UNIVERSIDADE DE BRASÍLIA
FACULDADE UNB PLANALTINA - FUP
PROGRAMA DE PÓS-GRADUAÇÃO EM GESTÃO PÚBLICA - PPGP

NÚBIA AUGUSTO DE SOUSA ROCHA

O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Brasília-DF
2023

NÚBIA AUGUSTO DE SOUSA ROCHA

O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Dissertação defendida junto ao Programa de Pós-Graduação em Gestão Pública, da Universidade de Brasília, como requisito obrigatório para obtenção do título de Mestre em Gestão Pública, orientada pelo professor Dr. Alexandre Nascimento de Almeida.

Brasília-DF

2023

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

RR672t

Rocha, Núbia
O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO / Núbia Rocha; orientador Alexandre Almeida. -- Brasília, 2023.
84 p.

Dissertação(Mestrado Profissional em Gestão Pública) -- Universidade de Brasília, 2023.

1. Tratamento de Dados Pessoais. 2. Poder Público. 3. Proteção de dados. 4. Privacidade. 5. Administração Pública. I. Almeida, Alexandre, orient. II. Título.

NÚBIA AUGUSTO DE SOUSA ROCHA

O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Dissertação de Mestrado Profissional submetida ao Programa de Pós-Graduação em Gestão Pública da Universidade de Brasília.

Comissão Examinadora constituída por:

_____

Professor Dr. Alexandre Nascimento de Almeida
Orientador – PPGP/FUP/UnB

_____

Professor Dr. Tiago Emmanuel Nunes Braga
Examinador Externo – Instituto Brasileiro de Informação em Ciência e Tecnologia

_____

Professor Dr. André Nunes
Examinador Interno – PPGP/FUP/UnB

_____

Professor Dr. Celso Vila Novas Souza Junior
Examinador Interno – PPGP/FUP/UnB

Brasília, 23 de fevereiro de 2023.

A minha avó Iraci (in memoriam) que, por meio de seu exemplo, ensinou às mulheres da família a manterem o foco e a determinação.

AGRADECIMENTOS

Aos meus amados pais, Maria Lúcia e Geraldo, que sempre tiveram a minha formação escolar como prioridade, independente das adversidades que enfrentaram;

Ao meu companheiro Tiago que sempre acreditou na minha capacidade de superação;

Às minhas amigas e aos meus amigos queridos que sempre tiveram uma palavra de conforto e incentivo quando o cansaço chegava;

À Universidade de Brasília, na figura do meu orientador, Alexandre de Almeida, pela busca na excelência do ensino superior;

À Autoridade Nacional de Proteção de Dados, pela compreensão e incentivo à minha formação acadêmica.

A todos aqueles que enfrentam a batalha exaustiva e por vezes frustrante de trabalhar e estudar simultaneamente;

A todos os que servem ao público e escolheram desse dom sua profissão;

Meu mais sincero obrigada!

“Agora vá lá mudar o mundo”
(Tiago Arruda Diniz Moraes)

RESUMO

Foi com a aceleração do desenvolvimento tecnológico e o aumento da importância da informação para a sociedade moderna que o direito à privacidade e à proteção de dados pessoais passou a ganhar destaque nos espaços públicos e privados. Seguindo a tendência mundial, o Brasil editou a Lei Geral de Proteção de Dados Pessoais (LGPD), em agosto de 2018, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade. A Lei contém um capítulo específico para as regras e responsabilidades no tratamento de dados pessoais pelo Poder Público. No entanto, ainda há muito a ser debatido sobre o tema. Com o objetivo de contribuir para o avanço da pesquisa sobre o tema, realizou-se a presente Dissertação, que está organizada em três artigos no formato *multipaper*. O primeiro artigo realizou um estudo bibliométrico com o objetivo de identificar tendências atuais e analisar o panorama das pesquisas desenvolvidas em âmbito global. Uma amostra de 55 artigos foi selecionada utilizando o *Methodi Ordinatio*. Os resultados apontam um aumento significativo da produção acadêmica sobre o tema nas últimas duas décadas, com predomínio de publicações em periódicos europeus. Os resultados evidenciam a atualidade do tema e a necessidade de se desenvolver mais pesquisas voltadas para o campo da Administração Pública. Por sua vez, o segundo artigo tem por objetivo identificar os principais pontos críticos para o tratamento de dados pessoais pelo Poder Público por meio de uma revisão sistemática da literatura. Os resultados mostram que a confiança, a transparência, a segurança da informação, a conformidade, o interesse público e o acesso à informação são os principais pontos de tensão abordados pela doutrina. Enfim, o terceiro artigo tem por objetivos estabelecer níveis de criticidade para os pontos identificados considerando a realidade brasileira, bem como investigar a existência de outros pontos críticos sobre os quais a teoria ainda não avançou, utilizando-se para tanto uma pesquisa com especialistas no tema. Os resultados apontam uma coerência entre o que foi verificado na teoria e a percepção dos especialistas. Outros 10 pontos críticos para o tratamento de dados pessoais pelo Poder Público foram mencionados pelos participantes. Em geral, os principais elementos de tensão identificados foram a falta de capacitação dos agentes públicos e o compartilhamento de dados pessoais.

PALAVRAS-CHAVE: Dados pessoais, Privacidade, Administração Pública, Poder Público, Pontos Críticos.

ABSTRACT

With the acceleration of technological development and the increasing in the importance of information for modern society, privacy and personal data protection gained prominence in public and private spaces. Following the world trend, Brazil enacted the General Personal Data Protection Act (LGDP) in 2018 to protect the fundamental rights of freedom and privacy. The act contains a specific chapter for the rules and responsibilities in personal data processing by the State. However, there is still much to be debated on the subject. This study, organized into three articles in a multi-paper format, was developed to contribute to advancing research in this field. The first article carried out bibliometric research to identify current trends and analyze the panorama of researches developed at the national and international levels on the subject. A sample of 55 articles was selected using the *Methodi Ordinatio*. The results point to a significant increase in academic production on the subject in the last two decades. There is a predominance of publications in European scientific papers. The results show the topicality of the issue and the need to develop more researchers in the field of Public Administration. The second article aims to identify the main critical points of personal data processing by the State, considered by the national and international literature on the subject through a systematic literature review. The results reveal that trust, transparency, cybersecurity, compliance, public interest, and access to information are the main points of tension considered by the doctrine. The third article aims to establish levels of criticality for the identified factors considering the Brazilian reality and investigate the existence of other critical points on which the theory has not yet advanced, using empirical research with specialists in the subject. The results show coherence between the ism and the specialists' perception. The specialists mentioned other ten critical points for personal data processing by the Government.

KEYWORDS: Personal Data, Privacy, Public Administration, State, Critical Points.

LISTA DE TABELAS

Artigo 1: O tratamento de dados pessoais pelo poder público: um estudo bibliométrico

Artigo 2: Pontos críticos para o tratamento de dados pessoais pelo poder público: uma revisão da literatura

Artigo 3: Pontos críticos para o tratamento de dados pessoais pelo poder público: um estudo empírico

LISTA DE GRÁFICOS

Artigo 1: O tratamento de dados pessoais pelo poder público: um estudo bibliométrico

LISTA DE ABREVIATURAS E SIGLAS

CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
Ci	Número de citações
CNN	Cable News Network
CNPD	Comissão Nacional de Proteção de Dados
EUA	Estados Unidos da América
FI	Fator de Impacto
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
Id	Identificação
JCR	Journal Citation Reports
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção da Dados Pessoais
OCDE	Organização para a Cooperação e Desenvolvimento
SJR	SCImago Journal Rank
SUS	Sistema Único de Saúde
TCU	Tribunal de Contas da União
TIC	Tecnologia da Informação e Comunicação

SUMÁRIO

O tratamento de dados pessoais pelo poder público: um estudo bibliométrico

The processing of personal data by the public authorities: a bibliometric study

Resumo

Foi com a aceleração do desenvolvimento tecnológico e o aumento da importância da informação para a sociedade moderna que o direito à privacidade e à proteção de dados pessoais passou a ganhar destaque nos espaços públicos e privados. Seguindo a tendência mundial, o Brasil editou a Lei Geral de Proteção de Dados Pessoais (LGPD), em agosto de 2018, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A Lei contém um capítulo específico para as regras e responsabilidades no tratamento de dados pessoais pelo Poder Público, no entanto, ainda há muito a ser debatido sobre o tema. Para tal, este trabalho realizou um estudo bibliométrico com o objetivo de identificar tendências atuais e analisar o panorama das pesquisas desenvolvidas em âmbito nacional e internacional sobre o tema. Uma amostra de 55 artigos foi selecionada utilizando o *Methodi Ordinatio*, metodologia que conduz a busca, seleção e análise de artigos científicos, para compor o portfólio de artigos utilizados neste estudo. Os resultados apontam um aumento significativo da produção acadêmica sobre o tema nas últimas duas décadas. Há predomínio de publicações em periódicos europeus. Os resultados evidenciam a atualidade do tema e a necessidade de se desenvolver mais pesquisas voltadas para o campo da Administração Pública.

Palavras-chave: Dados pessoais, Privacidade, Administração Pública, Poder Público, *Methodi Ordinatio*.

Abstract

With the acceleration of technological development and the increased importance of information for modern society, privacy and personal data protection began to gain prominence in public and private spaces. Following the world trend, Brazil enacted the General Personal Data Protection Law in August 2018, intending to protect the fundamental rights of freedom and privacy and the free development of the personality of the natural person. The Law contains a specific chapter for the rules and responsibilities in the processing of personal data by the State. However, there is still much to be debated on the subject. This paper carried out a bibliometric study to identify current trends and analyze the scenery of national and international research on the subject. A sample of 55 articles was selected using the Methodi Ordinatio, a methodology that conducts the search, selection, and analysis of scientific articles, to compose the portfolio used in this study. The results point to a significant increase in academic production on the subject in the last two decades. There is a predominance of publications in European journals. The results show the topicality of the issue and the need to develop more research focused on the field of Public Administration.

Keywords: Personal data, Privacy, Public Administration, State, *Methodi Ordinatio*.

1 Introdução

Dados pessoais podem ser entendidos como a própria expressão do ser humano. Garcia (2020) explica que dado pessoal é a informação relacionada a uma pessoa natural identificada ou identificável – ou seja, se um conjunto de informações for capaz de identificar um indivíduo, será considerado, neste contexto, como dado pessoal.

Com o avanço tecnológico e digital, a informação, expressa por dados pessoais, passa a assumir papel central para o desenvolvimento econômico. É a chamada economia de dados (CARVALHO; ANTUNES, 2020). Nessa nova modelagem econômica, informações oriundas da geolocalização, preferências e interesses pessoais inseridas cotidianamente em plataformas digitais *online*, como aplicativos de prestação de serviços e redes sociais, são captadas como dados e podem ser utilizadas para fins diversos como, por exemplo, a propaganda direcionada.

Foi este o contexto que fez surgir, a nível global, a necessidade de regulação acerca da proteção de dados, por meio de instrumentos que confiram poder de consentimento aos seus proprietários (CARVALHO; ANTUNES, 2020), à exemplo da *General Data Protection Regulation* (GDPR), legislação europeia sobre o tema promulgada em 2018.

Seguindo essa direção, o Brasil editou a Lei n° 13.709, de 14 de agosto de 2018, Lei Geral de Proteção da Dados Pessoais (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

No que se refere ao tratamento de dados pessoais pelo Poder Público, a literatura sobre o tema reconhece a importância e a necessidade de que este tenha sob seu controle dados pessoais de seus cidadãos, bem como a possibilidade de tratamento desses dados, para cumprimento de funções precípuas do Estado, tais como a elaboração e implementação de políticas públicas. Entretanto, essa prerrogativa gera ao Estado a obrigação de assegurar aos titulares de dados os seus direitos previstos na LGPD.

Portanto, o desafio do Estado reside em conciliar duas perspectivas que parecem apontar a caminhos opostos: de um lado, o entendimento de que o amplo tratamento de dados pelo Poder Público possibilita a construção de políticas públicas mais eficientes, a oferta de melhores serviços públicos e a desburocratização; de outro, a necessidade de mitigar os riscos para o titular de dados decorrentes desse tratamento (WIMMER, 2021).

Diante do exposto, o objetivo central deste trabalho é identificar o estágio atual das pesquisas sobre o tema, bem como analisar suas tendências. Para tanto, realizou-se um estudo

bibliométrico com a organização de um portfólio de estudos que permeia o debate acerca da utilização de dados pessoais à luz da execução de políticas públicas. O portfólio de artigos obtido neste trabalho é a base para o desenvolvimento da próxima fase da pesquisa, na qual pretende-se analisar os potenciais pontos críticos identificados na literatura para o tratamento de dados pessoais, necessários ao cumprimento do interesse público precípuo às funções do Estado.

Ressalta-se que não foram localizados outros estudos bibliométricos sobre o tratamento de dados pessoais pelo Poder Público. Nesse sentido, a importância deste trabalho é sustentada pela necessidade de se conhecer e sistematizar os estudos já realizados sobre o tema, permitindo a identificação de indicadores de tendência para as áreas de pesquisa relacionadas, bem como a prospecção de lacunas para elaboração de uma agenda de futuras pesquisas.

2 Metodologia

Este estudo consiste em uma análise bibliométrica da produção científica que relaciona a proteção de dados pessoais ao setor público. Segundo Araújo (2006, p. 12) a bibliometria é uma "técnica quantitativa e estatística de medição de índices de produção e de disseminação do conhecimento científico".

Para Soares, Picolli e Casagrande (2018), os indicadores bibliométricos contribuem para a investigação do volume de publicações, periódicos ou temas de determinada área. Nesse sentido, a bibliometria é utilizada em diversos campos do conhecimento para a obtenção de indicadores de avaliação da produção científica e utiliza como princípio a análise da atividade científica pelo estudo quantitativo das publicações com o objetivo de desenvolver indicadores cada vez mais confiáveis (SANTOS, 2003)

Este estudo adotou a metodologia *Methodi Ordinatio* para a busca, seleção e análise de artigos. O *Methodi Ordinatio* foi desenvolvido com base nas metodologias Cochrane e ProKnow-C, e é composto por nove etapas e utiliza três critérios de análise de uma publicação científica relevante: o número de citações, o fator de impacto e o ano de publicação (PAGANI; KOVALESKI; RESENDE, 2015).

A escolha dessa metodologia se deu em razão de sua proposta de classificar os artigos conforme a relevância científica previamente à análise completa dos textos, o que proporciona mais eficiência e celeridade à pesquisa realizada. A seguir serão descritas as etapas e os procedimentos adotados em cada uma delas para elaboração deste trabalho.

2.1 Aplicação da metodologia *Methodi Ordinatio*

A primeira etapa do *Methodi Ordinatio* consiste em estabelecer a intenção de pesquisa. Assim, foi definido que o propósito deste trabalho é produzir um portfólio bibliográfico composto por artigos científicos sobre o tratamento de dados pessoais pelo poder público.

Para a etapa seguinte, foi realizada uma pesquisa preliminar com diversas palavras-chave e bases de dados com o objetivo de explorar os resultados apresentados antes da definição dos termos e bases exatos para a busca. Assim, utilizou-se as palavras-chave em português "dados pessoais", "proteção de dados", "tratamento de dados pessoais", "Poder Público", "Estado" e "Setor Público"; e em inglês "*personal data*", "*data protection*", "*personal data treatment*" e "*Public Sector*". Foram utilizadas ainda combinações das palavras-chave e dos operadores booleanos *OR* e *AND* para investigar a relação entre os termos apresentados nos artigos.

As palavras-chave investigadas foram testadas para verificar os possíveis resultados obtidos nas seguintes bases de dados: Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES, *Web of Knowledge* e *Scopus*. O trabalho nesta etapa foi realizado com o auxílio do gerenciador de referências Zotero.

Na terceira etapa, foi definida a combinação das palavras-chave e das bases de dados a serem utilizadas. Assim, após explorar as possibilidades apresentadas na etapa anterior, foram estabelecidas as seguintes combinações de palavras-chave: em português, "dados pessoais" – no título – e "Poder Público", "Estado" e "Setor Público" – no corpo; em inglês, "*data protection*" – no título – e "*Public Sector*" – no corpo.

A escolha dos descritores se deu em razão da quantidade de artigos obtidos por meio das buscas, pela abrangência das palavras e pela pertinência dos resultados obtidos com o objetivo desta pesquisa. Os bancos de dados selecionados foram o Portal de Periódicos da CAPES e o *Scopus*. A escolha das plataformas deu-se em razão do grande volume de publicações apresentadas com as palavras-chave pesquisadas. Além disso, ambas possibilitam a seleção de artigos revisados por pares, o que garante maior confiabilidade aos estudos selecionados. Considerou-se ainda que as duas plataformas de pesquisa reúnem, em um único banco, diversas bases de dados, tais como a *Web of Science* e a *Science direct*, o que resulta em uma pesquisa mais abrangente.

Na etapa quatro foi realizada a pesquisa definitiva, a qual considerou as conclusões obtidas na etapa anterior. A busca foi realizada entre o período de 01/08/2022 a 12/08/2022. Não foram estabelecidas restrições de idioma e não foi utilizado nenhum critério de restrição

temporal com o objetivo de se obter o resultado mais amplo possível. Essa etapa resultou na identificação de 173 artigos. O resultado bruto da pesquisa trouxe artigos repetidos – i.e. presentes em mais de uma base de dados – e ainda alguns artigos não relacionados diretamente com o tema da pesquisa.

Dessa forma, foi necessário aplicar um procedimento de filtragem, quinta etapa do *Methodi Ordinatio*, com o objetivo de: eliminar as repetições; eliminar os artigos não relacionados ao tema por meio da leitura dos títulos e dos respectivos resumos; e eliminar livros e capítulos tendo em vista que para esses textos não é possível atribuir um fator de impacto – elemento necessário para aplicação da metodologia escolhida. Após a aplicação dos procedimentos de filtragem descritos acima, obteve-se um portfólio composto por 58 artigos.

Na etapa seguinte realizou-se a Identificação do fator de impacto, do ano de publicação e do número de citações. Para tanto, os artigos foram compilados em uma tabela eletrônica que continha o título do artigo, o nome do periódico em que foi publicado, o fator de impacto, o número de citações e o ano da publicação.

Para a identificação do fator de impacto, foi utilizado o indicador *Journal Citation Reports* (JCR) do ano de 2021, que consiste em uma métrica calculada a partir de dados indexados na plataforma *Web of Science*. Para aqueles periódicos cujo JCR não pôde ser localizado, foi utilizado o *SCImago Journal Rank* (SJR), métrica calculada pela plataforma *Scopus*. Ademais, em 15 artigos não foi identificado o fator de impacto por nenhuma das duas métricas citadas, casos em que o fator de impacto recebeu o valor zero. O número de citações dos artigos foi obtido utilizando-se o *Google Scholar* (2023), por meio de busca manual a partir do nome de cada artigo selecionado.

Na etapa sete, os artigos foram ordenados considerando os valores apresentados como resultado da equação *InOrdionatio* (PAGANI; KOVALESKI; RESENDE, 2015): *InOrdinatio* = (FI/1000) + (α * [10 - (AnoPesq – AnoPub)] + (Ci), onde FI representa o Fator de Impacto, α um fator de ponderação que varia de 1 a 10, a ser atribuído pelo pesquisador, AnoPesq é o ano em que a pesquisa foi realizada, AnoPub é o ano em que o artigo foi publicado e Ci é o número de citações do artigo.

Para esta pesquisa atribuiu-se o valor α = 10 uma vez que o tema se revelou recente no meio acadêmico e, portanto, valorizou-se artigos atualizados.

Na etapa 8, buscou-se o texto integral dos artigos selecionados. A localização foi feita diretamente nas plataformas selecionadas ou ainda nas páginas das revistas eletrônicas e no *Google Scholar*. Três artigos não foram localizados na íntegra, o que resultou em suas eliminações do portfólio.

A última etapa consistiu no exame dos 55 artigos selecionados, nesta fase realizou-se a leitura dos títulos, resumos e introdução dos trabalhos, com o objetivo de avaliar se o escopo dos artigos estava alinhado com o tema do presente estudo, e assim compor um portfólio adequado. Segundo Pagani, Kovaleski e Resende (2018), a quantidade de artigos que o pesquisador irá estabelecer para análise depende de valores e critérios pessoais. Para esta pesquisa, não foi excluído do portfólio nenhum artigo após a aplicação da fórmula *InOrdinátio*.

3 Resultados e discussão

Os artigos que compõe o portfólio bibliográfico, objeto desta pesquisa, obtido a partir da metodologia descrita na seção anterior, estão dispostos na Tabela 1.

Tabela 1. Relação de artigos ordenados após a aplicação da equação InOrdinatio

Id	Artigos selecionados (autores, título, revista)	FI	Ci	Ano	*InOrdinatio*
1	ALMEIDA, B. A. *et al*. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. **Ciência & Saúde Coletiva.**	1917	32	2020	113,92
2	YUAN, B.; LI, J. The policy effect of the general data protection regulation (GDPR) on the digital public health sector in the european union: an empirical investigation. **International journal of environmental research and public health**.	4614	35	2019	109,61
3	PLEGER, L. E.; GUIRGUIS, K.; MERTES, A. Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security. **Computers in Human Behavior**.	8957	10	2021	108,96
4	CHUA, H. N.; HERBLAND, A., WONG, S. F.; CHANG, Y. Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. **Telematics and Informatics**.	9140	49	2017	108,14
5	SARABDEEN, J., CHIKHAOUI, E., ISHAK, M. M. M. Creating standards for Canadian health data protection during health emergency–An analysis of privacy regulations and laws. **Heliyon.**	3776	0	2022	103,77
6	COMANDÈ, G.; SCHNEIDER, G. Differential data protection regimes in data-driven research: Why the GDPR is more research-friendly than you think. **German law jornal**.	0,764	0	2022	100,00
7	FÉLIX, V.; MONTEIRO, J. R. O uso de tecnologias e dados pessoais em políticas públicas de saúde no contexto da COVID-19. **civilistica.com.**	0,112	0	2022	100,00
8	SULE, M. J.; ZENNARO, M.; THOMAS, G. Cybersecurity through the lens of digital identity and data protection: issues and trends. **Technology in Society**.	6879	3	2021	99,87
9	BREWCZYŃSKA, M. Financial Intelligence Units: Reflections on the applicable data protection legal framework. **Computer Law & Security Review**.	2707	3	2021	95,71

10	LUBIS, M.; KARTIWI, M.; & ZULHUDA, S. Privacy and personal data protection in electronic voting: factors and measures. **Telkomnika (Telecommunication Computing Electronics and Control)**.	0,314	34	2018	94,00
11	PHILLIPS, B. UK further education sector journey to compliance with the general data protection regulation and the data protection act 2018. **Computer Law & Security Review.**	2707	1	2021	93,71
12	VAN LOENEN, B.; KULK, S.; PLOEGER, H. Data protection legislation: A very hungry caterpillar: The case of mapping data in the European Union. **Government Information Quarterly**.	8490	44	2016	92,49
13	MODESTO, J. A.; EHRHARDT JUNIOR, M. Danos colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pessoais no combate a COVID-19. **Revista Eletrônica de Direito e Sociedade online.**	0	11	2020	91
14	PIÑA-MONDRAGÓN, J. J. Tratamiento y protección de datos personales en el sector público de la salud. El tránsito hacia el expediente clínico electrónico. **Nova scientia.**	0,072	0	2021	90,00
15	NETO, A. B. S.; ISHIKAWA, L.; MACIEL, M. O tratamento de dados pessoais pelo poder público e o papel dos tribunais de contas. **Revista Direitos Culturais.**	0	0	2021	90
16	PALHARES, G. C. et al. A privacidade em tempos de pandemia e a escada de monitoramento e rastreio. **Estudos Avançados.**	0,231	8	2020	88,00
17	CHOROSZEWICZ, M.; MÄIHÄNIEMI, B. Developing a digital welfare state: Data protection and the use of automated decision-making in the public sector across six EU countries. **Global Perspectives.**	0	6	2020	86
18	ANDERSEN, M. R.; STORM, H. H. Cancer registration, public health and the reform of the European data protection framework: abandoning or improving European public health research?. **European Journal of Cancer.**	10002	43	2015	83,00
19	CARRILLO, E.; SEQUERA, M. personal data in the social security institute: exploratory analysis on some personal data protection practices in the social security system of the paraguayan state. **Revista de Direito, Estado e Telecomunicações.**	0,183	3	2020	83,00
20	FLÔRES, M. R.; SILVA, R. L. Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da administração pública: entre o dever público de informar e o direito do cidadão de ser tutelado. **Revista de Direito.**	0	3	2020	83
21	OLIVEIRA, A. C. S.; ARAÚJO, D. S. O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da Lei Geral de Proteção de Dados. **Liinc em Revista**	0	1	2020	81
22	MARTINS, H. et al. Tratamento de dados pessoais em aplicativos públicos relacionados ao coronavírus no Ceará. **Liinc em revista.**	0	1	2020	81
23	WILLIS, C. An overview of the UK's approach to ethnic data collection in the context of the Framework Convention on the Protection of National Minorities.	0	0	2020	80
24	MACIEL, M. Os tribunais de contas no exercício do controle externo de acordo com nova Lei Geral de Proteção de Dados Pessoais. **Revista Controle: Doutrinas e artigos.**	0	0	2020	80
25	ROQUE, A. A tutela coletiva dos dados pessoais na lei geral de proteção de dados pessoais (LGPD). **Revista Eletrônica de Direito Processual**.	0	8	2019	78

26	NAARTTIJÄRVI, M. Balancing data protection and privacy–The case of information security sensor systems. **Computer law & security review**.	2707	11	2018	73,70
27	ROSSI, M.; SANDHU, A. Incompatibility of financial blocking measures against gambling operators with data protection law: using banks to control citizens. **International Data Privacy Law**.	2500	0	2019	72,5
28	NETO, E. F.; DEMOLINER, K. S. Direito à Privacidade e Novas Tecnologias: Breves Considerações Acerca da Proteção de Dados Pessoais no Brasil e na Europa. **Revista internacional consinter de direito**.	0	0	2019	70
29	CORREIA, P. M. A. R.; JESUS, I. O. A.; PEREIRA, S. P. M. O tratamento de dados pessoais na administração pública portuguesa: o caso de estudo da opacidade da autoridade tributária. **Lex Humana**.	0	0	2019	70
30	LUBIS, M.; KARTIWI, M.; ZULHUDA, S. Current state of personal data protection in electronic voting: criteria and indicator for effective implementation. **TELKOMNIKA (Telecommunication Computing Electronics and Control)**.	0,314	16	2017	66,00
31	BUTLER, O. Obligations imposed on private parties by the GDPR and UK Data Protection Law: Blurring the public-private divide. **European Public Law**.	0	5	2018	65
32	MENEZES NETO, E. J.; MORAIS, J. L. B.; BEZERRA, T. J. D. S. L. O projeto de lei de proteção de dados pessoais (PL 5276/2016) no mundo do big data: o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos. **Revista Brasileira de Políticas Públicas**.	0,2	14	2017	64,00
33	MACHADO, J.; BIONI, B. R. A proteção de dados pessoais nos programas de Nota Fiscal: um estudo de caso do "Nota Fiscal paulista". **Liinc em revista**.	0	14	2016	54
34	RUARO, R. L.; RODRIGUEZ, D. P. O direito à proteção de dados pessoais na sociedade da informação. Revista Direito, Estado e Sociedade.	0	21	2014	41
35	ROSA, T. H.; FERRARI, G. M. R. Privacidade, intimidade e proteção de dados pessoais (aspectos brasileiros). **Argumenta Journal Law.**	0	0	2015	30
36	VON DIETZE, A.; ALLGROVE, A. M. Australian privacy reforms—an overhauled data protection regime for Australia. **International Data Privacy Law**.	2500	4	2014	26,5
37	CELLA, J. R. G.; ROSA, L. A. S. Controle social e necessidade de proteção de dados pessoais. **Revista de Direito Brasileira.**	0	9	2013	19
38	BLUME, P. The inherent contradictions in data protection law. **International Data Privacy Law**.	2500	12	2012	14,5
39	CHRISTO, E. D. Data protection in Trinidad and Tobago. **International Data Privacy Law**.	2500	0	2013	12,5
40	BLACK, G.; STEVENS, L. Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest. **Scripted**.	0	1	2013	11
41	BELLAMY, C.; PERRI 6; RAAB, C. Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part II. **Public administration.**	4013	76	2005	10,01
42	GREENLEAF, G. Promises and illusions of data protection in Indian law. International Data Privacy Law.	2500	13	2011	5,5

43	ADAMS, A. A.; MURATA, K.; ORITO, Y. The development of Japanese data protection. **Policy & Internet.**	4510	8	2010	-7,49
44	GOENS, D. The exploitation of Business Register data from a public sector information and data protection perspective: A case study. **Computer law & security Review**.	2707	6	2010	-11,29
45	NETTLETON, E.; WILLISON, C. Data protection: More powers for the information commissioner. **Journal of Database Marketing & Customer Strategy Management**.	0,144	1	2010	-18,99
46	STEFAN, E. E. Interference between the protection of personal data and contraventional legislation. **Perspectives of Law and Public Administration**.	0	1	2008	-39
47	JAWAHITHA, S. ISHAK, M.; MAZAHIR, M. E-data privacy and the personal data protection bill of Malaysia. **Journal of Applied Sciences**.	0,221	8	2007	-41,99
48	PERRI 6; RAAB, C.; BELLAMY, C. Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part I. **Public administration.**	4013	22	2005	-43,98
49	SCHULTE IN DEN BÄUMEN, T. Human genetic data from a data protection law perspective. **Bundesgesundheitsblatt-Gesundheitsforschung-Gesundheitsschutz**.	1595	1	2007	-47,40
50	BAINBRIDGE, D. I. Processing personal data and the data protection directive. **Information and Communications Technology Law**.	0	14	1997	-136
51	JACKSON, M. Data Protection Regulation in Australia after 1988. **International journal of law and information technology**.	0	6	1997	-144
52	BENNETT, C. J. Adequate Data Protection by the Year 2000: The Prospects for Privacy in Canada. **International Review of Law, Computers & Technology**.	0,362	4	1997	-145,99
53	JACKSON, M. The effect of the proposed national data protection regime on the health sector in Australia. **Australian Health Review.**	1837	0	1997	-148,16
54	BLUME, P. Information Infrastructure and Data Protection. The Danish Perspective. **International Journal of Law and Information Technology**.	0	3	1996	-157
55	HOWE, E. The United Kingdom's data protection act. **Government Information Quarterly**.	8490	3	1991	-198,51

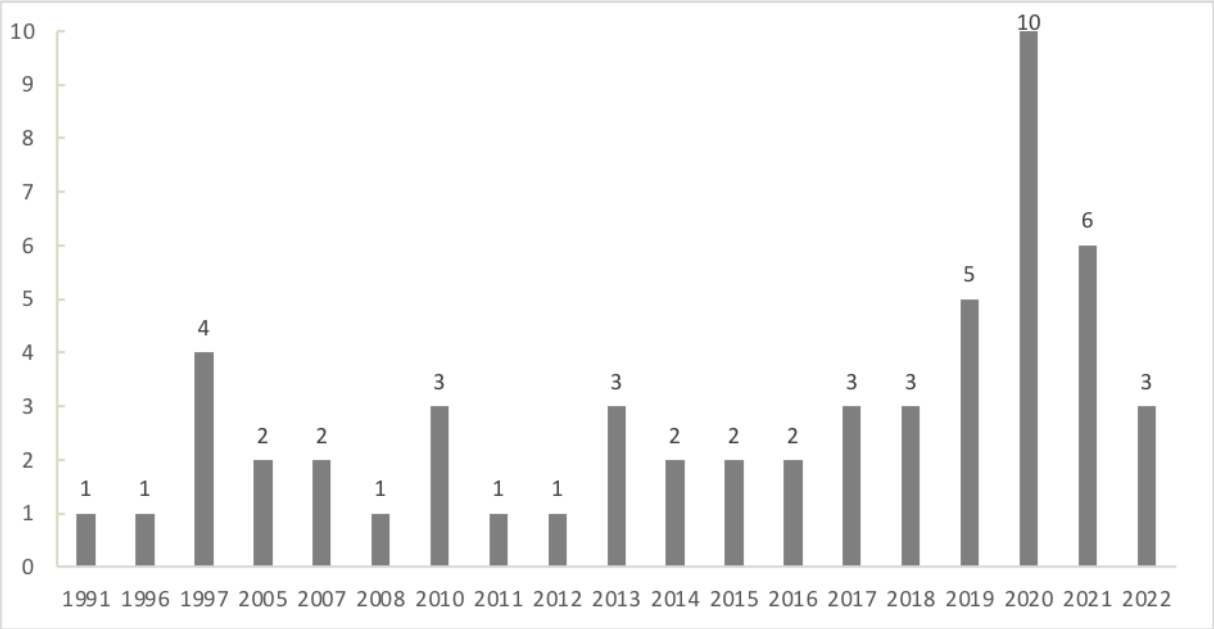
Fonte: Dados extraídos da pesquisa.

No que se refere ao ano de publicação dos artigos que compõem o portfólio, observa-se que embora não se tenha adotado nenhum critério de restrição temporal na pesquisa realizada, a metodologia limitou-se a 31 anos. No Gráfico 1 é possível verificar a evolução da quantidade de publicações relacionadas ao tema, a partir do referido ano.

A década de 1990 contou com 6 publicações, representando 11% do Portfólio. Já os anos 2000 contaram com 5 publicações (9%). Observa-se um salto no número de publicações na década que se segue – o Portfólio selecionado conta com 25 publicações entre 2010 e 2019, 45% do total. Ademais, só nos três últimos anos desta década (2020, 2021 e 2022), outros 19 artigos (35%) relacionados ao tema foram publicados. Destaca-se que a busca por artigos

publicados no ano de 2022 não foi realizada de forma completa, tendo em vista que a pesquisa ocorreu em agosto do referido ano.

Gráfico 1. Distribuição dos artigos por ano



Fonte: Dados extraídos da pesquisa

A evolução no número de artigos identificados demonstra que a produção acadêmica que associa proteção de dados pessoais com as atividades do Poder Público é relativamente recente. Este resultado está diretamente relacionado com a própria evolução da regulamentação do direito à privacidade e a proteção de dados. Segundo Doneda (2011), apenas nos últimos 40 anos foi possível verificar com clareza as construções legislativas e jurisprudenciais sobre o tema.

Foi somente em 1977, na Alemanha, que surgiu a primeira lei federal do mundo a tratar sobre o assunto, constituída com o objetivo de, dentre outros, enfrentar uma atividade Estatal: o censo (RUARO; RODRIGUEZ, 2010).

No Reino Unido, a primeira lei de proteção de dados foi estabelecida em julho de 1984 e, segundo Howe (1991), tratava-se de uma legislação complexa que buscava lidar com a tecnologia da informação em desenvolvimento à época. O trabalho mais antigo selecionado para compor o portfólio, datado de 1991, analisa esta lei e nele já constam considerações importantes sobre o tema no setor público.

Mais adiante, em 1995, surge a Diretiva 95/46/CE do Parlamento Europeu, de cumprimento obrigatório para todos os Países membros, para atuar diretamente sobre tratamento de dados pessoais e a livre circulação desses dados (UNIÃO EUROPEIA, 1995), que se consolidou anos depois, em 2016, na promulgação do Regulamento Geral de Proteção de Dados Europeu (GDPR).

Segundo Pinheiro (2021), o regulamento europeu desencadeou um "efeito dominó", que culminou com o surgimento de diversas leis de proteção de dados pessoais ao redor do mundo. Isso porque, com o GDPR, a União Europeia passou a exigir que os demais países e empresas que buscassem manter relações comerciais com o bloco também possuíssem legislações que garantissem os níveis estabelecidos para a proteção de dados pessoais.

Com o Brasil não foi diferente. Até meados de 2018, o País era um dos poucos entre as principais economias mundiais a não ter promulgado um marco regulatório de proteção de dados pessoais (GARCIA, 2020). Contudo, essa lacuna regulamentar foi suprida com a Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor em agosto daquele ano.

Dessa forma, a intensa produção acadêmica sobre o tema, percebida nos últimos anos, reflete a atualização normativa que o mundo vem enfrentando. Soma-se a isso o pensamento de Doneda (2011, p. 92), segundo o qual a sociedade atual vive um novo arranjo, baseado na informação:

> [...] a utilização sempre mais ampla de dados pessoais para as mais variadas atividades – identificação, classificação, autorização e tantas outras – torna tais dados elementos essenciais para que a pessoa possa se mover com autonomia e liberdade nos corredores do que hoje costumamos denominar de Sociedade da Informação.

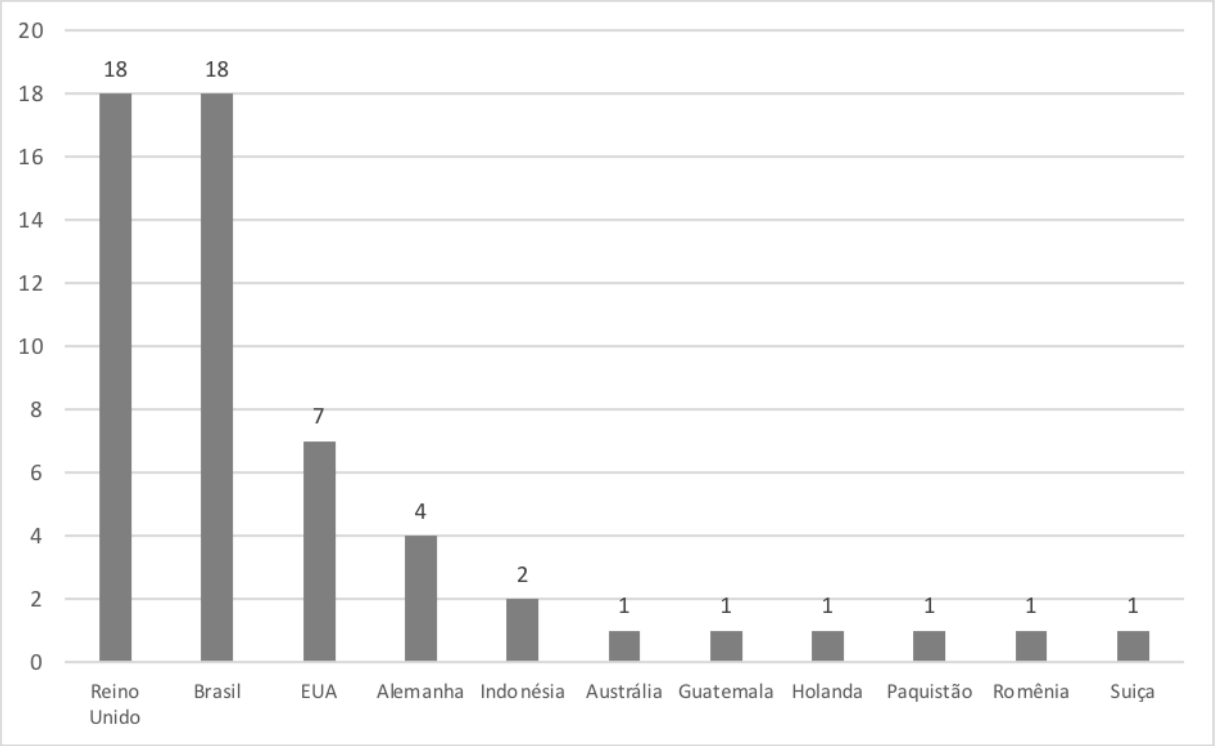
Quanto aos resultados referentes aos periódicos que compõem o portfólio, observa-se que os artigos selecionados estão distribuídos em um total de 42 revistas científicas, o que demonstra uma pulverização das pesquisas sobre o tema em diferentes periódicos. A revista que concentra a maior quantidade de publicações é a *International Data Privacy Law*, com 5 artigos, seguida da *Computer Law & Security Review*, com 4. Do periódico Liinc em Revista, constaram 3 artigos e das revistas *Government Information Quarterly*, *International journal of law and information technology, Public administration* e *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 2 artigos em cada. Nas demais revistas, verificou-se a seleção de apenas um único artigo.

No que se refere à distribuição geográfica das publicações, é possível observar no Gráfico 2 que a maioria dos periódicos que compõem o portfólio foram publicados em revistas

no Reino Unido e no Brasil. Em terceiro lugar encontram-se os Estados Unidos, seguidos pela Alemanha.

O Brasil aparece empatado em primeiro lugar na distribuição geográfica dos periódicos, esse resultado se justifica em razão da busca por artigos ter adotado também descritores em língua portuguesa, o que acaba por ampliar os resultados do País nas bases de dados pesquisadas.

Gráfico 2. Distribuição geográfica das publicações



Fonte: Dados extraídos da pesquisa

Somando-se a quantidade de publicações do Reino Unido, Alemanha, Holanda, Romênia e Suíça obtêm-se um total de 27 publicações. Isto equivale a dizer que as revistas Europeias concentram quase metade (47%) das publicações selecionadas para compor o portfólio.

Corrobora com esse resultado o entendimento de que, embora as primeiras noções do direito à privacidade tenham surgido na jurisprudência e doutrina norte-americanas (ZANINI, 2015; RUARO; RODRIGUEZ, 2010), diversos autores apontam que foi a União Europeia a assumir a vanguarda normativa sobre o tema e a influenciar outros países a estabelecerem regras

para a proteção de dados pessoais (YUAN; LI, 2019; NETO; ISHIKAWA; MACIEL, 2021; FLÔRES; SILVA, 2020).

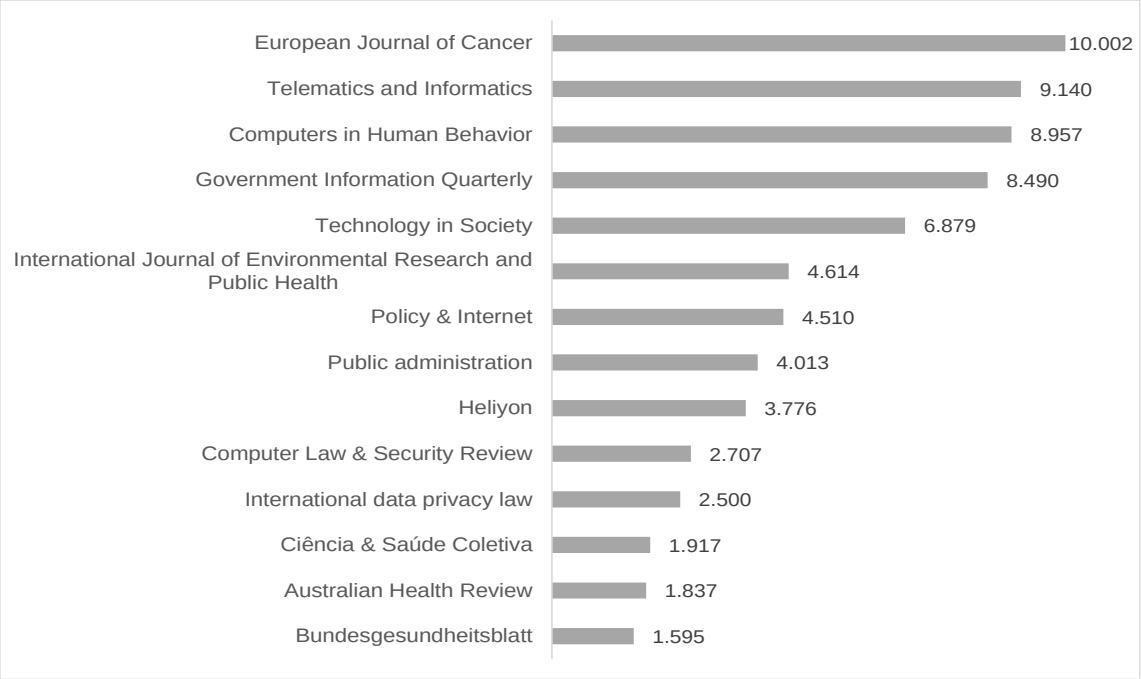
Soma-se a isso a avaliação de Sarabdeen, Chikhaoui e Ishak (2022), segundo os quais além da liderança regulamentar sobre privacidade, a legislação Europeia tem implicações transfronteiriças para outros países, o que acaba por influenciar o restante do globo.

Uma análise significativa em estudos bibliométricos envolve o fator de impacto dos periódicos. O Gráfico 3 apresenta os valores do JCR e o Gráfico 4 do SJR para os periódicos cujos indicadores apresentaram valores diferentes de zero. Esse indicador representa o número médio de citações de artigos publicados pelas revistas nos dois últimos anos anteriores à pesquisa.

Gráfico 3. Fator de Impacto – JCR

Fonte: Dados extraídos da pesquisa

Gráfico 4. Fator de Impacto - SJR



Fonte: Dados extraídos da pesquisa

Os resultados apresentados por esse indicador reforçam o protagonismo europeu sobre o tema. Tanto na base JCR, quanto na SJR, as revistas que ocupam a primeira posição e que, portanto, sob este critério, possuem maior impacto na produção científica neste campo, são oriundas do Reino Unido e da Alemanha, respectivamente.

Importa observar que embora os estudos nacionais tenham tido uma grande representatividade no portfólio selecionado, verifica-se que as revistas brasileiras não figuram em destaque neste indicador.

Além da distribuição geográfica e do fator de impacto das revistas científicas, também interessa investigar as categorias dos periódicos nos quais os artigos selecionados foram publicados. Para tanto, as revistas foram classificadas em sete categorias correspondentes ao seu principal campo de interesse – informação obtida por meio dos dados disponíveis nas bases *Web Of Science*, *Scopus* e nos endereços eletrônicos das próprias revistas.

Na tabela 3 é possível observar que a categoria Direito é a que apresenta o maior destaque, com 29 artigos. Importa destacar que um periódico pode apresentar mais de uma categoria, o que justifica o valor total de artigos por categoria de periódico (63) ser superior ao total de artigos selecionados para o portfólio (55).

Tabela 2. Distribuição dos artigos pela categoria dos periódicos

Categoria	Quantidade de Artigos
Direito	28
Multidisciplinar	8
Ciência da Informação	6
Ciências políticas	5
Ciência da Computação/Tecnologia/Engenharia	5
Saúde	5
Administração Pública	4

Fonte: Dados extraídos da pesquisa

Os resultados sugerem um caráter de multidisciplinaridade e transversalidade do tema, tendo em vista a variedade de áreas do conhecimento dos periódicos que publicaram artigos relacionados ao assunto. Observa-se que o número de publicações em periódicos voltados para a produção científica na área de Administração Pública se refere ao menor resultado (4), e representa apenas 7% do portfólio.

Importa destacar que a LGPD dispõe sobre o tratamento de dados pessoais não apenas por pessoa jurídica de direito privado, mas também de direito público, contando, inclusive, com um capítulo específico que contém as regras e responsabilidades para o tratamento de dados pessoais pelo Poder Público.

Dessa forma, tendo em vista a importância do tema e a tímida produção acadêmica voltada especificamente para a Administração Pública, observa-se que a relação entre proteção de dados pessoais e as atividades precípuas do Poder Público é tema ainda pouco explorado no meio acadêmico.

Outro dado interessante é a quantidade de artigos localizados em revistas voltadas para a saúde, que correspondem a 8% do portfólio. Embora, em uma primeira análise, pareça ser uma categoria pouco relacionada ao tema, é possível identificar uma tendência de crescimento desse tipo de pesquisa em razão da chamada “era da saúde digital”, na qual Yuan e Li (2019) apontam um número crescente de hospitais e instituições de saúde que passaram a adotar tecnologias de informação e comunicação (TIC) para apoiar e avançar suas práticas de saúde.

Ademais, a pandemia de Coronavírus, iniciada em 2020, também impulsionou a quantidade de estudos relacionando os temas saúde e proteção de dados pessoais. Isso porque, segundo Félix e Monteiro (2022), os dados pessoais são necessários para a formulação de

políticas públicas em saúde, e surgem como importantes instrumentos no combate à COVID-19.

O número de citações dos artigos também foi considerado como um indicador utilizado para atribuir grau de importância aos trabalhos que compõem o portfólio. Na tabela 2 estão mencionados os dez artigos que compõem o portfólio com o maior número de citações. Destaca-se que em oito artigos selecionados apenas uma citação foi registrada e treze artigos não tiveram nenhuma citação localizada.

Tabela 3. Artigos com maior número de citações que compõem o portfólio selecionado

Título	Citações
Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part II	76
Compliance to personal data protection principles: A study of how organizations frame privacy policy notices	49
Data protection legislation: A very hungry caterpillar	44
Cancer registration, public health and the reform of the European data protection framework: Abandoning or improving European public health research?	43
The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation	35
Privacy and Personal Data Protection in Electronic Voting: Factors and Measures	34
Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global	32
Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part I	22
O direito à proteção de dados pessoais na sociedade da informação	21
Current State of Personal Data Protection in Electronic Voting: Criteria and Indicator for Effective Implementation	16

Fonte: Dados extraídos da pesquisa

Observa-se que o artigo com o maior número de citações (76) foi ordenado na 42° posição após a classificação do portfólio pela equação *InOrdinátio*. Isso se deve ao fato de que se trata de um artigo publicado em 2005, ou seja, pouco atual para os critérios estabelecidos na metodologia (trabalho com mais de 10 anos). Entretanto, tendo em vista seu grande reconhecimento no meio científico, dada sua grande quantidade de citações, pode ser considerado um clássico sobre o tema.

4 Conclusão

O presente trabalho apresentou um breve estudo bibliométrico sobre o tratamento de dados pessoais pelo Poder Público. Foram analisados dados relacionados à distribuição dos estudos por ano, por país de publicação e por área de pesquisa dos periódicos.

Além disso, foi construído um portfólio bibliográfico composto de 55 artigos sobre o tema publicados nos últimos 31 anos. Para tanto, adotou-se o *Metodi Ordinatio* para a seleção, ordenação e exame dos artigos.

A partir da análise do número de publicações ao longo do tempo, verificou-se que a produção acadêmica sobre o tema vem se incrementando significativamente ao longo dos anos, um reflexo dos avanços tecnológicos e da regulamentação sobre proteção de dados pessoais. Dessa forma, conclui-se ser um tópico atual e de interesse contemporâneo para os pesquisadores da área.

Os resultados sugerem que o Reino Unido é um dos protagonistas no cenário internacional em publicações sobre o tema, representando 33% dos artigos selecionados. A produção nacional também foi amplamente considerada no portfólio, que contém 18 artigos (33%) publicados em revistas brasileiras.

Embora os Estados Unidos tenham sido pioneiros no debate sobre o direito à privacidade (ZANINI, 2015), apenas 7 artigos selecionados (12%), que relacionam o tratamento de dados pessoais pelo poder público, foram publicados em revistas americanas.

No que se refere às principais áreas de interesse dos periódicos que compõem o portfólio, observou-se a multidisciplinaridade do tema com publicações em diversos campos do conhecimento, tais como Ciência Política, Ciência da Computação, Saúde, dentre outros. A categoria Direito representou a liderança nas publicações (46%), enquanto a categoria Administração Pública, objeto de estudo desta pesquisa, representou apenas 7% dos estudos selecionados. Em vista disso, faz-se necessário e urgente o desenvolvimento de estudos sobre tratamento de dados pessoais com foco em administração, em especial, voltados para as peculiaridades da gestão pública.

Os resultados demonstram que a metodologia adotada para composição do portfólio de artigos sobre o tema privilegiou as pesquisas mais recentes, mas também considerou os artigos clássicos – que embora mais antigos, são reconhecidos cientificamente.

5 Referências

ARAÚJO, C. A. Bibliometria: Evolução Histórica e Questões Atuais. **Em Questão**, Porto Alegre, vol. 12, n. 1, p. 11- 32, jan./jun. 2006.

CARVALHO, L. F.; ANTUNES, J. P. A natureza jurídica da autoridade nacional de proteção de dados à luz da teoria do estado regulador: há espaço para a adoção do conceito material de descentralização administrativa no Brasil? **Revista de Direito, Estado e Telecomunicações,** vol. 12, n. 2, p. 118-132, 2020.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, Joaçaba, vol. 12, n. 2, p. 91–108, jul./dez. 2011.

FÉLIX, V.; MONTEIRO, J. R. O uso de tecnologias e dados pessoais em políticas públicas de saúde no contexto da COVID-19. **civilistica.com**, vol. 11, n. 1, p. 1-31, maio. 2022.

FLÔRES, M. R.; SILVA, R. L. Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da administração pública: entre o dever público de informar e o direito do cidadão de ser tutelado. **Revista de direito**, vol. 12, n. 02, p. 01–34, 2020.

GARCIA, R. C. de C. Proteção de dados pessoais no Brasil: uma análise da Lei nº 13.709/2018 sob a perspectiva da Teoria da Regulação Responsiva. **Revista de Direito Setorial e Regulatório**, vol. 6, n. 2, p. 45-58, out. 2020.

HOWE, E. The United Kingdom's data protection act. **Government Information Quarterly**, vol. 8, n. 4, p. 345-357. 1991.

NETO, A. B. S.; ISHIKAWA, L.; MACIEL, M. O tratamento de dados pessoais pelo poder público e o papel dos tribunais de contas. **Revista Direitos Culturais**, vol. 16, n. 40, p. 163–177, 2021.

PAGANI, R. N.; KOVALESKI, J.L.; RESENDE, L.M. Methodi Ordinatio: a proposed methodology to select and rank relevant scientific papers encompassing the impact factor, number of citation, and year of publication. **Scientometrics**, vol. 105, n. 40, p. 2109–2135. 2015.

PAGANI, R. N.; KOVALESKI, J. L.; RESENDE, L. M. M. Avanços na composição da Methodi Ordinatio para revisão sistemática de literatura. **Ciência da Informação**, vol. 46, n. 2. 2018.

PINHEIRO, P. P. **Proteção de Dados Pessoais:** Comentários à Lei n. 13.709/2018-LGPD. São Paulo: Editora Saraiva, 2021.

RUARO, R. L.; RODRIGUEZ, D. P. O direito à proteção de dados pessoais na sociedade da informação. **Direito, Estado e Sociedade**, n. 36, p. 178-199, jan./jun. 2010.

SANTOS, R. N. M. Produção científica: por que medir? O que medir? **Revista digital de Biblioteconomia e Ciência da Informação**, Campinas, vol. 1, n. 1, p. 22-38, jul./dez. 2003.

SARABDEEN, J., CHIKHAOUI, E., ISHAK, M. M. M. Creating standards for Canadian health data protection during health emergency: An analysis of privacy regulations and laws. Heliyon, vol. 8, n. 5, e09458, maio. 2022.

SOARES, S. V., PICOLLI, I. R. A., CASAGRANDE, J. L. Pesquisa bibliográfica, pesquisa bibliométrica, artigo de revisão e ensaio teórico em administração e contabilidade. **Administração: ensino e pesquisa**, Rio de Janeiro, vol. 19, n. 2, p. 308-339, maio/ago. 2018.

UNIAO EUROPEIA. Directiva 95/46/CE do Parlamento europeu e do conselho. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial** nº L 281, p. 31-50, 23 nov. 1995.

YUAN, B.; LI, J. The policy effect of the general data protection regulation (GDPR) on the digital public health sector in the European Union: An empirical investigation. **International journal of environmental research and public health**, vol. 16, n. 6, p. 1070. 2019.

WIMMER, M. Limites e possibilidade para o uso secundário de dados pessoais no poder público: lições da pandemia. **Revista Brasileira de Políticas Públicas**, vol. 11, n. 1, abr, 2021.

ZANINI, L. E. de A. O surgimento e o desenvolvimento do right of privacy nos Estados Unidos. **Revista Brasileira de Direito Civil**, Belo Horizonte, vol. 3, n. 01, p. 9-28, jan./mar. 2015.

ZOTERO. Zotero: Your personal research assistant. Página inicial. Disponível em: <https://www.zotero.org/>. Acesso em: 06 de jan. de 2022.

Pontos críticos para o tratamento de dados pessoais pelo poder público: uma revisão da literatura

Critical points of personal data processing by the public authorities: a literature review

Resumo

O tratamento de dados pessoais pelo poder público vem sendo marcado por uma tensão que reflete o desafio em equilibrar o desenvolvimento de políticas públicas mais eficientes e a proteção de dados pessoais. Soma-se a isso a aceleração do desenvolvimento tecnológico e o aumento da importância da informação para a sociedade moderna que empurra o Estado para iniciativas constantes de transformação digital. Assim, com o objetivo de identificar os principais pontos críticos para o tratamento de dados pessoais pelo Poder Público, abordados pela literatura nacional e internacional sobre o tema, este estudo realizou uma revisão sistemática da literatura. Os resultados evidenciam que os principais pontos de tensão abordados pela doutrina são: 1) a confiança dos cidadãos no Estado para o tratamento de seus dados pessoais; 2) o grau de transparência das informações disponibilizadas pelo Estado no que se refere ao tratamento dos dados pessoais do cidadão; 3) os mecanismos de segurança da informação e salvaguardas que garantam a proteção dos dados pessoais em posse do Estado; 4) a conformidade das instituições públicas com a legislação sobre o tema; 5) o interesse público motivador do tratamento dos dados; 6) e os desafios relacionados ao acesso à informação.

Palavras-chave: dados pessoais, poder público, políticas públicas, Lei Geral de Proteção de Dados, privacidade.

Abstract

The processing of personal data by public authorities has been marked by the tension that reflects the challenge of balancing the development of more efficient public policies and the protection of citizens' data. Added to this is the acceleration of technological development and the increased importance of information for modern society, which pushes the State towards constant digital transformation initiatives. Thus, intending to identify the main critical points for the processing of personal data by the State, addressed by the national and international literature on the subject, this study carried out a systematic review of the literature. The results show that the main points of tension addressed by the doctrine are: 1) citizens' trust in the State for the processing of their personal data; 2) the degree of transparency of the information made available by the State regarding the processing of the citizen's personal data; 3) information security mechanisms and safeguards that guarantee the protection of personal data held by the State; 4) compliance of public institutions with legislation on the subject; 5) the public interest motivating the processing of data; 6) and the challenges related to access to information.

Keywords: personal data, government, public policies, General Data Protection Law, privacy.

1 Introdução

Os dados pessoais tornaram-se um dos recursos mais valiosos na sociedade da informação (FÉLIX; MONTEIRO, 2022). Nesse cenário, assim como as organizações do setor privado, as instituições do setor público investem cada vez mais recursos para alcançar os benefícios previstos da coleta e análise de dados para a prestação de serviços públicos, a exemplo dos custos aparentemente mais baixos, melhor eficiência na produção de serviços, previsão e antecipação da demanda por serviços e desenvolvimento de intervenções direcionadas (CHOROSZEWICZ; MÄIHÄNIEMI, 2020).

Como sublinham Teixeira e Guerreiro (2022), o Poder Público é um dos grandes agentes de tratamento de dados, devido ao seu papel no planejamento e execução de políticas públicas. Ressalta-se ainda o contexto atual em que se observa maiores esforços de governo eletrônico e um aumento contínuo das aplicações de Tecnologia da Informação e Comunicação (TIC) no setor público. No Brasil, o Decreto 10.332, de 28 de abril de 2020, que institui a estratégia de Governo Digital, estabelece objetivos voltados à integração de sistemas de informação do governo, bem como o fomento à interoperabilidade de sistemas e a oferta de serviços consolidados em plataforma única.

Bioni (2021) destaca que a relação entre o Poder Público e os titulares de dados pessoais é notada pela assimetria entre os atores, uma vez que o Estado é visto como detentor de posição de superioridade, e o interesse público tende a prevalecer quando em conflito com o interesse do indivíduo.

Para Bellamy, Perry e Raab (2005), a tensão entre os objetivos de serviços públicos que exigem um compartilhamento de dados mais amplo e a proteção da privacidade representa um grande desafio para os formuladores de políticas públicas, reguladores e agentes de serviços públicos.

Logo, diante do contexto apresentado, a problemática do presente estudo centra-se no seguinte questionamento: quais os principais pontos de tensão apontados pela literatura para o tratamento de dados pessoais pelo poder público?

A relevância deste estudo decorre da necessidade de assegurar o direito à privacidade em face à manipulação de dados pessoais por agentes públicos. A partir deste trabalho, será possível identificar quais são os pontos críticos no tratamento de dados pessoais, à luz da execução de políticas públicas, abordados na literatura global. Além disso, a pesquisa contribui para o desenvolvimento da cultura de proteção de dados pessoais no setor público, o que é primordial para a consolidação de um Estado mais seguro e inclusivo.

1.1 O tratamento de dados pessoais pelo poder público

No Brasil, o tratamento de dados pessoais é regulamentado pela Lei 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre as operações envolvendo dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado (BRASIL, 2018) e constitui a principal parte do marco legal brasileiro em relação à coleta, ao armazenamento e ao uso de dados pessoais (OCDE, 2020).

Destaca-se que o objetivo da LGPD é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018). Nesse contexto, Flôres e Silva (2020) evidenciam que a LGPD não torna impossível gerir dados, tampouco oferece riscos à inovação. Pelo contrário, ela promove e determina mecanismos de controle e proteção do núcleo duro dos direitos fundamentais dos indivíduos.

Outro aspecto relevante sobre a LGPD é de que ela estabeleceu no ordenamento jurídico nacional o conceito de tratamento de dados pessoais, qual seja, toda operação realizada com dados pessoais, como as que se referem à 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, 2018).

Botelho (2020) evidencia que o tratamento de dados, conforme disposto na LGPD, abrange todo o ciclo de vida do dado, desde a sua coleta até a sua eliminação, ou ainda, nas palavras de Vainzof (2019, p. 116) “o conceito de tratamento abarca absolutamente todas as hipóteses de manuseio de dados”.

Para que o tratamento de dados pessoais seja considerado adequado deve-se estabelecer controles administrativos, técnicos e físicos necessários à proteção da confidencialidade, integridade e disponibilidade dos ativos de informação em conformidade com as normas técnicas voltadas à segurança da informação, além da adequação às exigências da LGPD (HINTZBERGEN et al., 2018), sobretudo porque a maneira como se dá o tratamento de dados pessoais pode afetar diretamente o direito à privacidade de qualquer indivíduo (ALVAREZ; TAVARES, 2017).

Oliveira e Araújo (2020) afirmam que o tratamento de dados pessoais é hoje uma realidade tanto no setor público como no privado, especialmente graças ao avanço das

tecnologias de informação e comunicação, tão difundidas pela internet, por meio da qual pessoas, entidades e organizações compartilham informações cotidianamente.

Assim, considerando a relevância da questão, a LGPD estabeleceu, em seu artigo 7°, um rol taxativo de hipóteses em que é permitido o tratamento de dados pessoais, tais como o consentimento pelo titular de dados, o cumprimento de obrigação legal, dentre outras (BRASIL, 2018).

Importa para o escopo deste trabalho ressaltar que uma das hipóteses previstas para o tratamento de dados pessoais permitidas pela LGPD se refere à execução de políticas pela administração pública:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> [...]
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; (BRASIL, 2018).

Stelzer *et al*. (2019) pontuam que o dado pessoal é ativo importante para a concretização de políticas públicas. Nesse sentido, o acesso à informação se tornou indispensável para o próprio poder público que realiza a coleta dos mais diversos dados os quais podem ser de interesse para a gestão pública (FLÔRES; SILVA, 2020).

Entretanto, observa-se que o tratamento de dados pessoais pelo Poder Público possui muitas peculiaridades, em virtude da necessidade de compatibilizar o exercício de prerrogativas estatais típicas e os princípios, regras e direitos estabelecidos na LGPD (BRASIL, 2022).

Oliveira e Araújo (2020) ressaltam que a grande preocupação reside em como os dados pessoais estão sendo tratados, compartilhados e armazenados. Segundo os autores, cabe aos entes públicos garantir que, no estabelecimento de políticas públicas, a eficiência da coleta, do tratamento, do uso, do monitoramento, do armazenamento e do compartilhamento de dados pessoais sejam realizados com o menor risco à privacidade dos seus titulares e, por conseguinte, do cidadão.

Wimmer (2021) destaca que não é novidade e nem exclusividade do Brasil as preocupações quanto ao tratamento de dados pessoais de posse do Poder Público, em especial quando utilizados para finalidade distinta daquela que justificou a sua coleta inicial. Ainda em 1974, uma Resolução do Conselho da Europa relacionava a proteção da privacidade de indivíduos frente a bases de dados eletrônicas no setor público.

Sob este aspecto, o tratamento de dados pessoais pelo poder público revela uma dicotomia já apontada por Taylor, Lips e Organ (2008), na qual, de um lado, encontram-se os estudos sobre o tema que apresentam críticas à ampla captura e tratamento de dados pessoais pelo Estado e, do outro, os estudos na área de Administração Pública que se posicionam favoráveis a essa prática.

Em suma, embora o poder público tenha em seu favor exceções trazidas pela própria LGPD no âmbito do tratamento dos dados pessoais, que se justificam no princípio administrativo basilar da supremacia do interesse público sobre o privado (OLIVEIRA; ARAÚJO, 2020), existem questões críticas para o tratamento de dados pessoais pelo Poder Público. Nesse sentido, o desafio do Estado reside em "assegurar a celeridade e a eficiência necessárias à execução de políticas e à prestação de serviços públicos com respeito aos direitos à proteção de dados pessoais e à privacidade" (BRASIL, 2022, p. 5).

2 Metodologia

A metodologia empregada nesta pesquisa é dedutiva, de natureza exploratória, apresenta uma abordagem qualitativa e teve como base uma revisão sistemática da literatura. Para Soares, Picolli e Casagrande (2018) essa metodologia de pesquisa se refere à uma investigação cientifica pautada por uma abordagem rigorosa preestabelecida para selecionar, comparar e sintetizar as evidências sobre o assunto de interesse.

Neste estudo, a revisão sistemática foi realizada a partir do Methodi Ordinatio, método que conduz a busca, seleção e análise de artigos científicos, considerando a relevância das publicações e utiliza como critérios o número de citações, o fator de impacto e o ano de publicação dos estudos (PAGANI; KOVALESKI; RESENDE, 2015).

Para a busca dos artigos relacionados foram estabelecidas as seguintes palavras-chave: em português, "dados pessoais", "Poder Público", "Estado" e "Setor Público"; em inglês, "*data protection*" e "*Public Sector*". Foram utilizados os operadores booleanos *OR* e *AND* para investigar a relação entre os termos apresentados nos artigos.

Os bancos de dados selecionados para a busca foram o Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES e o *Scopus*. A escolha das plataformas de pesquisa se justifica por reunirem, em um único banco, diversas bases de dados, tais como a *Web of Science* e a *Science direct*, o que resulta em uma pesquisa mais ampla.

A pesquisa nas bases de dados, realizada em agosto de 2022, contou apenas com artigos revisados por pares, com o objetivo de garantir maior confiabilidade dos estudos selecionados. Além disso, não foi imposta nenhuma restrição quanto ao idioma da publicação e não foi estabelecido nenhum limite de ano de publicação para a pesquisa.

A consulta preliminar segundo os critérios acima estabelecidos retornou 173 artigos. O material passou por análise e filtragem, sendo eliminados os artigos repetidos, aqueles cujos assuntos não estavam relacionados ao tema e os que não foram possíveis localizar o texto integral. Ao fim, 43 artigos científicos foram selecionados para leitura sistemática, cujos resultados das análises serão apresentados na seção a seguir.

Na análise dos artigos selecionados foi empregada a técnica da análise de conteúdo para identificação dos pontos críticos para o tratamento de dados pessoais pelo Poder Público. A técnica tem por objetivo "compreender criticamente o sentido das comunicações, seu conteúdo manifesto ou latente, as significações explícitas ou ocultas" (CHIZZOTTI, 2006, p. 98). Ademais, na visão de Flick (2009, p. 291), a análise de conteúdo é um dos procedimentos clássicos para a análise de materiais textuais.

Importa destacar que, durante a leitura do portfólio selecionado, buscou-se identificar ainda outros trabalhos relevantes por meio da análise das referências utilizadas nos artigos selecionados, sendo possível detectar ainda outros trabalhos relacionados ao tema de forma assistemática em razão do conteúdo apresentado.

3 Resultados e discussão

Da análise do portfólio bibliográfico selecionado, identificou-se que seis foram os pontos críticos mais destacados na literatura: 1) a confiança dos cidadãos no Estado para o tratamento de seus dados pessoais; 2) o grau de transparência das informações disponibilizadas pelo Estado no que se refere ao tratamento dos dados pessoais do cidadão; 3) os mecanismos de segurança da informação e salvaguardas que garantam a proteção dos dados pessoais em posse do Estado; 4) a conformidade das instituições públicas com a legislação sobre o tema; 5) o interesse público motivador do tratamento dos dados; 6) e os desafios relacionados ao acesso à informação. A tabela a seguir demonstra a proporção de artigos que abordam os pontos de tensão identificados em relação ao total do portfólio selecionado.

Tabela 1. Distribuição dos pontos críticos observados no portfólio

Ponto Crítico	Percentual de artigos que abordam o assunto
Confiança	21%
Transparência	26%
Segurança	21%
Conformidade	12%
Interesse Público	30%
Acesso à Informação	7%

Fonte: Dados extraídos da pesquisa

Depreende-se da Tabela 1 que o interesse público foi o assunto mais observado, sendo que 30% dos artigos que compõe o portfólio abordam direta ou indiretamente o assunto. Já o acesso à informação foi o menos frequente, sendo tratado em apenas 7% dos estudos selecionados. As seções a seguir elucidarão com maior detalhamento os resultados observados para os pontos críticos supracitados.

Registra-se que, de forma residual, a literatura sobre o tema também cita outros pontos críticos, tais como o emprego de tecnologias emergentes (inteligência artificial, aprendizado de máquina, robótica e *big data*) e a potencial discriminação algorítmica (SARABDEEN; CHIKHAOUI; ISHAK, 2022). Entretanto, não foram identificados estudos que abordassem tais assuntos com profundidade no portfólio bibliográfico selecionado.

3.1 Confiança

A literatura analisada aponta que a confiança da sociedade no Estado é um ponto crítico para a implementação de políticas públicas que exijam o tratamento de dados pessoais pelo Poder Público.

Os processos de digitalização no setor público levaram a um aumento de abordagens inovadoras para uma melhor prestação de serviços usando TICs. Os cidadãos, no entanto, muitas vezes guardam reservas em relação aos esforços de governo eletrônico devido a preocupações com a proteção de dados (PLEGER; GUIRGUIS; MERTES, 2021).

Ainda em 2005, Lips, Taylor e Bannister já apontavam que a confiança deve ser reconhecida como um dos conceitos centrais nas ambições dos governos para lidar com a sociedade da informação. Nesta esteira, Combe (2009) argumenta que a efetiva prestação de

serviços públicos por meio das TICs depende necessariamente de relações de confiança entre os cidadãos e o Estado.

Corroboram com este entendimento Pleger, Guirguis e Mertes (2021), segundo os quais a confiança é de particular importância no contexto da administração pública e da implementação de serviços eletrônicos do governo. Isto porque, para que os usuários estejam dispostos a fornecer informações pessoais *online*, eles devem ter confiança de que seus dados não serão usados de forma indevida (LANDWEHR, 2019).

Para Perry, Raab e Bellamy (2005) as práticas eficazes de proteção de dados são amplamente consideradas como condição necessária para construir a confiança popular nos serviços eletrônicos fornecidos pelo Estado e, portanto, como uma fonte significativa de vantagem competitiva na economia eletrônica global.

Países como o Reino Unido e a Índia, em que pese nutram boas intenções ao implementar sistemas que necessitam do tratamento de dados pessoais pelo Poder Público – a exemplo de Identidades Digitais –, na visão de Sule, Zennato e Thomas (2021), falharam em função da falta de confiança do usuário.

Segundo Sarabdeen, Chikhaoui e Ishak (2022), a perda de confiança do público para com os mecanismos de proteção de dados adotados pelo governo pode ser ainda mais grave em tempos de crise, – a exemplo da Pandemia de Coronavírus, em que diversos países disponibilizaram bancos de dados de saúde para ampla reutilização e tratamento diverso daqueles que haviam motivado sua coleta e uso original.

Almeida et al. (2020) entendem que, para ampliar a confiança dos indivíduos e da sociedade na utilização de seus dados, ainda que para responder a situações de legítimo interesse público, há de se estabelecer modelos de governança de dados mais justos, responsáveis e sustentáveis, que protejam e defendam princípios éticos e regulatórios, em especial quando se trata de dados pessoais compartilhados entre o setor público e o privado.

Nesse sentido, destaca-se o argumento de Black e Stevens (2013) de que, quando o Estado preza pela confiança do cidadão no tratamento de seus dados pessoais, os indivíduos sentem que seus direitos estão sendo tratados com respeito o que leva ao desenvolvimento de uma cultura de proteção de dados mais robusta no setor público.

3.2 Transparência

A transparência das operações utilizando dados pessoais pelo Estado é primordial para a sociedade informacional, pois proporciona ao cidadão o acesso a suas informações e contribui

para que o indivíduo possa acompanhar a administração de seus dados. Nesse sentido, ainda que estejam sendo utilizados para finalidade de interesse público, os dados compõem a personalidade do titular e requerem mecanismos efetivos de proteção (FÉLIX; MONTEIRO, 2022).

Cumpre registrar que a legislação brasileira prevê que o Poder Público deverá informar de maneira clara, transparente e acessível as hipóteses em que se realiza o tratamento de dados pessoais, bem como sua finalidade, os procedimentos adotados e as práticas utilizadas para tanto (MACIEL, 2020)

Para Almeida *et al.* (2020), ao considerar que dados podem ser utilizados e compartilhados por diferentes pessoas e organizações simultaneamente, as questões principais a serem harmonizadas giram em torno da governança responsável dos dados baseada na transparência para que se estabeleça um relacionamento equilibrado e justo entre indivíduos e organizações. Os autores reforçam ainda que dados coletados, compartilhados e utilizados em prol da execução de políticas públicas, a exemplo da saúde, precisam apresentar termos e condições claros e transparentes sobre os propósitos de acesso, compartilhamento, usos e responsabilidades.

Corroboram com este entendimento Modesto e Ehrhardt Junior (2020), segundo os quais os dados pessoais são extensão dos direitos de personalidade da pessoa natural, devendo-se garantir aos titulares dos dados informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento (responsáveis pela coleta e utilização dos dados), como expressão da transparência que deve ser mantida em operações deste tipo.

Segundo Pleger, Guirguis e Mertes (2021), o Estado é visto pelo cidadão como responsável por garantir a proteção de dados. Nesse sentido, ao exigir que o Estado forneça informações transparentes aos seus cidadãos, no que se refere ao tratamento de seus dados pessoais, uma questão importante deve ser abordada: a informação deve ser apropriada ao grupo-alvo para atender adequadamente às suas preocupações e o discurso público deve levar isso em conta.

Os autores argumentam ainda que a transparência também requer o envolvimento ativo do público e, portanto, os cidadãos precisam ser proativos em se informar. Nesse sentido, os autores incentivam os governos a dialogar com os cidadãos para melhor compreender sua perspectiva subjetiva em termos de proteção de dados e aumentar a transparência, de maneira compreensível, sobre como seus dados estão sendo utilizados.

O problema passa a residir quando o Estado deixa de ser transparente nas suas informações sobre o tratamento dos dados dos seus cidadãos. Segundo Palhares *et al.* (2020), diversos países vêm experimentando críticas quanto às medidas adotadas no tratamento de dados pessoais para atendimento de políticas públicas, sobretudo quando há falta de transparência e falta de diálogo com a população.

Percebe-se na literatura analisada que mecanismos garantidores da transparência no tratamento de dados pessoais pelo Poder Público podem atenuar os impactos da falta de confiança do cidadão, abordados na seção anterior. Segundo Martins *et al.* (2020), quanto mais transparência, mais confiança a sociedade tem na informação e, portanto, maior é a adesão esperada nas medidas implementadas pelo Estado.

Para Félix e Monteiro (2022) o tratamento de dados pessoais é necessário para elaboração e implementação de políticas públicas. Nesse sentido, não cabe questionar se o tratamento deve ou não ocorrer, mas sim debater como fazê-lo de forma eficiente e de modo a menos riscos para os cidadãos. Os autores concluem que a transparência é o caminho para que a própria população ativamente desempenhe seu papel social.

3.3 Segurança

Para Phillips (2021), a ocorrência de uma violação de dados pessoais é outra parte crítica da legislação de proteção de dados. Segundo o autor, apesar das organizações adotarem salvaguardas e medidas de mitigação por meio de políticas e técnicas de segurança, é inevitável que alguém manipule dados pessoais incorretamente ou ainda que criminosos cibernéticos ameacem a proteção de dados pessoais.

Este ponto também é abordado por Naarttijärvi (2018), segundo o qual a falta de segurança da informação implica em deficiências na proteção de dados armazenados em sistemas públicos de informação.

Corroboram com esse entendimento Perry, Raab e Bellamy (2005) ao destacarem que a segurança assume especial relevância quando se trata do compartilhamento de dados pessoais pelos governos. Sendo assim, o uso compartilhado ou outros tipos de tratamento de dados pessoais pela Administração Pública requer mecanismos e ferramentas que garantam a segurança da informação, a partir de medidas técnicas em que a proteção desses dados seja minimamente garantida (OLIVEIRA; ARAÚJO, 2020).

Na visão de Flôres e Silva (2020), a concessão dos dados por parte do cidadão confere grande responsabilidade ao ente público em armazená-los de forma segura, o que nem sempre

acontece. Van Slyke *et al.* (2006) aponta que os governos vêm sendo questionados por negligenciar as salvaguardas apropriadas na coleta de dados ou de não investir o suficiente na proteção desses dados.

Fato é que, ultimamente, violações de dados e roubos de identidade em grande escala tem se tornado cada vez mais comuns em todo o mundo (SULE; ZENNATO; THOMAS, 2021). Nesse sentido, Black e Stevens (2013) apontam que a imprensa de alto perfil vem relatando as violações graves de proteção de dados por organizações do setor público, geralmente envolvendo a perda de dados pessoais por meio de práticas inadequadas de manipulação e retenção de dados.

Em abril de 2020, a CNN reportou uma onda crescente de ataques cibernéticos a agências governamentais e instituições médicas dos EUA que lideravam a resposta à pandemia de coronavírus por grupos criminosos[1]. Em junho de 2020[2], o Primeiro-Ministro australiano admitiu que as atividades maliciosas cresceram ao longo dos meses, embora nenhuma grande violação de dados pessoais tenha sido registrada.

No Brasil, o cenário não é diferente. Em dezembro de 2021, foi noticiado que uma falha de segurança no Ministério da Saúde havia exposto os dados pessoais de mais de 243 milhões de brasileiros cadastrados no Sistema Único de Saúde (SUS)[3].

Por consequência, a literatura aponta uma convergência para o entendimento sintetizado por Mikkelsen *et al.* (2020), segundo o qual os dados devem ser suficientemente protegidos tanto tecnicamente contra riscos cibernéticos quanto organizacionalmente contra o compartilhamento não-autorizado. Entretanto, o cenário apresentado acima indica que ainda é um desafio para o Estado a defesa da proteção de dados pessoais por meio de medidas de segurança suficientes.

3.4 Conformidade

O grau de conformidade, ou de ausência dela, com a legislação sobre o tema também foi um fator apontado recorrentemente nos artigos selecionados. Para Chua, Herbland, Wong e Chang (2017), as organizações governamentais devem ser as líderes no cumprimento da regulação estipulada para reger os processos negociais e defender as leis e ordens a nível

[1] https://edition.cnn.com/2020/04/25/politics/us-china-cyberattacks-coronavirus-research/index.html
[2] https://www.bbc.com/news/world-australia-46096768
[3] https://saude.estadao.com.br/noticias/geral,nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes,70003536340

nacional. Na visão dos autores, o Estado deve servir de modelo para convencimento das organizações não-governamentais de que a conformidade com a legislação deve ser levada a sério.

Sob esse aspecto, a criticidade reside no sentido de que a literatura investigada aponta que, em diversos países, o setor público não está aderente às imposições da legislação para garantia da proteção de dados pessoais.

Um estudo realizado na Malásia investigou o grau de conformidade das organizações quanto à sua legislação de proteção de dados pessoais e apontou que as organizações governamentais do país têm pontuação de conformidade inferior quando comparadas as organizações não-governamentais (CHUA; HERBLAND; WONG; CHANG, 2017).

Black e Stevens (2013) relatam que uma auditoria realizada entre fevereiro de 2010 e julho de 2012 pelo *Information Commissioner's Office* (ICO), autoridade de proteção de dados pessoais do Reino Unido, investigou organizações do setor público e privado quanto à conformidade geral com a legislação aplicável. O resultado da auditoria demonstrou que os órgãos públicos, via de regra, apresentam registros de conformidade insatisfatórios, especialmente quando comparados a organizações do setor privado. Como consequência, o ICO impôs multas fiduciárias a vinte diferentes órgãos do setor público por violações de proteção de dados, em contraste marcante com as penalidades aplicadas contra apenas três empresas privadas.

Em um estudo realizado na Dinamarca, Blume (2012) revela que em certos casos, a exemplo dos prazos para armazenamento e eliminação de dados pessoais, a tradição administrativa prevaleceu e, em muitos aspectos, a prática seguida pelas autoridades públicas não está em total conformidade com a legislação do país.

Mais um exemplo se dá em um estudo de caso que analisou a deliberação da Comissão Nacional de Proteção de Dados (CNPD) no âmbito de processo de investigação e inquérito contra a Autoridade Tributária de Portugal (CORREIA; JESUS; PEREIRA, 2019). A Comissão concluiu que o tratamento de dados pessoais realizado pelo órgão público não estava em conformidade com a lei, recomendando diversos procedimentos para que fossem atendidas as imposições legais.

No Brasil, o cenário não se revelou diferente. No primeiro trimestre de 2021, o Tribunal de Contas da União realizou auditoria que buscou avaliar as ações governamentais e os riscos à proteção de dados pessoais por meio da elaboração de diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD. O Tribunal

concluiu que 55% dos Órgãos não haviam sequer conduzido iniciativas para identificar e planejar as medidas necessárias à adequação à normativa (TCU, 2022).

Assim, ao considerar que as autoridades públicas processam a maioria dos dados pessoais de uma população (BLUME, 2012), as consequências da desconformidade com a legislação aplicável podem ser inúmeras. Black e Stevens (2013) citam, como um exemplo, que a falta de orientações sobre a conformidade do setor público no tratamento de dados pessoais pode resultar em uma falta de padronização entre as diferentes organizações deste setor. Como é o caso do Reino Unido, em que há práticas diversas, aumentando a desinformação e a falta de confiança em cada organização individual promove ainda mais uma cultura de cautela por parte dos cidadãos.

Percebe-se ainda que a não-adequação à legislação também está diretamente relacionada ao estabelecimento de um ambiente de mais ou menos confiança do cidadão no que se refere ao tratamento de seus dados pessoais pelo Poder Público. Segundo Sarabdeen, Chikhaoui e Ishak (2022), o cumprimento dos princípios para a proteção de dados pessoais permite construir a confiança da comunidade nas medidas governamentais e organizacionais, ainda que o processamento de dados esteja dentro das exceções permitidas pela legislação aplicável.

Nesse sentido, Chua, Herbland, Wong e Chang (2017), recomendam que o Estado deve rever sua estratégia de proporcionar um ambiente propício e mecanismos de monitoramento eficazes para avançar em direção a um nível mais alto de conformidade.

Para Blume (2012) a falta de conformidade constatada no setor público se dá em grande medida em razão da legislação sobre o tema abranger tanto o setor público quanto o privado. Na visão do autor, uma regulamentação separada tornaria mais óbvio que a proteção de dados faz parte do Direito Administrativo, podendo ser redigida em melhor conformidade com outras regras administrativas e determinar com mais precisão como e em que medida os dados pessoais podem ser processados por este setor.

Wimmer (2021) destaca que a plena observância da LGPD pelo Poder Público requererá mudanças de cultura e de procedimentos, como por exemplo a incorporação da prática de elaboração de relatórios de impacto à proteção de dados pessoais antes da adoção de novos procedimentos, métodos e tecnologias, bem como a consideração de tais preocupações também quando da edição de atos normativos dotados de generalidade e abstração.

3.5 Interesse Público

O interesse público deve ser o alicerce de qualquer operação de uso de dados pessoais, uma vez que, quando a Administração Pública atua no campo da privacidade e dos dados pessoais, o tratamento é um ato administrativo e, como tal, detém como pressuposto de validade a finalidade pública (OLIVEIRA; ARAÚJO, 2020).

Importa observar o que a legislação sobre o tema estabelece. O Regulamento Geral sobre a Proteção de Dados europeu definiu, em seu artigo 6°, que o tratamento de dados pessoais é legítimo para a execução de uma missão realizada no interesse público ou no exercício da autoridade oficial investida no controlador (CORREIA; JESUS; PEREIRA, 2019). No que se refere à legislação brasileira, a LGPD impôs, em seu artigo 23, às pessoas jurídicas de direito público a observância da finalidade pública, a persecução do interesse público, quando exercerem atividade de tratamento de dados pessoais (OLIVEIRA; ARAÚJO, 2020).

Nesse sentido, Maciel (2020) destaca que é necessário que a coleta de dados pessoais tenha como finalidade sua utilização para fins do interesse público, de modo que o seu resultado venha a ser revertido em proveito de toda a sociedade e para a melhoria dos serviços públicos.

Assim, uma vez que a relação entre o Estado e seus cidadãos deriva de um processo contínuo, o tratamento dos dados pessoais deve ser baseado em justificativas que demonstrem que o processamento de seus dados se dará apenas quando estiver relacionado ao interesse público da sociedade como um todo (BLACK; STEVENS, 2013).

Considerando este aspecto, a tensão sobre o interesse público reside na delicada interação entre a proteção de dados pessoais, por um lado, e a prestação de serviços públicos, por outro (SARABDEEN; CHIKHAOUI; ISHAK, 2022).

Para Black e Stevens (2013), o é essencial examinar como os interesses concorrentes podem ser ponderados, sendo o interesse público o fator decisório. Na visão dos autores, a tentativa de equilibrar o interesse público com os direitos e liberdades fundamentais de um indivíduo é, por vezes, insatisfatória e desigual.

Corroboram com esse entendimento Sarabdeen, Chikhaoui e Ishak (2022) ao afirmarem que o êxito das medidas de implementação para utilização de dados pessoais pelo Poder Público depende do equilíbrio entre o interesse público de usar os dados e o direito privado de proteger os mesmos dados.

Nesse sentido, Modesto e Ehrhardt Junior (2020) entendem que o estabelecimento do ponto de equilíbrio no tratamento dos dados pessoais em prol do interesse coletivo é tarefa bastante árdua, razão pela qual os limites precisam ser construídos na análise do caso concreto.

Perry, Raab e Bellamy (2005) destacam que os Estados têm frequentemente recorrido à noção de interesse público, justificando o tratamento de dados pessoais, por exemplo, para travar uma guerra contra o terrorismo, combater o crime ou proteger o erário público.

Um contraponto a esse argumento é apresentado por Neto e Demoliner (2019) ao chamar atenção que, embora não se possa discordar que a tutela do Estado sobre a privacidade deve levar em conta as exigências da defesa nacional e pública, existe o risco de que, nas mãos de determinados agentes de segurança, a ponderação entre interesses igualmente tutelados seja desvirtuada de modo que, em nome da segurança nacional, seriam tolerados abusos dos mais diversos.

Nesse sentido Wimmer (2021) ressalta que o uso e tratamento de dados pessoais pelo Poder Público tem sido historicamente polemizado a partir de duas linhas interpretativas distintas: de um lado, destacam-se os riscos associados à vigilância e ao controle da sociedade; de outro, a eficiência e a modernização do Estado.

Sob esse aspecto, Bioni (2021) pondera que a privacidade deve ser encarada como um bem comum, o qual detém particular importância para o estado democrático de direito, uma vez que garante a participação deliberativa e heterogênea entre os cidadãos em contraste às sociedades totalitárias. A privacidade não beneficia, portanto, somente o indivíduo, mas, colateralmente, a sociedade como um todo, revelando-se enquanto elemento constitutivo da própria vida em sociedade.

Nesse sentido, a criticidade sobre este elemento é reforçada ao constatar os aspectos contrapostos: embora o interesse público seja o cerne para o tratamento de dados pelo Poder Público, a privacidade e o direito à proteção de dados pessoais também são de interesse público, necessários inclusive para manutenção do Estado democrático de direito.

3.6 Acesso à Informação

Outro ponto crítico identificado na literatura é a conciliação do direito ao acesso à informação pública com a proteção de dados pessoais. Para Wimmer (2021), a aparente tensão entre publicidade e privacidade tem sido sublinhada no contexto da necessidade de conciliar regras que impõem ao Estado um alto grau de disponibilização de informações quanto às suas atividades com as que exigem que dados pessoais sejam tratados de maneira a preservar a sua intimidade, vida privada, honra e imagem.

Flôres e Silva (2020) defendem que um dos maiores desafios da Administração Pública no Brasil é atender às regras previstas na Lei de Acesso à Informação (LAI) (BRASIL, 2011),

frente às garantias estabelecidas na LGPD. Somam-se a esse entendimento Oliveira e Araújo (2020), segundo os quais aos gestores públicos incube um grande desafio de acomodar o acesso à informação, que deve reger os atos da Administração Pública, ao passo que observam o regime jurídico de proteção de dados pessoais.

Destaca-se que, para além de ser um direito de todos, o acesso à informação é essencial para as sociedades democráticas, uma vez que ao se manterem informados sobre as ações do Estado, a população adquire condições de exercer certo controle social (FLÔRES; SILVA, 2020). Entretanto, Gonçalves (2019) ressalta que ações da Administração Pública, ainda que bem-intencionadas, que visam ao atendimento do direito ao acesso à informação e do princípio da publicidade, também podem ferir os direitos da personalidade ao permitir o acesso a terceiros ou tornar públicos dados pessoais.

A despeito dos argumentos apresentados até aqui, que colocam o acesso à informação como um desafio para a proteção de dados pessoais pelo Poder Público, Wimmer (2021) entende que os dois direitos podem ser harmonizados. A autora sustenta que:

> Apesar de adotarem lógicas distintas e, inclusive, terminologias distintas, observa-se que tanto a LAI como a LGPD buscam materializar seus princípios orientadores de modo a construir uma narrativa que permita aliar a lógica de transparência e a lógica de proteção. A LAI, por exemplo, introduz a ideia de consentimento para viabilizar a divulgação de informações pessoais; a LGPD faz referência explícita à LAI para operacionalizar o exercício de direitos nela previstos perante o Poder Público; além disso, indica que o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. A ideia de qualidade dos dados está presente em ambas as normas, assim como a preocupação com a segurança (WIMMER, 2021).

Nesse sentido, embora se constate um possível atrito entre privacidade e publicidade, quando as legislações sobre acesso à informação e proteção de dados pessoais são colocadas em perspectivas contrapostas, é possível buscar uma compatibilização entre as leis, na medida em que se verificam outras formas de disponibilizar o acesso à informação de maneira menos gravosa ao titular de dados pessoais (BRASIL, 2022).

4 Conclusão

Este estudo buscou investigar os principais pontos críticos abordados pela literatura para o tratamento de dados pessoais pelo Poder Público, tendo como base uma revisão sistemática sobre o tema. Como resultado, foram identificados seis elementos de tensão destacados nos

artigos analisados: confiança, transparência, conformidade, segurança, interesse público e acesso à informação.

A literatura aponta que a confiança dos cidadãos no Estado para o tratamento de seus dados pessoais é elemento fundamental para implementação de políticas públicas, em especial no que se refere à digitalização de serviços e às iniciativas de governo eletrônico. Verificou-se ainda que outros pontos críticos identificados, tais como a segurança da informação e a transparência, podem afetar ainda mais a confiança do titular de dados nas ações do Poder Público.

O grau de transparência das informações disponibilizadas pelo Estado no que se refere ao tratamento dos dados pessoais do cidadão é também considerado um ponto de tensão pela literatura, pois quando o Poder Público deixa de fornecer informações claras, precisas e de fácil acesso sobre a guarda e o tratamento de dados pessoais, há uma afronta ao direito de personalidade da pessoa natural.

A literatura também aponta uma convergência para o entendimento de que o Poder Público deve se cercar de mecanismos de segurança da informação e salvaguardas que garantam a proteção dos dados pessoais em posse do Estado. Entretanto, verifica-se ser cada vez mais comum a prática de violações de dados e roubo de identidade em grande escala demonstrando que a segurança é um ponto crítico para o Estado quando da guarda e tratamento de dados pessoais.

Em que pese a sociedade atribuir ao Estado, enquanto ente regulador e garantidor da proteção de dados pessoais, o dever de ser exemplo de cumprimento das regras, com o intuito de propiciar o convencimento das organizações não governamentais de que a conformidade com a legislação deve ser seguida, a falta de conformidade das instituições públicas com a legislação sobre o tema foi identificada em estudos realizados em diversos países.

A doutrina destaca, ainda, o interesse público como principal motivador para o tratamento de dados pessoais pelo Estado. Todavia, faz-se necessária uma avaliação quanto ao seu uso indiscriminado sob o pretexto do bem coletivo, tendo em vista que a privacidade e o direito à proteção de dados pessoais também é de interesse público – necessários inclusive para manutenção do Estado democrático de direito – e devem ser observados a fim de se buscar um equilíbrio entre os dois horizontes da análise.

Por fim, a literatura destaca ainda uma aparente tensão entre privacidade e publicidade, quando a legislação sobre acesso à informação e proteção de dados pessoais são colocados em perspectivas contrapostas. Entretanto, é possível vislumbrar uma harmonização entre as leis, na

medida em que se verifique outras formas de disponibilizar o acesso à informação de maneira menos gravosa ao titular de dados pessoais.

Diante do exposto, conclui-se que o tratamento de dados pessoais pelo Poder Público possui vários aspectos relevantes que impõem diversos desafios ao gestor público, que ao planejar, implementar e avaliar políticas públicas, deve considerar os pontos críticos abordados neste estudo.

5 Referências

ALMEIDA, B. A. et al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. **Ciencia & saude coletiva**, vol. 25, n. suppl 1, p. 2487–2492, 2020.

ALVAREZ, B. A.; TAVARES, L. A. Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil. *In*: ONODERA, M. V. K.; FILIPPO, T. B. G. (Org.). **BRASIL e EUA:** temas de direito comparado. São Paulo: Escola Paulista da Magistratura, 2017.

BELLAMY, C.; PERRI 6; RAAB, C. Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part II. **Public administration**, vol. 83, n. 2, p. 393–415, 2005.

BIONI, B. R. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 3 ed. Rio de Janeiro: Editora Forense, 2021.

BLACK, G.; STEVENS, L. Enhancing data protection and data processing in the public sector: The critical role of proportionality and the public interest. **SCRIPT-ed**, vol. 10, n. 1, p. 93–122, 2013.

BLUME, P. The inherent contradictions in data protection law. **International data privacy law**, vol. 2, n. 1, p. 26–34, 2012.

BOTELHO, M. C. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. **Revista de Direitos Sociais e Políticas Públicas**, Bebedouro, vol. 8, n. 2, p. 197-231, 2020.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo:** Tratamento de dados pessoais pelo poder público. Brasília, DF, 2022.

BRASIL. Lei n º 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação. Brasília, DF: Presidência da República, 2018.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

CHIZZOTTI, A. Pesquisa qualitativa em ciências humanas e sociais. São Paulo: **Cortex**, 2006.

CHOROSZEWICZ, M.; MÄIHÄNIEMI, B. Developing a digital welfare state: Data protection and the use of automated decision-making in the public sector across six EU countries. **Global Perspectives**, vol. 1, n. 1, 2020.

CHUA, H. N.; HERBLAND, A., WONG, S. F.; CHANG, Y. Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. **Telematics and informatics**, vol. 34, n. 4, p. 157–170, 2017.

COMBE, C. Observations on the UK transformational government strategy relative to citizen data sharing and privacy. Transforming Government People Process and Policy, vol. 3, n. 4, p. 394–405, 2009.

CORREIA, P. M. A. R.; JESUS, I. O. A.; PEREIRA, S. P. M. o tratamento de dados pessoais na administração pública portuguesa: o caso de estudo da opacidade da autoridade tributária. **Lex Humana**, vol. 11, n. 2, p. 128-142, 2019.

NETO, E. F.; DEMOLINER, K. S. Direito à privacidade e novas tecnologias: Breves considerações acerca da proteção de dados pessoais no Brasil e na Europa. **Revista internacional Consinter de direito**, vol. 7, n. 7, p. 19–40, 2018.

FÉLIX, V.; MONTEIRO, J. R. O uso de tecnologias e dados pessoais em políticas públicas de saúde no contexto da COVID-19. **civilistica.com**, vol. 11, n. 1, p. 1-31, maio. 2022.

FLICK, U. Introdução à pesquisa qualitativa. São Paulo: **Artmed**, 2009.

FLÔRES, M. R.; SILVA, R. L. Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da administração pública: entre o dever público de informar e o direito do cidadão de ser tutelado. **Revista de direito**, vol. 12, n. 02, p. 01–34, 2020.

GOOGLE SCHOLAR. **Número de Citações**. Disponível em: <http://scholar.google.com>. Acesso em 24 de jan. 2023.

GONÇALVES, T. C. N. M. **Gestão de dados pessoais e sensíveis pela administração pública federal: desafios, modelos e possíveis impactos com a nova lei**. Dissertação (Mestrado em Direito) – Centro Universitário de Brasília, Brasília, 2019.

HINTZBERGEN, J. et. al. **Fundamentos de segurança da informação:** com base na ISSO 27001 e na ISSO 27002. Rio de Janeiro: Brasport, 2018.

LANDWEHR, C. 2018: A big year for privacy. **Communications of the ACM**, vol. 62, n. 2, p. 20–22, 2019.

LIPS, M.; TAYLOR, J. A.; BANNISTER, F. Public administration in the information society: Essays on risk and trust. **Information polity**, vol. 10, n. 1,2, p. 1–9, 2005.

MACIEL, M. Os tribunais de contas no exercício do controle externo de acordo com nova Lei Geral de Proteção de Dados Pessoais. **Revista Controle: Doutrinas e artigos**, vol. 18, n. 1, p. 20-45. 2020.

MARTINS, H. et al. Tratamento de dados pessoais em aplicativos públicos relacionados ao coronavírus no Ceará. **Liinc em revista**, vol. 16, n. 2, p. e5387, 2020.

MIKKELSEN, D.; SOLLER, H.; STRANDELL-JANSSON, M. **Privacy, security, and public health in a pandemic year**. Disponível em: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/privacy-security-and-public-health-in-a-pandemic-year. Acesso em: 14 jan. 2023.

MODESTO, J. A.; EHRHARDT JUNIOR, M. Danos colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pessoais no combate a COVID-19. **Revista Eletrônica Direito e Sociedade - REDES**, vol. 8, n. 2, p. 143, 2020.

NAARTTIJÄRVI, M. Balancing data protection and privacy – The case of information security sensor systems. **Computer law & security review**, vol. 34, n. 5, p. 1019-1038, 2018.

OCDE. **A Caminho da Era Digital no Brasil.** Paris: OECD Publishing, 2020.

OLIVEIRA, A. C. S.; ARAÚJO, D. S. O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da Lei Geral de Proteção de Dados. **Liinc em Revista**, Natal, vol. 16, n. 2, p. e5318, dez. 2020.

PAGANI, R. N., KOVALESKI, J.L., RESENDE, L.M. Methodi Ordinatio: a proposed methodology to select and rank relevant scientific papers encompassing the impact factor, number of citation, and year of publication. **Scientometrics**, vol. 105, n. 40, p. 2109–2135. 2015.

PALHARES, G. C. et al. A privacidade em tempos de pandemia e a escada de monitoramento e rastreio. **Estudos Avançados**, vol. 34, n. 99, p. 175–190, 2020.

PERRI 6; RAAB, C.; BELLAMY, C. Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part I. **Public administration**, vol. 83, n. 1, p. 111–133, 2005.

PHILLIPS, B. UK further education sector journey to compliance with the general data protection regulation and the data protection act 2018. **Computer law and security report**, vol. 42, n. 105586, p. 105586, 2021.

PLEGER, L. E.; GUIRGUIS, K.; MERTES, A. Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security. **Computers in human behavior**, vol. 122, n. 106830, p. 106830, 2021.

SARABDEEN, J., CHIKHAOUI, E., ISHAK, M. M. M. Creating standards for Canadian health data protection during health emergency: An analysis of privacy regulations and laws. **Heliyon**, vol. 8, n. 5, e09458, maio. 2022.

SOARES, S. V., PICOLLI, I. R. A., CASAGRANDE, J. L. Pesquisa bibliográfica, pesquisa bibliométrica, artigo de revisão e ensaio teórico em administração e contabilidade. **Administração: ensino e pesquisa**, Rio de Janeiro, vol. 19, n. 2, p. 308-339, maio/ago. 2018.

SULE, M. J.; ZENNARO, M.; THOMAS, G. Cybersecurity through the lens of digital identity and data protection: Issues and trends. **Technology in society**, vol. 67, n. 101734, p. 101734, 2021.

STELZER, J. et al. **A lei geral de proteção de dados pessoais e os desafios das instituições de ensino superior para a adequação**. 2019. Trabalho apresentado ao XIX Colóquio Internacional de Gestão Universitária, Florianópolis, 2019.

TAYLOR, J. A.; LIPS, M.; ORGAN, J. Identification practices in government: citizen surveillance and the quest for public service improvement. **Identity in the information society**, vol. 1, n. 1, p. 135–154, 2008.

TEIXEIRA, T.; GUERREIRO, R. M. **Lei Geral de Proteção de Dados Pessoais (LGPD): Comentada Artigo por Artigo**. São Paulo: Editora Saraiva, 2022.

TRIBUNAL DE CONTAS DA UNIÃO. **Acórdão nº 1384/2022**, TCU/Plenário, 21 jun. 2022. Disponível em: <https://bit.ly/3MyEYFv>. Acesso em: 15 out. 2022.

VAN SLYKE, C. *et al.* Concern for information privacy and online consumer purchasing. **Journal of the Association for Information Systems**, vol. 7, n. 6, p. 415–444, 2006.

VAINZOF, R. In: MALDONADO, V. N.; BLUM, R. O. (Coord.). **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, Thomson Reuters Brasil, 2019.

WIMMER, M. O regime jurídico do tratamento de dados pessoais pelo poder público. *In*: BIONI, B. (Org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

Pontos críticos para o tratamento de dados pessoais pelo poder público: um estudo empírico

Critical points of personal data processing by the public authorities: an empirical study

Resumo

A Lei Geral de Proteção de Dados Pessoais, editada no Brasil em agosto de 2018, estabelece como uma das bases legais para o tratamento de dados pessoais a execução de políticas públicas pelo Estado. Uma revisão sistemática da literatura identificou a existência de seis pontos críticos que representam desafios para os gestores públicos na elaboração e implementação de políticas que exijam o tratamento de dados pessoais. O objetivo desta pesquisa é de estabelecer os níveis de criticidade dos fatores identificados pela revisão de literatura, bem como verificar a existência de outros pontos críticos sobre os quais a literatura ainda não avançou. Para tanto, um grupo de 11 especialistas foi selecionado para participar da pesquisa que utilizou o Método Delphi, técnica que consiste na aplicação de um conjunto de questionários de modo sequencial e individual, a fim de estabelecer um diálogo entre os participantes e construir uma resposta coletiva. Os resultados apontam uma coerência entre o que foi verificado na teoria e a percepção dos especialistas. Outros 10 pontos críticos para o tratamento de dados pessoais pelo Poder Público foram mencionados pelos participantes. Em geral, os principais elementos de tensão identificados foram a falta de capacitação dos agentes públicos e o compartilhamento de dados pessoais.

Palavras-chave: Dados Pessoais, Privacidade, Poder Público, Método Delphi, Políticas Públicas.

Abstract

The General Data Protection Law, enacted in Brazil in August 2018, establishes the execution of public policies by the State as one of the legal bases for the processing of personal data. A systematic review of the literature identified the existence of six critical points that represent challenges for public managers in the elaboration and implementation of policies that require the processing of personal data. The objective of this research is to establish the levels of criticality of the factors identified by the literature review, as well as to verify the existence of other critical points on which the literature has not yet advanced. Therefore, a group of 11 specialists was selected to participate in the research that used the *Delphi Method*, a technique that consisted of applying a set of sessions sequentially and individually to establish a dialogue between the participants and build a collective response. The results show coherence between what was verified in theory and the specialists' perception. Another 10 critical points for the processing of personal data by the Government were mentioned by specialists.

Keywords: Personal Data, Privacy, Government, *Delphi Method*, Public Policies.

1 Introdução

O avanço tecnológico, somado ao fato de que a elaboração de políticas públicas e dos programas sociais utilizam cada vez mais os dados pessoais do cidadão, levou a um aumento do poder informacional do Estado (MACHADO; BIONI, 2016).

Tradicionalmente, a proteção dos dados pessoais tem sido compreendida como o direito de autodeterminação do indivíduo quanto as suas informações pessoais. Nessa linha, o consentimento do titular dos dados seria o pilar normativo para as autorizações sobre o tratamento dos seus dados pessoais (BIONI, 2021).

Entretanto, essa lógica não é a base da maior parte do tratamento de dados pessoais realizada pelo Estado. No que se refere às bases legais para o tratamento de dados pessoais pelo Poder Público, a Lei Geral de Proteção de Dados (LGPD) prevê duas hipóteses centrais: (i) execução de políticas públicas; e (ii) execução de competências legais ou atribuições legais do serviço público (WIMMER, 2021).

Seguindo esse entendimento, Neto, Ishikawa e Maciel (2021) salientam que o direito fundamental à proteção dos dados pessoais não é um direito absoluto, e deve ser conciliado com a necessidade de execução das funções da própria Administração Pública que, por sua vez, precisarão ser exercitadas com total respeito ao titular de dados.

Bellamy, Perry e Raab (2005) destacam que os gestores públicos enfrentam um grande desafio na tentativa de equilibrar a tensão que se revela entre os objetivos de serviços públicos que exigem o tratamento de dados pessoais e a proteção da privacidade. Esse conflito tem sido explorado na literatura, destacando os seguintes pontos de criticidade:

1) A confiança dos cidadãos no Estado. Os indivíduos tentam sentir que seus direitos estão sendo respeitados quando o Poder Público preza pela confiança do titular de dados, o que permite o desenvolvimento de uma cultura de proteção de dados pessoais mais forte no setor público (BLACK; STEVENS, 2013);

2) A transparência das operações utilizando dados pessoais pelo Estado. Este fator contribui para que o indivíduo possa acompanhar a administração de seus dados (FÉLIX; MONTEIRO, 2022). Deve-se garantir que os dados coletados, compartilhados e utilizados em prol da execução de políticas públicas possuam termos e condições claros e transparentes sobre os propósitos de acesso, compartilhamento, usos e responsabilizações (ALMEIDA *et al.*, 2020);

3) A segurança da informação. A falta desse fator implica em deficiências na proteção de dados pessoais (NAARTTIJÄRVI, 2018). Apesar das organizações adotarem salvaguardas

e medidas de mitigações por meio de políticas e técnicas de segurança, há riscos de que alguém manipule dados pessoais incorretamente ou ainda que criminosos cibernéticos ameacem a proteção de dados pessoais (PHILLIPS, 2021);

4) A conformidade das instituições públicas. O Estado deve demonstrar liderança no comprimento da legislação (CHUA; HERBLAND; WONG; CHANG, 2017). Entretanto, estudos apontam que, em diversos países, o setor público não está aderente às imposições da legislação aplicável ao tratamento de dados pessoais;

5) O interesse público motivador do tratamento dos dados. Embora este fator seja o alicerce para o tratamento de dados pessoais pelo Poder Público (OLIVEIRA; ARAÚJO, 2020), faz-se necessário observar o equilíbrio entre o interesse público em tratar os dados e os direitos e liberdades fundamentais de um indivíduo na proteção dos mesmos dados (SARABDEEN; CHIKHAOUI; ISHAK, 2022); e

6) O direito ao acesso a informações públicas. Este fator impõe ao Estado um alto grau de disponibilização de informações quanto às suas atividades, entretanto, a divulgação dessa informação deve observar também a proteção dos dados pessoais de maneira a preservar a intimidade, vida privada, honra e imagem do indivíduo (WIMMER, 2021).

Assim, considerando os resultados gerais apresentados na literatura, este estudo tem por objetivo analisar os pontos críticos para o tratamento de dados pessoais pelo Poder Público à luz da percepção de especialistas no tema. Dessa forma, pretende-se estabelecer níveis de criticidade, hierarquizando os fatores de tensão para a realidade brasileira.

Tendo em vista a atualidade da matéria, é possível que a literatura ainda não tenha identificado outros potenciais pontos de tensão. Dessa forma, a pesquisa com especialistas investigará a existência de outros pontos críticos sobre os quais a teoria ainda não avançou.

Ressalta-se que na revisão bibliográfica não foram localizados estudos empíricos produzidos no Brasil sobre o tema. A partir desta pesquisa será possível agregar a visão de gestores públicos e de estudiosos da área aos conceitos já estabelecidos pela literatura nacional e internacional, bem como confirmar ou refutar as teorias empregadas. Portanto, a proposição de pontos críticos ainda não explorados pela literatura deve possibilitar a avaliação para uma agenda de futuras pesquisas.

2 Metodologia

A pesquisa adota a abordagem qualitativa. Seu desenvolvimento envolve procedimentos que poderão surgir ao longo da sua realização, bem como a análise de dados intuitivamente

construída a partir das particularidades para os temas gerais e as interpretações feitas pelo pesquisador acerca do significado dos dados (CRESWELL, 2017).

O estudo se caracteriza pelo seu caráter exploratório e sua natureza descritiva. Para Cervo, Bervian e Silva (2007, p. 76), a pesquisa exploratória "realiza descrições precisas da situação e quer descobrir as relações existentes entre seus elementos componentes". Além disso, segundo os mesmos autores, a pesquisa descritiva observa, registra, analisa e correlaciona os fatos, buscando conhecer as diversas situações e relações que ocorrem no objeto de estudo.

Com o objetivo de identificar os pontos críticos relacionados ao tratamento de dados pessoais pelo Poder Público foi realizada uma revisão sistemática da literatura, que será detalhada na seção Referencial Teórico. Para se estabelecer os níveis de criticidade, bem como investigar a existência de outros pontos críticos sobre os quais a teoria ainda não avançou, ou seja, o Referencial Analítico, realizou-se a aplicação de questionários junto a especialistas pelo método *Delphi*.

Segundo Marconi e Lakatos (2003), a aplicação de questionários tem como vantagem a não-exposição do entrevistado à influência do pesquisador, conferindo maior liberdade e segurança nas respostas; a possibilidade de que as pessoas o respondam no momento a elas mais conveniente; a obtenção de respostas mais rápidas e mais precisas; além de possibilitar mais uniformidade na avaliação, em virtude da natureza impessoal do instrumento.

2.1 Referencial Teórico

A identificação dos pontos críticos para o tratamento de dados pessoais pelo Poder Público ocorreu a partir de uma revisão sistemática da literatura, utilizando-se para tanto o *Methodi Ordinatio*. Segundo Pagani, Kovaleski e Resende (2015), esse método tem por objetivo realizar a procura, seleção e exame de trabalhos científicos, utilizando como base a relevância dos estudos e tem como critério a atualidade do artigo (ano de publicação), a quantidade de citações e seu fator de impacto.

As buscas foram realizadas no Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES e no *Scopus*, uma vez que esses bancos de dados reúnem diversas outras bases, ampliando o resultado da pesquisa. As palavras-chaves utilizadas na busca foram: em português, "dados pessoais", "Poder Público", "Estado" e "Setor Público"; em inglês, "*data protection*" e "*Public Sector*". Os operadores *booleanos OR* e *AND* foram utilizados para relacionar os termos investigados.

Após a aplicação do *Methodi Ordinatio*, 43 artigos foram selecionados para compor o portfólio, considerando apenas artigos gratuitos, completos, em língua portuguesa, inglesa ou espanhola, revisados por pares e publicados entre os anos de 2005 e 2022. Ademais, outros trabalhos relevantes foram identificados de forma assistemática por meio da análise das referências dos artigos selecionados pela revisão sistemática.

A partir do portfólio bibliográfico, pode-se identificar a existência de seis principais pontos críticos para o tratamento de dados pessoais pelo Poder Público, conforme as referências consultadas e detalhadas na Tabela 1.

Tabela 1. Pontos críticos identificados na revisão sistemática da literatura

Ponto Crítico	Referências
Confiança	Almeida et al. (2010); Bellamy, Perri e Raab (2005); Black e Stevens (2013); Lubis, Kartiwi e Zulhuda (2018); Martins et al. (2020); Perri, Raab, e Bellamy (2005); Pleger, Guirguis e Mertes (2021); Sarabdeen, Chikhaoui e Ishak (2022); Sule, Zennaro e Thomas (2021).
Transparência	Almeida et al. (2010); Félix e Monteiro (2022); Machado e Bioni (2016); Maciel (2020); Martins et al. (2020); Modesto e Ehrhardt Junior (2020); Naarttijärvi (2018); Neto, Ishikawa e Maciel (2021); Palhares et al. (2020); Pleger, Guirguis e Mertes (2021); Sule, Zennaro e Thomas (2021).
Segurança	Black e Stevens (2013); Flôres e Silva (2020); Naarttijärvi (2018); Oliveira e Araújo (2020); Perri, Raab e Bellamy (2005); Phillips (2021); Pleger, Guirguis e Mertes (2021); Sarabdeen, Chikhaoui e Ishak (2022); Sule, Zennaro e Thomas (2021).
Conformidade	Black e Stevens (2013); Blume (2012); Chua, Herbland, Wong e Chang (2017); Correia, Jesus e Pereira (2019); Sarabdeen, Chikhaoui e Ishak (2022).
Interesse Público	Almeida et al. (2010); Bellamy, Perri e Raab (2005); Black e Stevens (2013); Comandè e Schneider (2022); Correia, Jesus e Pereira (2019); Félix e Monteiro (2022); Flôres e Silva (2020); Maciel (2020); Modesto e Ehrhardt Junior (2020); Neto e Demoliner (2019); Oliveira e Araújo (2020); Perri, Raab e Bellamy (2005); Sarabdeen, Chikhaoui e Ishak (2022).
Acesso à Informação	Félix e Monteiro (2022); Flôres e Silva (2020); Oliveira e Araújo (2020);

Fonte: Dados extraídos da pesquisa

2.2 Método *Delphi*

Para a aplicação do questionário foi utilizado o método *Delphi*. Segundo Freitas e Marque (2018), essa técnica consiste em um conjunto de questionários a serem respondidos, de maneira sequencial e individual, com informações resumidas sobre as respostas do grupo aos questionários anteriores, de modo a se estabelecer uma espécie de diálogo entre os participantes e, gradualmente, construir uma resposta coletiva.

Gupta e Clarke (1996) ressaltam que o método é vantajoso na medida em que propicia a captura de um grande número de variáveis interrelacionadas e características multidimensionais comuns à maioria dos problemas complexos, além de lidar com aspectos criativos e abertos de um problema, uma vez que motiva o pensamento independente e a formação gradual de soluções de grupo.

O que diferencia o método *Delphi* de uma pesquisa comum é o *feedback* das informações coletadas do grupo e a oportunidade de os participantes modificarem ou refinarem seus julgamentos com base nas respostas do grupo. Dessa forma, a técnica tenta projetar um espaço em que os indivíduos com experiências em diferentes disciplinas ou especialidades contribuam com informações ou julgamentos para uma área problemática, compartilhando conhecimento com o grupo na busca de um consenso entre as distintas opiniões (LINSTONE; TUROFF, 1975).

Para este trabalho, quinze especialistas foram convidados a participar da pesquisa. Considerando o caráter multidisciplinar do tema, os participantes convidados possuem experiências profissionais complementares – gestores públicos, pesquisadores e representantes da sociedade civil – com formações acadêmicas diversas – Direito, Administração, Tecnologia da Informação, entre outras.

A seleção dos convidados teve como critérios a experiência profissional de, no mínimo, dois anos de atuação em proteção de dados pessoais – para os gestores públicos e representantes da sociedade civil – e curso de doutorado concluído ou em andamento – para os pesquisadores. Apenas onze dos especialistas convidados aceitaram participar da pesquisa.

Na aplicação dos questionários, a comunicação foi escrita, por meio eletrônico, realizada em duas rodadas para a coleta de dados. Para Giovinazzo (2001), a aplicação de duas rodadas é suficiente quando o método *Delphi* é realizado em meio eletrônico, tendo em vista que etapas adicionais poderiam não despertar o interesse dos especialistas.

Antes do envio dos formulários, estes foram testados por um especialista com o objetivo de verificar a clareza das perguntas. As sugestões recebidas foram incorporadas no questionário.

Para elaboração e aplicação dos formulários eletrônicos, foi utilizado o aplicativo gratuito de gerenciamento de pesquisas *Google Forms*.

O questionário inicial foi semiestruturado, composto por duas seções. Na primeira, foram apresentados os seis pontos críticos para o tratamento de dados pessoais pelo Poder Público identificados na revisão de literatura, os especialistas foram convidados a julgar os níveis de criticidade para cada fator, por meio de uma escala de Diferencial Semântico com dez pontos (de 1 – Não é crítico – a 10 – Extremamente crítico). Além disso, os participantes puderam justificar abertamente a resposta oferecida em cada fator. Na segunda seção, os especialistas foram convidados a indicar um ou mais pontos críticos que não foram identificados na literatura. O primeiro formulário foi aplicado em novembro de 2022 e encontra-se disponível no Apêndice A.

Após a obtenção das respostas na primeira aplicação do questionário, as frequências das respostas nos seis pontos críticos foram calculadas e as suas respectivas justificativas analisadas e sintetizadas, gerando o documento para o *feedback* das informações. Esse documento foi disponibilizado junto ao questionário na segunda rodada de coleta de dados.

Para Freitas e Marque (2018), ao utilizar a técnica *Delphi* na construção dos questionários para a segunda rodada de aplicação, parte-se da análise das respostas do grupo de especialistas ao primeiro questionário, sendo de extrema importância que, nesses questionários, verifique-se retorno da informação anterior, analisada e resumida, para apreciação do painel de especialistas.

O segundo questionário apresentou a posição individual de cada especialista junto com a síntese das respostas coletivas, facilitando a comparação entre a posição individual e a do grupo. Nesse momento, os participantes foram convidados a refletir sobre suas respostas, podendo alterar ou manter seus julgamentos quanto ao nível de criticidade de cada fator analisado, atingindo avaliação definitiva sobre cada ponto. O segundo formulário foi aplicado em janeiro de 2023 e encontra-se no Apêndice B deste trabalho.

Após a classificação e organização das informações coletadas nas duas rodadas, foram estabelecidas as relações existentes entre os dados, tais como pontos de divergência, convergência, tendências, princípios de causalidade e possibilidade de generalização, levando-se em conta, a pertinência, relevância e autenticidade das informações (PÁDUA, 2018).

3 Resultados e discussão

3.1 Nível de criticidade

Os resultados demonstram que, na visão dos especialistas consultados, todos os pontos de tensão identificados na literatura para o tratamento de dados pessoais pelo Poder Público possuem alto grau de criticidade, tendo em vista que todos alcançaram um valor médio superior a sete (Tabela 2).

Tabela 2. Média dos níveis de criticidade atribuídos pelos especialistas

Ponto Crítico	Média do nível de criticidade
Confiança	8
Transparência	8
Segurança	8,8
Conformidade	9,1
Interesse Público	8,6
Acesso à Informação	7,7

Fonte: Dados extraídos da pesquisa

A conformidade das instituições públicas com a legislação sobre o tema foi o elemento que alcançou o maior nível de criticidade, apontando o valor médio de 9,1 firmado pelos especialistas ao final da segunda aplicação do questionário.

Na percepção dos especialistas, a conformidade com a legislação relacionada à proteção de dados pessoais é fundamental e envolve a adoção de protocolos e instâncias de governança internos capazes de atribuir responsabilidades para implementar pontos de controle e supervisão do tratamento de dados pessoais nas instituições. Entretanto, para os participantes, a conformidade ainda se encontra em estágio inicial nas instituições públicas. A pesquisa também apontou a necessidade de maiores investimentos e capacitação de gestores públicos para fomento da conformidade em proteção de dados no âmbito do Poder Público.

A opinião dos especialistas vai ao encontro do que foi verificado pela revisão da literatura sobre o tema, onde constatou-se que as administrações públicas de vários países, incluindo o Brasil, não se encontram em plena conformidade com as legislações sobre proteção de dados pessoais.

Uma auditoria realizada pela Autoridade de Proteção de Dados do Reino Unido demonstrou que os órgãos públicos geralmente têm registros de conformidade insatisfatórios, especialmente quando comparados a organizações do setor privado (BLACK; STEVENS, 2013). De igual modo, na Dinamarca, a prática seguida pelas autoridades públicas não está em total conformidade com a regulamentação sobre o tema (BLUME, 2012). Um estudo desenvolvido na Malásia também constatou que "as organizações governamentais têm pontuação de conformidade inferior às organizações não governamentais" (CHUA; HERBLAND; WONG; CHANG, 2017).

O segundo maior nível de criticidade foi atribuído aos mecanismos de segurança da informação e salvaguardas que garantam a proteção dos dados pessoais em posse do Estado, que pontuou um valor médio de 8,8.

Os especialistas apontaram que a segurança da informação é um elemento essencial para a proteção de dados pessoais, e está diretamente relacionada à confiança dos titulares no uso dos serviços públicos. Ainda, na visão dos participantes, os casos de vazamentos de dados pessoais em posse do Estado e de incidentes de segurança contribuem para a percepção de que as entidades públicas encontram-se inadequadas no que se refere aos padrões de segurança da informação.

A avaliação dos especialistas dialoga com Pleger, Guirguis e Mertes (2021), segundo os quais os cidadãos por vezes têm reservas em relação aos esforços do governo em prover serviços eletrônicos, em razão das preocupações com a proteção de dados e segurança. Soma-se a isso o entendimento de Sule, Zennato e Thomas (2021), que considera os casos de violações massivas de dados pessoais capazes de afetar indiretamente as decisões dos usuários de serviços eletrônicos e a confiança no ecossistema digital.

Ainda sob este aspecto, destacou-se que a proteção de dados pessoais, bem como o processo de adequação das instituições à legislação pressupõe uma abordagem ampla e multidisciplinar, de modo a não se resumir exclusivamente à adoção de medidas de segurança da informação.

O interesse público, motivador do tratamento dos dados, obteve o terceiro maior nível de criticidade, com valor médio de 8,6. Para os especialistas, este deve ser o fundamento precípuo de qualquer operação envolvendo dados pessoais pelos entes públicos. Corroboram com esse entendimento Oliveira e Araújo (2020), ao afirmarem que o interesse público deve ser o alicerce do Poder Público para o tratamento de dados pessoais.

Os especialistas destacaram ainda que o interesse público é um conceito indeterminado e que deve ser justificado em concreto, ou seja, com a definição de finalidades específicas para

o tratamento dos dados. Nesta mesma linha de entendimento, Modesto e Ehrhardt Júnior (2020) afirmam que os limites para se alcançar o equilíbrio no tratamento dos dados pessoais em benefício do interesse público devem ser construídos na análise do caso concreto.

Para os participantes, o interesse público evidencia a assimetria nas relações entre o cidadão e o Estado. Essa percepção é reforçada pelo entendimento de que o Estado goza de posição proeminente em relação ao titular de dados, e que, essa assimetria de poderes se reflete na prevalência do interesse público diante do interesse individual (BIONI, 2021).

No que se refere à confiança dos cidadãos no Estado para o tratamento de seus dados pessoais, a média do nível de criticidade atribuído pelos especialistas foi de 8,0. Segundo os participantes, esse atributo é essencial para conferir sustentabilidade às ações do Estado, mas a percepção revela um cenário nacional de desconfiança.

Nesse aspecto, foi destacado que a confiança decorre da transparência de como os dados pessoais são tratados pelo Poder Público, e que há aumento do nível de criticidade caso haja ascensão de governos autoritários. Os participantes também relacionaram a confiança como consequência natural da conformidade e da segurança da informação.

Também foi pontuado que a desconfiança pode levar ao boicote do cidadão quando o Estado requer seus dados pessoais. Na linha desse entendimento, Landwehr (2019) destaca que os usuários de serviços públicos devem confiar que seus dados estão sendo usados adequadamente para que haja disposição em fornecê-los.

O grau de transparência das informações disponibilizadas pelo Estado no que se refere ao tratamento dos dados pessoais do cidadão também atingiu um valor médio de criticidade de 8,0. Na visão dos especialistas, esse ponto é essencial para evitar abusos e usos indevidos dos dados pessoais e sua ausência pode gerar ações judiciais ou contestação de políticas públicas.

Relatou-se ainda a percepção de ausência de clareza na utilização dos dados pessoais do cidadão pela Administração Pública, bem como a necessidade de se organizar as bases de dados por meios seguros para cumprimento da transparência e de desenvolvimento de mecanismos para informar como os dados pessoais são tratados no âmbito do serviço prestado à sociedade.

Ainda sobre esse aspecto, foi pontuado que a transparência está diretamente ligada à confiança do cidadão, corroborando com o resultado observado na revisão de literatura sobre o tema. Para Martins *et al.* (2020), quanto mais transparência, mais confiança a sociedade tem na informação e, portanto, maior é a adesão esperada nas medidas implementadas pelo Estado.

O menor valor médio de criticidade (7,7) foi atribuído aos desafios relacionados ao acesso à informação. Este ponto levanta a necessidade de conciliar a legislação que garante o

direito à disponibilização de informações relativas às atividades estatais com o direito à proteção de dados pessoais.

Nesse quesito, observa-se a percepção de que entidades têm deixado de atender pedidos de acesso à informação fundamentados na legislação pertinente por suposta vedação da Lei Geral de Proteção de Dados Pessoais. Entretanto, na visão dos especialistas, acesso à informação, privacidade e proteção de dados não são conceitos e normas incompatíveis entre si e podem coexistir de forma harmônica.

Essa percepção encontra amparo na visão de Wimmer (2021), pois observa-se que as leis brasileiras de acesso à informação e proteção de dados pessoais buscam materializar seus princípios orientadores de modo a construir uma narrativa que possibilite aliar transparência com proteção de dados, apesar de adotarem lógicas distintas.

3.2 Pontos críticos não abordados na literatura pesquisada

Além dos seis pontos críticos para o tratamento de dados pessoais pelo Poder Público identificados na revisão da literatura, os especialistas foram convidados a contribuir com até três outros fatores que, em suas visões, poderiam ser considerados, em igual medida, pontos de tensão. Nesta seção do questionário foram obtidas vinte e nove respostas, sendo que sete foram eliminadas por já estarem relacionadas aos pontos críticos identificados na revisão de literatura ou por não ser possível compreender adequadamente o fator abordado pelo participante. Após análise e consolidação obteve-se outros dez pontos críticos identificados pelos especialistas (Tabela 3).

Tabela 3. Outros pontos críticos identificados pelos especialistas

Ponto Crítico	Quantidade de especialistas que mencionaram o ponto crítico	Distribuição
Capacitação de agentes públicos	5	45%
Compartilhamento de dados	4	36%
Finalidade do tratamento	2	18%
Abordagem não baseada em riscos	2	18%
Minimização da coleta de dados	2	18%
Desconhecimento dos cidadãos	2	18%
Prestação de contas	2	18%

Discriminação	1	9%
Governança de bases de dados	1	9%
Eliminação de dados pessoais	1	9%

Fonte: Dados extraídos da pesquisa

A falta de conscientização e capacitação dos agentes públicos foi identificada como um ponto crítico por 45% dos especialistas, que destacaram que a falta de equipe com qualificação na área de proteção de dados pessoais tem implicações diretas no processo de conformidade das instituições com a legislação sobre o tema.

Nesse aspecto, os dados apresentados em uma auditoria realizada pelo Tribunal de Contas da União (TCU) que buscou avaliar as ações governamentais para adequação à legislação de proteção de dados pessoais corroboram com a percepção dos especialistas. Segundo o TCU (2022, p. 84):

> Em relação à "Capacitação", as respostas demonstram que a minoria das organizações, 29%, possui Plano de Capacitação que abrange a proteção de dados pessoais, o que representa um risco organizacional, uma vez que a LGPD é uma legislação técnica e de difícil compreensão, que exige estudo para que as organizações adquiram maturidade no tema. Além disso, a pesquisa demonstrou que quase metade das organizações que elaboraram o plano, 46%, não considerou a necessidade de que pessoas que exercem funções com responsabilidades essenciais relacionadas à proteção de dados pessoais deveriam receber treinamento diferenciado.

O compartilhamento de dados pessoais pelo Poder Público foi mencionado por 36% dos especialistas. Segundo Perry, Raab e Bellamy (2005), o compartilhamento de dados abrange a divulgação de dados pessoais entre instituições e inclui a transferência de bancos de dados completos, bem como informações de registros de indivíduos. Para os autores, o compartilhamento de dados também é usado para dar suporte a várias funções do Estado, incluindo o planejamento e avaliação de políticas públicas, a alocação de recursos e a aplicação de sanções ou outros controles.

A literatura mostra que práticas de compartilhamento estão sendo cada vez mais comuns na Administração Pública. Choroszewicz e Mäihäniemi (2020) apontam que, atualmente, há uma pressão oriunda do interior das administrações públicas para facilitar o compartilhamento e a combinação de conjuntos de dados entre diferentes autoridades, bem como para permitir um uso mais abrangente dos dados.

No Brasil, a intenção de desburocratizar procedimentos, de combater fraudes, e de melhorar a qualidade e a efetividade das políticas públicas, baseando-as em evidências e

indicadores concretos, tem impulsionado o compartilhamento de bases de dados na Administração Pública (WIMMER, 2021).

Para Félix e Monteiro (2022), o compartilhamento de dados pode implicar em riscos para os titulares em razão das informações deles extraídas. Os autores entendem que, para reduzir tais riscos, faz-se necessário o planejamento das políticas públicas, além da aplicação de medidas de proteção dos dados.

Outro resultado observado foi a relação existente entre o compartilhamento de dados com a finalidade que motivou a sua obtenção. Segundo Neto, Ishikawa e Maciel (2021, p. 169) "qualquer compartilhamento realizado pela Administração Pública, no exercício de suas funções, deverá se dar, exclusivamente, para a finalidade específica de execução de políticas públicas". A utilização de dados pessoais para finalidades diversas das que motivaram a sua coleta original foi apontada como um fator crítico por 18% dos especialistas.

Dois especialistas destacaram a presença de uma abordagem não baseada em riscos pelo poder público. A Lei Geral de Proteção de Dados Pessoais, em diversos artigos do seu texto, faz referência ao risco e à necessidade de avaliação dos seus possíveis efeitos nas operações de tratamento de dados pessoais, a fim de avaliar o seu impacto no que diz respeito aos direitos e liberdades individuais dos titulares de dados (GOMES, 2020). Entretanto, os especialistas apontam que os agentes públicos, via de regra, não estão preparados para realizar análises de risco, o que pode ser um obstáculo na adequação de procedimentos para atendimento da Lei como, por exemplo, a elaboração de relatórios de impacto à proteção de dados pessoais.

A minimização da coleta ou da obtenção de dados pessoais também foi identificada por dois especialistas consultados (18%). Segundo a percepção dos participantes, esse ponto está relacionado ao princípio da necessidade, segundo o qual a Administração Pública deve utilizar apenas os dados estritamente necessários para o desenvolvimento da atividade em prol do interesse público. Assim, o não-atendimento ao conceito da minimização pode levar ao tratamento excessivo de dados pessoais, por vezes desnecessários ao atendimento da finalidade que motivou a coleta.

A falta de conhecimento dos cidadãos sobre o assunto também foi objeto de duas respostas (18%). Esse posicionamento encontra respaldo nos estudos de Christo (2012), segundo o qual a maioria da população desconhece seus direitos no que concerne à privacidade e à proteção de dados pessoais. Nessa linha, o autor entende que o Estado deve realizar campanhas de educação pública sobre o tema, que possibilitem aos indivíduos maior empoderamento sobre seus direitos e responsabilidades, bem como maior conhecimento sobre as consequências de suas ações.

A prestação de contas sobre a forma como o Poder Público trata os dados pessoais também é um ponto de tensão, apontado por dois especialistas. Corroboram com esse entendimento Modesto e Ehrhardt Júnior (2020), segundo os autores a prestação de contas ocorre com a demonstração, por parte do agente responsável pelo tratamento, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, incluem as medidas para prevenção e proteção aos direitos nelas assegurados.

O princípio da não discriminação foi identificado como um ponto crítico por um participante. Importa observar que a Lei Geral de Proteção de Dados Pessoais veda a realização de tratamento para fins discriminatórios ilícitos ou abusivos. Entretanto, conforme Matiuzzo, Schertel e Fujimoto (2021, p. 450), a crescente utilização de algoritmos e os desenvolvimentos recentes da ciência da computação no campo da Inteligência Artificial (IA) apresentam desafios a esse princípio:

> [...] no que concerne à discriminação algorítmica, é preciso reconhecer que, primeiramente, essa ferramenta já é uma realidade, seu uso se expande a cada dia, e, portanto, seria pouco razoável e produtivo pensar na eliminação do uso de sistemas automatizados. Em segundo lugar, destaca-se que esses sistemas podem ser extremamente eficientes, trazendo inúmeros benefícios, se utilizados de forma estruturada e com base em parâmetros legais mínimos. Dessa forma, os esforços devem ser centrados em desenvolver mecanismos que garantam segurança e um grau de controle dos resultados obtidos via automação, mitigando os riscos de discriminação inerentes à técnica estatística empregada.

A eliminação, um dos tipos de tratamento de dados pessoais, também foi identificada como um ponto de tensão por um especialista. A Lei Geral de Proteção de Dados Pessoais define a eliminação como "a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado e determina que, no âmbito e nos limites técnicos das atividades, os dados pessoais serão eliminados após o término de seu tratamento" (BRASIL, 2018). Sob este prisma, a experiência internacional revela que a tradição administrativa é a de manutenção dos dados, tornando a exclusão uma exceção, ainda que a legislação imponha o contrário (BLUME, 2012).

Por fim, a governança de bancos e bases de dados pessoais foi outro ponto crítico colocado por um dos especialistas. Almeida *et al.* (2020) destacaram a importância desse aspecto, segundo os autores, ao considerar que dados podem ser utilizados e compartilhados por diferentes organizações simultaneamente, a governança responsável dos dados baseada na

transparência é uma das principais questões a serem harmonizadas para que haja confiança e relacionamentos equilibrados e justos entre indivíduos e organizações.

4 Conclusão

Por meio de uma revisão sistemática da literatura e uma pesquisa com especialistas, este trabalho buscou estabelecer os níveis de criticidade dos fatores de tensão para o tratamento de dados pessoais pelo Poder Público para a realidade brasileira. O presente estudo também teve por objetivo investigar a existência de outros pontos críticos sobre os quais a teoria ainda não avançou.

Os resultados demonstram que a conformidade das instituições públicas é o elemento de maior criticidade. Na percepção dos especialistas, este atributo ainda se encontra em estágio inicial de implementação nas instituições públicas brasileiras e envolve a adoção de protocolos e instâncias de governança internos com responsabilidades para implementar pontos de controle e supervisão do tratamento de dados pessoais.

Em seguida, encontram-se os mecanismos de segurança da informação, que foram considerados pelos especialistas como elemento essencial, embora não exclusivo, para a proteção de dados pessoais, e estão diretamente relacionados com a confiança dos cidadãos.

Na terceira posição encontra-se o interesse público motivador do tratamento dos dados, sendo considerado pelos especialistas o fundamento mais precípuo de qualquer operação envolvendo dados pessoais pelo Poder Público.

Na sequência, a confiança dos cidadãos no Estado para o tratamento de seus dados pessoais e o grau de transparência das informações disponibilizadas obtiveram o mesmo nível de criticidade. Enfim, os desafios relacionados ao acesso à informação foram elencados ao último grau de criticidade.

Diante do que foi apresentado até aqui, verifica-se que, por meio da metodologia adotada, foi possível confirmar e complementar, com base na perspectiva dos participantes, os resultados obtidos na pesquisa bibliométrica e na revisão da literatura sobre o tema.

Observa-se ainda que nenhum dos seis fatores de tensão identificados na revisão sistemática da literatura apresentou nível de criticidade inferior a sete, depreendendo-se desse resultado que, segundo a percepção dos especialistas, todos os aspectos elencados possuem um alto grau de criticidade no cenário nacional. Dessa forma, pode-se concluir que o tratamento de dados pessoais pelo Poder Público possui desafios semelhantes aos enfrentados em outros países e requer aperfeiçoamento para garantir a plena observância da legislação.

Além disso, os especialistas foram capazes de identificar outros dez pontos críticos para o tratamento de dados pessoais pelo Poder Públicos, não explorados profundamente pela literatura selecionada no portfólio bibliográfico. São eles: 1) a capacitação de agentes públicos; 2) o compartilhamento de dados pessoais em posse do Poder Público; 3) finalidade do tratamento; 4) abordagem não baseada em riscos; 5) minimização da coleta de dados; 6) desconhecimento dos cidadãos; 7) prestação de contas; 8) discriminação; 9) governança de bases de dados; e 10) eliminação de dados pessoais coletados.

O número significativo de pontos de tensão abordado pelos especialistas demonstra que, no Brasil, o tratamento de dados pessoais pelo Poder Públicos ainda apresenta diversos desafios não explorados pela literatura nacional e internacional sobre o tema.

Uma limitação ao desenvolvimento deste trabalho foi a ausência de estudos prévios que explorassem pesquisas com especialistas. Dessa forma, só foi possível analisar e comparar os resultados frente à teoria investigada, não sendo viável sua comparação com outros estudos semelhantes. Assim, os outros pontos de tensão abordados pelos especialistas têm o potencial de embasar uma agenda de futuras pesquisas que permitam explorar com maior profundidade o referencial teórico de cada fator, bem como suas implicações para o tratamento de dados pessoais pelo Poder Público.

5 Referências

ALMEIDA, B. A. et al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. **Ciencia & saude coletiva**, vol. 25, n. suppl 1, p. 2487–2492, 2020.

BELLAMY, C.; PERRI 6; RAAB, C. Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part II. **Public administration**, vol. 83, n. 2, p. 393–415, 2005.

BIONI, B. R. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 3 ed. Rio de Janeiro: Editora Forense, 2021.

BLACK, G.; STEVENS, L. Enhancing data protection and data processing in the public sector: The critical role of proportionality and the public interest. **SCRIPT-ed**, vol. 10, n. 1, p. 93–122, 2013.

BLUME, P. The inherent contradictions in data protection law. **International data privacy law**, vol. 2, n. 1, p. 26–34, 2012.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

CERVO, A. L.; BERVIAN, P. A., SILVA, R. **Metodologia científica.** 6. ed. São Paulo: Pearson Prentice Hall, 2007.

CRESWELL, J. W. **Projeto de Pesquisa:** Métodos qualitativos, quantitativos e misto. São Paulo: Artmed, 2017.

CHOROSZEWICZ, M.; MÄIHÄNIEMI, B. Developing a digital welfare state: Data protection and the use of automated decision-making in the public sector across six EU countries. **Global Perspectives**, vol. 1, n. 1, 2020.

CHRISTO, E. D. Data protection in Trinidad and Tobago. **International data privacy law**, vol. 3, n. 3, p. 202–209, 2013.

CHUA, H. N.; HERBLAND, A., WONG, S. F.; CHANG, Y. Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. **Telematics and informatics**, vol. 34, n. 4, p. 157–170, 2017.

COMANDÈ, G.; SCHNEIDER, G. Differential data protection regimes in data-driven research: Why the GDPR is more research-friendly than you think. **German law journal**, vol. 23, n. 4, p. 559–596, 2022.

CORREIA, P. M. A. R.; JESUS, I. O. A.; PEREIRA, S. P. M. o tratamento de dados pessoais na administração pública portuguesa: o caso de estudo da opacidade da autoridade tributária. **Lex Humana**, vol. 11, n. 2, p. 128-142, 2019.

FÉLIX, V.; MONTEIRO, J. R. O uso de tecnologias e dados pessoais em políticas públicas de saúde no contexto da COVID-19. **civilistica.com**, vol. 11, n. 1, p. 1-31, maio. 2022.

FLÔRES, M. R.; SILVA, R. L. Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da administração pública: entre o dever público de informar e o direito do cidadão de ser tutelado. **Revista de direito**, vol. 12, n. 02, p. 01–34, 2020.

FREITAS, D.; MARQUES, J. B. V. Método DELPHI: caracterização e potencialidades na pesquisa em Educação. **Pro-Posições**, São Paulo, vol. 29, n. 2 p. 389-415, 2018.

GIOVINAZZO, R. Modelo de aplicação da metodologia Delphi pela Internet: vantagens e ressalvas. **Administração online**, vol. 2, n. 2, abr./jun. 2001.

GOMES, M. C. O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In: PALHARES, F. (Coord.). **Temas atuais de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2020.

GOOGLE FORMS. **Formulários Google**: criador de formulários on-line. Página incial. Disponível em: https://www.google.com/intl/pt-BR/forms/about/. Acesso em: 14 jan. 2023.

GUPTA, U. G.; CLARKE, R. E. Theory and application of the Delphi technique: a bibliography (1975-1994). **Technological Forecasting and Social Change**, vol. 53, p. 185-211, 1996.

LANDWEHR, C. 2018: A big year for privacy. **Communications of the ACM**, vol. 62, n. 2, p. 20–22, 2019.

LINSTONE, H. A.; TUROFF, M. **Delphi Method: Techniques and Applications**. Boston: Addison-Wesley Educational, 1975.

LUBIS, M.; KARTIWI, M.; ZULHUDA, S. Current state of personal data protection in electronic voting: Criteria and indicator for effective implementation. **TELKOMNIKA (Telecommunication Computing Electronics and Control)**, vol. 16, n. 1, p. 290, 2018.

MACHADO, J.; BIONI, B. R. A proteção de dados pessoais nos programas de Nota Fiscal: um estudo de caso do "Nota Fiscal paulista". **Liinc em revista**, vol. 12, n. 2, 2016.

MACIEL, M. Os tribunais de contas no exercício do controle externo de acordo com nova Lei Geral de Proteção de Dados Pessoais. **Revista Controle: Doutrinas e artigos**, vol. 18, n. 1, p. 20-45. 2020.

MARCONI, M. de A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MARTINS, H. et al. Tratamento de dados pessoais em aplicativos públicos relacionados ao coronavírus no Ceará. **Liinc em revista**, vol. 16, n. 2, p. e5387, 2020.

MATIUZZO, M.; SCHERTEL, L. Discriminação Algorítmica à luz da Lei Geral de Proteção de Dados. In: BIONI, B. (Org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

MODESTO, J. A.; EHRHARDT JUNIOR, M. Danos colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pessoais no combate a COVID-19. **Revista Eletrônica Direito e Sociedade - REDES**, vol. 8, n. 2, p. 143, 2020.

NAARTTIJÄRVI, M. Balancing data protection and privacy – The case of information security sensor systems. **Computer law & security review**, vol. 34, n. 5, p. 1019-1038, 2018.

NETO, A. B. S.; ISHIKAWA, L.; MACIEL, M. O tratamento de dados pessoais pelo poder público e o papel dos tribunais de contas. **Revista Direitos Culturais**, vol. 16, n. 40, p. 163–177, 2021.

NETO, E. F.; DEMOLINER, K. S. Direito à privacidade e novas tecnologias: Breves considerações acerca da proteção de dados pessoais no Brasil e na Europa. **Revista internacional Consinter de direito**, vol. 7, n. 7, p. 19–40, 2018.

OLIVEIRA, A. C. S.; ARAÚJO, D. S. O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da Lei Geral de Proteção de Dados. **Liinc em Revista**, Natal, vol. 16, n. 2, p. e5318, dez. 2020.

PÁDUA, E. M. M. **Metodologia da pesquisa:** aborgagem teórico-prática. São Paulo: Papirus, 2018.

PAGANI, R. N., KOVALESKI, J.L., RESENDE, L.M. Methodi Ordinatio: a proposed methodology to select and rank relevant scientific papers encompassing the impact factor,

number of citation, and year of publication. **Scientometrics**, vol. 105, n. 40, p. 2109–2135. 2015.

PERRI 6; RAAB, C.; BELLAMY, C. Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part I. **Public administration**, vol. 83, n. 1, p. 111–133, 2005.

PHILLIPS, B. UK further education sector journey to compliance with the general data protection regulation and the data protection act 2018. **Computer law and security report**, vol. 42, n. 105586, p. 105586, 2021

PLEGER, L. E.; GUIRGUIS, K.; MERTES, A. Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security. **Computers in human behavior**, vol. 122, n. 106830, p. 106830, 2021.

SARABDEEN, J., CHIKHAOUI, E., ISHAK, M. M. M. Creating standards for Canadian health data protection during health emergency: An analysis of privacy regulations and laws. **Heliyon**, vol. 8, n. 5, e09458, maio. 2022.

SULE, M. J.; ZENNARO, M.; THOMAS, G. Cybersecurity through the lens of digital identity and data protection: Issues and trends. **Technology in society**, vol. 67, n. 101734, p. 101734, 2021.

TRIBUNAL DE CONTAS DA UNIÃO. **Acórdão nº 1384/2022**, TCU/Plenário, 21 jun. 2022. Disponível em: https://bit.ly/3MyEYFv. Acesso em: 15 out. 2022.

WIMMER, M. O regime jurídico do tratamento de dados pessoais pelo poder público. *In*: BIONI, B. (Org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

APÊNDICE A – Questionário 1

1 Apresentação

Olá, meu nome é Núbia Rocha, sou aluna de Mestrado do Programa de Pós Graduação em Gestão Pública, da Universidade de Brasília - UnB. Tendo em vista sua experiência profissional, acredito que sua contribuição pode acrescentar muito para o meu estudo, cuja finalidade é exclusivamente acadêmica.

Será aplicada a metodologia *Delphi*, em que um grupo de especialistas é convidado a responder um questionário, podendo modificar a sua opinião a partir do acesso a opinião do grupo em uma segunda aplicação do questionário.

Informo que os dados pessoais coletados serão utilizados exclusivamente para fins deste estudo, sendo eliminados após o uso. A identificação de e-mail é feita apenas para realizar o feedback das respostas do grupo. Respostas individuais não serão divulgadas.

O tempo médio para responder é de 10 minutos. Desde já, agradeço a sua participação e coloco-me à disposição para esclarecimentos pertinentes à pesquisa através do e-mail nubiaaugusto@gmail.com.

2 Contextualização

Alguns fatores de tensão para o tratamento de dados pessoais pelo Poder Público são:

- **Confiança:** quando o Estado preza pela confiança do cidadão no tratamento de seus dados pessoais, os indivíduos sentem que seus direitos estão sendo tratados com respeito o que leva ao desenvolvimento de uma cultura de proteção de dados mais robusta no setor público.

- **Transparência:** a transparência das operações utilizando dados pessoais pelo Estado contribui para que o indivíduo possa acompanhar a administração de seus dados. Nesse sentido, deve-se garantir que os dados coletados, compartilhados e utilizados em prol da execução de políticas públicas possuam termos e condições claros e transparentes sobre os propósitos de acesso, compartilhamento, usos e responsabilizações.

- **Segurança da informação:** a falta de segurança da informação implica em deficiências na proteção de dados armazenados em sistemas públicos de informação. Apesar das organizações adotarem salvaguardas e medidas de mitigações por meio de políticas e técnicas de segurança,

há riscos de que alguém manipule dados pessoais incorretamente ou ainda que criminosos cibernéticos ameacem a proteção de dados pessoais.

- **Conformidade:** o Estado deve estabelecer mecanismos que garantam a plena observância da legislação, entretanto, estudos apontam que, em diversos países, o setor público não está aderente às imposições da legislação aplicável ao tratamento de dados pessoais.

- **Interesse público:** embora o interesse público seja o alicerce para o tratamento de dados pessoais pelo Poder Público, faz-se necessário observar o equilíbrio entre o interesse público em tratar os dados e os direitos e liberdades fundamentais de um indivíduo na proteção dos mesmos dados.

- **Acesso à informação:** o direito ao acesso a informações públicas impõe ao Estado um alto grau de disponibilização de informações quanto às suas atividades, entretanto, a divulgação dessa informações deve observar também a proteção dos dados pessoais de maneira a preservar a intimidade, vida privada, honra e imagem do individuo.

Por favor, indique o grau de criticidade desses aspectos e justifique sua resposta.

Q1. Sobre a **confiança** dos cidadãos no Estado para o tratamento de seus dados pessoais, atribua um nível de criticidade.

Não é crítico	1	2	3	4	5	6	7	8	9	10	Extremamente crítico

Justifique sua resposta: _____

Q2. Sobre o grau de **transparência** das informações disponibilizadas pelo Estado, no que se refere ao tratamento dos dados pessoais do cidadão, atribua um nível de criticidade.

Não é crítico	1	2	3	4	5	6	7	8	9	10	Extremamente crítico

Justifique sua resposta: _____

Q3. Sobre os mecanismos de **segurança da informação** e salvaguardas que garantam a proteção dos dados pessoais em posse do Estado, atribua um nível de criticidade.

Não é crítico	1	2	3	4	5	6	7	8	9	10	Extremamente crítico

Justifique sua resposta: _____

Q4. Sobre a **conformidade** das instituições públicas com a legislação sobre o tema, atribua um nível de criticidade.

Não é crítico	1	2	3	4	5	6	7	8	9	10	Extremamente crítico

Justifique sua resposta: _____

Q5. Sobre o **interesse público** motivador do tratamento dos dados, atribua um nível de criticidade.

Não é crítico	1	2	3	4	5	6	7	8	9	10	Extremamente crítico

Justifique sua resposta: _____

Q6. Sobre os desafios relacionados ao **acesso à informação**, atribua um nível de criticidade.

Não é crítico	1	2	3	4	5	6	7	8	9	10	Extremamente crítico

Justifique sua resposta: _____

Q7. Por favor, identifique até 3 pontos críticos DIFERENTES dos já analisados na seção anterior:

Ponto crítico 1: _____

Ponto crítico 2: _____

Ponto crítico 3: _____

APÊNDICE B – Questionário 2

1 Apresentação

Olá! Muito obrigada pela sua participação na primeira etapa desta pesquisa.

Esta é a última etapa da metodologia *Delphi*, e consiste no compartilhamento das respostas consolidadas na etapa anterior para uma nova rodada de avaliação sobre o tema, a partir da perspectiva dos especialistas participantes da pesquisa.

Após a leitura dos resultados apresentados, você poderá refletir sobre as justificativas apontadas para cada ponto crítico analisado e informar se gostaria de alterar sua resposta fornecida na primeira etapa.

Para fins desta pesquisa, considere o nível de criticidade como sendo o grau de relevância dos fatores de tensão identificados, ponderando os seus impactos para a execução da atividade pública.

Informo que os dados pessoais coletados serão utilizados exclusivamente para fins deste estudo, sendo eliminados após o uso. A identificação de e-mail é feita apenas para realizar o *feedback* das respostas do grupo. Respostas identificadas não serão divulgadas.

O tempo médio para responder o formulário é de 15 minutos.

Desde já, agradeço a sua participação e coloco-me à disposição para esclarecimentos pertinentes à pesquisa através do e-mail nubiaaugusto@gmail.com.

Q1. **Confiança** dos cidadãos no Estado para o tratamento de seus dados pessoais:

A confiança na proteção dos dados em posse do Estado passa pela criação e fomento de ferramentas e mecanismos que possibilitem que os titulares de dados tenham a percepção que seus dados são tratados com respeito e boa fé, levando ao desenvolvimento de uma cultura de proteção de dados no setor público.

Resposta individual	Resposta do Grupo	
1. Sobre a **confiança** dos cidadãos no Estado para o tratamento de seus dados pessoais, atribua um nível de criticidade:	Distribuição das respostas	
Campo individualizado: Indicação da nota atribuída ao participante na primeira rodada	10	45%
	9	0%
	8	18%
	7	9%
	6	9%
	5	9%
	4	9%
	3	0%
	2	0%
	1	0%
	Média:	**8**
Justificativa apresentada:	Síntese das respostas	
Campo individualizado: Justificativa da nota apresentada pelo participante na primeira rodada	- Existência de assimetria de informação; - Confiança é elemento crítico e essencial para conferir sustentabilidade às ações estatais; - Não há clareza de quais dados estão sendo coletados e para qual finalidade estão sendo tratados; - Aumento do nível de criticidade caso haja ascensão de governos autorirários; - Importância da percepção de que o Estado respeita os direitos dos titulares; - Credibilidade como fator fundamental; - O cenário nacional é de desconfiança; - A confiança decorre da transparência de como os dados pessoais são tratados; - Elemento crítico e essencial para conferir sustentabilidade às ações do estatais; - A desconfiança pode levar ao boicote por parte do cidadão quando o Estado requer seus dados pessoais; - A confiança é consequência natural da conformidade e da segurança da informação; - Há necessidade de criação e fomento de uma estratégia nacional para aumentar a confiança entre Estado e sociedade;	

a. Agora, considerando as notas atribuídas e as justificativas apresentadas pelos especialistas, você gostaria de alterar a sua resposta inicial?

( ) Sim

( ) Não

b. Se sim, por gentileza, indique o nível de criticidade para este fator?

Não é crítico	1	2	3	4	5	6	7	8	9	10	Extremamente crítico

c. Gostaria de acrescentar algum comentário adicional sobre esse item? _____

Q2. Grau de **transparência** das informações disponibilizadas pelo Estado:

A transparência no uso dos dados pessoais em posse do Estado contribui para que o titular possa acompanhar e entender como seus dados são tratados. Nesse sentido, deve-se garantir que os dados coletados, compartilhados e utilizados em prol da execução de políticas públicas possuam práticas de transparência que permitam compreender como se dará o acesso, compartilhamento, usos e responsabilizações no tratamento dos dados.

Resposta individual	**Resposta do Grupo**	
2. Sobre o grau de **transparência** das informações disponibilizadas pelo Estado, no que se refere ao tratamento dos dados pessoais do cidadão, atribua um nível de criticidade.	Distribuição das respostas	
Campo individualizado: Indicação da nota atribuída ao participante na primeira rodada	10	36%
	9	18%
	8	9%
	7	18%
	6	0%
	5	9%
	4	0%
	3	9%
	2	0%
	1	0%
	Média:	**8**
Justificativa apresentada:	Síntese das respostas	
Campo individualizado: Justificativa da nota apresentada pelo participante na primeira rodada	- Elemento diretamente ligado à confiança do cidadão; - Dever ético dos agentes públicos; - Necessidade de desenvolver mecanismos para informar como os dados pessoais são tratados no âmbito do serviço prestado à sociedade; - Essencial para evitar abusos e usos indevidos dos dados pessoais; - Subsidio para o controle democrático sobre as ações estatais baseadas em dados pessoais; - A ausência de transparência pode gerar judicialização ou contestação de políticas públicas;- Percepção de ausência de clareza na utilização dos dados pessoais do cidadão pela Administração Pública - Necessidade de organização das bases de dados em meios seguros como pré-requisito para o atendimento da transparência;	

a. Agora, considerando as notas atribuídas e as justificativas apresentadas pelos especialistas, você gostaria de alterar a sua resposta inicial?

( ) Sim

( ) Não

b. Se sim, por gentileza, indique o nível de criticidade para este fator?

Não é crítico	1	2	3	4	5	6	7	8	9	10	Extremamente crítico

c. Gostaria de acrescentar algum comentário adicional sobre esse item? _____

Q3. Mecanismos de **segurança da informação** e salvaguardas que garantam a proteção dos dados pessoais em posse do Estado:

A falta de segurança da informação implica em riscos na proteção dos dados em posse do Estado. Apesar da adoção de salvaguardas e medidas de mitigação por meio de políticas e técnicas de segurança, há riscos de manipulação indevida de dados pessoais, incidentes de segurança e outros crimes cibernéticos.

Resposta individual	**Resposta do Grupo**	
3. Sobre os mecanismos de **segurança da informação** e salvaguardas que garantam a proteção dos dados pessoais em posse do Estado, atribua um nível de criticidade.	Distribuição das respostas	
Campo individualizado: Indicação da nota atribuída ao participante na primeira rodada	10	55%
	9	27%
	8	9%
	7	0%
	6	0%
	5	0%
	4	0%
	3	9%
	2	0%
	1	0%
	Média:	**8,9**
Justificativa apresentada:	Síntese das respostas	
Campo individualizado: Justificativa da nota apresentada pelo participante na primeira rodada	- Os casos de vazamentos de dados pessoais em posse do Estado e de incidentes de segurança contribuem para a percepção de que as entidades públicas estão inadequadas no que se refere aos padrões de segurança da informação; - Elemento essencial para a proteção de dados pessoais; - Está relacionada com a confiança dos titulares no uso dos serviços públicos; - Baixos investimentos em Segurança da Informação geram um risco aos cidadãos, que fornecem seus dados ao Estado por força de obrigações legais; - A importância da segurança da informação aumenta na exata medida da sensibilidade dos dados pessoais tratados.	

a. Agora, considerando as notas atribuídas e as justificativas apresentadas pelos especialistas, você gostaria de alterar a sua resposta inicial?

( ) Sim

( ) Não

b. Se sim, por gentileza, indique o nível de criticidade para este fator?

Não é crítico	1	2	3	4	5	6	7	8	9	10	Extremamente crítico

c. Gostaria de acrescentar algum comentário adicional sobre esse item? _____

Q4. **Conformidade** das instituições públicas com a legislação sobre proteção de dados pessoais:

O Estado deve estabelecer mecanismos que garantam a plena observância da legislação, entretanto, estudos apontam que, em diversos países, o setor público não está aderente às imposições da legislação aplicável ao tratamento de dados pessoais.

Resposta individual	**Resposta do Grupo**	
4. Sobre a **conformidade** das instituições públicas com a legislação sobre o tema, atribua um nível de criticidade.	Distribuição das respostas	
Campo individualizado: Indicação da nota atribuída ao participante na primeira rodada	10	55%
	9	27%
	8	0%
	7	0%
	6	9%
	5	9%
	4	0%
	3	0%
	2	0%
	1	0%
	Média:	**8,9**
Justificativa apresentada:	Síntese das respostas	
Campo individualizado: Justificativa da nota apresentada pelo participante na primeira rodada	- A conformidade com a legislação relacionada à proteção de dados pessoais é fundamental para que seus agentes compreendam a criticidade e a relevância do tema; - Percepção de que a conformidade dos entes à LGPD ainda está em estágio inicial; - A conformidade é aspecto fundamental, pois envolve a adoção de protocolos e instâncias de governança internos que irão implementar pontos de controle e de supervisão sobre o uso dos dados pessoais pela instituição pública. - A falta de capital humano e de recursos financeiros nas organizações do setor público contribuem para a falta de conformidade; - É essencial maiores investimentos e capacitação de gestores para fomento da conformidade em proteção de dados no âmbito do poder público- Existência de mais meios de imposição de conformidade no setor público do que no setor privado, ainda que a coerção pecuniária da fiscalização seja impossibilitada para entes públicos.	

a. Agora, considerando as notas atribuídas e as justificativas apresentadas pelos especialistas, você gostaria de alterar a sua resposta inicial?

( ) Sim

( ) Não

b. Se sim, por gentileza, indique o nível de criticidade para este fator?

Não é crítico	1	2	3	4	5	6	7	8	9	10	Extremamente crítico

c. Gostaria de acrescentar algum comentário adicional sobre esse item? _____

Q5. **Interesse público** motivador do tratamento dos dados pessoais:

Embora o interesse público seja o alicerce para o tratamento de dados pessoais pelo Poder Público, faz-se necessário observar o equilíbrio entre o interesse público em tratar os dados e os direitos e liberdades fundamentais do titular.

Resposta individual	Resposta do Grupo	
5. Sobre o **interesse público** motivador do tratamento dos dados, atribua um nível de criticidade.	Distribuição das respostas	
Campo individualizado: Indicação da nota atribuída ao participante na primeira rodada	10	36%
	9	9%
	8	27%
	7	18%
	6	0%
	5	0%
	4	9%
	3	0%
	2	0%
	1	0%
	Média:	**8,3**
Justificativa apresentada:	Síntese das respostas	
Campo individualizado: Justificativa da nota apresentada pelo participante na primeira rodada	- O interesse público deve ser o fundamento mais precípuo do tratamento de dados pessoais pelo ente público; - O interesse público deve ser justificado em concreto; - A falta de transparência prejudica a avaliação quanto a preservação do interesse público no tratamento de dados pessoais; - Interesse público é um conceito indeterminado; - A definição de finalidades específicas deve ser elemento norteador do interesse público no tratamento de dados pessoais. - Faz-se necessário balizar o interesse público com as salvaguardas estabelecidas na LGPD; - As práticas de compartilhamento de dados e atribuição de novas finalidades para o tratamento pelo poder público é um ponto de atenção. - O interesse público evidencia a assimetria nas relações entre o cidadão e o Estado.	

a. Agora, considerando as notas atribuídas e as justificativas apresentadas pelos especialistas, você gostaria de alterar a sua resposta inicial?

( ) Sim

( ) Não

b. Se sim, por gentileza, indique o nível de criticidade para este fator?

Não é crítico	1	2	3	4	5	6	7	8	9	10	Extremamente crítico

c. Gostaria de acrescentar algum comentário adicional sobre esse item? _____

Q6. **Acesso à Informação:**

O direito ao acesso a informações públicas impõe ao Estado um alto grau de disponibilização de informações quanto às suas atividades, entretanto, a divulgação dessas informações deve

observar também a proteção dos dados pessoais de maneira a preservar a intimidade, vida privada, honra e imagem do individuo.

Resposta individual	Resposta do Grupo	
6. Sobre os desafios relacionados ao **acesso à informação**, atribua um nível de criticidade.	Distribuição das respostas	
Campo individualizado: Indicação da nota atribuída ao participante na primeira rodada	10	27%
	9	27%
	8	9%
	7	9%
	6	0%
	5	18%
	4	0%
	3	0%
	2	0%
	1	9%
	Média:	**7,5**
Justificativa apresentada:	Síntese das respostas	
Campo individualizado: Justificativa da nota apresentada pelo participante na primeira rodada	- Percepção de que entidades deixam de atender a pedidos de informação fundamentados na LAI por suposta vedação da LGPD; - Pedidos de informação podem ser atendidos em conformidade com a LAI e com a LGPD; - Acesso à informação, privacidade e proteção de dados não são conceitos e normais incompatíveis entre si e podem coexistir e funcionar de forma harmônica; - Uma cultura de proteção de dados só é possível se houver alinhamento com a transparência e o acesso à informação; - Inexistência de impasse real entre acesso à informação e proteção de dados pessoais.	

a. Agora, considerando as notas atribuídas e as justificativas apresentadas pelos especialistas, você gostaria de alterar a sua resposta inicial?

( ) Sim

( ) Não

b. Se sim, por gentileza, indique o nível de criticidade para este fator?

Não é crítico	1	2	3	4	5	6	7	8	9	10	Extremamente crítico

c. Gostaria de acrescentar algum comentário adicional sobre esse item? _____