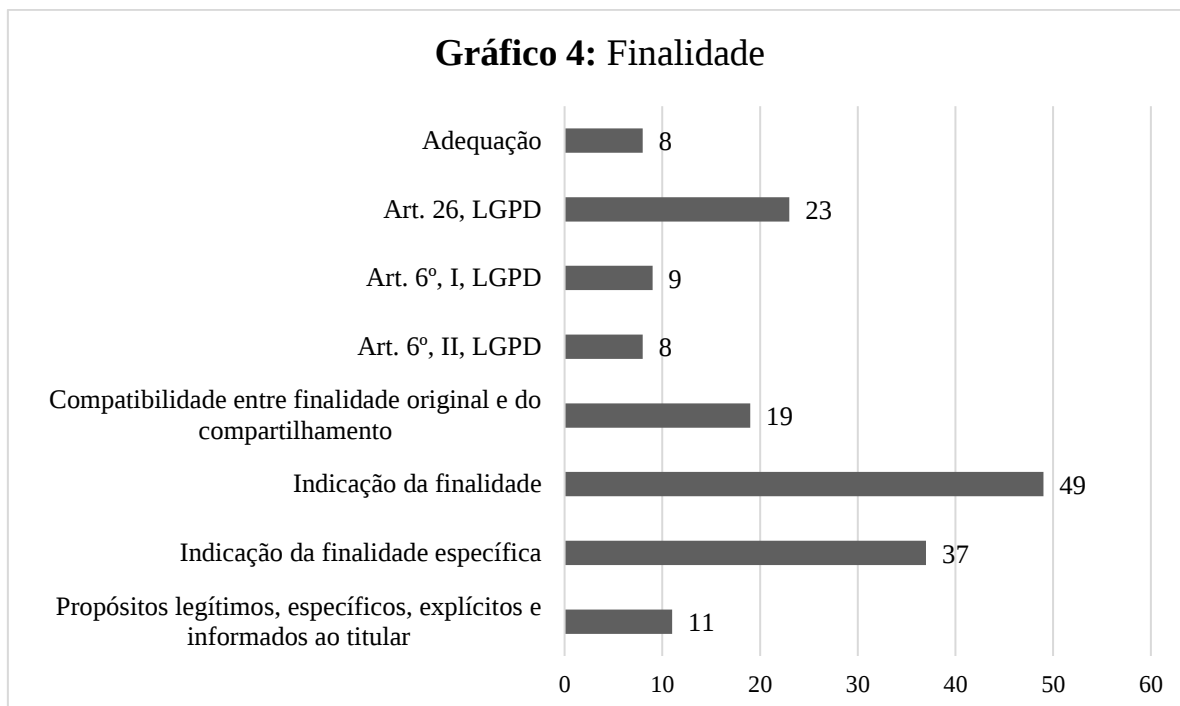
conceituado como a “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento” (Brasil, 2018a).

Estão relacionados também ao princípio da necessidade, eis que a finalidade do tratamento precisa estar devidamente apontada para saber quais dados pessoais são necessários àquela finalidade. Registra-se “o princípio segundo o qual não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado de dados”, assim, o risco reside mais na finalidade e nas possibilidades do tratamento em si do que no tipo de dados tratados (Mendes, 2020, p. 11).

Em decorrência dessas disposições, foram criados os seguintes códigos para o grupo de código “Finalidade”:

- a) Adequação;
- b) Art. 26, LGPD;
- c) Art. 6º, I, LGPD;
- d) Art. 6º, II, LGPD,
- e) Compatibilidade entre finalidade original e do compartilhamento,
- f) Indicação da finalidade,
- g) Indicação da finalidade específica,
- h) Propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Da análise dos documentos, extraiu-se o seguinte:



Fonte: elaboração própria com dados da ferramenta *Atlas.ti*.

A finalidade específica refere-se à indicação precisa de qual iniciativa, ação ou programa será executado ou de qual atribuição legal será cumprida mediante o compartilhamento de dados pessoais (Brasil, 2023a, p. 31).

Considera-se dentro do princípio da adequação o código da adequação em si, do art. 6º, II, LGPD, e da compatibilidade entre finalidade original e do compartilhamento. Os demais códigos estão relacionados ao princípio da finalidade.

Tanto o princípio da finalidade como o da adequação apresentaram bastante relevância nos documentos analisados.

Em relação ao princípio da finalidade, há amplo debate sobre o tema. Como afirmado por Wimmer (2021b, p. 135), parte importante da doutrina entende que os dados pessoais devem ser tratados de acordo com as funções específicas do órgão público e com a finalidade específica que justificou sua coleta inicial. Contudo, a finalidade não pode configurar um impedimento absoluto ao uso secundário de dados, exigindo-se que a nova finalidade seja compatível com a original. Isso confere ao titular dos dados pessoais a previsibilidade do resultado da disponibilização desses dados (Tasso, 2022, RL-1.8).

No contexto internacional sobre o tema, que pode ser transportado para o Brasil, Wimmer (2021b, p. 137) registra a possibilidade de “superar a incompatibilidade de finalidades

por meio do consentimento do titular ou com base em previsão legal específica, necessária e proporcional, observando-se o pleno respeito aos demais princípios e direitos associados à proteção de dados pessoais”.

Exigir o consentimento do titular quando houver necessidade de compartilhar seus dados para uma nova política pública inviabilizaria a própria implementação dessa política. Nesse ponto, atividades públicas e privadas são diversas, enquanto o tratamento de dados pessoais pelo poder público orienta-se pelo respaldo legal, a atividade do setor privado é centrada no consentimento informado (Silva; Tarter, 2021, p. 472). Assim, adota-se, neste estudo, o entendimento de Silva e Tarter (2021, p. 475), para os quais a base legal para tratamento de dados pelo Poder Público deve amparar-se em previsão legal, dispensando-se o consentimento pelo titular dos dados pessoais. No mesmo sentido, Pironti e Ziliotto (2021, p. 418) entendem que o consentimento no tratamento de dados pessoais pelo Poder Público pode ser considerado como exceção, ou seja, o Poder Público não depende de consentimento do titular para execução de políticas públicas.

Contudo, é relevante registrar que “eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento de cumprir as demais obrigações previstas na normativa, como a necessidade de ser dada ampla publicidade à dispensa de consentimento pelos órgãos e entidades públicas” (Silva; Tarter, 2021, p. 476).

Finalidade e adequação, indicação dos dados pessoais que serão compartilhados, todos os códigos relacionados à finalidade visam também implementar as diretrizes de boa governança já citadas nos demais capítulos, especialmente àquelas que dizem respeito ao foco no cidadão, que colocam o cidadão no centro da tomada de decisões.

6.5 Duração do tratamento

O instrumento que permite o compartilhamento de dados pessoais deve estipular o seu prazo de duração, que deve se limitar ao estritamente necessário para o atendimento da finalidade do compartilhamento. Objetiva a “reavaliação periódica do instrumento que autorizou o compartilhamento, incluindo a possibilidade de sua adequação a novas disposições legais e regulamentares ou a previsão de novas medidas de segurança, de acordo com as tecnologias disponíveis” (Brasil, 2023a, p. 33). A ANPD também sugere que seja inserido no

instrumento se os dados pessoais devem ser conservados ou eliminados após o término do tratamento (Brasil, 2023a, p. 33).

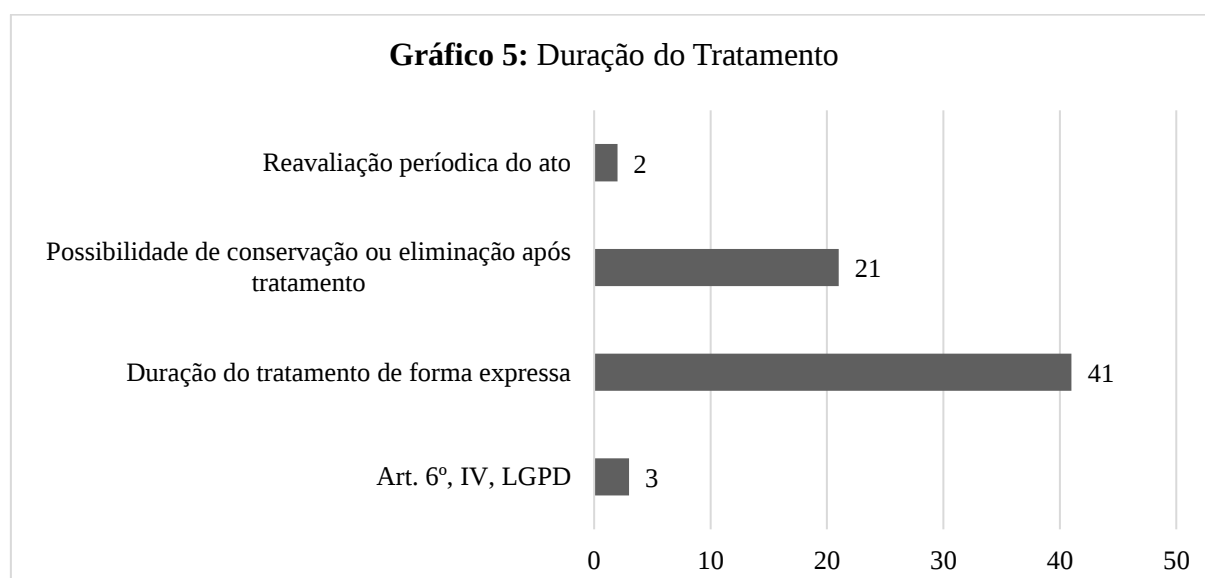
Com base nas recomendações da ANPD, foram criados os seguintes códigos para o grupo de código “Duração do tratamento”:

- a) Art. 6º, IV, LGPD;
- b) Duração do tratamento de forma expressa;
- c) Possibilidade de conservação ou eliminação após tratamento;
- d) Reavaliação periódica do ato.

A duração do tratamento está relacionada ao princípio do livre acesso, previsto no art. 6º, IV, da LGPD, que define o princípio como a “garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais” (Brasil, 2018a).

O princípio também está expresso no art. 9º da LGPD ao tratar sobre o direito de o titular dos dados pessoais ter acesso facilitado às informações sobre o tratamento de seus dados, incluindo a forma e duração do tratamento.

A análise dos documentos por meio dos códigos restou assim tratada:



Fonte: elaboração própria com dados da ferramenta *Atlas.ti*.

A duração do tratamento de forma estrita diz respeito ao período necessário ao cumprimento da finalidade do compartilhamento de dados pessoais, nos termos do Despacho PGE/PCA nº 00196/2022 da Procuradoria-Geral do Estado do Espírito Santo, que relaciona a duração do tratamento também à necessidade (Espírito Santo, 2022).

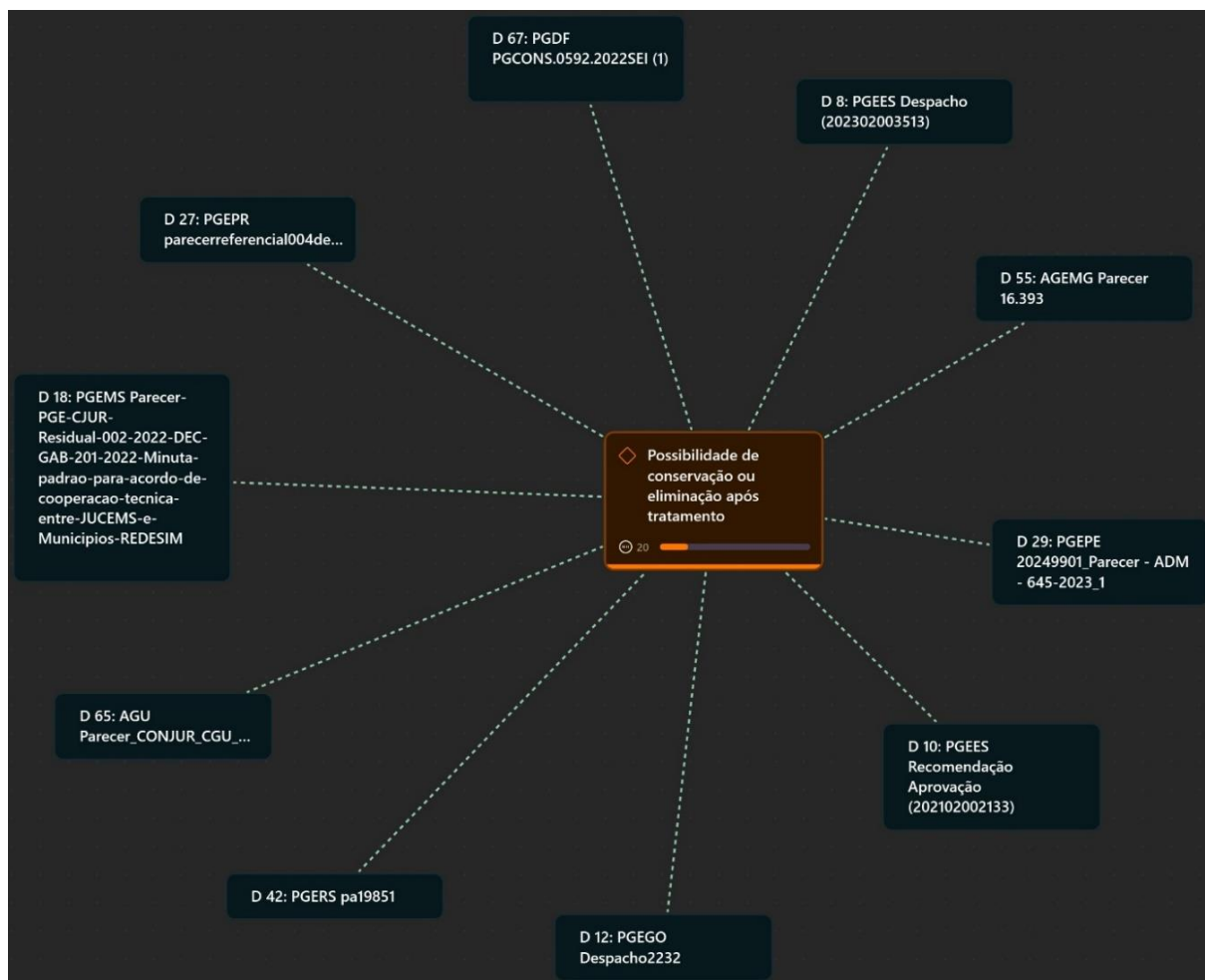
Em relação à reavaliação periódica do ato, entende-se que está intimamente relacionada à previsão sobre a possibilidade de prorrogação do acordo de cooperação técnica ou convênio de adesão que formalizou o compartilhamento de dados pessoais. Tal como apontado pelo Parecer PGE/MS/CJUR-RESIDUAL/Nº 002/2022 da Procuradoria-Geral do Estado do Mato Grosso do Sul, deve ser estipulada cláusula de vigência, “podendo ser prorrogado por sucessivos períodos até o limite de sessenta meses, desde que justificado e com vista à continuidade e ou à conclusão do programa, projeto ou atividade objeto do termo” (Mato Grosso do Sul, 2022, p. 5).

O limite de sessenta meses estava previsto na Lei nº 8.666/93. Na Nova Lei de Licitações, o prazo pode ser prorrogado respeitada a “vigência máxima decenal” (Brasil, 2021). No caso, observado o prazo, a prorrogação do compartilhamento de dados pessoais deve ser justificada e ter por finalidade continuar ou concluir o programa, projeto ou atividade para o qual o compartilhamento foi efetuado.

A reavaliação periódica do ato teve poucas recorrências nesse grupo de códigos, mas é relevante registrar que, no código “Formalizado em atenção às normas que regem o procedimento administrativo”, uma das cláusulas a serem estipuladas no termo que formalizará o compartilhamento de dados pessoais é justamente a possibilidade de prorrogação do ajuste. E a cada prorrogação, é realizada a reavaliação do ato.

Em relação à possibilidade de conservação ou eliminação após o tratamento, apesar de apresentar 21 recorrências, apenas 10 documentos citaram referido requisito, tal como se observa do diagrama exportado do *Atlas.ti*:

Diagrama: Possibilidade de conservação ou eliminação de dados pessoais após o tratamento



Fonte: Diagrama exportado do *Atlas.ti*.

Considerando que o compartilhamento deve ser efetivado apenas pelo período necessário para alcançar a finalidade pretendida, é relevante definir o que será feito com os dados após esse período. Assim, “se o tratamento deu-se em razão do exercício de uma competência ou obrigação legal, os dados serão preservados enquanto ainda forem essenciais para o exercício dessa competência e tal avaliação deve ser feita em cada caso concreto” (Parecer nº 00304/2023/CONJUR-CGU/CGU/AGU).

Recorda-se que a LGPD determina, como regra, em seu art. 16, a eliminação dos dados pessoais, autorizada a conservação para as finalidades ali disciplinadas (Brasil, 2018a). Por essa razão, a Procuradoria-Geral do Estado do Pernambuco, no Parecer nº 0645/2023, determina que seja providenciada a eliminação segura dos dados obtidos, “após o término do tratamento,

exceto quando necessários ao atendimento das finalidades previstas no art. 16 da Lei Federal nº 13.709/2018, quando estará autorizada a sua conservação” (Pernambuco, 2023).

Considerando, assim, que a regra da LGPD é a eliminação dos dados pessoais, caso o instrumento não discipline a matéria, deve ser providenciada a eliminação dos dados. Como a sua manutenção é exceção, isso deve ser expressamente autorizado pela parte que concedeu acesso aos dados pessoais.

A previsão de prazo de duração e a reavaliação periódica constituem formas de implementar o princípio da confiabilidade, na diretriz que indica o monitoramento e a avaliação dos efeitos dos serviços e das políticas públicas. O compartilhamento dos dados pessoais está vinculado àquela atividade fim que justificou o ato e, portanto, o próprio monitoramento da atividade fim é indicativo para permanecer ou cessar o compartilhamento.

6.6 Transparência e direitos dos titulares

Constitui boa prática de governança que o compartilhamento de dados pessoais pelo Poder Público seja disponibilizado nos sítios eletrônicos dos órgãos e entidades que compartilham dados. A transparência também constitui um princípio expressamente previsto no inciso VI do art. 6º da LGPD, englobando tanto à garantia de acesso a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento como os respectivos agentes de tratamento (Brasil, 2018a).

Nos termos do inciso I do art. 23 da LGPD, devem ser fornecidas “informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos” (Brasil, 2018a).

Além dessas informações, conforme defendido por Langenegger (2023, p. 323-325), há uma série de desdobramentos práticos da transparência: a) “evitar termos técnicos e linguagem abstrata que permita divergência de interpretação”; b) clareza sobre os riscos envolvidos; c) “a informação deve ser facilmente encontrada e ser disponibilizada de forma a evitar a fadiga informacional”; e d) disponibilização de forma gratuita.

A transparência objetiva “inspirar no titular de dados a credibilidade no ente público controlador dos dados e a necessária responsabilidade a que está submetido, numa clara relação

com um princípio peculiar da lei protetiva nacional, o da responsabilização e prestação de contas” (Tasso; 2022, RL-1.8).

A ANPD recomenda que sejam “delimitadas as obrigações das partes no que se refere: (i) à divulgação das informações exigidas pela LGPD; e (ii) às responsabilidades e aos procedimentos a serem observados visando ao atendimento de solicitações apresentadas pelos titulares” (Brasil, 2023a, p. 33).

De acordo com a decisão no julgamento conjunto da ADI 6649 e da ADPF 695 do STF, o design dos mecanismos de compartilhamento deve ser sensível a valores humanos e atender aos direitos dos titulares dos dados, abarcando: “i) o direito de ser informado sobre o tratamento; ii) o direito de acesso à informação; iii) o direito à explicação, em caso de dúvida; e iv) o direito de retificação de dados incorretos, inclusive por meio do *habeas data*” (Brasil, 2023b).

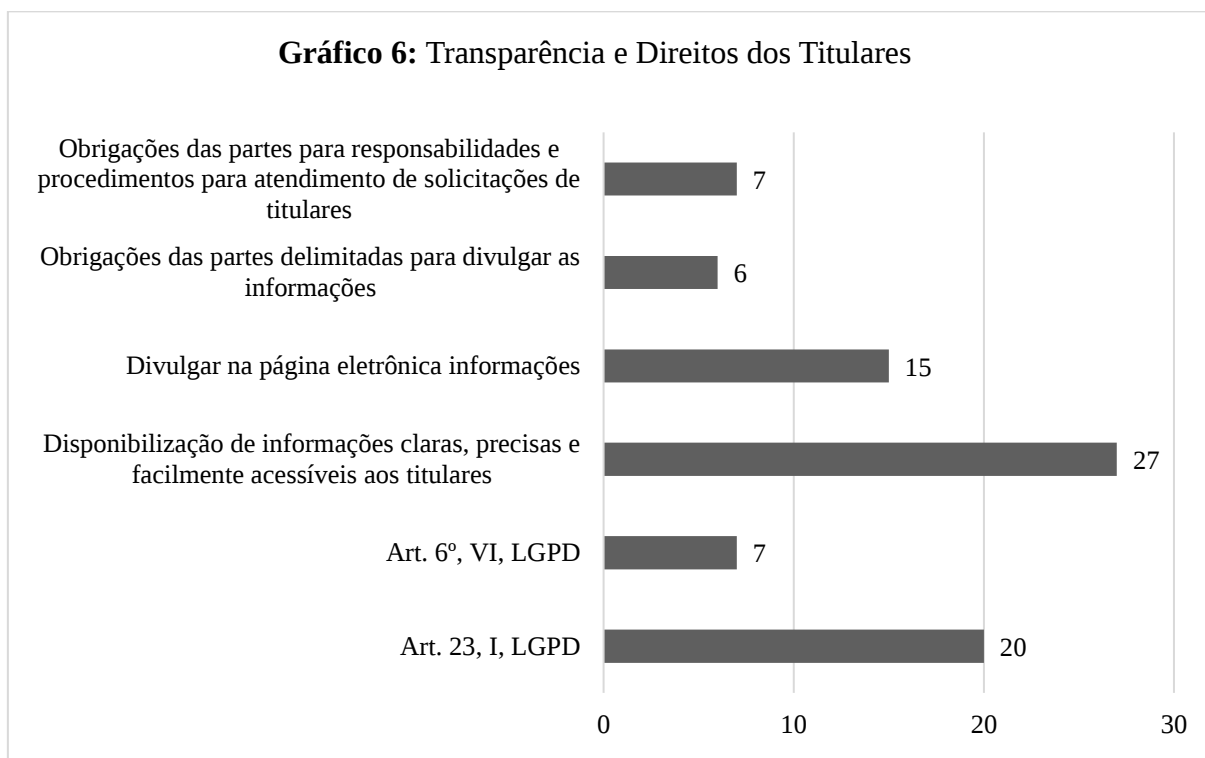
O direito de ser informado é atendido com a devida disponibilização do compartilhamento realizado nos sítios eletrônicos das entidades envolvidas⁷. Já os direitos de acesso à informação, à explicação e à retificação exigem cláusula que aponte qual parte terá essa responsabilidade e se relaciona com o princípio da capacidade de resposta, que visa atender de forma eficiente às demandas do cidadão.

Para o grupo de código “Transparência e direitos dos titulares”, foram criados os seguintes códigos:

- a) Art. 23, I, LGPD;
- b) Art. 6º, VI, LGPD;
- c) Disponibilização de informações claras, precisas e facilmente acessíveis aos titulares sobre a realização do compartilhamento e sobre como exercer seus direitos;
- d) Divulgar na página eletrônica informações;
- e) Obrigações das partes delimitadas para divulgar as informações;
- f) Obrigações das partes para responsabilidades e procedimentos para atendimento de solicitações de titulares.

⁷ Sobre o tema, o STF, na decisão no julgamento conjunto da ADI 6649 e da ADPF 695 do STF, esclarece: “O direito à informação, por motivos de ordem prática, não precisa ser individualizado em todos os casos, sobretudo se em tela tratamentos de grandes volumes de dados, quando a informação pode ser divulgada de modo coletivo, por meio de avisos gerais e da publicação na internet, nos sites oficiais, tudo conforme dispuser a Autoridade Nacional de Proteção de Dados, segundo o disposto no art. 23, § 1º, da LGPD.”

Em análise dos documentos, extraíram-se as seguintes informações:



Fonte: elaboração própria com dados da ferramenta *Atlas.ti*.

Ainda, fazendo a devida seleção dos códigos pertencentes ao grupo de código “Transparência e direitos dos titulares”, tem-se que, dos 43 documentos analisados, menos da metade, ou seja, 21 documentos, trouxeram a previsão sobre a transparência e o direito dos titulares. A transparência é dever do Poder Público de grande relevância que possibilita justamente que os titulares tenham acesso às informações sobre o compartilhamento que está sendo realizado com seus dados pessoais. Está relacionada ao princípio do livre acesso e permite que os titulares tenham acesso facilitado sobre a forma e a duração do tratamento.

Analisando-se em conjunto os artigos 6º, IV e VI, e 23, I, da LGPD, bem como o Guia Orientativo da ANPD, a transparência abrange a divulgação das seguintes informações: forma, duração, previsão legal e finalidade do tratamento, procedimentos e práticas utilizadas para tratamento e agente de tratamento envolvidos, responsabilidades e procedimentos para atender às solicitações dos titulares dos dados pessoais.

Em relação às solicitações dos titulares dos dados pessoais, a Procuradoria-Geral do Estado do Espírito Santo, no Despacho PGE/PPE nº 00067/2023, sugere a seguinte cláusula:

X.X.1.2. Ao receber o requerimento de um titular de dados, na forma prevista nos artigos 16 e 18 da Lei Federal nº 13.709/2018, o CONVENIENTE deverá:

X.X.1.2.1. Notificar imediatamente o CONCEDENTE; e

X.X.1.2.2. Auxiliá-la, quando for o caso, na elaboração da resposta ao requerimento; X.X.1.2.3. Eliminar todos os dados pessoais tratados com base no consentimento em até 30 (trinta) dias corridos, contados a partir do requerimento do titular (Espírito Santo, 2023).

Consoante se observa, prestigia-se a mútua cooperação entre os órgãos priorizando-se o atendimento da demanda do titular dos dados pessoais.

A transparência constitui-se em um dos pilares para a construção de um governo aberto e representa o compromisso com a divulgação das atividades desenvolvidas, prestando informações confiáveis, relevantes e tempestivas à sociedade (Brasil, 2018b, p. 53), tendo como principal diretriz a implementação de boas práticas de transparência.

6.7 Prevenção e segurança

Prevenção e segurança são princípios constantes da LGPD, previstos, respectivamente, nos incisos VIII e VII do art. 6º. Prevenção é a “adoção de medidas para prevenir a ocorrência de danos” (Brasil, 2018a), decorre do objetivo da LGPD de mudar a cultura no tratamento de dados pessoais para mitigação de riscos e está relacionada ao conceito de *privacy by design*, que é pautado em sete princípios fundamentais:

- Proativo, não Reativo; Preventivo, não Corretivo: adoção de postura preventiva e medidas proativas e não reativas, de modo a evitar incidentes de violação à privacidade;
- Privacidade como Configuração Padrão: a configuração padrão de qualquer sistema deve preservar a privacidade do usuário. Ou seja, dados pessoais devem ser protegidos automaticamente, mesmo quando não há qualquer ação do titular, pois a tutela estará embutida no sistema;
- Privacidade Incorporada ao Design: a privacidade deve estar incorporada à arquitetura de sistemas e aos modelos de negócio, de forma que a proteção de dados pessoais se torna um componente essencial da própria funcionalidade do tratamento;
- Funcionalidade Completa – Soma Positiva, não Soma Zero: devem ser acomodados todos os interesses e objetivos envolvidos, evitando falsas dicotomias que levem à mitigação de direitos (como privacidade v. segurança);
- Segurança de Ponta a Ponta – Proteção Completa de Ciclo de Vida: como a segurança de dados é incorporada ao sistema antes da coleta, a prevenção e as medidas de segurança se estendem para todo o ciclo de vida dos dados envolvidos, de ponta a ponta;
- Visibilidade e Transparência – Manter em Aberto: deve ser assegurado que todos os envolvidos sejam informados de forma suficientemente transparente acerca dos componentes e do modelo de operação do tratamento de dados de acordo com as premissas e objetivos combinados; e
- Respeito à Privacidade do Usuário – Manter Centrado no Usuário: exige que os agentes do tratamento respeitem os interesses dos usuários, mantendo altos padrões de privacidade (Vainzof, 2022, PG-1.2) (Tradução nossa).

Por sua vez, as medidas de segurança, técnicas e administrativas, visam proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (Brasil, 2018a). Devem “estar previstas nos atos que regem e autorizam o compartilhamento de dados” (Brasil, 2023a, p. 34).

As medidas técnicas se referem ao uso de recursos dos sistemas que mantêm os dados pessoais. As medidas administrativas visam à promoção da conformidade das ações com a LGPD e à organização da segurança da informação na instituição. As medidas técnicas, como o uso de firewalls, métodos criptográficos e controles de conteúdo, devem ficar acompanhadas das medidas administrativas (Menke; Goulart, 2023, p. 348).

Para pesquisar o ponto, foram criados os seguintes códigos:

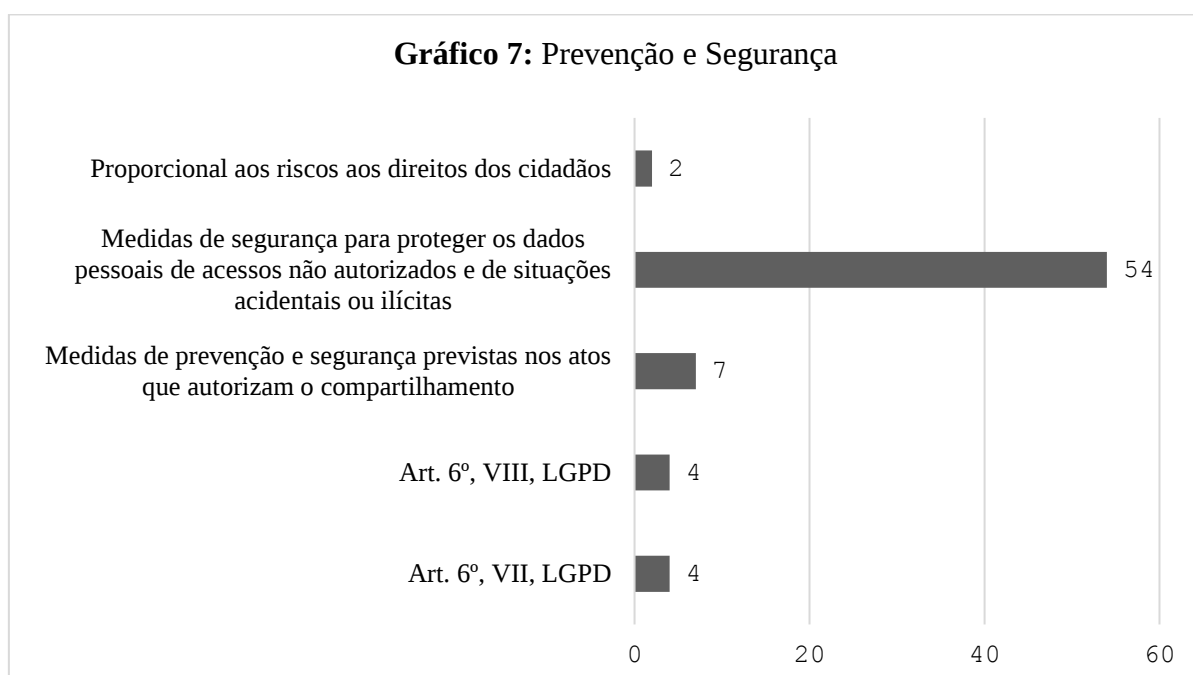
- a) Art. 6º, VII, LGPD;
- b) Art. 6º, VIII, LGPD;

c) Medidas de prevenção e segurança previstas nos atos que autorizam o compartilhamento;

d) Medidas de segurança para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

e) Proporcional aos riscos aos direitos dos cidadãos.

Dos documentos analisados, tem-se o seguinte:



Fonte: elaboração própria com dados da ferramenta *Atlas.ti*.

As medidas de prevenção e segurança se repetem ao longo dos documentos analisados e visam evitar o compartilhamento de dados pessoais com quem não tenha necessidade de conhecê-los, bem como evitar vazamento de dados ou sua destruição, perda, alteração, comunicação ou difusão. Além da expressa previsão dos princípios e seus conceitos nos instrumentos que visam compartilhar dados pessoais, há deveres que decorrem diretamente da sua aplicação.

O primeiro dever refere-se à obrigação de documentar, registrar ou especificar quais medidas de segurança e prevenção são adotadas, pois essas medidas podem ser exigidas a qualquer momento.

O segundo dever traz a obrigação de comunicação imediata sobre incidentes de segurança. O receptor de dados pessoais tem a obrigação de comunicar, de forma imediata, “a ocorrência de qualquer risco, ameaça ou incidente de segurança que possa acarretar comprometimento ou dano potencial ou efetivo a Titular de dados pessoais” (Mato Grosso do Sul, 2022, p. 18, Parecer 2/2022). De acordo com o Despacho PGE/PPE nº 67/2023 da Procuradoria Geral do Estado do Espírito Santo, as obrigações podem ser assim delimitadas:

X.X.3.1. A CONVENIENTE deverá notificar a CONCEDENTE imediatamente sobre a ocorrência de incidentes de segurança relacionados a dados pessoais, fornecendo informações suficientes para que a CONCEDENTE cumpra quaisquer deveres de comunicação, dirigidos à Autoridade Nacional de Proteção de Dados e/ou aos titulares dos dados, acerca do incidente de segurança (Espírito Santo, 2023).

A comunicação imediata pode estar prevista com um prazo determinado. Assim, por exemplo, a Procuradoria-Geral do Estado de Santa Catarina determina que a comunicação ocorra em um prazo de até 24 (vinte e quatro) horas (Santa Catarina, 2022, p. 31):

X.X.3.2. As partes deverão adotar as medidas cabíveis para auxiliar na investigação e na mitigação das consequências de cada incidente de segurança.

(...)

X.X.5.4. Se o CONCEDENTE constatar que dados pessoais foram utilizados pelo CONVENIENTE para fins ilegais, ilícitos, contrários à moralidade ou mesmo para fins diversos daqueles necessários ao cumprimento deste Convênio, o CONVENIENTE será notificado para promover a cessação imediata desse uso, sem prejuízo da rescisão do Convênio e de sua responsabilização pela integralidade dos danos causados.

O terceiro dever é o auxílio na investigação e na mitigação das consequências do incidente, inclusive em eventuais auditorias que se fizerem necessárias, com a possibilidade de cessação imediata do uso dos dados pessoais, quando constatar sua utilização para fins ilegais, ilícitos, contrários à moralidade ou para fins diversos dos previstos.

Sob o olhar das boas práticas de governança, a observância de medidas de prevenção e segurança busca atender aos princípios da integridade, da confiabilidade e da responsabilidade. Como parte do controle de gestão de riscos, a previsão expressa nos instrumentos sobre a forma de ação em caso de incidente de segurança faz emergir o caráter preventivo, vez que a existência

de um plano de respostas de incidentes possibilita a reação antecipada para enfrentar os mais variados cenários (Menke; Goulart, 2023, p. 359).

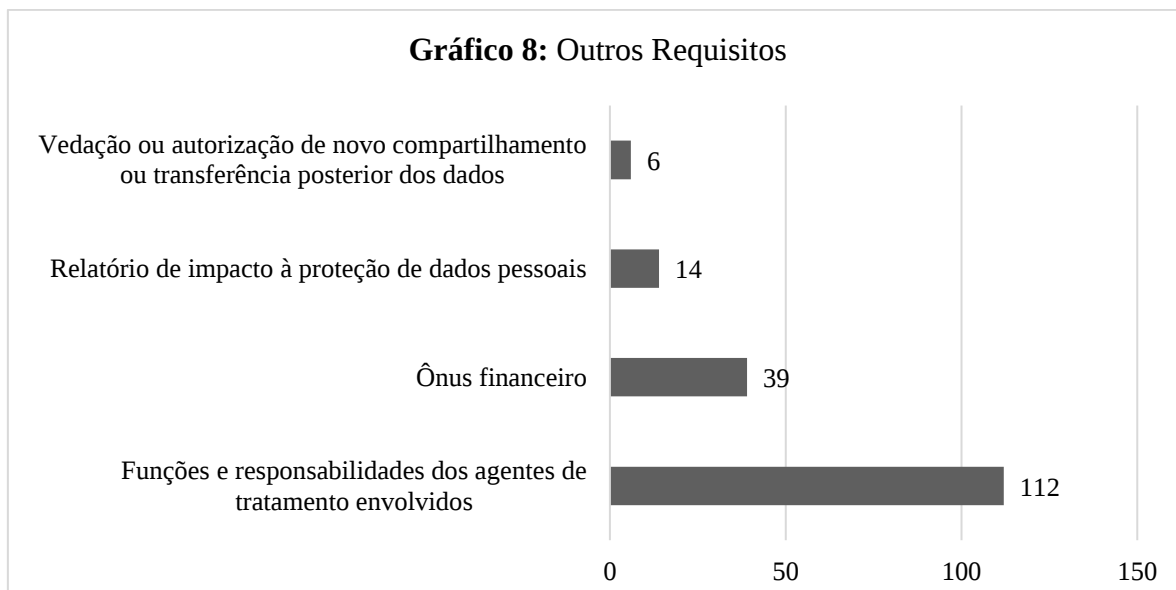
6.8 Outros requisitos

Nesse tópico, a ANPD traz justamente algumas possibilidades de se atender a “outros requisitos, que decorram das peculiaridades do caso concreto ou de determinações provenientes de normas específicas” (Brasil, 2023a, p. 34). A ANPD traz então alguns exemplos de outros requisitos que podem ser exigidos. Assim, tem-se a possibilidade ou não de um novo compartilhamento de dados pessoais pelo órgão recebedor, eventuais ônus financeiros decorrentes do acesso a sistemas, as responsabilidades dos agentes de tratamento envolvidos no compartilhamento e a elaboração do relatório de impacto à proteção de dados pessoais.

Dentro do grupo de códigos “Outros requisitos”, foram criados os seguintes códigos:

- a) Funções e responsabilidades dos agentes de tratamento envolvidos;
- b) Ônus financeiro;
- c) Relatório de impacto à proteção de dados pessoais;
- d) Vedação ou autorização de novo compartilhamento ou transferência posterior dos dados.

Analisados os documentos, tem-se o seguinte gráfico:



Fonte: elaboração própria com dados da ferramenta *Atlas.ti*.

Para melhor compreensão de cada um desses requisitos, os temas serão tratados de forma separada nos seguintes subcapítulos.

6.8.1 Funções e responsabilidades dos agentes de tratamento

Os agentes de tratamento são objeto de um guia orientativo próprio, elaborado pela ANPD, denominado Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Não cabe ao presente estudo o aprofundamento sobre os conceitos de agentes de tratamento e suas implicações.

De relevante do Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado (Brasil, 2022a, p. 7), anota-se que “a organização é o agente de tratamento para os fins da LGPD, já que é esta que estabelece as regras para o tratamento de dados pessoais, a serem executadas por seus representantes ou prepostos” e “para cada operação de tratamento de dados pessoais, portanto, a mesma organização poderá ser controladora e operadora”. Por sua vez, “os funcionários atuarão em subordinação às decisões do controlador, não se confundindo, portanto, com os operadores de dados pessoais”.

No caso do Poder Público, pelas suas peculiaridades, “as atribuições de controlador, por força da desconcentração administrativa, são exercidas pelos órgãos públicos que

desempenham funções em nome da pessoa jurídica da qual fazem parte, fenômeno que caracteriza a distribuição interna das competências” (Brasil, 2022a, p. 10).

Assim, considerando-se a subordinação administrativa a que estão submetidos os agentes públicos dentro de cada estrutura organizacional, entende-se que as obrigações dos agentes de tratamento, a depender do caso, podem ser a eles estendidas. Por esse motivo, neste código de “Funções e responsabilidades dos agentes de tratamento” englobaram-se também as atribuições de ambas as partes atuantes no processo de compartilhamento de dados pessoais.

Por essa razão, propõe como requisito, a ser observado no compartilhamento de dados pessoais, a determinação de funções e responsabilidades das partes envolvidas no compartilhamento de dados pessoais, que, neste capítulo, será denominado apenas como funções e responsabilidades das partes envolvidas.

Dentre as funções das partes envolvidas, algumas apresentaram elevada recorrência nos documentos analisados.

A primeira diz respeito a obrigações de sigilo e confidencialidade (com 20 recorrências). Em verdade, esse dever já é abordado nas legislações relativas ao funcionalismo público. Como exemplo, a Lei nº 8.112/90 determina como dever do servidor guardar sigilo sobre assunto da repartição (Brasil, 1990b).

Assim, a previsão dessa atribuição é decorrência de um dever institucional do Poder Público. Por mais razões ainda, o Decreto nº 10.046/2019 definiu que “o compartilhamento de dados sujeitos a sigilo implica a assunção, pelo recebedor de dados, dos deveres de sigilo e auditabilidade impostos custodiante dos dados” (Brasil, 2019).

A Procuradoria-Geral do Estado de Santa Catarina, no Parecer nº 150/2022-PGE, sugere a seguinte cláusula para observância do dever de sigilo:

1. Os cooperantes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis repassadas em decorrência da execução do objeto do termo de cooperação, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), sendo vedado o repasse das informações a outras pessoas físicas ou jurídicas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do termo de cooperação (Santa Catarina, 2022)

De outro modo, a Procuradoria-Geral do Estado do Paraná vai além para determinar que, na minuta padronizada de termo de convênio aprovada pelo Parecer Referencial nº 04/2022-PGE, seja firmado “termo de compromisso e confidencialidade, em que se responsabiliza pelo cumprimento da LGPD e pelo disposto no presente convênio” (Paraná, 2022). A Procuradoria-Geral do Estado de Pernambuco também exige o compromisso formal de preservar a confidencialidade e segurança dos dados (Parecer nº 0645/2023).

A segunda função diz respeito ao compromisso que deve ser firmado pelas partes para resguardar e proteger a intimidade, vida privada, honra e imagem dos titulares dos dados pessoais, observando as normas e políticas internas relacionadas a coleta, guarda, tratamento, transmissão e eliminação de dados pessoais, especialmente as previstas na LGPD. Essa cláusula é denominada pela Procuradoria-Geral do Estado do Espírito Santo como “Proteção de dados, coleta e tratamento”.

Apesar de parecer uma cláusula óbvia, eis que os deveres impostos pela LGPD se aplicam tanto aos entes que concedem acesso a dados pessoais como àqueles que recebem dados pessoais, a cláusula sugerida impõe uma peculiaridade, que quase passa despercebida. Diz respeito à observância das normas internas e políticas internas relativas à proteção de dados pessoais. Ou seja, a política interna de um ente, quando da formalização do compartilhamento de dados pessoais, se estende ao outro ente que receberá esses dados.

Da mesma forma, dentro dessa função, deve-se dispor sobre a necessidade de observância dos protocolos de segurança determinados pelo ente que concede acesso aos dados pessoais.

Como terceira função, cita-se o dever de fiscalização da execução do ajuste firmado, devendo ser indicados os agentes públicos responsáveis por essa fiscalização. Essa função condiz com a boa prática de governança de definir de forma clara os papéis dos agentes envolvidos, para que sejam desempenhados de forma efetiva.

Consoante se observa dos estudos apresentados nos capítulos anteriores, há outras funções que surgem dos demais requisitos. Em verdade, todo requisito traz em si uma obrigação a ser observada pelas partes envolvidas. Assim, por exemplo, quando foram abordadas as normas de segurança e suas implicações.

Em relação à responsabilidade das partes envolvidas, tema amplamente citado nos documentos analisados, o STF, na decisão no julgamento conjunto da ADI 6649 e da ADPF 695, concluiu que o compartilhamento de dados pessoais contrário aos parâmetros

estabelecidos importa a responsabilidade civil do Estado pelos danos causados aos titulares dos dados, preservado o direito de regresso contra os agentes públicos responsáveis pelo ato ilícito, em caso de dolo ou culpa. Ainda, sem prejuízo de eventuais punições disciplinares, bem como punições por improbidade administrativa, nos termos do art. 11, inciso IV, da Lei nº 8.429/1992, e incidência de outras tipificações legais, a depender do caso concreto.

O requisito está diretamente relacionado aos princípios da prestação de contas e da responsabilidade e com a diretriz de boa governança específica sobre “prestar contas às partes interessadas e implementar mecanismos eficazes de responsabilização dos agentes” (Brasil, 2020a, p. 49).

6.8.2 Ônus financeiro

O instrumento que disciplinar as normas incidentes sobre o compartilhamento de dados pessoais deve trazer cláusula sobre o ônus financeiro. Deve estar previsto se haverá o repasse de recursos entre os órgãos que compartilham os dados.

Dos documentos analisados, 24 trataram do ônus financeiro e, em todos eles, houve determinação de ausência de repasse de recursos financeiros, ou seja, os acordos são celebrados a título gratuito. Isso decorre, inclusive, até pela natureza dos acordos de cooperação, que são ajustes que não envolvem repasse de recursos financeiros, como já afirmado neste trabalho.

No entanto, a ausência de repasses financeiros não significa a ausência de gastos financeiros com a execução do ajuste. Por isso, determina-se que cabe a cada uma das partes arcar “com o custeio das despesas inerentes a execução das ações e obrigações sob sua competência” (Rio de Janeiro, 2023, p. 4). Nesse sentido, recomenda-se que haja o detalhamento das ações materiais e recursos humanos e financeiros que serão gastos por cada órgão, ainda que indiretos (Rio de Janeiro, 2024, p. 6).

6.8.3 Relatório de impacto à proteção de dados pessoais

O relatório de impacto à proteção de dados pessoais é conceituado no inciso XVII do art. 5º da LGPD como a “documentação do controlador que contém a descrição dos processos

de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos” (Brasil, 2018a).

Conforme apontado por Langenegger (2023, p. 314), “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”. Em 06 de abril de 2023, a ANPD publicou, em seu sítio eletrônico, “Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais”.

Em um dos quesitos, determinou-se que, enquanto não for editado regulamento específico sobre a definição de alto risco, pode-se adotar como parâmetro o conceito do art. 4^o do Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte, aprovado pela Resolução nº 2/2022.

Analisando-se citado dispositivo legal, o alto risco é determinado pela coexistência de um critério geral e um critério específico, tendo a ANPD elaborado o seguinte gráfico explicativo:

⁸ Art. 4º Para fins deste regulamento, e sem prejuízo do disposto no art. 16, será considerado de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados:

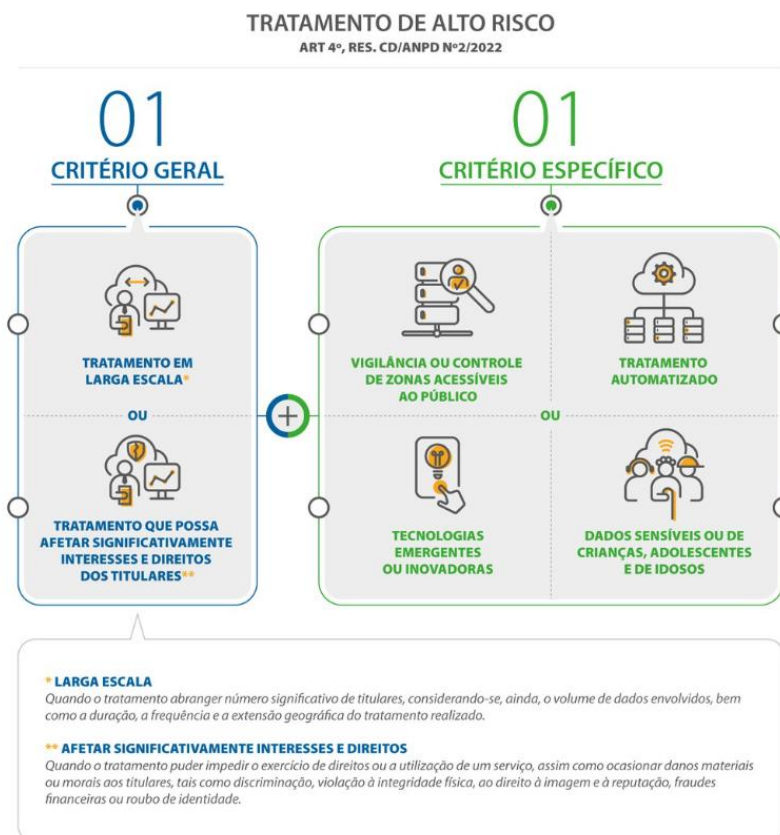
I - critérios gerais:

a) tratamento de dados pessoais em larga escala; ou
b) tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;

II - critérios específicos:

a) uso de tecnologias emergentes ou inovadoras;
b) vigilância ou controle de zonas acessíveis ao público;
c) decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou
d) utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos (Brasil, 2022).

Gráfico 9: Critérios para definição de tratamento de alto risco



Fonte: sítio eletrônico da ANPD (https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p6).

Contudo, a própria ANPD ressalva que os critérios não são exaustivos, podendo-se verificar alto risco em outras situações que não as elencadas na citada Resolução.

Em relação aos documentos analisados, o Relatório de Impacto foi citado em apenas 8 documentos. Dos achados encontrados, é relevante citar a obrigação prevista em alguns casos de que o ente que recebe os dados pessoais pode ser provocado para colaborar na elaboração do relatório de impacto à proteção de dados pessoais (Mato Grosso do Sul, 2022, p. 17). Apesar de parecer óbvio que eventual colaboração possa ser solicitada, é recomendável que os instrumentos que compartilhem dados pessoais tragam a disposição de forma expressa.

Todas essas informações são convergentes com a diretriz de boa governança para a implementação de um sistema eficaz de gestão de riscos. A ANPD, em seu sítio eletrônico, abordou o tema em questão específica sobre os critérios e metodologias a serem utilizados para a gestão de riscos, pelo qual destacou que “a identificação e análise dos fatores de risco devem ser documentadas e justificadas para que possam demonstrar que as decisões tomadas em

relação à gestão de riscos foram as medidas mais adequadas com base nas informações disponíveis” (ANPD, 2023).

Ainda em relação às diretrizes de governança, a publicação do Relatório de Impacto representa “uma forma de cumprir com o princípio da transparência e de assegurar meios para a *accountability* social sobre como dados pessoais são tratados por determinados órgãos ou entidades públicas” (Langenegger, 2023, p. 316).

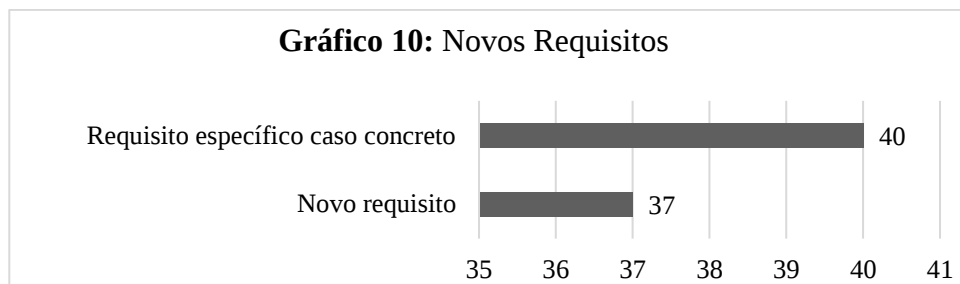
6.8.4 Vedação ou autorização de novo compartilhamento

Da mesma forma que o requisito anterior, também a previsão de vedação ou autorização de novo compartilhamento foi citada em reduzidos documentos analisados, precisamente 4. Desses, 3 vedaram expressamente o novo compartilhamento de dados pessoais pela parte que os recebe, sendo das Procuradorias dos Estados do Mato Grosso do Sul, Paraná e Rio de Janeiro. O baixo índice de citação não afasta a relevância do requisito. Em não havendo previsão expressa no instrumento que permitiu o compartilhamento de dados pessoais e havendo interesse no novo compartilhamento, recomenda-se que o órgão que cedeu os dados deva ser consultado, previamente, para cumprir a exigência de autorização de compartilhamento. O novo compartilhamento, caso autorizado, deve cumprir todos os requisitos citados.

6.9 Novos requisitos

Como destacado no Subcapítulo “Outros Requisitos”, a ANPD não esgotou o tema dos requisitos para o compartilhamento de dados pessoais no Poder Público, abrindo a possibilidade para a existência de “outros requisitos, que decorram das peculiaridades do caso concreto ou de determinações provenientes de normas específicas” (Brasil, 2023a, p. 34). Disciplinou, no Guia Orientativo, os principais requisitos, mas autorizou que novos requisitos surjam de acordo com as peculiaridades de cada caso concreto.

Por esse motivo, foi criado o grupo de código “Novos requisitos” com os códigos “Novo requisito” e “Requisito específico do caso concreto”, com a seguinte incidência:



Fonte: elaboração própria com dados da ferramenta *Atlas.ti*.

Em relação ao código “Requisito específico caso concreto”, a análise concluiu que se referem a normas locais sobre o tema, que, em sua maioria, já estão inseridas dentro de algum dos requisitos abordados no presente estudo, ou a informações de dados pessoais específicos, como exemplo o tratamento de dados de crianças, que exige o consentimento dos pais ou responsáveis⁹. De toda forma, não demandam uma análise aprofundada para o presente estudo.

Com base na análise dos dados obtidos com o código “Novo requisito”, apresenta-se os seguintes parâmetros, que serão tratados nos subcapítulos seguintes: a) vedação ou autorização para transferência internacional; b) princípios da qualidade do dado e da não discriminação; e c) indicação do encarregado de dados.

6.9.1 Vedação ou autorização para transferência internacional

O requisito pode ser entendido como a vedação de transferência de dados pessoais para fora do território do Brasil sem o prévio consentimento do ente que concede acesso aos dados pessoais. Caso o consentimento seja realizado, o receptor deve observar as normas de proteção e privacidade de dados do país de destino, no que for aplicável. No Parecer PGE/PCA nº

⁹ Sobre o tema o Parecer nº 0447/2021, da Procuradoria-Geral do Estado de Pernambuco: “Percebe-se que o tratamento de dados de crianças tem como condição sine qua non o consentimento dos pais ou responsáveis, podendo ser usados sem tal consentimento apenas em duas hipóteses. Uma delas, conforme exposto acima, é a proteção da criança. Considerando seu conceito subjetivo, “proteção” pode ser entendido como a proteção à vida e à incolumidade física, que também são possibilidades de tratamento de dado pessoal sensível sem consentimento do titular, conforme alínea 'e', do inciso II, do artigo 11 da LGPD. Alinhe-se, ad cautelam, que as exceções previstas para a coleta do dado também são extensíveis ao seu compartilhamento, já que este é uma das operações possíveis dentro do processo de tratamento do dado.”

00103/2022, da Procuradoria-Geral do Estado do Espírito Santo, recomenda-se a inserção da seguinte cláusula:

X.X.4. Transferência internacional.

É vedada a transferência de dados pessoais pela CONVENIENTE para fora do território do Brasil sem o prévio consentimento, por escrito, da CONCEDENTE, e demonstração da observância da adequada proteção desses dados, cabendo ao CONVENIENTE a responsabilidade pelo cumprimento da legislação de proteção de dados ou de privacidade de outro(s) país(es) que for aplicável (Espírito Santo, 2022)

Além do mais, é relevante registrar que, para a transferência internacional, a LGPD exige o enquadramento em uma das hipóteses previstas no art. 33:

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do [art. 1º da Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional (Brasil, 2018a).

Ou seja, além dos requisitos aqui abordados, deve-se observar o Capítulo V da LGPD, específico para a transferência internacional de dados.

6.9.2 Princípios da qualidade do dado e da não discriminação

O Despacho nº 2232/2020-GAB da Procuradoria-Geral do Estado de Goiás cita o Guia de Boas Práticas: Lei Geral de Proteção de Dados (LGPD) – Guia de Boas Práticas para Implementação na Administração Pública Federal, com o objetivo de auxiliar na densificação dos princípios da LGPD. Dentre os itens do Guia de Boas Práticas, a PGE/GO cita a verificação de conformidade do tratamento de dados quanto aos princípios da LGPD, conforme Anexo a esta dissertação.

Os itens constantes do Guia de Boas Práticas foram abordados ao longo deste estudo em seus capítulos próprios. Destaca-se, nesta oportunidade, os princípios da qualidade do dado e da não discriminação, dos quais emergem duas atribuições que devem ser observadas pelo Poder Público.

Para o cumprimento do princípio da qualidade do dado, é necessário definir procedimento de verificação contínua quanto à exatidão, à clareza, à relevância e à atualização dos dados pessoais. Por sua vez, para o atendimento do princípio da não discriminação, deve ser inserida cláusula com o compromisso de não realizar o tratamento do dado para fins discriminatórios, ilícitos ou abusivos.

6.9.3 Indicação do encarregado de dados

No Guia Orientativo: Tratamento de dados pessoais pelo Poder Público, no subcapítulo “Transparência e livre acesso” do capítulo “Princípios”, destacou-se que “deve ser objeto de divulgação a identidade e as informações de contato do encarregado (art. 41, § 1º)” (Brasil, 2023a, p. 27). A LGPD regulamentou o tema de forma expressa para o Poder Público no inciso III do art. 23:

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do [art. 1º da Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

(...)

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei (Brasil, 2018a).

No mesmo sentido, a indicação do encarregado de dados foi exigida nos documentos analisados (com 12 recorrências). Sobre o tema, destaca-se recomendação da Procuradoria-Geral do Distrito Federal, no Parecer nº 592/2022-PGDF/PGCONS, para inserção de cláusula no instrumento que permite o compartilhamento de dados pessoais com a indicação do encarregado e sua identificação. “Recomenda-se incluir disposição acerca da forma de substituição do encarregado (art. 23, III, c/c o art. 39 c/c o art. 41 da LGPG), caso os servidores indicados na cláusula terceira deixem de exercer tal encargo”, devendo essa substituição ser comunicada a outra parte em tempo razoável (Distrito Federal, 2022).

A recomendação de cláusula específica não se perfaz de caráter obrigatório, considerando que o requisito de divulgação da identificação do encarregado de dados pode ser suprido com a disponibilização da informação nos sítios eletrônicos dos entes. Esse o entendimento da Advocacia-Geral da União no Parecer n. 00304/2023/CONJUR-CGU/CGU/AGU.

Dentre as atribuições do encarregado de dados, a Procuradoria-Geral do Estado do Rio de Janeiro insere a possibilidade de o encarregado colaborar para a elaboração da minuta do instrumento que permite o compartilhamento de dados pessoais.

6.10 Considerações finais sobre os dados analisados

Dentre os 43 documentos analisados, é relevante registrar que não foram encontradas divergências entre eles. Para a formalização do compartilhamento de dados pessoais no Poder Público, foram exigidos requisitos semelhantes entre si, consubstanciados nos subcapítulos acima expostos.

Contudo, destaca-se que, dos 43 documentos analisados, em 16 documentos, a advocacia pública não aprofundou a análise sobre o tema, limitando-se a citar as disposições legais sem adentrar no mérito de cada requisito. Além do mais, desses 16, em 3 documentos, a advocacia pública limitou-se a analisar o caso do compartilhamento de dados pessoais à luz da Lei nº 8.666/93, preocupando-se apenas com o processo administrativo para a formalização do ajuste.

Outra informação que merece destaque é que apenas 5 documentos citaram o Guia Orientativo - Tratamento de dados pessoais pelo Poder Público, da ANPD. Considerando o papel de relevância da ANPD na área de proteção de dados pessoais, entendo que as advocacias públicas devem desempenhar suas atribuições com observância às normas orientadoras publicadas pela ANPD para garantir a própria observância à LGPD.

7 CONSIDERAÇÕES FINAIS

O trabalho, embasado em pesquisa bibliográfica e análise de dados, estudou os documentos jurídicos elaborados pelas advocacias públicas da União, dos Estados e do DF, com base nos parâmetros definidos pela ANPD, no Guia Orientativo - Tratamento de dados pessoais pelo Poder Público, e pelo STF, na decisão no julgamento conjunto da ADI 6649 e da ADPF 695 do STF. Consoante se observa do estudo sobre as orientações e parâmetros utilizados para o compartilhamento de dados pessoais no Poder Público, tem-se que, de forma geral, as manifestações jurídicas das advocacias públicas convergem com as orientações da ANPD e do STF.

Os requisitos para o compartilhamento de dados pessoais no Poder Público foram delimitados no presente estudo, divididos em base legal, formalização e registro, objeto, finalidade, duração do tratamento, transparência e direitos dos titulares, prevenção e segurança, outros requisitos e novos requisitos.

A base legal trata da obrigatoriedade de se observar dois pressupostos, quais sejam, indicação e enquadramento em uma das bases legais previstas na LGPD, art. 7º, art. 11 ou art. 23, e justificativa de interesse público.

Para cumprimento da formalização e registro, tem-se o desdobramento em três orientações: ato formal, formalização em atenção às normas gerais que regem os procedimentos administrativos, que abarca também a instauração de processo administrativo, e a formalização em atenção à obrigatoriedade de registro, que engloba o art. 37 da LGPD.

O ato formal normalmente utilizado pelas advocacias públicas é o acordo/termo/convênio de cooperação técnica ou termo/convênio de adesão. É relevante trazer a perspectiva apresentada pelo estudo sobre os instrumentos que concretizam a celeridade no processo de compartilhamento de dados pessoais. O primeiro diz respeito à utilização de instrumento padrão para o compartilhamento de dados pessoais, ou seja, aprova-se um modelo de minuta que poderá ser utilizado por todos os órgãos e entidades que têm interesse em acessar determinados dados pessoais. Nesse instrumento, as cláusulas são pré-definidas e cabe ao órgão receptor de dados aceitá-las.

Sobre o tema, viu-se que alguns Estados dispensam a celebração de ato formal, desde que observadas as disposições da LGPD. Ou seja, mesmo nessas hipóteses, os parâmetros aqui trazidos devem ser observados.

O segundo instrumento de celeridade trata do Parecer Referencial, que pode apresentar como anexo minuta padronizada de convênio de cooperação técnica ou termo de adesão e respectivo plano de trabalho, com cláusulas pré-definidas. Os pareceres referenciais são instrumentos utilizados pelas diversas advocacias públicas para padronizar o seu entendimento administrativo, conferindo, assim, maior celeridade à tramitação do processo, dispensando-se a análise jurídica pela advocacia pública. Havendo parecer referencial sobre determinado tema, está cumprida a etapa de análise jurídica determinada pela ANPD.

As opções por minuta padronizada e pelo parecer referencial não são excludentes, podendo-se adotar as duas medidas para imprimir ainda mais celeridade ao processo de compartilhamento de dados pessoais.

Para a formalização em atenção às normas gerais que regem os procedimentos administrativos, deve-se observar as normas da Nova Lei de Licitações. Sugere-se a utilização do modelo desenvolvido pela Procuradoria-Geral do Estado do Paraná no Parecer Referencial nº 04/2022-PGE, pelo qual o Plano de Trabalho deve conter as seguintes cláusulas: a) dados cadastrais dos partícipes; b) objeto a ser executado; c) justificativa; d) metas; e) especificações das ações; f) etapas e fases de execução; g) vigência; h) denúncia; e i) gratuidade. Por sua vez, a minuta de convênio apresenta as seguintes cláusulas: a) objeto; b) formas de cooperação; c) obrigações dos partícipes; d) sigilo, utilização e divulgação; e) responsabilidades financeiras; f) gerenciamento e fiscalização; g) vigência, alteração e rescisão; h) denúncia; i) legislação aplicável aos casos omissos; j) publicação; e k) foro.

Em relação à formalização em atenção à obrigatoriedade de registro, citam-se os seguintes parâmetros: a) viabilidade de fornecimento dos registros sempre que for solicitado; b) os registros devem ser mantidos com condições de rastreabilidade e de prova eletrônica a qualquer tempo; e c) indicação das pessoas que serão encarregadas das operações de tratamento dos dados pessoais. Como estudado, o registro é importante ferramenta para a prestação de contas e identificação de eventual responsabilidade no caso de vazamento ou perda de dados.

No objeto, devem ser identificados quais dados serão compartilhados, observando-se o princípio da necessidade. De forma sucinta, a resposta a três questionamentos, quais, por que e para que, bem resumem o atendimento do objeto, da base legal e da finalidade do

compartilhamento de dados pessoais. A propósito, a finalidade abarca tanto o princípio da finalidade como o princípio da adequação. O princípio da finalidade diz respeito à realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular. O princípio da adequação exige a compatibilidade do tratamento com as finalidades informadas ao titular.

Sobre a duração do tratamento, o ajuste que permitir o compartilhamento deve estipular o seu prazo de duração, limitando-se ao estritamente necessário para o atendimento da finalidade do compartilhamento. Do requisito duração do tratamento, decorrem três obrigações. A primeira trata da estipulação do prazo de duração de forma expressa. A segunda refere-se à possibilidade de conservação ou eliminação após o tratamento. Nesse ponto, destacou-se que a regra da LGPD é a eliminação dos dados pessoais após o encerramento da finalidade. Caso o instrumento não discipline a matéria, deve ser providenciada a eliminação dos dados. Caso o ente deseje conservar os dados pessoais, deve ser expressamente autorizado pela parte que concedeu acesso aos dados pessoais. A terceira obrigação traz a necessidade de reavaliação periódica do ato. Observado o prazo decenal previsto na Nova Lei de Licitações, a prorrogação do compartilhamento deve ser justificada e ter por finalidade continuar ou concluir o programa, projeto ou atividade para o qual o compartilhamento foi efetuado.

Outro requisito diz respeito à transparência e direitos dos titulares. A disponibilização do compartilhamento dos dados pessoais nos sítios eletrônicos é relevante mecanismo da boa prática de governança, que outorga credibilidade ao ente público.

Os direitos dos titulares dos dados abarcam o direito de ser informado sobre o tratamento, o direito de acesso à informação, o direito à explicação, em caso de dúvida, e o direito de retificação de dados incorretos. O direito de ser informado é atendido com a devida disponibilização do compartilhamento realizado nos sítios eletrônicos das entidades envolvidas. Já os direitos de acesso à informação, à explicação e à retificação exigem cláusula que aponte qual parte terá essa responsabilidade. A ideia é prestigiar a mútua cooperação entre os órgãos priorizando-se o atendimento da demanda do titular dos dados pessoais.

As medidas de prevenção e segurança visam evitar o compartilhamento de dados pessoais com quem não tenha necessidade de conhecê-los, bem como evitar vazamento de dados ou sua destruição, perda, alteração, comunicação ou difusão. Delas decorrem três deveres. O primeiro é a obrigação de registrar quais medidas de segurança e prevenção são adotadas, isso pode ser exigido a qualquer momento do ente que recebe os dados pessoais. O

segundo refere-se à obrigação de comunicar, imediatamente, quaisquer incidentes de segurança. E o terceiro dever é a obrigação de auxiliar na investigação e na mitigação das consequências do incidente, inclusive o auxílio em auditorias, podendo-se, a qualquer momento, haver a cessação imediata do compartilhamento de dados pessoais, quando constatar sua utilização para fins ilegais, ilícitos, contrários à moralidade ou para fins diversos dos previstos.

Foram explicitados outros requisitos: funções e responsabilidades das partes envolvidas, ônus financeiro, relatório de impacto à proteção de dados pessoais e vedação ou autorização de novo compartilhamento, bem como novos requisitos: vedação ou autorização para transferência internacional, princípios da qualidade do dado e da não discriminação e indicação de encarregado de dados.

Desses, merecem destaque as funções e responsabilidades das partes envolvidas no compartilhamento de dados pessoais, estipulando-se as seguintes obrigações: a) sigilo e confidencialidade; b) compromisso de proteção à intimidade, vida privada, honra e imagem dos titulares dos dados pessoais, observando as normas e políticas internas relacionadas a coleta, guarda, tratamento, transmissão e eliminação de dados pessoais, especialmente as previstas na LGPD; e c) fiscalização da execução do ajuste firmado, devendo ser indicados os agentes públicos responsáveis por essa fiscalização.

Sobre a responsabilidade das partes envolvidas, o compartilhamento de dados pessoais contrário aos parâmetros estabelecidos importa a responsabilidade civil do Estado pelos danos causados aos titulares dos dados, preservado o direito de regresso contra os agentes públicos responsáveis pelo ato ilícito, em caso de dolo ou culpa. Isso sem prejuízo de eventuais punições disciplinares, bem como punições por improbidade administrativa, nos termos do art. 11, inciso IV, da Lei nº 8.429/1992, e incidência de outras tipificações legais, a depender do caso concreto.

Os outros requisitos apresentam solução mais simplificada. Sobre o ônus financeiro, os instrumentos analisados determinaram que não haveria repasse de recursos. Entretanto, cabe a cada uma das partes arcar com o custeio das despesas inerentes a execução das ações e obrigações sob sua competência. No caso do relatório de impacto à proteção de dados pessoais, a parte que recebe os dados pessoais pode ser provocada para colaborar na sua elaboração. E, no que se refere à vedação ou autorização de novo compartilhamento, recomendou-se que, se não houver previsão expressa no instrumento e houver interesse no novo compartilhamento, o órgão que cedeu os dados deve ser consultado, previamente, para cumprir a exigência de

autorização de compartilhamento. O novo compartilhamento, caso autorizado, deve cumprir todos os requisitos citados.

Sobre os novos requisitos, caso haja autorização para transferência internacional, deve ser observado o Capítulo V da LGPD, além de todos os requisitos já citados. Para o cumprimento do princípio da qualidade do dado, é necessário definir procedimento de verificação contínua quanto à exatidão, à clareza, à relevância e à atualização dos dados pessoais. Por sua vez, para o atendimento do princípio da não discriminação, deve ser inserida cláusula com o compromisso de não realizar o tratamento do dado para fins discriminatórios, ilícitos ou abusivos. E a indicação do encarregado de dados refere-se à inserção de cláusula no instrumento com a indicação do encarregado e sua identificação, podendo a exigência ser suprida se houver tal informação divulgada no sítio eletrônico do ente.

Consoante se observa, respondendo à pergunta de pesquisa deste trabalho, os requisitos foram explicitados de forma aprofundada pelo presente estudo, com a indicação dos parâmetros e as orientações que devem ser seguidas para sua devida observância. Como recomendação geral aos entes, é relevante registrar a sugestão de utilização de instrumentos de padronização para o compartilhamento de dados pessoais, como as minutas padronizadas de acordos de cooperação e termos de adesão e a elaboração e aprovação de pareceres referenciais.

Evidente que o estudo aprofundou o tema, mas há questões que poderiam ampliar ainda mais o debate. Como sugestão para a continuação da pesquisa, cita-se o papel dos atores de controle na proteção de dados pessoais. A continuidade do estudo demandaria pesquisa de todas as manifestações dos Tribunais de Contas da União, dos Estados e do DF, bem como das Controladorias Internas desses entes federados.

REFERÊNCIAS BIBLIOGRÁFICAS

ALTOUNIAN, Cláudio Sarian; DE SOUZA, Daniel Luiz; LAPA, Leonard Renne Guimarães. *Gestão e Governança Pública para Resultados: uma visão prática*. 2.ed. atual. Belo Horizonte: Fórum, 2020.

ANPD. Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais. 06 abr. 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p6. Acesso em: 11 ago. 2024.

BARBIERI, Carlos. **Governança de Dados**: Práticas, conceitos e novos caminhos. Rio de Janeiro: Alta Books, 2019.

BINENBOJM, Gustavo. **Poder de polícia, ordenação, regulação**: transformações político-jurídicas, econômicas e institucionais do direito administrativo ordenador [livro eletrônico]. 3. ed. Belo Horizonte: Fórum, 2020. Disponível em: <https://www.forumconhecimento.com.br/livro/L1408/E4272/27968>. Acesso em: 11 ago. 2024.

BIONI, Bruno Ricardo. **Xeque-mate**: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPOPAI/USP Grupo de pesquisa em políticas públicas para o acesso à informação, 2015. Disponível em: https://www.academia.edu/28752561/Xeque_Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 11 ago. 2024.

BOULLOSA, Rosa de Freitas. **Mirando ao revés de política pública**: contextos, conteúdos e desafios em tempos de crise. Publicações da Escola da AGU: Direito e Sociedade III – Políticas Públicas, Urbanismo e Judicialização na Administração Pública. Brasília, v. 11, n. 04, pp. 89-105, out./dez. 2019. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/Publ-Esc-AGU_v.11_n.04.pdf. Acesso em: 11 ago. 2024.

BRASIL. Advocacia-Geral da União. **Parecer nº 15/2013/CÂMARA PERMANENTE CONVÊNIOS/DEP CONSU/PGF/AGU**. 2013a. Disponível em: <https://www.gov.br/agu/pt-br/composicao/procuradoria-geral-federal-1/arquivos/PARECERN152013CAMARAPERMANENTECONVENIOSDEPCONSUGFA GU.pdf/view>. Acesso em: 11 ago. 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo:** tratamento de dados pessoais pelo Poder Público. 2023a. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 11 ago. 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** 2022a. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-agentes-de-tratamento-e-encarregado-defeso-eleitoral.pdf>. Acesso em: 11 ago. 2024.

BRASIL. Comitê Central de Governança de Dados. **Guia de Boas Práticas:** Lei Geral de Proteção de Dados (LGPD). 2020a. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 11 ago. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 ago. 2024.

BRASIL. Consultoria-Geral da União *et al.* **Manual de boas práticas consultivas.** 4ª ed. Brasília: AGU, 2016. Disponível em: <https://www.gov.br/agu/pt-br/assuntos-1/Publicacoes/cartilhas/ManualdeBoasPraticasConsultivas4Edicaorevistaeampliadaaversaomartphone.pdf>. Acesso em: 15 de agosto de 2023.

BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019.** Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/ato2019-2022/2019/decreto/d10046.htm. Acesso em: 11 ago. 2024.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 11 ago. 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. 1990a. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 11 ago. 2024.

BRASIL. **Lei nº 8.112, de 11 de dezembro de 1990.** Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. 1990b.

Disponível em: https://www.planalto.gov.br/ccivil_03/leis/18112cons.htm. Acesso em: 11 ago. 2024.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011.** Disciplina a formação e consulta a bancos de dados com informações de adimplimento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. 2011a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112414.htm. Acesso em: 11 ago. 2024.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. 2011b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Acesso em: 11 ago. 2024.

BRASIL. **Lei nº 12.813, de 16 de maio de 2013.** Dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego; e revoga dispositivos da Lei nº 9.986, de 18 de julho de 2000, e das Medidas Provisórias nºs 2.216-37, de 31 de agosto de 2001, e 2.225-45, de 4 de setembro de 2001. 2013b. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12813.htm#art6. Acesso em: 11 ago. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 11 ago. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de dados Pessoais (LGPD). 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 11 ago. 2024.

BRASIL. **Lei nº 14.133, de 1º de abril de 2021.** Lei de Licitações e Contratos Administrativos. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/114133.htm. Acesso em: 11 ago. 2024.

BRASIL. Presidência da República. **Guia da política de governança pública.** Brasília: Casa Civil da Presidência da República, 2018b. Disponível em: <https://www.gov.br/casacivil/pt-br/assuntos/downloads/guia-da-politica-de-governanca-publica>. Acesso em: 11 ago. 2024.

BRASIL, Senado Federal. **Justificação à proposta de Emenda Constitucional n. 17/2019,** proposta em 12.03.2019, de lavra do Senador Eduardo Gomes. Disponível em:

<https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 11 ago. 2024.

BRASIL, Supremo Tribunal Federal (Plenário). **Decisão no julgamento conjunto da ADI 6649 e da ADPF 695**. Ministro Relator Gilmar Mendes. DJE publicado em 19/06/2023. 2023b. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf>. Acesso em: 11 ago. 2024.

BRASIL, Supremo Tribunal Federal (Plenário). **Decisão no referendo na Medida Cautelar na ADI 6.387**. Ministro Relator Rosa Weber. DJE publicado em 12/11/2020. 2020b. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf>. Acesso em: 11 ago. 2024.

BRASIL, Tribunal de Contas da União (TCU). **Referencial Básico de Governança Organizacional para organizações públicas e outros entes jurisdicionados ao TCU**. 3.ed. Brasília: TCU, Secretaria de Controle Externo da Administração do Estado – SecexAdministração, 2020c. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-publica-a-3-edicao-do-referencial-basico-de-governanca-organizacional.htm>. Acesso em: 11 ago. 2024.

DA SILVA, Mayara Rocumback Vieira. **A proteção de dados pessoais e seus desafios regulatórios**. Revista da Faculdade de Direito, Universidade de São Paulo, v. 114, pp. 791-815, jan./dez. 2019. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/176613/164085>. Acesso em: 11 ago. 2024.

DISTRITO FEDERAL. **Decreto nº 42.094, de 13 de maio de 2021**. Aprova o Regimento Interno da Procuradoria-Geral do Distrito Federal e dá outras providências. 2021a. Disponível em: https://www.sinj.df.gov.br/sinj/Norma/31b81251fb17411b918f1c7efc4a9e8e/Decreto_42094_13_05_2021.html. Acesso em: 11 ago. 2024.

DISTRITO FEDERAL. **Lei Orgânica do Distrito Federal**. Brasília, 1993. Disponível em: <https://www.sinj.df.gov.br/sinj/Norma/66634/LODF.html>. Acesso em: 11 ago. 2024.

DISTRITO FEDERAL. Procuradoria-Geral do Distrito Federal. **Plano estratégico PGDF 2020-2025: 1º versionamento**. 2021b. Disponível em: <https://www.pg.df.gov.br/wp-content/uploads/2021/12/Plano-Estrategico-1o-Versionamento-V.-02.12.pdf>. Acesso em: 11 ago. 2024.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: MENDES, Laura Schertel, DONEDA, Danilo, SARLET, Ingo Wolfgang, RODRIGUES JR, Otavio Luiz. **Tratado de Proteção de Dados Pessoais**. 2.ed. Rio de Janeiro: Forense, 2023a. pp. 3-20.

DONEDA, Danilo. A Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados. In: MENDES, Laura Schertel, DONEDA, Danilo, SARLET, Ingo Wolfgang, RODRIGUES JR, Otavio Luiz. **Tratado de Proteção de Dados Pessoais**. 2.ed. Rio de Janeiro: Forense, 2023b. pp. 461-472.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: Fundamentos da Lei Geral de Proteção de Dados [livro eletrônico]. 2ª Ed. São Paulo: Thomson Reuters Brasil, 2021.

FRAGOSO, Nathalie; VALENTE, Mariana; LANGENEGGER, Natalia; RUIZ, Juliana Pacetta. **Proteção de dados pessoais em políticas de proteção social**: contribuições a partir do estudo sobre o Programa Bolsa Família, diagnósticos e recomendações nº 6. São Paulo: InternetLab, 2021. Disponível em: <https://internetlab.org.br/wp-content/uploads/2021/10/Protecao-de-Dados-Pessoais-em-Politicas-de-Protecao-Social.pdf>. Acesso em: 11 ago. 2024.

GARCIA, Lara Rocha; FERNANDES, Edson Aguilera; GONÇALVES, Rafael Augusto Moreno; BARRETTO, Marcos Ribeiro Pereira. **Lei Geral de Proteção de Dados Pessoais (LGPD)**: guia de implantação. São Paulo: Blucher, 2020.

GASIOLA, Gustavo Gil; MACHADO, Diego; MENDES, Laura Schertel. O tratamento de dados pessoais pela Administração Pública: transparência, bases legais e limites constitucionais. In: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio (Coord.). **A Lei Geral de Proteção de Dados Pessoais LGPD**: aspectos práticos e teóricos relevantes no setor público e privado. São Paulo: Thomson Reuters Brasil, 2021.

JUSTEN FILHO, Marçal. **Curso de Direito Administrativo** [livro eletrônico]. 5.ed. São Paulo: Thomson Reuters Brasil, 2018. Disponível em: <https://next-proview.thomsonreuters.com/launchapp/title/rt/monografias/91049397/v13/document/157101016/anchor/a-157101016>. Acesso em: 11 ago. 2024.

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

LOUREIRO, Beatriz Faria de Almeida; BLEME, Nicolle; MIRANDA, Rodrigo Fontenelle de A. Boas Práticas e Governança na LGPD. In: PIRONTI, Rodrigo (coord.). **Lei Geral de Proteção de Dados no Setor Público**. Belo Horizonte: Fórum, 2021.

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2. ed. Porto Alegre: Arquipélago Editorial, 2019. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico]. 4.ed. São Paulo: Thomson Reuters Brasil, 2022.

MENDES, Laura Schertel. **Autodeterminação informativa: a história de um conceito**. Pensar: Revista de Ciências Jurídicas, v. 25, p. 1-18. Fortaleza: Universidade de Fortaleza, out./dez. 2020. Disponível em: <https://ojs.unifor.br/rpen/article/view/10828/pdf>. Acesso em: 11 ago. 2024.

MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados**. Revista de Direito do Consumidor, v. 120, pp. 469-483. São Paulo: RT, nov./dez. 2018. Disponível em: https://www.academia.edu/42741127/Reflex%C3%B5es_iniciais_sobre_a_nova_lei_geral_de_prote%C3%A7%C3%A3o_de_dados. Acesso em: 11 ago. 2024.

MENDES, Laura Schertel; RODRIGUES JR, Otavio Luiz; DA FONSECA, Gabriel Campos Soares. O Supremo Tribunal Federal, a Proteção Constitucional dos Dados Pessoais e a Positivação superveniente de um Direito Fundamental Autônomo. In: MENDES, Laura Schertel, DONEDA, Danilo, SARLET, Ingo Wolfgang, RODRIGUES JR, Otavio Luiz. **Tratado de Proteção de Dados Pessoais**. 2.ed. Rio de Janeiro: Forense, 2023. pp. 61-71.

MENKE, Fabiano; GOULART, Guilherme Damasio. Segurança da Informação e Vazamento de Dados. In: MENDES, Laura Schertel, DONEDA, Danilo, SARLET, Ingo Wolfgang, RODRIGUES JR, Otavio Luiz. **Tratado de Proteção de Dados Pessoais**. 2.ed. Rio de Janeiro: Forense, 2023. pp. 341-361.

MIRANDA, Gilson Delgado; DORIA, Erika; BARBOSA, Liliane Magaste. **Compartilhamento e tratamento de dados pessoais pelo setor público no Brasil: uma análise do Decreto n. 10.046/2019**. Cadernos Direito Actual, volumen ordinário, n. XVIII, 2022. Disponível em: <https://www.cadernosdedereitoactual.es/ojs/index.php/cadernos/article/view/806>. Acesso em: 11 ago. 2024.

PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). 3ª Ed. São Paulo: Saraiva, 2021. In: PIRONTI, Rodrigo (coord.). **Lei Geral de Proteção de Dados no Setor Público**. Belo Horizonte: Fórum, 2021.

PIRONTI, Rodrigo; TESSEROLLI, Eduardo Ramos Caron. A Lei Geral de Proteção de Dados e o tratamento de dados sensíveis pela Justiça Eleitoral. In: PIRONTI, Rodrigo (coord.). **Lei Geral de Proteção de Dados no Setor Público**. Belo Horizonte: Fórum, 2021.

PIRONTI, Rodrigo; ZILIOOTTO, Mirela Miró. O direito à autodeterminação informativa e a questão do consentimento no tratamento de dados pessoais pela Administração Pública. In: PIRONTI, Rodrigo (coord.). **Lei Geral de Proteção de Dados no Setor Público**. Belo Horizonte: Fórum, 2021.

REIS, Natanrry; CHEDE, Gabriel. A Autoridade Nacional de Proteção de Dados: Função Sancionadora ou de Acultramento. In: PIRONTI, Rodrigo (coord.). **Lei Geral de Proteção de Dados no Setor Público**. Belo Horizonte: Fórum, 2021. pp. 367-377.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. In: MOARES, Maria Celina Bodin de (org.). Rio de Janeiro: Renovar, 2008.

SECCHI, Leonardo. Instrumentos de políticas públicas. In: BOULLOSA, Rosana de Freitas (org.). **Dicionário para a formação em gestão social**. Salvador: CIAGS/UFBA, 2014. pp. 103-105. Disponível em: <https://ud10.arapiraca.ufal.br/repositorio/publicacoes/3056>. Acesso em: 11 ago. 2024.

SILVA, Roberta Zumblick Martins; TARTER, Ana Luisa. Inteligência artificial e direitos fundamentais: a dispensa de consentimento em atividades do poder público. In: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antônio (coord.). **A Lei Geral de Proteção de Dados Pessoais**: aspectos práticos e teóricos no setor público e privado. São Paulo: Thomson Reuters Brasil, 2021.

TASSO, Fernando Antonio. Capítulo IV. Do tratamento de dados pessoais pelo Poder Público. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD: Lei Geral de Proteção de Dados Pessoais Comentada** [livro eletrônico]. 4ª Ed. São Paulo: Thomson Reuters Brasil, 2022. RL-1.8.

TEIXEIRA, Tarcisio. **LGPE e E-commerce**. 2ª Ed. São Paulo: Saraiva, 2021.

UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR)**. Regulation (EU) 2016/679. Disponível em: <https://gdpr-info.eu/>. Acesso em: 11 ago. 2024.

VAINZOF, Rony. Capítulo I. Disposições Preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD: Lei Geral de Proteção de Dados Pessoais Comentada** [livro eletrônico]. 4ª Ed. São Paulo: Thomson Reuters Brasil, 2022. RL-1.2.

VIOLA, Mario; DE TEFFÉ, Chiara Spadaccini. Tratamento de Dados Pessoais na LGPD: estudos sobre as bases legais dos artigos 7º e 11. In: MENDES, Laura Schertel, DONEDA, Danilo, SARLET, Ingo Wolfgang, RODRIGUES JR, Otavio Luiz. **Tratado de Proteção de Dados Pessoais**. 2.ed. Rio de Janeiro: Forense, 2023. pp. 115-146.

WIMMER, Miriam. A LGPD e o balé dos princípios: tensões e convergências na aplicação dos princípios de proteção de dados pessoais ao setor público. In: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antônio (coord.). **A Lei Geral de Proteção de Dados Pessoais: aspectos práticos e teóricos no setor público e privado**. São Paulo: Thomson Reuters Brasil, 2021a. pp. 163-186.

WIMMER, Miriam. **Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia**. Revista Brasileira de Políticas Públicas, v. 11, pp. 123-142. Brasília: UniCeub, abr./2021. 2021b. Disponível em: <https://www.publicacoes.uniceub.br/RBPP/article/view/7136>. Acesso em: 11 ago. 2024.

WIMMER, Miriam. O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. In: In: MENDES, Laura Schertel, DONEDA, Danilo, SARLET, Ingo Wolfgang, RODRIGUES JR, Otavio Luiz. **Tratado de Proteção de Dados Pessoais**. 2.ed. Rio de Janeiro: Forense, 2023. pp. 273-291.

XAVIER, Luciana Pedroso; XAVIER, Marília Pedroso; SPALER, Mayara Guibor. Capítulo 3. Primeiras impressões sobre o tratamento de dados pessoais nas hipóteses de interesse público e execução de contratos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro** [livro eletrônico]. 3ª Ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2023.

ZENKNER, Marcelo; SPINELLI, Mário. A LGPD e sua aplicação nas empresas estatais. In: PIRONTI, Rodrigo (coord.). **Lei Geral de Proteção de Dados no Setor Público**. Belo Horizonte: Fórum, 2021. pp. 291-306.

ANEXO: Guia de Boas Práticas: Lei Geral de Proteção de Dados (LGPD) – Guia de Boas Práticas para Implementação na Administração Pública Federal (p. 29):

2.1.2 Verificação de conformidade do tratamento de dados quanto aos princípios da LGPD

Uma vez identificada(s) a(s) hipótese(s) de tratamento aplicável(is) às situações específicas de processamento de dados por órgãos e entidades da Administração Pública Federal, deve-se partir para outras questões importantes para a verificação da conformidade quanto aos princípios da LGPD.

Para tanto, o órgão ou entidade pública deverá analisar outras questões, detalhadas a seguir.

1. Identifique a finalidade para a qual o tratamento de dado é necessário. Os propósitos devem ser legítimos, específicos e explícitos (princípio da finalidade).
 2. Defina como a finalidade do tratamento será informada ao titular, o que deve ser realizado antes do início do tratamento do dado (princípio da finalidade).
 3. No caso de tratamento de dados que tenha sido iniciado antes da vigência da Lei, indique que providências serão tomadas para comunicar o titular sobre o tratamento realizado e a finalidade a qual se destina (princípio da finalidade).
 4. Garanta que o tratamento do dado será apenas para a finalidade informada ao titular (princípio da adequação). Quaisquer mudanças na finalidade de tratamento deverão ser também comunicadas ao titular do dado.
 5. Ao planejar a forma de tratamento de dados, atente para limitar a utilização ao mínimo de informações necessárias, garantindo abrangência pertinente e proporcional à consecução das finalidades informadas ao titular (princípio da necessidade).
 6. Ao decidir realizar o tratamento de dados, defina antecipadamente os mecanismos e procedimentos que os titulares dos dados deverão utilizar para consultar o conteúdo, a forma e a duração do tratamento dos seus dados pessoais, de maneira facilitada e gratuita (princípio do livre acesso).
 7. Garanta que quaisquer alterações quanto à finalidade especificada para o tratamento do dado; à forma ou à duração do tratamento; ao controlador responsável pelo dado; ou, ainda, à abrangência de compartilhamento sejam comunicadas ao titular (princípio do livre acesso).
 8. Defina procedimento de verificação contínua quanto à exatidão, à clareza, à relevância e à atualização dos dados do titular. O objetivo é manter-se fiel à finalidade de tratamento informada (princípio da qualidade do dado).
 9. Observe a necessidade de garantir ao titular a opção de obter facilmente informações claras e precisas, mediante requisição, sobre o tratamento que é dado a seus dados e sobre os respectivos agentes de tratamento (princípio da transparência).
- Observação: Os órgãos e entidades deverão garantir o acesso às informações sobre o tratamento do dado do titular, resguardadas as informações de acesso restrito, conforme legislação vigente. Vide item 2.4, sobre publicidade.
10. Defina e documente as medidas técnicas e administrativas que serão adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (princípio da segurança).
 11. Identifique e registre as medidas que serão adotadas para prevenir a ocorrência de danos ao titular ou a terceiros em virtude do tratamento de dados pessoais (princípio da prevenção).
 12. Comprometa-se a não realizar o tratamento do dado para fins discriminatórios ilícitos ou abusivos (princípio da não discriminação).
 13. Comprometa-se a adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (princípio da responsabilização e prestação de contas).