Digital government and the handling of sensitive data in the execution of public policies: challenges and possibilities[1]

Gobierno digital y el manejo de datos sensibles en la ejecución de políticas públicas: desafíos y posibilidades

Júlia Oselame Graf[2]
University of Santa Cruz do Sul (Brasil)
ORCID: https://orcid.org/0000-0002-2662-6963

Caroline Müller Bitencourt[3]
University of Santa Cruz do Sul (Brasil)
ORCID: https://orcid.org/0000-0001-5911-8001

Recibido: 28-10-2023
Aceptado: 12-04-2024

Abstract

The research aims to investigate the characteristics and risks associated with the handling of sensitive data in the implementation of public policies within the digital government model. To achieve this, a hypothetical-deductive method and bibliographic and documentary procedures are employed, proposing an interdisciplinary discussion on technological advancement, data protection, transparency, and public policies. The justification revolves around the importance of a comprehensive, cohesive system that genuinely protects

[1] We thank Laura Hernández for her research assistance and two anonymous reviewers for their insightful comments.

[2] (juliagrafadv@gmail.com). Ph.D. student in Law at the University of Santa Cruz do Sul - UNISC. PROSUC/CAPES Fellowship, Modality II. Master of Law and Social Justice from the Federal University of Rio Grande - FURG. Bachelor of Law from the Federal University of Rio Grande - FURG with a sandwich period at the Faculty of Law at the University of Porto, Portugal. Currently pursuing a degree in Digital Marketing and Data Science. Lawyer.

[3] (carolinemb@unisc.br). Ph.D. in Law from the University of Santa Cruz do Sul. Post-doctorate from PUC/PR. Specialization in Public Law. Tenured Professor at the Graduate Program in Law - Master's and Doctorate - UNISC. Head of the Department of Law at the University of Santa Cruz do Sul. Member of the Euro-Latin American Faculty Network of Administrative Law. Member of the Social Administrative Law Network. Coordinator of the research group on social and administrative control of public policies and public service. Member of the Human Development Research Group at PUC/PR. Lawyer.

sensitive personal data, considering the need to keep pace with technological developments and maintain a minimum level of security in the digital age at both national and international levels. There is no doubt that the judicious and strategic use of data has the potential to drive substantial improvements in policy evaluation, decision-making, and the relationship between government and citizens. However, dealing with personal data also means addressing risks with responsibility, transparency, and respect for individual rights.

Keywords: Digital Government; Public Policies; Data Protection; Big Data; Artificial Intelligence.

Resumen

La investigación tiene como objetivo investigar las características y riesgos asociados con el tratamiento de datos sensibles en la ejecución de políticas públicas dentro del modelo de gobierno digital. Para lograrlo, se utiliza un método hipotético-deductivo y procedimientos bibliográficos y documentales, proponiendo una discusión interdisciplinaria sobre el avance tecnológico, la protección de datos, la transparencia y las políticas públicas. La justificación se centra en la importancia de un sistema completo y cohesivo que realmente proteja los datos personales sensibles, considerando la necesidad de mantenerse al día con el desarrollo tecnológico y mantener un nivel mínimo de seguridad en la era digital a nivel nacional e internacional. No hay duda de que el uso juicioso y estratégico de los datos tiene el potencial de impulsar mejoras sustanciales en la evaluación de las políticas públicas, la toma de decisiones y la relación entre el gobierno y los ciudadanos. Sin embargo, manejar datos personales también implica abordar los riesgos con responsabilidad, transparencia y respeto a los derechos individuales.

Palabras-clave: Gobierno Digital; Políticas Públicas; Protección de Datos; Big Data; Inteligencia Artificial.

1. Introduction

The significance of a comprehensive and cohesive system that genuinely protects sensitive personal data is fundamental to keeping pace with technological advancements and maintaining a minimum level of security in the digital age at both national and international levels. This is because everyone is entangled in this endless technological web, which still presents many unresolved gaps, even for experts in information systems, software engineers, and other professionals in the field.

The research question guiding this specific inquiry is: “What have been the characteristics and risks associated with the handling of sensitive data in the implementation of public policies within the digital government model?”

Structured in two parts, the present study aims to contextualize the Brazilian situation and investigate the characteristics and risks associated with the handling of sensitive data in the execution of public policies within the framework of digital government. It is essential to ensure the proper operation of the public management system to guarantee unrestricted technological progress, assuming that users can trust that the generated information will not be manipulated or used for different purposes.

To achieve this, the first chapter of the development, titled “Data Protection as a Fundamental Right: the Duty of Transparency in the Face of Technological Advancement,” will seek to reflect on the duty of protecting fundamental rights by the State with a focus on data protection.

The second chapter, titled “Public Management and the Handling of Sensitive Data: Risks and Potentialities Using Digital Technologies, Big Data, and AI,” will build upon the insights from the previous chapter. It will delve into concepts related to sensitive data and discuss issues concerning artificial intelligence, big data, and the handling of data by public administration in the execution of public policies.

In light of this, through the hypothetical-deductive method and bibliographic and documentary procedures, we propose an interdisciplinary discussion on technological advancement, data protection, transparency, and public policies. As hypotheses, it is possible to point out the following: (i) Technological advancement and the increased collection and use of sensitive data in public policies may increase the risks of privacy and security violations. (ii) The enforcement of the General Data Protection Law may have positively influenced awareness regarding the importance of protecting sensitive data but may not have been sufficient to ensure effective external control over the handling of such data. (iii) Data interoperability may assist in the evaluation of public policies.

Thus, technological advancement and widespread access to individuals’ information and data are prominent features of the digital space. Consequently, the issue of how to protect this data becomes a common concern in Brazil and worldwide. Although it is not yet possible to measure the extent of certain information, there is a recognized need for legal regulation and response. Faced with an abundance of information and accessibility, the law seeks to establish a minimum level of reasonableness in the handling and disclosure of specific information.

2. Data Protection as a Fundamental Right: The Duty of Transparency in the Face of Technological Advancement

Understanding the normative and philosophical perspectives that reinforce the importance of a comprehensive, coherent system that genuinely protects sensitive personal data is crucial to keep pace with technological development and maintain a minimum level of security in the digital age at both national and international levels[4]. This is because everyone is entangled in this endless technological web, which presents many unexplained gaps, even for prominent experts in information systems, software engineers, and other professionals in the field. In this regard, Ingo Sarlet (2021) emphasizes the importance of law in regulating and effectively protecting the affected fundamental rights.

> Therefore, the Law, as an organizational and regulatory normative structure of these spheres and their respective relationships, could not avoid being summoned to deal with the phenomenon. However, its dynamism and complexity increasingly challenge the capacity of conventional legal systems (here understood broadly, both internationally and nationally) to achieve satisfactory outcomes, particularly when it comes to ensuring a minimum level of effective protection for the affected human and fundamental rights (Sarlet 2021: 57).

The concern guides the field of law because when we speak of technological innovation, we are talking about evolution beyond the scope of law. There is a race underway, and the law tirelessly seeks to adapt to reality - the abstract is no longer sufficient. The digital realm is already unfolding. In this sense, it is noted that there is a noticeable gap; however, this gap cannot signify an open path for the commission of illegalities and violations of fundamental rights.[5]

[4] For complementary purposes, it is noteworthy that "with regard to Brazil, it is imperative to mention, in this context, the relevance of the GDPR for the development of the LGPD, which incorporated a series of institutes, principles, and rules from the European norm. Furthermore, even though Brazil is not bound by European law in general, not even with respect to human and fundamental rights, for the purpose of data transfer, Brazil must comply with the parameters of European regulations, which in itself, given the impact on trade relations between European countries and ours, implies a certain (in the relevant aspect) regulatory framework symmetry" (Sarlet 2021: 64).

[5] Hoffmann-Riem observes that "digital transformation has increased the complexity of the regulatory field. [...] In addition to relatively simple algorithms, algorithmic systems with learning capabilities, and their respective use for various purposes, are becoming increasingly widespread. Associated with this is the increasing complexity of dealing with algorithms and the tasks to be performed, as well as the information necessary for such operations, especially processing operations. The emergence of new information technologies and potential uses, including systems that have now become everyday objects (smartphones, tablets, search systems, databases, robots, blockchain, etc.), increases the complexity of dealing with the possibilities of digital transformation. This complexity is also increasing due to the growing network of different systems and their hardware and software components, not only with the increasing issues related to the global network and, therefore, data processing in remote regions and in different clouds. In addition, the speed of computation is increasing. [...] Complexity also increases with the number and diversity of actors involved. This makes it more challenging to assign responsibilities and, for example, enforce obligations. In case of

Tércio Sampaio Ferraz Júnior points out that “the inviolability of data confidentiality (Article 5, XII) is correlated with the fundamental right to privacy (Article 5, X)” (Ferraz Júnior 1993: 440) and emphasizes that an individual has the right to “exclude from the knowledge of third parties what is only pertinent to him and concerns his unique way of being in the context of his private life” (Ferraz Júnior 1993: 440).

Furthermore, there is a strong argument that data protection is a fundamental right independent of privacy. In this regard, Lynskey points out:

> […] the link between the rights to data protection and privacy can be broadly conceptualized in three ways: (i) data protection and privacy are separate but complementary rights; (ii) data protection is a subset of the right to privacy; and (iii) data protection is an independent right which serves a multitude of functions including, but not limited to, the protection of privacy (Lynskey 2015: 90).

Stefano Rodotà works with what he calls the “third paradox of privacy,” in which he discusses four trends: “(i.) from the right to be left alone to the right to maintain control over information that concerns me; (ii.) from privacy to the right to informational self-determination; (iii.) from privacy to non-discrimination; and (iv.) from confidentiality to control” (Rodotà 2008: 97-98).

> [...] The classification of these data in the category of “sensitive” data, particularly protected against the risks of circulation, stems from their potential inclination to be used for discriminatory purposes. To ensure the fullness of the public sphere, stringent conditions for the circulation of this information are determined, and they receive a strong “private” status, mainly expressed through the prohibition of their collection by certain entities (e.g., employers) and the exclusion of legitimacy for certain forms of collection and circulation. This can be referred to as the “second paradox of privacy” (Rodotà 2008: 96).

In the same vein, Caitlin Mulhollan suggests that “if traditionally the right to privacy is associated with the right to be left alone, contemporarily it can be argued that privacy has evolved to include in its content the protection of sensitive data and their control by the data subject” (Mulhollan 2018: 172).

In the context of public policies, transparency presents itself as a challenge that needs to be addressed. There is a need for the disclosure of procedures, policies, and practices involving the collection, processing, and use of citizens’ data. Eduardo Schiefler et al. argue that within the technological context, particularly driven by rapid transformations and the imperative to protect

functional failure of institutions or infrastructures, it is also not easy to determine whether the cause was hardware, software, the type of service, or the information entered for processing.” (Hoffmann-Riem 2022: 59-60).

fundamental rights, the debate intensifies around the concept of digital public administration. This concept, achieved through the use of the latest information and communication technologies and the operation of electronic administrative processes, aims to enhance efficiency, transparency, social participation, control, bureaucracy simplification, agility, equality, and equal treatment in the provision of public services (Schiefler; Cristóvam; Sousa 2020: 100).

In Brazil, despite the delayed development of a law focused on the regulation of personal data processing, the significance of Law 13.709/2018 is emphasized. It represents a normative milestone to be observed and improved, especially in a surveillance society characterized by hyperexposure and indiscriminate data usage. In this context, Zygmunt Bauman highlights the state of surveillance experienced:

> “Liquid surveillance” is less a complete way of specifying surveillance and more a guiding principle, a way to situate changes in this area in the fluid and disruptive modernity of today. Surveillance particularly softens in the realm of consumption. Old constraints loosen as fragments of personal data obtained for one purpose are easily repurposed for another. Surveillance spreads in previously unimaginable ways, reacting to and reproducing liquidity. Without a fixed container but driven by the demands of “security” and influenced by the relentless marketing of technology companies, security spreads everywhere (Bauman 2013: 7).

Leal and Maas address significant issues regarding the connection between the State, particularly its duty of protection, and individuals, whose relationship extends beyond the subjective dimension of rights into the objective dimension. This means that there is “the idea that the State has a duty to protect fundamental rights, and it is the State’s responsibility to protect them even when it is not directly involved in that relationship” (Leal; Maas 2020: 49).

Based on this, two concepts are put forth to prevent indiscriminate state action, namely: (i.) prohibition of insufficient protection (Untermaβverbot); and (ii.) prohibition of excess (Übermaβverbot). These concepts are therefore “conceived as parameters of the effectiveness of fundamental rights and are closely connected to the principle of proportionality” (Leal; Maas 2020: 50).

Furthermore, it is worth noting the existence of a constitutional provision that elevates the protection of personal data as a fundamental right, especially in Article 5, LXXIX, where it is stated that “the right to the protection of personal data, including in digital media, is guaranteed, pursuant to the law” (Brazil, 1988). However, in practice, there is a slow progression of the law in the realm of electronic processes, which is far from attempting to promote and materialize an effective public policy for data protection.

Indeed, considering the use of technology to anticipate potential societal issues is an important pillar for the desired outcome, particularly the protection and realization of fundamental rights. Thus, problems such as the lack of transparency regarding which data is being processed in the implementation of public policies appear contradictory.

> The specific problems of successful regulation and ensuring its success arise from the limited transparency, or rather, the lack of transparency, in many approaches to the use of algorithmic systems. This has consequences, especially concerning responsibility and the possibility of controlling and reviewing risks (Hoffmann-Riem 2022: 61-62).

Regarding this issue, Hoffmann-Riem (2022) emphasizes that the procedures used and the results obtained are only accessible to the affected individuals or the public in a limited way. This is where a concern arises about the handling of data in the implementation of public policies. There are currently no clear answers on how external oversight will work, either to discover which data is being processed or to determine responsibility for any data leaks or misuse.

3. Public Management and the Handling of Sensitive Data: Risks and Opportunities Using Digital Technologies, Big Data, and AI

In the previous chapter, it was possible to understand the concept of data protection as a fundamental right and the duty of the State to protect fundamental rights. Building on that foundation, we will now analyze the challenges and potentialities that guide data processing in the execution of public policies. These include (i.) sensitive data, (ii.) Big Data, and (iii.) artificial intelligence, as well as aspects related to technological development.

Ruíz and Becerra (2022) point out that artificial intelligence is increasingly being recognized as a crucial tool for shaping public policies, as highlighted by the OECD in its principles. By adopting transparency and explainability as guidelines, AI can not only predict and recommend but also make decisions. This recognition of AI as a vital component for effective policies is reinforced by its combination with transparency laws and public education about its use. However, the development and implementation of AI also raise important issues regarding regulation, data protection, and ethical use, highlighting the need for a solid legal framework to ensure that these technologies benefit society without compromising fundamental rights. In this context, while AI can be seen as an ally of the state in improving public management processes, its use requires a careful balance between innovation and regulation to mitigate potential risks and ensure its effectiveness.

The debate about data protection in the context of public policy implementation is essential since it involves a fundamental right that requires care and attention from policymakers. In this context, it is crucial to question the limits of data processing and sharing, even when it comes to public policies. This is where the need arises to develop guidelines that facilitate external control of this information, ensuring a minimum level of security for citizens without hindering technological progress.[6]

Therefore, it is necessary to address concepts related to big data, artificial intelligence, and transparency applied to the current context in Brazil concerning data protection. Wolfgang Hoffmann-Riem (2022) highlights that the term "Big Data" refers to situations in which digital technologies are used to handle large and diverse quantities of data:

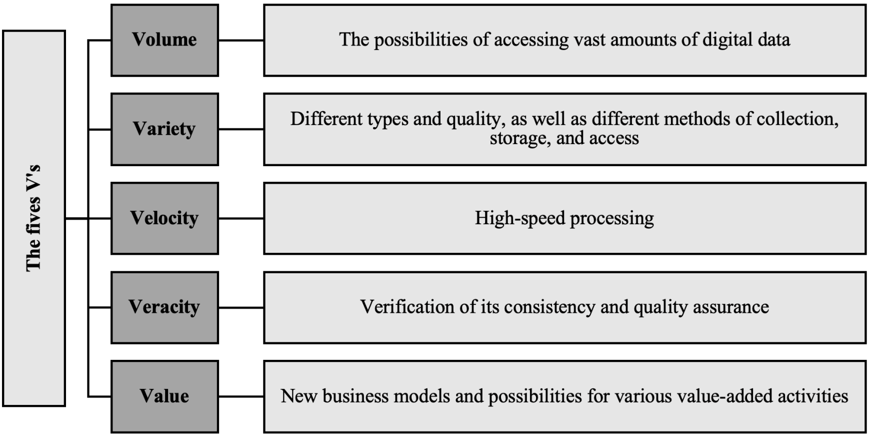
> The term "Big Data" refers to situations in which digital technologies are used to handle large and diverse quantities of data, as well as the various possibilities of combining, evaluating, and processing this data by both private and public authorities in different contexts (Hoffmann-Riem 2022: 19).

The internet has made searching and, consequently, tracking much easier and widely accessible worldwide. You don't have to look far to realize that we are immersed in this type of monitoring system. Google knows everything we search for, Facebook and other social networks identify our bubbles and personal preferences. Mobile phone providers know who we talk to, our location, and our neighbors' locations. Healthcare systems know how many times we use public healthcare services or how many times we test positive for Covid-19, and so on. This means that nothing we are discussing is new, but concerns arising from the use of this type of data are beginning to gain much more prominence with data sharing and artificial intelligence[7], the risks and potentialities of which have not yet been fully measured.

[6] Furthermore, Tavares and Bitencourt point out that "the promotion of innovation in the exercise of social control over Public Administration should be encouraged. Through innovation labs, whose legal basis lies in the Digital Government Law, as well as other open and shared spaces for creation and innovation, there is a latent potential to be explored through the use of intelligent technologies, including artificial intelligence, data science, and big open data, for the conduct of social audits." (Tavares; Bitencourt 2022: 164-165).

[7] Hoffmann-Riem points out that "currently, the computing and analytical capabilities of computers are being expanded, and the possibilities for the application and performance of algorithms are growing and changing rapidly. Artificial intelligence is particularly important for this. This term specifically refers to the effort to digitally replicate decision structures similar to human ones, i.e., to design a computer in such a way and, in particular, to program it using so-called neural networks in such a way that it can process problems as independently as possible and, if necessary, further develop the programs used." (Hoffmann-Riem 2022: 17).

Graph 1 - Characteristics for Identifying Big Data


The fives V's
Volume
The possibilities of accessing vast amounts of digital data
Variety
Different types and quality, as well as different methods of collection, storage, and access
Velocity
High-speed processing
Veracity
Verification of its consistency and quality assurance
Value
New business models and possibilities for various value-added activities

Source: Compiled by the authors based on the concepts of Wolfgang Hoffmann-Riem, 2022.

For Viktor Mayer-Schonberger et al. (2013: 138), when handled responsibly, big data is a useful tool for rational decision-making. Used recklessly, it can become an instrument of the powerful, who can turn it into a source of repression, either simply frustrating customers and employees or, worse, harming citizens. Moreover, they emphasize that the risks are higher than are generally recognized. The dangers of not governing big data regarding privacy and prediction, or being misled about the meaning of the data, go far beyond trivialities like targeted online advertising.

Additionally, Big Data Analytics is highlighted as "of particular importance for data evaluation and expanding data usage possibilities, especially with the help of artificial intelligence" (Hoffmann-Riem 2022: 20)[8]. According to the author, different analytical procedures are used for different purposes, including: (i.) descriptive analysis; (ii.) predictive analysis; and (iii.) prescriptive analysis.

[8] Vanice do Valle points out that "misunderstanding actually arises from a certain fascination with an idea of absolute objectivity that the so-called 'exact' fields seem to offer. In the era of AI, the combination of sophisticated technology with big data - an aggregated mass of information and potentially rich learning - appears to fulfill the promise of unveiling the hidden, a revelation that can only be achieved with an objective detachment that only the machine could ensure. However, despite the deceptive nature of the term itself ('exact sciences'), even in this field, the purity of objectivity is not guaranteed. In the field of artificial intelligence, contamination can occur in relation to the data itself from which it starts or even from the different perspectives from which they are treated in the commands translated into algorithms" (Valle 2020: 190).

Table I - Big Data Analytics - Characteristics of Analytical Procedures

Descriptive Analysis	Predictive Analysis	Prescriptive Analysis
It is used to sift and prepare the material for evaluation purposes. An example field is the use of Big Data for Data Mining and data recording and systematization.	It aims to identify indicators for a possible causal relationship - although largely disconnected from a process of understanding - but in the form of statistically significant correlations, on this basis, events should be predicted with a certain probability.	It aims at recommendations for action, in order to use descriptive and predictive knowledge to achieve specific objectives, such as personalized pricing selection or strategies and tactics to influence attitudes and behaviors.

Source: Compiled by the authors based on the concepts of Wolfgang Hoffmann-Riem, 2022.

The General Data Protection Law (LGPD) considers sensitive data to be any "personal data on racial or ethnic origin, religious belief, political opinion, union membership, or religious, philosophical, or political organization affiliation, data related to health or sexual life, genetic or biometric data when linked to a natural person" (Brazil, 2018).

Despite concerns about the use of such data, Article 11[9] of the same law provides that the processing of sensitive personal data may occur, even without the consent of the data subject, in cases where it is essential for the shared processing of data necessary for the execution, by the public administration, of public policies provided for in laws or regulations.

Moreover, Article 3 of Law No. 14.129/2021 lists some principles and guidelines for Digital Government and public efficiency, among them, interoperability of systems and the promotion of open data are highlighted in Article XIV. Therefore, there is a concern to promote a desirable integration of data, as emphasized by Vanice do Valle and Fabrício Motta:

[9] Article 11. The processing of sensitive personal data may only occur in the following cases: I - when the data subject or their legal representative consents, in a specific and prominent manner, for specific purposes; II - without the consent of the data subject, in cases where it is indispensable for: a) compliance with a legal or regulatory obligation by the data controller; b) shared processing of data necessary for the execution of public policies envisaged by laws or regulations by the public administration; c) conducting research by a research organization, with the anonymization of sensitive personal data whenever possible; d) the regular exercise of rights, including in contracts and in judicial, administrative, and arbitral proceedings, the latter in accordance with Law No. 9,307 of September 23, 1996 (Arbitration Law); e) the protection of the life or physical integrity of the data subject or a third party; f) the protection of health, exclusively, in procedures carried out by healthcare professionals, healthcare services, or health authorities; or g) ensuring fraud prevention and the security of the data subject in the processes of identification and authentication of registration in electronic systems, subject to the rights mentioned in Article 9 of this Law, except in cases where fundamental rights and freedoms of the data subject requiring the protection of personal data prevail (Brazil, 2018).

> A second component revealing an expanded view of what a digital government should be in a federative republic with the extent and complexity that is characteristic of ours is the adoption of concepts such as interoperability of systems (Article 3, XIV); a national database of public services (Article 4, III); and government as a platform (Article 4, VII). The commands mentioned here demonstrate a concern to promote a desirable integration not only of data in the strict sense, available to each administrative structure, but also of inputs that may result directly or indirectly from the demands brought by users of public services or even by the general public in relation to administrative action (Valle; Motta 2022: 47).

When it comes to technological advancement, personal data, and privacy, we are dealing with something that is already part of our daily lives, as people relinquish their privacy every day when they use the internet and input various pieces of information that are automatically collected. However, when it comes to data processing for the execution of public policies, it is noted that these are data that do not even require the consent of the data subject. Therefore, guidelines need to be implemented.

There is no doubt that the careful and strategic use of data has the potential to drive substantial improvements in the evaluation of public policies, decision-making, and the relationship between the government and citizens. However, dealing with personal data also means addressing the risks with responsibility, transparency, and respect for individual rights.

Data protection in the context of artificial intelligence (AI) is crucial given the digital and automated environment in which everyone is immersed. AI, with its high capacity to analyze large volumes of data and the potential to make decisions based on the collected data, brings forth various concerns regarding the privacy and security of sensitive personal data.

Article 5 of the General Data Protection Law provides some important definitions that will guide the dynamics of data protection, including: (i.) personal data: information related to an identified or identifiable natural person; (ii.) sensitive personal data: personal data about racial or ethnic origin, religious belief, political opinion, membership in a union or religious, philosophical, or political organization, data related to health or sexual life, genetic or biometric data, when linked to a natural person; (iii.) processing: any operation performed with personal data, including collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, deletion, evaluation, or control of information, modification, communication, transfer, dissemination, or extraction; (iv.) consent: a free, informed, and unequivocal expression by which the data subject agrees to the processing of their personal data for a specific purpose (Brazil, 2018).

Furthermore, two principles of personal data processing should be emphasized: (i.) security: the use of technical and administrative measures capable of protecting personal data from unauthorized access and from accidental or unlawful situations of destruction, loss, alteration, communication, or dissemination; and (ii.) prevention: the adoption of measures to prevent damage from the processing of personal data (Brazil, 2018). Therefore, reflecting on the protection of sensitive data in the midst of technological advancement involves recognizing the benefits of the digital environment but also understanding (and combating) its drawbacks.

The fundamental question to be considered, however, does not lie in the doubt regarding whether technological tools increase the risk to privacy, but it is necessary to think and analyze this new paradigm, which is the essence of this risk, what we are actually dealing with, since any metamorphosis requires new approaches and specific regulations. Data interoperability and the improvement of evaluations within the realm of public policies emerge as an asset that enables the simulation of scenarios related to potential issues.

Thus, the word "challenge" mentioned in the title of this article is justified by the fact that the field of artificial intelligence, big data, and data protection still lacks regulation and answers, meaning it is a consequence of novelty, the race that the law is running behind technology to ensure citizens have a minimum level of security. Therefore, balancing regulatory policies that protect fundamental rights without stifling technological progress is a significant challenge. To achieve this balance, we need the commitment of the public administration to embrace innovation and assume the desired leadership role in the realm of public policies.

4. Conclusion

The contemplation of protecting sensitive data in the face of technological advancement involves embracing the benefits of the digital realm while also understanding and mitigating its drawbacks. On one hand, we have the potential to leverage data for enhancing the formulation, management, implementation, and evaluation of public policies. This synergy with innovation, particularly through the utilization of data by artificial intelligence, is undeniable.

Within the realm of Artificial Intelligence, it is crucial to underscore its potential capabilities precisely because this technology can provide more precise data. In other words, as we confront a new paradigm, it becomes imperative to reconsider these emerging concepts and rights, especially since the race is already in progress.

On the other hand, this presents a new challenge: determining how to incorporate transparency and access to information to achieve effective external control, particularly concerning the data processed in the execution of public policies.

The discourse surrounding data protection is indispensable, as it represents a fundamental right demanding scrutiny and diligence from the state itself. However, it is equally important to question the limits, which data is being processed and shared, even in the context of public policies. This is the point at which we explore the feasibility of external control over this data or the establishment of a mechanism that ensures the security of citizens without compromising technological advancement.

In this regard, it is noteworthy that individuals are now immersed in the digital world, whether voluntarily or involuntarily. In essence, numerous databases containing personal information warrant attention, as this has a profound impact on data sharing. This sharing must be organized with a clear and transparent purpose to enable social oversight.

Consequently, the emphasis on regulation within this paradigm is necessary. Such regulation should not signify technological regression but rather should seek to prevent the indiscriminate use of data, which could violate various fundamental rights.

The use of the word “challenge” in the title of this article is entirely justified by the fact that the fields of artificial intelligence, big data, and data protection still lack regulation and definitive answers. In essence, this challenge stems from the novelty, the race that the legal system is pursuing to keep up with technology and ensure that citizens have a minimum level of security.

Balancing regulatory policies that protect fundamental rights without stifling technological progress is a formidable challenge. Achieving this equilibrium necessitates a commitment from public administration to embrace innovation and assume the pivotal leadership role in shaping public policies.

Artificial intelligence can significantly assist in data processing, enabling the simulation of scenarios related to potential problems, not only to address established issues but also to prevent them. In this context, transparency serves as a vital means of social control, particularly to elucidate how these technologies have been implemented.

Therefore, reflecting on the protection of sensitive data amid technological progress necessitates the recognition of the benefits of the digital environment while also understanding and mitigating risks. The data protection hinges on the potential for effective external control over data processed in the execution of public policies, as the judicious and strategic use of data has the potential to drive substantial improvements in policy evaluation, decision-making, and the relationship between the government and its citizens. However, handling personal data also entails the responsibility to address risks with transparency, respect for individual rights, and a profound sense of accountability.

References

Bauman, Zygmunt. 2013. *Vigilância Líquida:* diálogos com David Lyon. Rio de Janeiro: Zahar.

Brazil. 1988. Constitution of the Federative Republic of Brazil. Retrieved from https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Accessed 20 July 2023.

Brazil. 2018. Law No 13.709, August 14, 2018. Retrieved fromhttps://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed 20 July 2023.

Brazil. 2021. Law No 14.129, March 29, 2021. Retrieved from https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Accessed 20 July 2023.

Ferraz Júnior, Tércio Sampaio. 1993. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito, Universidade de São Paulo, 88, 439-459. https://www.revistas.usp.br/rfdusp/article/view/67231

Hoffmann-Riem, Wolfgang. 2022. *Teoria Digital do Direito Digital: Transformação Digital: Desafios para o Direito*. Rio de Janeiro: Forense.

Leal, Mônia Clarissa Hennig, & Maas, Rosana Helena. 2020. Dever de proteção estatal, proibição de proteção insuficiente e controle jurisdicional de Políticas Públicas. Rio de Janeiro: Lumen Juris.

Lynskey, Orla. 2015. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press.

Mayer-Schönberger, Viktor, & Cukier, Kenneth. 2013. *Big Data:* A Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt.

Mulholland, Caitlin Sampaio. 2018. Dados Pessoais Sensíveis e a tutela de Direitos Fundamentais: Uma análise à Luz da Lei Geral de Proteção de Dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, 19(3), 159-180. https://doi.org/10.18759/rdgf.v19i3.1603

Rodotà, Stefano. 2008. *A vida na sociedade da vigilância***:** a privacidade hoje. Rio de Janeiro: Renovar.

Ruíz, Luis Germán Ortega, & Becerra, Jairo. 2022. *La Inteligencia Artificial en la decisión jurídica y política*. Araucaria, 24(49). https://doi.org/10.12795.10

Sarlet, Ingo Wolfgang. 2021. Fundamentos Constitucionais: o direito fundamental à proteção de dados. In D. Doneda et al. (Eds.), *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense.

Schiefler, Eduardo André Costa, Cristóvam, José Sérgio da Silva, & Sousa, Thanderson Pereira de. 2020. Administração Pública digital e a problemática da desigualdade no acesso à tecnologia. *International Journal of Digital Law*, 1(2), 97-116. https://doi.org/10.47975/IJDL/1schiefler

Tavares, André Afonso, & Bitencourt, Caroline Muller. 2022. A Lei do Governo Digital e os Laboratórios de inovação: inteligência artificial, ciência de dados e big open data como ferramentas de apoio à auditoria social e controle social. In F. Motta & V. R. Lírio Valle (Eds.), *Governo Digital e a Busca por Inovação na Administração Pública: a lei nº 14.129, de 29 de março de 2021.* Belo Horizonte: Fórum.

Valle, Vanice Lírio do. 2020. Inteligência artificial incorporada à Administração Pública: mitos e desafios teóricos. A&C – *Revista de Direito Administrativo & Constitucional*, 20(81), 179-200. https://doi.org/10.21056/aec.v20i81.1346

Valle, Vanice Lírio do, & Motta, Fabrício. 2022. Governo digital: mapeando possíveis bloqueios institucionais à sua implantação. In F. Motta & V. R. Lírio Valle (Eds.), *Governo Digital e a Busca por Inovação na Administração Pública: a lei nº 14.129, de 29 de março de 2021*. Belo Horizonte: Fórum.