Computer Law & Security Review 54 (2024) 106023

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

Critical points for the processing of personal data by the government: An empirical study in Brazil

Núbia Augusto de Sousa Rocha [a], Alexandre Nascimento de Almeida [b,*], André Nunes [b], Humberto Angelo [c]

[a] Brazilian Telecommunications, Graduate in Public Administration, University of Brasília (PPGP/UnB), DF, Brazil, 70640-440
[b] University of Brasília, Planaltina campus (UnB/FUP), University Area n, 1 – Vila Nossa Senhora de Fátima, Planaltina, DF, Brazil, 73.300-000
[c] Forestry Engineering Department, Technology Faculty, University of Brasília (EFL/FT/UnB), DF, Brazil, 70.910-900

ARTICLE INFO

Keywords:
Privacy
Delphi method
Public policies

ABSTRACT

The General Law for the Protection of Personal Data (LGPD), issued in Brazil in August 2018, establishes as one of the legal bases for the processing of personal data the execution of public policies by the State. 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. To this end, a group of 11 specialists was selected to participate in the research that used the Delphi Method, a technique that consists of applying a set of questionnaires sequentially and individually, in order to establish a dialog between the participants and build a collective response. The results indicate a coherence between what was verified in the theory and the perception of the specialists. Another 10 critical points for the processing of personal data by the government were mentioned by the participants. In general, the main elements of tension identified addressed the lack of training of public officials and the sharing of personal data.

1. Introduction

The technological advance, added to the fact that the elaboration of public policies and social programs increasingly use the personal data of the citizen, has led to an increase in the informational power of the State.[1] The increase in this informational power allows the creation and implementation of more effective public policies, but exposes concerns about the confidentiality of this data.

Following a global regulatory trend regarding data protection, Brazil published in august 2018 the General Data Protection Law (LGPD), which regulates the processing of personal data, including in digital media, by natural persons or legal entities governed by public or private law, with the aim of protecting the fundamental rights of freedom and privacy and free development of the natural person's personality.[2]

Traditionally, the protection of personal data has been understood as the right of self-determination of the individual regarding his or her personal information. In this line, the consent of the data subject would be the normative pillar for authorizations on the processing of their personal data.[3]

However, this logic is not the basis of most of the processing of personal data carried out by the State. With regard to the legal bases for the processing of personal data by the Brazilian government, the General

* Corresponding author at: University of Brasília, Planaltina campus (UnB/FUP), University Area n., 1 – Vila Nossa Senhora de Fátima, Planaltina, DF, Brazil, 73.300-000.
E-mail address: alexalmeida@unb.br (A.N. de Almeida).

[1] Machado, J., & Bioni, B. R. (2016). The protection of personal data in Nota Fiscal programs: a case study of the "Nota Fiscal paulista". *Liinc in Review*, 12 (2), 350-364. https://doi.org/10.18617/liinc.v12i2.919.

[2] Rocha, N. A. de S., Almeida, A. N. de, Braga, T. E. N., & Nunes, A. (2023). O tratamento de dados pessoais pelo poder público: um estudo bibliométrico. *Liinc Em Revista, 19*(2), e6455. https://doi.org/10.18617/liinc.v19i2.6455.

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

https://doi.org/10.1016/j.clsr.2024.106023
Received 9 July 2023; Received in revised form 25 March 2024; Accepted 12 July 2024

Data Protection Law (LGPD) provides for two central hypotheses: (i) execution of public policies; and (ii) execution of legal powers or legal attributions of the public service.[4]

Following this understanding, Neto, Ishikawa and Maciel[5] point out that the fundamental right to the protection of personal data is not an absolute right, and must be reconciled with the need to perform the functions of the Public Administration itself, which, in turn, will need to be exercised with full respect for the data subject. Therefore, the State's challenge is reconciling two perspectives that seem to point in opposite directions: on the one hand, the understanding that the broad processing of data by the Estate enables the construction of more efficient public policies, the offering of better public services and debureaucratization; on the other hand, the need to mitigate the risks for the data subject arising from this processing.[6]

Bellamy, Perry and Raab[7] point out that public managers face a great challenge in trying to balance the tension that reveals itself between the objectives of public services that require the processing of personal data and the protection of privacy. This conflict has been explored in the literature, highlighting the following points of criticality:

1) The trust of citizens in the State. Individuals tend to feel that their rights are being respected when the government values the trust of the data subject, which allows the development of a stronger personal data protection culture in the public sector[8];
2) The transparency of operations using personal data by the State. This factor contributes so that the individual can follow the administration of their data.[9] It should be ensured that the data collected, shared and used for the implementation of public policies have clear and transparent terms and conditions on the purposes of access, sharing, uses and accountability[10];
3) Information security. The lack of this factor implies deficiencies in the protection of personal data.[11] Although organizations adopt safeguards and mitigation measures through security policies and techniques, there are risks that someone will mishandle personal data or that cybercriminals threaten the protection of personal data[12];
4) The conformity of public institutions. The state must demonstrate leadership in the length of legislation.[13] However, studies indicate that, in several countries, the public sector is not adhering to the impositions of the legislation applicable to the processing of personal data;
5) The public interest motivating the processing of the data. Although this factor is the foundation for the processing of personal data by the public power,[14] it is necessary to observe the balance between the public interest in processing data and the fundamental rights and freedoms of an individual in the protection of the same data[15]; and
6) the right of access to public information. This factor imposes on the State a high degree of availability of information regarding its activities, however, the disclosure of this information must also observe the protection of personal data in order to preserve the intimacy, private life, honor and image of the individual.[16]

Thus, considering the general results presented in the literature, this study aims to analyze the critical points for the treatment of personal data by the government in the light of the perception of experts on the subject. Thus, it is intended to establish levels of criticality, hierarchizing the factors of tension for the Brazilian reality, and the results can be extrapolated, provided that the respective international contexts are observed and the due limitations are considered.

In view of the topicality of the matter, it is possible that the literature has not yet identified other potential points of tension. Therefore, research with experts will investigate the existence of other critical points on which the theory has not yet advanced.

It is noteworthy that in the bibliographic review were not found empirical studies produced in Brazil on the subject. From this research it was possible to add the view of public managers and scholars of the area to the concepts already established by the national and international literature, as well as to confirm or refute the theories employed. Therefore, the proposition of critical points not yet explored by the literature should enable the evaluation for an agenda of future research.

2. Methodology

The research adopted the qualitative approach, has an exploratory character and descriptive nature. For Cervo, Bervian and Silva,[17] exploratory research "performs precise descriptions of the situation and wants to discover the relationships between its component elements." In addition, according to the same authors, descriptive research observes, records, analyzes and correlates the facts, seeking to know the various situations and relationships that occur in the object of study.

In order to identify the critical points related to the processing of personal data by the government, a systematic review of the literature was carried out, which will be detailed in the Theoretical Reference section. To establish the levels of criticality, as well as to investigate the existence of other critical points on which the theory has not yet advanced, that is, the Analytical Framework, questionnaires were

[4] Wimmer, M. (2021). 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.

[5] Neto, A. B. S., Ishikawa, L., & Maciel, M. (2021). O tratamento de dados pessoais pelo poder público e o papel dos tribunais de contas. *Revista Direitos Culturais*, 16 (40), 163-177. https://doi.org/10.20912/rdc.v16i40.604.

[6] Wimmer, M. (2021). Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia. *Revista Brasileira de Políticas Públicas, 11*(1).

[7] Bellamy, C., Perri, S., & Raab, C. (2005). Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part II. *Public administration*, 83 (2), 393-415. https://doi.org/10.1111/j.0033-3298.2005.00455.x.

[8] Black, G., & Stevens, L. (2013). Enhancing data protection and data processing in the public sector: The critical role of proportionality and the public interest. *SCRIPT-ed*, 10 (1), 93-122. https://doi.org/10.2966/scrip.100113.93.

[9] Félix, V., & Monteiro, J. R. (2022). O uso de tecnologias e dados pessoais em políticas públicas de saúde no contexto da COVID-19. *civilistica.com*, 11 (1), 1-31.

[10] Almeida, B. A. *et al*. (2020). Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. *Ciência & Saúde Coletiva*, 25 (1), 2487-2492. https://doi.org/10.1590/1413-81232020256.1.11792020.

[11] Naarttijärvi, M. (2018). Balancing data protection and privacy – The case of information security sensor systems. *Computer law & security review*, 34 (5), 1019-1038. https://doi.org/10.1016/j.clsr.2018.04.006.

[12] Phillips, B. (2021). UK further education sector journey to compliance with the general data protection regulation and the data protection act 2018. *Computer law and security report*, 42, 105586. https://doi.org/10.1016/j.clsr.2021.105586.

[13] Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and informatics*, 34 (4), 157-170. https://doi.org/10.1016/j.tele.2017.01.008.

[14] Oliveira, A. C. S., & Araújo, D. S. (2020). O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da Lei Geral de Proteção de Dados. *Liinc em Revista*, 16 (2), e5318. https://doi.org/10.18617/liinc.v16i2.5318.

[15] Sarabdeen, J., Chikhaoui, E., & Ishak, M. M. M. (2022). Creating standards for Canadian health data protection during health emergency: An analysis of privacy regulations and laws. *Heliyon*, 8 (5), e09458. https://doi.org/10.1016/j.heliyon.2022.e09458.

[16] Wimmer (n 4).

[17] Cervo, A. L., Bervian, P. A., & Silva, R. (2007). *Metodologia científica*. 6. ed. São Paulo: Pearson Prentice Hall.

applied to specialists by the *Delphi* method.

According to Marconi and Lakatos,[18] the application of questionnaires has the advantage of not exposing the interviewee to the influence of the researcher, conferring greater freedom and security in the answers; the possibility that people will respond to it at the most convenient time for them; obtaining faster and more accurate answers; in addition to allowing more uniformity in the evaluation, due to the impersonal nature of the instrument.

2.1. Theoretical reference

The identification of the critical points for the processing of personal data by the government occurred from a systematic review of the literature, using the *Methodi Ordinatio*. According to Pagani, Kovaleski and Resende,[19] this method aims to search, select and examine scientific papers, based on the relevance of the studies and has as a criterion the topicality of the article (year of publication), the number of citations and its impact factor.

The searches were carried out in the Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) and in *Scopus*, since these databases bring together several other databases, expanding the result of the research. The keywords used in the search were: in Portuguese, "personal data", "Public Power", "State" and "Public Sector"; in English, "data protection" and "Public Sector". The Boolean operators "OR" and "AND" were used to relate the terms investigated.

After the application of the *Methodi Ordinatio*, 43 articles were selected to compose the portfolio, considering only free, complete articles in Portuguese, English or Spanish, peer-reviewed and published between the years 2005 and 2022. In addition, other relevant studies were identified in an unsystematic manner through the analysis of the references of the articles selected by the systematic review.

From the bibliographic portfolio, it is possible to identify the existence of six main critical points for the processing of personal data by the government, according to the references consulted and detailed in Table 1.

2.2. Delphi method

The *Delphi* method was used to apply the questionnaire. According to Freitas and Marques,[20] this technique consists of a set of questionnaires to be answered, sequentially and individually, with summarized information about the group's responses to the previous questionnaires, in order to establish a kind of dialog between the participants and, gradually, build a collective response.

Gupta and Clarke[21] point out that the method is advantageous in that it provides the capture of a large number of interrelated variables and multidimensional characteristics common to most complex problems, in addition to dealing with creative and open aspects of a problem, since it motivates independent thinking and the gradual formation of group solutions.

What sets the *Delphi* method apart from a regular survey is the feedback from the information gathered from the group and the opportunity for participants to modify or refine their judgments based on the group's responses. Thus, the technique tries to design a space in which individuals with experiences in different disciplines or specialties contribute information or judgments to a problem area, sharing knowledge with the group in the search for a consensus between the different opinions.[22]

For this work, fifteen specialists were invited to participate in the research. Considering the multidisciplinary character of the theme, the invited participants have complementary professional experiences – public managers, researchers and representatives of civil society – with diverse academic backgrounds – Law, Administration, Information Technology, among others.

The selection of the guests had as criteria the professional experience of at least two years of experience in the protection of personal data – for public managers and representatives of civil society – and a doctoral course completed or in progress – for the researchers. Only eleven of the invited experts agreed to participate in the research.

In the application of the questionnaires, the communication was written, by electronic means, carried out in two rounds for data collection. For Giovinazzo,[23] the application of two rounds is sufficient when the *Delphi* method is performed in electronic media, considering that additional steps could not arouse the interest of specialists.

Before submitting the forms, they were tested by an expert in order to verify the clarity of the questions. The suggestions received were incorporated into the questionnaire. For the elaboration and application of the electronic forms, the free application of search management *Google Forms* was used.

The initial questionnaire was semi-structured and divided into two parts. In the first, the six critical points for the treatment of personal data by the government identified in the literature review were presented, the experts were invited to judge the levels of criticality for each factor, by means of a semantic differential scale with ten points (from 1 – Not critical – to 10 – Extremely critical). In addition, participants were able to openly justify the answer offered in each factor. In the second part, the experts were asked to indicate one or more critical points that were not identified in the literature. The first form was applied for in November 2022 and is available in Appendix A.

After obtaining the answers in the first application of the questionnaire, the frequencies of the answers in the six critical points were calculated and their respective justifications analyzed and synthesized, generating the document for the feedback of the information. This document was made available along with the questionnaire in the second round of data collection.

For Freitas and Marques,[24] when using the *Delphi* technique in the construction of the questionnaires for the second round of application, it starts from the analysis of the responses of the group of experts to the first questionnaire, and it is extremely important that, in these questionnaires, there is a return of the previous information, analyzed and summarized, for the appreciation of the panel of experts.

The second questionnaire presented the individual position of each specialist along with the synthesis of the collective responses, facilitating the comparison between the individual position and that of the group. At this point, the participants were invited to reflect on their answers, being able to change or maintain their judgments regarding the level of criticality of each factor analyzed, reaching a definitive evaluation on each point. The second round of data collection took place three (3) months after the first round, in January 2023.

After the classification and organization of the information collected in the two rounds, the existing relationships between the data were

[18] Marconi, M. of A., & Lakatos, E. M. (2003). *Fundamentals of scientific methodology*. 5. ed. São Paulo: Atlas.

[19] Pagani, R. N., Kovaleski, J. L., & Resende, L. M. (2015). Methodi Ordinatio: a proposed methodology to select and rank relevant scientific papers encompassing the impact factor, number of citations, and year of publication. *Scientometrics*, 105 (40), 2109-2135. https://doi.org/10.1007/s11192-015-1744-x.

[20] Freitas, D., & Marques, J. B. V. (2018). Delphi Method: characterization and potentialities in research in Education. *Pro-Positions*, 29 (2), 389-415. https://doi.org/10.1590/1980-6248-2015-0140.

[21] Gupta, U. G., & Clarke, R. E. (1996). Theory and application of the Delphi technique: a bibliography (1975-1994). *Technological Forecasting and Social Change*, 53 (2), 185-211. https://doi.org/10.1016/S0040-1625(96)00094-7.

[22] Linstone, H. A., & Turoff, M. (1975). *Delphi Method: Techniques and Applications*. Boston: Addison-Wesley Educational.

[23] Giovinazzo, R. (2001). Modelo de aplicação da metodologia Delphi pela Internet: vantagens e ressalvas. *Administração online*, 2 (2), 1-11.

[24] Freitas and Marques (n 69).

established, such as points of divergence, convergence, trends, principles of causality and possibility of generalization, taking into account the relevance, relevance and authenticity of the information.[25]

3. Results and discussion

3.1. Criticality level

The results show that, in the view of the experts consulted, all the points of tension identified in the literature for the processing of personal data by the government have a high degree of criticality, considering that all of them reached an average value higher than 7 (seven) (Table 2).

The compliance of public institutions with the legislation on the subject was the element that reached the highest level of criticality, indicating the average value of 9.1 by the experts at the end of the second application of the questionnaire. In the perception of the experts, compliance with legislation related to the protection of personal data is fundamental and involves the adoption of protocols and internal governance instances capable of assigning responsibilities to implement control points and supervision of the processing of personal data in institutions. However, for the participants, compliance is still at an early stage in Brazilian public institutions. The research also pointed out the need for greater investments and training of public managers to foster compliance in data protection within the scope of public power.

The opinion of the experts about the compliance of public institutions in Brazil is in line with what was verified in the studies by Black and Stevens,[26] Blume[27] and Chua, Herbland, Wong and Chang[28] on the international scenario, which found that the public administrations of several countries are not in full compliance with the legislation on the protection of personal data.

An audit carried out by the UK Data Protection Authority demonstrated that public bodies often have poor compliance records, especially when compared to private sector organisations.[29] Similarly, in Denmark, the practice followed by public authorities is not in full compliance with the regulations on the subject.[30] A study conducted in Malaysia also found that "government organizations have lower compliance scores than non-governmental organizations".[31]

The second highest level of criticality was attributed to information security mechanisms and safeguards that guarantee the protection of personal data held by the State, which scored an average value of 8.8. The experts pointed out that information security is an essential element for the protection of personal data, and is directly related to the trust of the holders in the use of public services. Still, in the view of the participants, the cases of leaks of personal data in the possession of the State and security incidents contribute to the perception that public entities are inadequate with regard to information security standards.

The experts' assessment is in dialog with Pleger, Guirguis and Mertes,[32] according to which citizens sometimes have reservations about government efforts to provide electronic services, due to concerns about data protection and security. Added to this is the understanding of Sule, Zennato and Thomas,[33] which considers the cases of massive breaches of personal data capable of indirectly affecting the decisions of users of electronic services and trust in the digital ecosystem.

In some cases, data breaches are so significant that they gain coverage in the press. In the US, a growing wave of cyberattacks on government agencies and medical institutions leading the coronavirus pandemic response was reported by CNN in 2020.[34] In the same year, Australia faced widespread cyber attacks, covering all levels of government as well as essential services and businesses.[35] In Brazil, the scenario is no different. In December 2021, the press reported a security breach at the Ministry of Health that had allegedly exposed the personal data of more than 243 million Brazilians.[36]

Also under this aspect, it was highlighted that the protection of personal data, as well as the process of adaptation of the institutions to the legislation presupposes a broad and multidisciplinary approach, so as not to be limited exclusively to the adoption of information security measures.

The public interest, motivator of data processing, obtained the third highest level of criticality, with an average value of 8.6. For experts, this should be the primary foundation of any operation involving personal data by public entities. They corroborate this understanding Oliveira and Araújo,[37] when they affirm that the public interest should be the foundation of the public power for the processing of personal data.

The experts also stressed that the public interest is an indeterminate concept and that it must be justified in concrete, that is, with the definition of specific purposes for the processing of data. In this same line of understanding, Modesto and Ehrhardt Júnior[38] affirm that the limits to achieve balance in the processing of personal data for the benefit of the public interest must be built in the analysis of the concrete case.

For the participants, the public interest evidences the asymmetry in the relations between the citizen and the State. This perception is reinforced by the understanding that the State enjoys a prominent position in relation to the data subject, and that this asymmetry of powers is reflected in the prevalence of the public interest over the individual interest.[39]

Regarding this aspect, Wimmer[40] points out that several authors have discussed the challenges of balancing privacy and other opposing interests, considering the difficulty of quantifying a complex value such as privacy and an approach data protection as being individual, which places them in an unfavorable situation when faced with the public interest. In this scenario, it becomes hard to think about situations in which the right to privacy overrides the broader interests of society, such as the provision of health care, welfare benefits, housing services, or national security and surveillance.[41]

With regard to citizens' trust in the State for the processing of their personal data, the average criticality level attributed by the experts was 8.0. According to the participants, this attribute is essential to confer sustainability to the actions of the State, but the perception reveals a national scenario of mistrust. In this aspect, it was highlighted that trust stems from the transparency of how personal data is treated by the government, and that there is an increase in the level of criticality if there is a rise of authoritarian governments. Participants also linked trust as a natural consequence of compliance and information security.

It was also pointed out that distrust can lead to the boycott of the citizen when the State requires his personal data. In line with this

[25] Pádua, E. M. M. (2018). *Metodologia da pesquisa: abordagem teórico-prática*. São Paulo: Papirus.
[26] Black and Stevens (n 8).
[27] Blume (n 49).
[28] Chua, Herbland, Wong and Chang (n 13).
[29] Black and Stevens (n 8).
[30] Blume (n 49).
[31] Chua, Herbland, Wong and Chang (n 13).
[32] Pleger, Guirguis and Mertes (n 25).
[33] Sule, Zennato and Thomas (n 27).
[34] https://edition.cnn.com/2020/04/25/politics/us-china-cyberattacks-coronavirus-research/index.html.
[35] https://www.bbc.com/news/world-australia-46096768.
[36] https://saude.estadao.com.br/noticias/geral,nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes,70003536340.
[37] Oliveira and Araújo (n 14).
[38] Modesto and Ehrhardt Júnior (n 33).
[39] Bioni (n 3).
[40] Wimmer (n 4).
[41] Black and Stevens (n 8).

Table 1
Critical points in the processing of personal data identified in the literature.

Critical Point	References
Confidence	1,2,3,4,5,6,7,8
Transparency	9,10,11,12,13,14,15,16,17,18,19
Safety	20,21,22,23,24,25,26,27,28
Compliance	29,30,31,32,33
Public Interest	34,35,36,37,38,39,40,41,42,43,44,45,46
Access to Information	47,48,49

[1] Almeida *et al.* (n 10).
[2] Bellamy, Perri and Raab (n 7).
[3] Black and Stevens (n 8).
[4] Lubis, M., Kartiwi, M., & Zulhuda, S. (2018). Current state of personal data protection in electronic voting: Criteria and indicator for effective implementation. *TELKOMNIKA*, 16 (1), 290–301. http://doi.org/10.12928/telkomnika.v16i1.7718.
[5] Martins, H. *et al.* (2020). Tratamento de dados pessoais em aplicativos públicos relacionados ao coronavírus no Ceará. *Liinc em revista*, 16 (2), e5387. https://doi.org/10.18617/liinc.v16i2.5387.
[6] Pleger, L. E., Guirguis, K., & Mertes, A. (2021). Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security. *Computers in human behavior*, 122, 106,830. https://doi.org/10.1016/j.chb.2021.106830.
[7] Sarabdeen, Chikhaoui and Ishak (n 15).
[8] Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: Issues and trends. *Technology in society*, 67, 101,734. https://doi.org/10.1016/j.techsoc.2021.101734.
[9] Almeida *et al.* (n 10).
[10] Félix and Monteiro (n 9).
[11] Machado and Bioni (n 1).
[12] Maciel, M. (2020). 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*, 18 (1), 20–45. https://dialnet.unirioja.es/servlet/articulo?codigo=7671526.
[13] Martins et al. (n 24).
[14] Modesto, J. A., & Ehrhardt Junior, M. (2020). Danos colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pessoais no combate a COVID-19. *Revista Eletrônica Direito e Sociedade - REDES*, 8 (2), 1–19. https://doi.org/10.18316/REDES.v8i2.6770.
[15] Naarttijärvi (n 11).
[16] Neto, Ishikawa and Maciel (n 5).
[17] Palhares, G. C. *et al.* (2020). A privacidade em tempos de pandemia e a escada de monitoramento e rastreio. *Estudos Avançados*, 34 (99), 175–190. https://doi.org/10.1590/s0103-4014.2020.3499.011.
[18] Pleger, Guirguis and Mertes (n 25).
[19] Sule, Zennaro and Thomas (n 27).
[20] Black and Stevens (n 8).
[21] Flôres, M. R., & Silva, R. L. (2020). 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*, 12 (02), 01–34. https://doi.org/10.32361/2020120210327.
[22] Naarttijärvi (n 11).
[23] Oliveira and Araújo (n 14).
[24] Perri, S., Raab, C., & Bellamy, C. (2005). Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part I. *Public administration*, 83 (1), 111–133. https://doi.org/10.1111/j.0033-3298.2005.00440.x.
[25] Phillips (n 12).
[26] Pleger, Guirguis and Mertes (n 25).
[27] Sarabdeen, Chikhaoui and Ishak (n 15).
[28] Sule, Zennaro and Thomas (n 27).
[29] Black and Stevens (n 8).
[30] Blume, P. (2012). The inherent contradictions in data protection law. *International data privacy law*, 2 (1), 26–34. https://doi.org/10.1093/idpl/ipr020.
[31] Chua, Herbland, Wong and Chang (n 13).
[32] Correia, P. M. A. R., Jesus, I. O. A., & Pereira, S. P. M. (2019). O tratamento de dados pessoais na administração pública portuguesa: o caso de estudo da opacidade da autoridade tributária. *Lex Humana*, 11 (2), 128–142.
[33] Sarabdeen, Chikhaoui and Ishak (n 15).
[34] Almeida *et al.* (n 10).
[35] Bellamy, Perri and Raab (n 7).
[36] Black and Stevens (n 8).
[37] Comandè, G., & Schneider, G. (2022). Differential data protection regimes in data-driven research: Why the GDPR is more research-friendly than you think. *German law journal*, 23 (4), 559–*596*. https://doi.org/10.1017/glj.2022.30.
[38] Correia, Jesus and Pereira (n 51).
[39] Félix and Monteiro (n 9).
[40] Flôres and Silva (n 40).
[41] Maciel (n 31).
[42] Modesto and Ehrhardt Jr. (n 33).
[43] Neto, E. F., & Demoliner, K. S. (2018). Direito à privacidade e novas tecnologias: Breves considerações acerca da proteção de dados pessoais no Brasil e na Europa. *Revista internacional Consinter de direito*, 7 (7), 19–40. https://doi.org/10.19135/revista.consinter.0007.01.
[44] Oliveira and Araújo (n 14).
[45] Perri, Raab and Bellamy (n 43).
[46] Sarabdeen, Chikhaoui and Ishak (n 15).
[47] Félix and Monteiro (n 9).
[48] Flôres and Silva (n 40).
[49] Oliveira and Araújo (n 14).

Table 2
Average of criticality levels assigned by experts.

Critical Point	Average criticality level
Confidence	8
Transparency	8
Safety	8,8
Compliance	9,1
Public Interest	8,6
Access to Information	7,7

Table 3
Other critical points identified by experts.

Critical Point	Number of experts who mentioned the critical point	Distribution
Training of public agents	5	45 %
Data Sharing	4	36 %
Purpose of processing	2	18 %
Non-risk-based approach	2	18 %
Minimization of data collection	2	18 %
Ignorance of citizens	2	18 %
Accountability	2	18 %
Discrimination	1	9 %
Database governance	1	9 %
Deletion of personal data	1	9 %

understanding, Landwehr[42] highlights that users of public services must trust that their data is being used properly so that there is a willingness to provide it. An opposing idea about this opinion presented by the experts refers to the unbalance in the relationship between public and private, discussed above, since the relationship between citizens and State, unlike the relationship with private sector, is compulsory and is configured as a precondition for the exercise of citizenship.[43]

The degree of transparency of the information made available by the State regarding the processing of the citizen's personal data also reached an average criticality value of 8.0. In the view of experts, this point is essential to avoid abuses and misuse of personal data and its absence can generate lawsuits or challenge of public policies.

It was also reported the perception of lack of clarity in the use of the citizen's personal data by the public administration, as well as the need to organize the databases by secure means to comply with transparency and to develop mechanisms to inform how personal data are treated within the scope of the service provided to society.

Still on this aspect, it was pointed out that transparency is directly linked to citizen trust, corroborating the result observed in the literature review on the subject. For Martins et al.,[44] the more transparency, the more trust society has in information and, therefore, the greater the expected adherence to the measures implemented by the State.

The lowest mean criticality value (7.7) was attributed to challenges related to access to information. This point raises the need to reconcile the legislation guaranteeing the right to the provision of information relating to state activities with the right to the protection of personal data.

In this regard, it is observed the perception that entities have failed to meet requests for access to information based on the pertinent legislation for supposed prohibition of the LGPD in Brazil. However, in the view of experts, access to information, privacy and data protection are not concepts and norms incompatible with each other and can coexist harmoniously.

This perception finds support in the view of Wimmer,[45] because it is observed that the Brazilian laws of access to information and protection of personal data seek to materialize their guiding principles in order to build a narrative that makes it possible to combine transparency with data protection, despite adopting different logics.

3.2. Critical points not addressed in the researched literature

In addition to the six critical points for the processing of personal data by the government identified in the literature review, the experts were invited to contribute up to three other factors that, in their view, could be considered, in equal measure, points of tension. In this part of the questionnaire, twenty-nine answers were obtained, seven of which were eliminated because they were already related to the critical points identified in the literature review or because of difficulty in understanding the point addressed by the participant. After analysis and consolidation, ten other critical points identified by the experts were obtained (Table 3).

The lack of awareness and training of public agents was identified as a critical point by 45 % of the experts, who highlighted that the lack of qualified staff in the area of personal data protection has direct implications for the process of compliance of institutions with the legislation on the subject in Brazil.

In this aspect, the data presented in an audit conducted by the Federal Audit Court (TCU) that sought to evaluate government actions to comply with personal data protection legislation corroborate the perception of experts. According to TCU[46]:

> In relation to "Training", the answers show that the minority of organizations, 29 %, have a Training Plan that covers the protection of personal data, which represents an organizational risk, since the LGPD is a technical and difficult to understand legislation, which requires study for organizations to acquire maturity in the subject. In addition, the survey showed that nearly half of the organizations that drafted the plan, 46 percent, did not consider the need for people

[42] Landwehr, C. (2019). 2018: A big year for privacy. *Communications of the ACM*, 62 (2), 20-22. https://doi.org/10.1145/3300224.
[43] Wimmer (n 4).
[44] Martins *et al.* (n 24).
[45] Wimmer (n 4).
[46] TCU. (2022) *Acórdão nº 1384/2022*, TCU/Plenário, 21 jun. 2022. https://bit.ly/3MyEYFv.

performing functions with essential responsibilities related to the protection of personal data to receive differentiated training.

The sharing of personal data by the government was mentioned by 36 % of the experts. According to Perry, Raab and Bellamy,[47] data sharing encompasses the disclosure of personal data between institutions and includes the transfer of complete databases as well as information from individual records. For the authors, data sharing is also used to support various functions of the state, including the planning and evaluation of public policies, the allocation of resources, and the application of sanctions or other controls.

The literature shows that sharing practices are becoming increasingly common in public administration. Choroszewicz and Mäihäniemi[48] pointed out that, currently, there is pressure coming from within public administrations to facilitate the sharing and combination of data sets between different authorities, as well as to allow a more comprehensive use of the data.

In Brazil, the intention to reduce bureaucracy, to combat fraud, and to improve the quality and effectiveness of public policies, based on evidence and concrete indicators, has driven the sharing of databases in public administration.[49]

For Félix and Monteiro,[50] the sharing of data can imply risks for the holders due to the information extracted from them. The authors understand that, in order to reduce such risks, it is necessary to plan public policies, in addition to the application of data protection measures.

Another result observed was the relationship between the sharing of data with the purpose that motivated its obtainment. According to Neto, Ishikawa and Maciel[51] "any sharing carried out by the public administration, in the exercise of its functions, should take place, exclusively, for the specific purpose of executing public policies." The use of personal data for purposes other than those that motivated its original collection was pointed out as a critical factor by 18 % of the experts.

Two experts highlighted the presence of a non-risk-based approach by the government. The LGPD, in several articles of its text, refers to the risk and the need to evaluate its possible effects on personal data processing operations, in order to assess its impact with regard to the individual rights and freedoms of data subjects.[52] However, experts point out that public agents, as a rule, are not prepared to perform risk analyses, which can be an obstacle in the adequacy of procedures to comply with the Law, such as the preparation of impact reports on the protection of personal data.

The minimization of the collection or collection of personal data was also identified by two experts consulted (18 %). According to the perception of the participants, this point is related to the principle of necessity, according to which the Public Administration should use only the data strictly necessary for the development of the activity for the benefit of the public interest. Thus, non-compliance with the concept of minimization can lead to excessive treatment of personal data, sometimes unnecessary to meet the purpose that motivated the collection.

The lack of knowledge of citizens on the subject was also the subject of two responses (18 %). This position is supported by the studies of Christo,[53] according to which the majority of the population is unaware of their rights regarding privacy and the protection of personal data. Christo[54] understands that the State should carry out public education campaigns on the subject, which enable individuals to be more empowered about their rights and responsibilities, as well as greater knowledge about the consequences of their actions.

Accountability for how the government treats personal data is also a point of tension, as pointed out by two experts. Corroborate with this understanding Modesto and Ehrhardt Junior,[55] according to the authors the rendering of accounts occurs with the demonstration, by the agent responsible for the treatment, of the adoption of effective measures and capable of proving the observance and compliance with the rules of protection of personal data and, include the measures for prevention and protection of the rights guaranteed in them.

The principle of non-discrimination was identified as a critical point by one participant. It is important to note that the LGPD prohibits the performance of treatment for discriminatory, illicit or abusive purposes. However, according to Matiuzzo, Schertel and Fujimoto,[56] the increasing use of algorithms and recent developments in computer science in the field of Artificial Intelligence (AI) present challenges to this principle:

> […] With regard to algorithmic discrimination, it is necessary to recognize that, first, this tool is already a reality, its use expands every day, and, therefore, it would be unreasonable and productive to think about eliminating the use of automated systems. Secondly, it is noteworthy that these systems can be extremely efficient, bringing numerous benefits, if used in a structured way and based on minimum legal parameters. Thus, efforts should be focused on developing mechanisms that guarantee safety and a degree of control of the results obtained through automation, mitigating the risks of discrimination inherent to the statistical technique employed.

Deletion, one of the types of processing of personal data, has also been identified as a point of tension by an expert. The LGPD defines elimination as "the deletion of data or set of data stored in a database, regardless of the procedure employed and determines that, within the scope and technical limits of the activities, personal data will be eliminated after the end of its treatment".[57] Under this perspective, international experience reveals that the administrative tradition is the maintenance of data, making exclusion an exception, even if the legislation imposes the opposite.[58]

Finally, the governance of databases and personal databases was another critical point raised by one of the experts. Almeida et al.[59] highlighted the importance of this aspect, according to the authors, when considering that data can be used and shared by different organizations simultaneously, responsible data governance based on transparency is one of the main issues to be harmonized so that there is trust and balanced and fair relationships between individuals and organizations.

4. Final considerations

Through a systematic review of the literature and research with specialists, this work sought to establish the levels of criticality of the stress factors for the treatment of personal data by the public power for the Brazilian reality. The present study also aimed to investigate the

[47] Perry, Raab and Bellamy (n 43).

[48] Choroszewicz, M., & Mäihäniemi, B. (2020). Developing a digital welfare state: Data protection and the use of automated decision-making in the public sector across six EU countries. *Global Perspectives*, 1 (1), 12910. https://doi.org/10.1525/gp.2020.12910.

[49] Wimmer (n 4).

[50] Félix and Monteiro (n 9).

[51] Neto, Ishikawa and Maciel (n 5).

[52] Gomes, M. C. O. (2020). *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.

[53] Christo, E. D. (2013). Data protection in Trinidad and Tobago. *International data privacy law*, 3 (3), 202-209. https://doi.org/10.1093/idpl/ipt013.

[54] ibid 202-209.

[55] Modesto and Ehrhardt Junior (n 33).

[56] Matiuzzo, M., & Schertel, L. (2021). *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.

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

[58] Blume (n 49).

[59] Almeida *et al.* (n 10).

existence of other critical points on which the theory has not yet advanced.

The results demonstrate that the conformity of public institutions is the most critical element. In the perception of the experts, this attribute is still in the initial stage of implementation in Brazilian public institutions and involves the adoption of protocols and internal governance instances with responsibilities to implement control points and supervision of the processing of personal data.

Next, we found the information security mechanisms, which were considered by experts as an essential, although not exclusive, element for the protection of personal data, and are directly related to the trust of citizens.

In the third position, the public interest motivating the processing of the data was identified, being considered by the specialists the most important foundation of any operation involving personal data by the public power.

Subsequently, the trust of citizens in the State for the treatment of their personal data and the degree of transparency of the information made available obtained the same level of criticality. Finally, the challenges related to access to information were listed to the last degree of criticality.

In view of what was presented, it was verified that it is possible to confirm and complement, based on the perspective of the participants, the results obtained in the bibliometric research and in the literature review on the subject. It was also observed that none of the six stress factors identified in the systematic review of the literature presented a criticality level lower than 7 (seven), inferring from this result that, according to the perception of the experts consulted, all the aspects listed have a high degree of criticality in the Brazilian scenario. Thus, it can be concluded that the processing of personal data by the government has challenges similar to those faced in other countries and requires improvement to ensure full compliance with the legislation.

In addition, the experts were able to identify ten other critical points for the processing of personal data that are not explored by the literature, they were: 1) the training of public agents; 2) the sharing of personal data held by the government; 3) purpose of the treatment; 4) non-risk-based approach; 5) minimization of data collection; 6) ignorance of citizens; 7) accountability; 8) discrimination; 9) database governance; and 10) deletion of personal data collected.

The significant number of points of tension addressed by the experts demonstrated that, in Brazil, the processing of personal data by the public authorities still presents several challenges not explored by the national and international literature on the subject.

A limitation to the development of this study was the absence of previous studies that explored research with specialists. Thus, it was only possible to analyze and compare the results against the theory investigated, and its comparison with other similar studies was not feasible. Thus, the other points of tension addressed by the experts have the potential to support an agenda of future research that allows to explore in greater depth the theoretical framework of each factor, as well as its implications for the treatment of personal data by the government.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.clsr.2024.106023.