Data protection and public institutions in Brazil: new challenges, old administrative practices*

O poder público e a proteção de dados pessoais no Brasil: novos desafios, velhas práticas administrativas

*Lucas Borges de Carvalho***

ABSTRACT

Since its discussion in National Congress, the General Data Protection Law has generated resistance within the public sector in Brazil, in general, based on the conception that its rules are an obstacle to innovation and the efficient execution of public policies and services. The article argues that this rhetoric of efficiency and innovation masks old administrative practices. On the one hand, broad discretionary prerogatives, immune to social and jurisdictional control. On the other hand, the lack of transparency in the processing of personal data by public institutions. Based on recent

* Article received on 14 November 2022 and approved on 10 Jan. 2023. DOI: https:// doi.org/10.12660/rda.v282.2023.89347.

** Autoridade Nacional de Proteção de Dados (ANPD), Brasília, DF, Brasil. PHd in Law at Universidade de Brasília. Federal attorney. Advisor to the Board of Directors of ANPD. E-mail: lucasbcarvalho@gmail.com.

Supreme Court decisions, it is argued that data protection rights have a relevant political dimension, which promotes transparency and guarantees data subjects control over the flow of their information in society. This is a necessary legal barrier to avoid misuse and restrain surveillance risks and discriminatory practices.

KEYWORDS

administrative discretion — data protection — democracy — General Data Protection Law (LGPD) — transparency

RESUMO

Desde a sua tramitação no Congresso Nacional, a Lei Geral de Proteção de Dados Pessoais gerou resistências no âmbito do setor público no país, em geral fundadas na concepção de que suas normas constituem um entrave à inovação e à execução eficiente de políticas e serviços públicos. O artigo sustenta que essa retórica da eficiência e da inovação encobre o recurso a velhas práticas administrativas. De um lado, amplas prerrogativas discricionárias, imunes ao controle social e jurisdicional. De outro, a falta de transparência das operações com dados pessoais realizadas por instituições públicas. Amparado em decisões recentes do Supremo Tribunal Federal, argumenta-se que direito à proteção de dados pessoais possui uma relevante dimensão política, que promove a transparência e garante aos titulares de dados o controle sobre o fluxo de suas informações na sociedade. Trata-se de uma necessária barreira jurídica para evitar desvios de finalidade e conter os riscos de vigilância e de práticas discriminatórias.

PALAVRAS-CHAVE

democracia — discricionariedade administrativa — Lei Geral de Proteção de Dados Pessoais (LGPD) — proteção de dados pessoais — transparência

Introduction

In April 2018, during the processing of the *Lei Geral de Proteção de Dados Pessoais* (LGPD) in the National Congress, the federal government prepared a substitute for the then Bill of Law (PL) no. 330/2013 with the aim of excluding

the public authority from application of data protection rules. At the time, the proposal was defended using the argument that "in a digital environment, the flow of data cannot have many strings attached". It was claimed that there would already be enough "data protection jurisprudence" in the public sector, such as the provisions of Law no. 12.527, November 18, 2011 (Access to Information — LAI). Furthermore, "the need to seek the consent of the citizen for the implementation of each public policy would be an obstacle", a reason for which the suggested model would guarantee "security to the citizen's data without stifling innovation."[1]

At the end of the legislative process, the federal government's controversial proposal was not accepted. As a consequence, the final wording of the LGPD included an express provision for the application of its rules to legal entities of public law (art. 1), which must observe general principles, such as those of need, purpose and suitability (art. 6), in addition to specific obligations of transparency (art. 23). Likewise, users of public services important rights were ensured, such as access to data and correction of incomplete, inaccurate or outdated data (art. 18, II and III), opposition to treatment carried out without consent (art. 18, paragraph 2) and review of automated decisions (art. 20). Finally, in case of irregularities, *Autoridade Nacional de Proteção de Dados* (ANPD) may apply administrative sanctions to public entities and bodies (art. 52, paragraph 3).

Despite the express decision taken at the legislative level, the approval of the LGPD did not remove the influence and persistence of the conception that the legislative protection of personal data is an obstacle to innovation and implementation of effective public policies and services. As will be demonstrated in this work, this conception supported, directly or indirectly, diverse institutional reactions to the changes brought about by the LGPD, leading to a kind of interpretative dispute around the definition of limits, more or less broad, to the way in which public institutions until then dealt with the personal data of citizens.

The hypothesis developed here is that, despite the rhetoric of efficiency and innovation, resistance to new legal provisions is based on old and well-known administrative practices, associated, on the one hand, with the defence of broad

---

[1] SOPRANA, Paula. Governo quer lei de proteção de dados que tira responsabilidade do Poder Público. O Globo, 11 abr. 2018. Available at: https://glo.bo/3d75ym1. Accessed on: 14 Oct. 2022; LEMOS, Ronaldo. Privacidade vale também para governo. Folha de S.Paulo, 16 abr. 2018. Available at: https://bit.ly/2NcpvwV. Accessed on: 14 Oct. 2022.

discretionary prerogatives, immune to social and jurisdictional control; and, on the other, secrecy and lack of transparency of operations involving personal data carried out by public entities and bodies. Therefore, ultimately, what is at stake in the application of the LGPD to the public sector is the need to establish adequate mechanisms to guarantee rights, accountability to society and public control over the treatment of personal data handled by public institutions.

The methodological approach is based on a comprehensive legal analysis, of a historical nature, based on a bibliographic review on the subject, analysis and discussion of the applicable legislation, documents, information released by the press, paradigmatic cases and recent decisions, especially of the Supreme Court (STF). Thus, we propose an analytical construct, employing critical evaluation of the different conceptions of the processing of personal data by the public authority, as well as the actual process of application of the norms established by LGPD.

In addition to this introduction and the conclusion, the article is divided into three parts. In the first, we focus on the veto of some devices of the LGPD and the successive initiatives aimed at postponing its validity. As will be demonstrated, both initiatives were justified under the argument that the new data protection legislation could make unfeasible or affect the continuity of the provision of public services The second part demonstrates that recourse to broad discretionary prerogatives is a recurrent practice in the processing of personal data in the public sector, many often associated with generic purposes and potential abuse of purpose. The third part discusses the political dimension of the right to data protection of personal data, related to the transparency obligations established by the LGPD and, more generally, democratic control of authorities and public institutions.

1. Vetoes and validity of the LGPD

The dispute around the definition of limits to the application of LGPD to the public sector was established, broadly and openly, soon after the publication of the law, in August 2018. Indeed, arguments similar to those presented during the legislative procedure, expressing a reactive conception of the norms for the protection of personal data, can be identified: (i) in the reasons that justified part of the vetoes presented by the President of the Republic; (ii) in the successive initiatives aimed at postponing the effectiveness of the law.

Regarding the first aspect, the veto to art. 28 of LGPD, which established a simple obligation of transparency, determining that "the communication or shared use of personal data between bodies and entities governed by public law shall be publicized, pursuant to item I of the lead paragraph of art. 23 of this Law". Thus, for example, if a Ministry provides access to a given database for a local authority, this should be disclosed. According to art. 23, I, cited at the end of the vetoed device, dissemination should cover the sharing of "clear and up-to-date information on the legal provision, the purpose, procedures and practices used to carry out these activities, in easily accessible sources, preferably on their websites".

Despite the clarity and objectivity of the rule, the veto was justified through the argument that the "unrestricted publicity" foreseen in the norm could "bring about the regular exercise of some public actions such as those of supervision, control and administrative police".[2] As can be seen, underlying the reasons for the veto is the conception that the norms for the protection of data — or, more specifically, certain transparency obligations established by the LGPD — would be incompatible with the exercise of essential activities of the public authority, such as inspection, control and administrative supervision.

On the same occasion, three items of art. 52 authorized the ANPD to apply sanctions prohibiting and suspending the activity of data processing, as well as the partial suspension of the operation of the database. Subsequently, with the enactment of Law no. 13.853, July 8 2019, these sanctions were re-included in the LGPD. Once again, however, they were subject to a veto, which also excluded § 3 of art. 52, a device which authorized the application of these and other sanctions to public authorities. The reasons for this veto followed the same discursive pattern adopted in the case of art. 28 of the LGPD. In this sense, it was considered that the rules in question could generate "insecurity for those responsible for this information [...], which could cause damage [...] to public entities, with the potential to affect the continuity of public services".[3]

Therefore, similar to the proposal presented during the processing of the LGPD, the aforementioned vetoes also express the view that the new data protection legislation could "prevent" or "affect the continuity" of the provision of public services. Faced with these obvious "losses" and the related

---

[2] BRASIL. Presidência da República. Mensagem de Veto nº 451, de 14 de agosto de 2018. Available at: https://bit.ly/2N6fp0T. Accessed on: 14 Oct. 2022.

[3] Presidência da República. Mensagem de Veto nº 288, de 8 de julho de 2019. Available at: https://bit.ly/2CkTYqE. Accessed on: 14 Oct. 2022.

"legal uncertainty" generated, the best thing to do would be to limit, even partially, the impact of the law on the public sector. It should be emphasized that, despite the justification presented in the vetoes, the provisions in question strengthen essential guarantees for the protection of rights, either by imposing the necessary transparency for operations with personal data carried out by public entities and bodies, or by providing that, in case of irregularities, the ANPD may impose sanctions on the respective actors.

In response to the relative failure of these initiatives, especially in light of the overthrow of the veto of art. 52 by the National Congress, with the consequent reestablishment of the administrative sanctions applicable by the ANPD,[4] the strategy of postponing the validity of the LGPD arose. The original wording of the law provided its entry into force within 18 months, i.e., February 2020. However, after the publication of Provisional Measure (MP) no. 869, December 27, 2018, later the aforementioned Law no. 13.853/2019, the deadline was extended to 24 months, that is, August 2020, except for provisions relating to the installation and powers of the ANPD, whose validity was brought forward to December 2018.

During the Covid-19 pandemic, the validity of the main provisions of the LGPD was once again extended, this time to May 2021, as determined by MP No. 959, of April 29, 2020. The justification presented was that of "a possible insufficiency of a part of society due to the economic and social impact of the crisis caused by the pandemic of the Coronavirus".[5] At the same time, in a similar initiative by the National Congress, Law no. 14.010, of June 10, 2020, was approved and sanctioned, extending to August 2021 the validity of articles 52 to 54 that deal with administrative sanctions. In the end, after successive postponement measures, the LGPD, which had been approved in August 2018, with an original forecast of validity from February 2020, only came into full force in August 2021.

Although often presented with the exceptional and temporary measure, necessary to give public and private organizations a period of adaptation or to mitigate the social and economic effects of the pandemic, this handling of the validity of the LGPD can be seen as a point along a continuous line, integrated, still, by the attempt to exclude the public authority from the effect of the law

---

4 URUPÁ, Marcos. Congresso derruba vetos na LGPD. Teletime, 25 set. 2019. Available at: https://bit.ly/3rXjlFy. Accessed on: 14 Oct. 2022.

5 BRASIL. Presidência da República. Medida Provisória nº 959, de 29 de abril de 2020. Exposição de Motivos nº 00168/2020. Available at: https://bit.ly/30RKHRb. Accessed on: 14 Oct. 2022.

and from vetoes to instruments that foresaw transparency obligations and the application of sanctions to entities and public bodies. In all these cases, there is a similar discursive pattern, which expresses a design reactive to data protection rules and which will be adopted in concrete cases involving the processing of personal data by the power authority in the following years, as demonstrated in the next sections of this article.

This scenario is reinforced by the omission of the Executive Branch and the related non-compliance with the provisions of the LGPD, in force since December 2018, which provided for the approval of the regimental structure and the installation of the ANPD. In addition to the negative impact on guaranteeing the right to protection of data, the delay in the installation of the regulating body, effected only in November 2020, with the appointment of its governing body, was also presented, in a circular manner, as a reason to postpone the validity of the LGPD. In practice, all scenarios seemed to generate legal uncertainty, whether in terms of full and immediate application of the law, or of postponing the validity of its main devices.[6]

In this regard, it is important to mention that the postponement of the LGPD for about three years was not enough for entities and federal public bodies to implement basic measures required by the new law. According to a recent audit carried out by the *Tribunal de Contas da União* (TCU), from a total of 382 organizations audited, 76.7% are at a level classified as "inexpressive" or "initial" in terms of adequacy to the LGPD. About 20% are at the "intermediate" level and only 2.9% were considered at "enhanced".[7]

More specifically, this means that among these organizations, only 14% identified the personal data being handled in its internal processes, including those shared with third parties. In turn, only 17% identified all the business entities that carry out processing of personal data. The percentage is also reduced (11%) in relation to public organizations that identified

---

[6] For example, in justifying PL nº 1.027/2020, which proposed the postponement of the effectiveness of the main provisions of the LGPD to February 2022, Senator Otto Alencar claimed that, "in the face of the non-installation of the ANPD [...] there is, in fact, a legal impossibility, so that companies and entities of the Public Administration consider themselves compliant with the LGPD. This is because [...] there is no way for an entity to adapt to a law that is not regulated. […] It can be seen that the current situation has generated serious legal uncertainty, both for public managers as well as for private companies, who are forced to commit resources and efforts to adapt to a law that lacks regulation". BRASIL. Senado Federal. Projeto de Lei nº 1.027/2020. Available at: https://bit.ly/2NfDoe1. Accessed on: 14 Oct. 2022.

[7] BRASIL. Tribunal de Contas da União. Acórdão nº 13842/2022. Relator ministro Augusto Nardes, TCU/Plenário, 21 jun. 2022, p. 83. Available at: https://bit.ly/3MyEYFv. Accessed on: 15 Oct. 2022.

and documented the purposes of the processing of personal data. In the same way, although the majority (69%) appointed a person in charge, 82% of organizations do not have a registry established to consolidate related information with the characteristics of personal data processing activities.[8]

As for measures to promote transparency and guarantee rights, the rapporteur for the judgment, Minister Augusto Nardes, highlighted the following:

> In this regard, it was found that 75% of organizations have not yet prepared documentation relating to the privacy policy, which demonstrates that due transparency is not afforded. For cases in which the organization reported that it had a Privacy (or similar) Document, they had to confirm if artifact was published on the internet. The responses showed that most organizations do not clearly and concisely communicate information relating to the processing of personal data. As for the mechanisms for meeting the rights of subjects, since the organization must implement them to accord with the nine rights established in art. 18 of the LGPD, the answers showed that only 14% of organizations complied with the guidance for these rights listed in art. 18 of LGPD.[9]

As can be seen, there is a low implementation of basic measures aimed at compliance of federal public organizations with the legislation of personal data protection. Many of these organizations have not even carried out the mapping of processes and the identification of which data is processed and for what purposes, which indicates that these procedures are unknown or are carried out in a discretionary and unstructured way, that is, without due assessment and motivation regarding adequacy to the LGPD. In turn, the opacity of operations using personal data is attested by the small index of organizations that elaborated and published a policy of privacy or that have instituted mechanisms to meet the rights of subjects.

In short, the information collected by the TCU reveals the existence and the predominance of a reactive posture in the federal public sector in the face of implementation of the LGPD, which may have been encouraged by the

---

[8] Ibid., p. 84.
[9] Ibid., p. 85.

successive postponement of the validity of the law or, still, by the conception that the legislation protection of personal data represents an obstacle to innovation and efficient execution of public policies and services.

2. Discretionary use of personal data by public authorities

In the book *A guerra do fim do mundo*,, based on the historical facts of Canudos (1896-1897), Mario Vargas Llosa tells how a group of sertanejos resisted the Brazilian Army at the end of the 19th century, until the military troops completely destroyed the area. This only happened on the fourth expedition to Canudos, in the interior of Bahia. Antônio Conselheiro and followers maintained their ideals contrary to a series of changes that followed the Proclamation of the Republic in 1889, such as the separation of Church and State, civil marriage, the secularization of cemeteries and, more important for the purposes of this work, the realization of a new population census. At the time, it was believed that the data collected by the State would actually be used for discriminatory purposes, including religious and racial persecution, the latter with the aim of reestablishing slavery.[10]

Distrust of data collection by the State was not an isolated event exclusive to Canudos. About 40 years earlier, in 1852, a popular uprising in Pernambuco, known as the War of Marimbondos, which

spread to other provinces of the Empire, led the government to suspend the application of a law that determined the carrying out of the census and the official establishment of registration of births and deaths. Like Antônio Conselheiro, the population feared that the information obtained based on the new legislation, which became known as the "Captivity Law", was used to identify and enslave the poorest.

---

[10] "But, yes, something had changed with the Republic. For the evil and confusion of the world: the Church was separated from the State, freedom of worship and the secularization of cemeteries, which would no longer be assigned to parishes but to municipalities. […] This, as, no doubt, all the other strange, suspicious dispositions I was learning of in villages: the statistical map, the census, the decimal metric system. To the astonished sertanejos who came to ask him what all that meant, the Counselor explained, slowly: they wanted to know the color of people in order to restore slavery and return black people to their masters, and religion, to identify Catholics when persecution began. Without raising their voices, they were urged not to respond to such questionnaires or accept that the meter and the centimeter replaced the rod and the palm." VARGAS LLOSA, Mario. A guerra do fim do mundo. Rio de Janeiro: Alfaguara, 2008. p. 33-34.

The revolt led to the postponement of the census for about 20 years and the establishment

of the official public record for nearly four decades. Although the authorities ensured that there was no threat to the individual freedom, Guillermo de Jesus Palacios y Olivares recalls that the fear that data was used for other purposes was widespread, especially among the population that "carried with them the stigma of color, accustomed to the proverbial discretion of a slave-owning society."[11] Also according to the author:

> The Registry and the Census Law were explicitly aimed at counting and discovering the number of the free and poor, and thereby making them public and notorious before the State authority, with name, address and family status; beyond this, it made overcoming the barrier of slavery enormously difficult, as it improved the mechanisms for identifying the legal status of these sectors of the population, including many debtors, fugitives from captivity. […] In terms of the legal status of the free and poor [the Registry] confirmed the freedom of those who could testify to this condition, and threatened to return to slavery the unfortunate ones who did not furnish the documentation needed to substantiate their personal independence.[12]

These historical events demonstrate that the controversies associated with the processing of personal data by public authorities in Brazil has a long history, marked by distrust regarding the risks of personal data allocation for undeclared purposes incompatible with the law. In this sense, it is considered that the citizen is the weakest link, vulnerable in the relationship established with public institutions, since personal information is collected on a compulsory basis and, if safeguards have not been adopted, may be used for abusive purposes, associated with discriminatory or surveillance practices.

The main difference between the present day and the 19th century is that the mechanisms for collecting information from citizens are very well established and structured, involving massive amounts of personal data, often stored in digital format and treated in an automated way. This expansion of

---

[11] PALACIOS Y OLIVARES, Guillermo. Revoltas camponesas no Brasil escravista: a "Guerra dos Marimbondos" (Pernambuco, 1851-1852). Almanack Braziliense, n. 3, maio 2006, p. 30. Available at: https://bit.ly/3TG0Zow. Accessed on: 23 Oct. 2022.

[12] Ibid., p. 30.

data collection is the result of the essential change in the role of the State, which, over the last few decades, has assumed the function of formulating public policies and guaranteeing social rights, such as in education, health and work. In this sense, personal data constitute a relevant input to increase the efficiency of state action, for example, through the sharing of information between entities and public bodies or, even, through the production of evidence that underpins the formulation of public policies. As Miriam Wimmer points out:

> The question of how well the state should know its citizens has been faced in different contexts and at different historical moments, wherein, while the treatment of personal data by the State is a prerequisite for the exercise of citizenship, the expansion of the amount and variety of personal data held by the State raises risks of rights violations. In other words, the visibility of the State over its citizens allows it to expand its capacity of intervention, with the objectives of possibly harmful or just social purposes (e.g., enabling the distribution of social benefits).[13]

In the context of the 21st century, one of the characteristic elements of mass collection of personal data is the generation of a "behavioral surplus", that is, a kind of surplus value, which transcends the original purposes of the operation.[14] As a consequence, even after exhausting its initial objectives, the use of a set of personal data tends to remain attractive and valuable for other purposes. Subsequent and ongoing use of personal data generates significant additional value — be it public, political or economic — at a reduced marginal cost, particularly in view of the possibility of making new inferences from data analysis techniques or from simple aggregation of new information, among other possibilities, always aimed at controlling, predicting and directing behaviors.[15]

---

[13] WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. In: MENDES, L.; DONEDA, D.; SARLET, I.; RODRIGUES JR., O. (Org.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 273.

[14] ZUBOFF, Shoshana. The age of surveillance capitalism: the fight for a human future at the new frontier of power. Nova York: Public Affairs, 2019. p. 74-75.

[15] The author reports Google as the pioneer in the use of this surplus and, in a way more broadly, in the formation of the essential structures of "surveillance capitalism". In that in the beginning, the data generated by the company's search engine was used just to increase the quality of service. With the passage of time, and in view of the need to generate revenue for its shareholders, the company realized the value of the collected data, and began to use it for a different purpose: the sale of advertisements. In the words of the author, "these behavioral data available beyond the improvement of the service constituted a surplus and it was with support of this that the then young company found the way for the generation of exponential and sustainable profits to guarantee its survival". Ibid., p. 74.

Thus, for example, information from low-income families that are part of the *Cadastro Único para Programas Sociais do Governo Federal* (CadÚnico) can be used for the formulation and management of public policies (art. 13, Decree No. 11.016, of March 29, 2022), as in the case of the identification of beneficiaries of the emergency aid granted during the Covid-19 pandemic (Law no. 13.982, April 2, 2020). Although granting this specific benefit was not part of the original purpose of CadÚnico, the information contained therein was used legitimately to subsidize this new public policy.

As this trivial example demonstrates, in the public sector, the treatment of personal data for purposes other than those that justified in the collection, must, among other conditions, always serve a public purpose. The LGPD has express rules in this regard, such as the provisions of art. 26, according to which the shared use of personal data by public authorities must meet the "specific purpose of executing public policies".

Often, however, the legitimacy of the shared use of data by public authorities is controversial. A public purpose can contravene another public purpose or certain fundamental rights. Doubts may also arise as to the limits applicable to the competencies of an authority to access or carry out the processing of personal information. The legislation may not be clear on these aspects, the justifications presented may be fragile or, even, lead to deviation from purpose and significant personal risk.

In the face of a conflict of this type, the STF ruled against the sharing of personal data obtained by *Instituto Brasileiro de Geografia e Estatística* (IBGE) and *Instituto Nacional de Estudos e Pesquisas* (Inep). The data in question, which had been collected for statistical purposes, would be used, respectively, to allow the Federal Prosecutor to identify children not registered in the city of Bauru (SP) and the TCU to carry out an audit in the *Bolsa Familia* Program. Although, in both cases, the sharing of data was intended to serve public purposes, the Court understood that, in the specific case, statistical secrecy should prevail along with the original purpose, under penalty of violating the privacy and intimacy of the subjects. Furthermore, if ruled, sharing would jeopardize the trust in research bodies by the interviewees and the continuity of these activities.[16]

The central point to be considered is that, driven by legitimate motives or not, public authorities have structural incentives to appropriate benefits

[16] BRASIL. Supremo Tribunal Federal. Suspensão de Liminar nº 1.103. Rel. min. Cármen Lúcia. 2 maio 2017; BRASIL. Supremo Tribunal Federal. Mandado de Segurança nº 36.150. Rel. min. Roberto Barroso. 10 dez. 2018.

and behavioral surpluses generated by the various personal databases stored by public or private institutions. Thus, often, these same authorities start to defend their prerogatives to such data based on the existence of broad discretionary powers, that is, a free decision-making space, immune to jurisdictional control and legitimized only by abstract and generic legal concepts, such as public interest.[17]

In this regard, in May 2019, the Ministry of Education asked Inep for access to the Higher Education Census database with the purpose of enabling the execution of a new public policy: issuance of digital student portfolios. Critics of the measure pointed to the existence of surveillance risks on students and abandonment of centers of learning at a time when protests were taking place across the country against budget cuts in education. Inep, in turn, refuted sharing of the data, vis-à-vis statistical secrecy, according to arguments presented in the aforementioned case judged by the STF.[18]

Faced with the impasse, MP no. 895, September 6, 2019, was issued, which authorized the Ministry to issue the digital student card and gave it broad discretionary power to collect and share personal data of students and professors, in addition to other information to be defined in an administrative act. The only limitation foreseen in the norm was that the sharing should meet the generic purpose of "formulation, implementation, execution, evaluation and monitoring of public policies, observing the rules and specific procedures that guarantee their security, protection and confidentiality", pursuant to art. 1-B, § 4, Law no. 12.933, September 26, 2013, as amended by MP nº 895/2019.

In turn, the privacy policy of the "Student ID" application, through which the digital cards were made available, provided that the data collected "are the property of the MEC".[19] On the one hand, this patrimonial view reveals

---

17 For a critique of this conception of administrative discretion, see BINENBOJM, Gustavo. Uma teoria do direito administrativo: direitos fundamentais, democracia e constitucionalização. 2. ed. Rio de Janeiro: Renovar, 2008. p. 38-42.

18 MARIZ, Renata. MEC quer acessar dados sigilosos de alunos para emitir nova carteirinha estudantil. O Globo, 16 maio 2019. Available at: https://glo.bo/2H1Odgu. Accessed on: 18 Oct. 2022.

19 BRASIL, Ministério da Educação. Política de privacidade do aplicativo ID Estudantil. 2020. Available at: https://bit.ly/38FDG80. Accessed on: 18 Oct. 2022. It is common for programs and government applications not to have privacy policies or, those that have it, adopt generic wording, as verified by ABREU, Jacqueline; MASSARO, Heloisa; LAGO, Lucas. As políticas de privacidade de apps do governo. InternetLab, maio 2018. Available at: https://bit.ly/2ZtuQWE. Accessed on: 18 Oct. 2022; and MACHADO, Jorge; BIONI, Bruno. A proteção de dados pessoais nos programas de Nota Fiscal: um estudo de caso do 'Nota Fiscal Paulista'. Liinc em Revista, Rio de Janeiro, v. 12, n. 2, p. 350-364, nov. 2016.

the misunderstanding regarding the legal nature of the collected information, which pertains to "inseparable aspects of the subject", as noted by Danilo Doneda,[20] not pertinent, therefore, to restrictions arising from a real right. On the other hand, it expresses the understanding that the citizen is a mere "data provider",[21] without any power to control the use of personal information, given the related discretionary prerogatives attributed to the "owner" of the personal data.

Once again, the privacy policy disclosed by the MEC confirms this understanding. Indeed, among other general purposes, the data — which, it is worth emphasizing, was originally collected for the issuance of student wallets — could also be used "for other purposes by the Public Administration: audits, statistical analysis, data science, and studies to launch new public services or to improve existing ones, as well as procedures and communications."[22] In practice, in view of the breadth of the aforementioned "objectives of Public Administration", student data could be shared, unrestrictedly and on a discretionary basis, with any other public body and intended for any purposes.

MP No. 895/2019 expired in February 2019, without being considered by the National Congress. However, just over a year later, the federal government resorted to similar legal grounds to edit MP No. 954, of April 17, 2020, which required telecommunications service providers to furnish IBGE with personal data of all its consumers for the purposes of "official statistical production". Sharing of this data would allow face-to-face interviews for the duration of the restrictions imposed by the Covid-19 pandemic.

Despite the undeniable exceptionality of the situation and the relevance of maintenance of official surveys, MP nº 954/2020 reflected, with some

---

[20] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 84. The author criticizes the doctrinal position that supports the existence of "ownership of personal data", given "the multiplicity of issues and interests around personal data, which are not limited to heritage vectors and which would be irremediably harmed if considered only – or mostly – in terms of economic value. Ibid., p. 146.

[21] According to Stefano Rodotà, "the new situation determined by the use of computers in the processing of personal information makes it increasingly difficult to consider the citizen as a simple 'data provider', without any power of control. In fact, the obligation to provide data cannot simply be considered as the counterpart of the social benefits that, directly or indirectly, the citizen can access and enjoy. The collected information not only enables public and private organizations to plan and execute their programs, but allows for the emergence of new concentrations of power or the strengthening of already existing powers: consequently, citizens have the right to exercise direct control over those to whom the information provided will attribute a growing surplus-power". RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 36-37.

[22] BRASIL, Ministério da Educação, Política de privacidade do aplicativo ID Estudantil, op. cit.

variations, the same conception presented in the case of student portfolios: the use for a generic purpose, the lack of transparency as to the motivation of the act and the attribution of wide discretionary powers to the public power to process a massive amount of personal data. For these and other reasons, MP No. 954/2020 was suspended by precautionary measure issued by Minister Rosa Weber, of the STF, expressly noting that the normative act:

> does not delimit the object of the statistics to be produced, nor the specific purpose, nor the amplitude. It also does not clarify the need to furnish data nor how it will be effectively used […]. In this light, by not properly defining how and for what purposes the data collected will be used, MP no. 954/2020 does not offer conditions for assessing its suitability and necessity, understood as the compatibility of the treatment for the informed purposes and its limitation to the minimum necessary to achieve its purposes.[23]

Still during the coronavirus pandemic and just over a month after the decision of the STF, Intercept Brasil revealed that the National Department of Trânsito (Denatran) had authorized the Brazilian Intelligence Agency (Abin) access to sensitive personal data of 76 million Brazilians who have a National Driver's License. The obscure transaction would be carried out to meet the general purpose of ensuring the "operation of intelligence activity".[24]

In a petition addressed to the STF, in the course of the *Arguição de Descumprimento de Preceito Fundamental* (ADPF) nº 695, which questioned the operation, the General Attorney of the Union defended its legality and adherence to Decree no. 10.046, October 9, 2019, a rule that would allow "the sharing of more fluid data between bodies and entities of the Public

---

[23] BRASIL. Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6387. Rel. min. Rosa Weber. 24 abr. 2020. The precautionary measure was endorsed by the Plenary of the STF, by 10 votes to one, defeating Justice Marco Aurélio, in a session held on 7 May 2020.

[24] DIAS, Tatiana; Martins, Rafael. Documentos vazados mostram que Abin pediu ao Serpro dados e fotos de todas as CNHs do país. The Intercept, 6 jun. 2020. Available at: https://bit.ly/2B6uSvy. Accessed on: 2 Nov. 2022. It is worth mentioning that the full Term of Authorization no. 7/2020, signed in March 2020 between the parties, was not even presented to the STF. Minister Gilmar Mendes highlighted the "obscure nature" of the operation, emphasizing that, in the extract published in the Official Gazette, there was no "relevant information neither about the nature of the shared data nor the parameters of sharing". BRASIL. Supremo Tribunal Federal. Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental nº 695. Rel. min. Gilmar Mendes. 24 jun. 2020.

Administration". Furthermore, he argued that "intelligence activity is a kind of public policy consolidated in the Brazilian order", which would authorize the sharing of data to serve this purpose. For such reasons, the most appropriate hypothesis would be a "deference for the choice of elected representatives", recognizing the capacity of the Executive Power to decide on the matter:

> Along these lines, the pragmatic structuring of the data between public administration bodies or entities is belongs to the sphere of the Executive Power, leaving the Judiciary to respect the discretionary scope of the other Powers, especially when observing the rules and principles that shape administrative action.[25]

Although the authorization to share data with Abin has been revoked by Denatran, the STF proceeded with the judgment of the action. The final decision was handed down in September 2022, together with the *Ação Direta de Inconstitucionalidade* (ADI) nº 6.649, which questioned the abstract constitutionality of Decree no. 10.046/2019.

In his vote, rapporteur Minister Gilmar Mendes maintained that the treatment of personal data by the public authorities must observe three constitutional guidelines: (i) detailed and exhaustive justification of the purposes; (ii) limitation to the data strictly necessary to achieve the purposes, adopting prevention and safety measures proportionate to the risks involved; and (iii) transparency and duty of dissemination vis-a-vis information relating to treatment, guaranteeing the subject a sufficient level of control as to legality.[26]

Thus, in a vote that was endorsed by the other members of the court, minister Gilmar Mendes took a stand against the conception that data processing can be conducted at discretion or with broad deference to the choices of elected representatives. This is because the regime of constitutional protection of privacy "leads to the abandonment of any interpretation that allows a broad and unrestricted sharing of personal data between agencies and entities of the Federal Public Administration".[27]

---

[25] BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 695. Manifestação do advogado-geral da União. 20 jun. 2020.

[26] BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 695. Voto do relator, ministro Gilmar Mendes. 15 set. 2022. p. 27.

[27] Ibid., p. 43.

Finally, he stressed that, despite the importance of using new technologies and digital tools by the government, the search for efficiency and the institution of best management practices cannot serve "manoeuvring for non-compliance with the principle of legality" and neither constitutes "a blank check for the public administrator". In the same way, it is not "a license to disregard the ethical precepts that inform the constitutional regime, including the mechanisms for the protection of personal data".[28]

As can be seen, the most recent decisions of the STF established objective and binding legal parameters, which limit the field of action in terms of the discretion of public authorities. In line with the provisions of the LGPD, the court made it clear that the processing of personal data by the public authority presupposes a clear and precise delimitation of its legal basis, the value or public benefit generated and the adherence of the operation to the legal powers of the bodies and entities involved. Therefore, the purpose must be, effectively, specific, demanding indication, also clearly and precisely, of which initiative, action or project will be made possible by the data usage.

This is an argumentative burden and a requirement that must be assumed by public managers, moving away from — recognizing, in advance, as illegitimate — any hypothesis of processing of personal data without adequate motivation, based solely on generic purposes, such as "formulation, execution and evaluation of policy activities", "official statistical production" and "intelligence activities".

The protection of personal data constitutes the basis of public confidence in the institutions, as may be extracted from the events that gave rise to the Marimbondo War in the mid-nineteenth century. Similarly, nowadays, the growing supply of digital technologies services, which are intended to be simpler, more practical and efficient, is only viable and sustainable if accompanied by measures that promote transparency and ensure the holders control over their personal data. In the last analysis, and this is the main meaning of the provisions established by the LGPD and reaffirmed by the STF, it is all about establishing a necessary legal barrier to avoid misuse of purpose and contain the risks of surveillance and discriminatory practices.

---

[28] Ibid., p. 51-52.

3. Transparency and the political dimension of the right protect personal data

According to Norberto Bobbio, democracy is the "regime of visible power" or, the "government of the public power in public".[29] This definition assumes that the principle of transparency is the basis of democracy, so that visibility of the actions of the rulers constitutes a necessary presupposition for the exercise of control of these same actions by citizens.

Therefore, one of the main threats to the realization of democratic ideals comes from the persistence of secrecy as an administrative practice. This practice gives rise to the so-called "invisible power", which gains space through the actions of the secret services, through obscure relationships established between authorities and large economic groups and, mainly, by growing vigilance over citizens, made possible by the technical means of control of information and communication.

As for this last aspect, Bobbio pointed out, at the end of the 20th century, the existence of strong risks of new technologies being used for a kind of inversion of the democratic equation, consistent in the amplitude action of mechanisms of control of individuals by the State. In his words:

> And why couldn't the same use of computers make possible a capillary knowledge of the citizens of a large State by whom holds the power? […] Whether this prospect is a nightmare or fate no one is in a position to predict. It would be a trend opposed that which gave life to the ideal of democracy as a precept of visible power: the trend no longer towards maximum control of power by citizens, but towards maximum control of subjects by those in power.[30]

Nowadays, in fact, the risks of control and surveillance of citizens by state institutions is expanding, due to the intense process of digital transformation over the last decades, which affects all social and economic sectors. Among other factors, the digital transformation is driven by the spread of internet access, by the proliferation of portable electronic devices and the growing use of algorithms and artificial intelligence systems, such as those that allow the recognition of a person based on their biometric data.

---

[29] BOBBIO, Norberto. O futuro da democracia. São Paulo: Paz e Terra, 2000. p. 98.
[30] Ibid., p. 120.

In the public sector, among other innovations, the digitization process allows information that, a few decades ago, was registered only analogically, often printed on documents filed in lockers in various public offices, to be stored in digital format, on computers with high processing capacity. With this, it is possible not only to expand and accelerate the collection of personal data, but to infer new information or cross-referencing between the various databases, for multiple purposes, in particular through its shared use with other public bodies and private entities.

In this respect, a study carried out by the Organization for Economic Cooperation and Development (OECD) highlights that the ability to easily reference and recycle stored data is one of the factors that have driven the digital transformation. Indeed,

> Digitization increases the use and value of past information, making it more accessible, useful and reusable. Scanning has made text searchable, compressible, easily manipulated and linkable [to other information], and allows archives to be preserved, analyzed, indexed, reused, reinterpreted and resold. […] The technological capacity of preserve and use past information and combine it with new information continues to sustain a rapid expansion of the digital economy.[31]

As mentioned, this innovation process is fundamental in increasing the efficiency of State action. At the same time, the risks of abuse and violation of rights increase, arising from the misuse of your personal data. In this context, in addition to ensuring a private space, away from third-party interference, the right to the protection of personal data assumes a policy linked to the subject's control over the flow of information in society[32] and, more specifically, the effective democratic control of public authorities by citizens.

---

[31] ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. Vectors of digital transformation. OECD Digital Economy Papers, n. 273, jan. 2019. p. 15. Available at: https://bit.ly/3fDfbQx. Accessed on: 6 Nov. 2022.

[32] According to Stefano Rodotà, "in the information society, definitions tend to prevail regarding the functional aspects of privacy that, in different ways, make reference to the possibility of a subject knowing, controlling, addressing, and interrupt the flow of information related to them. Thus privacy can be defined more precisely, in a first approximation, as the right to maintain control over one's information. Stefano Rodotà, A vida na sociedade da vigilância, op. cit., p. 92. Along the same lines, Laura Schertel Mendes argues that the right to data protection can be conceived in a double dimension, which consists, at the same time, of: "(i) the protection of the individual against the risks that threaten their personality in view of the collection, processing, use and circulation of personal data and (ii) attributing to the individual the guarantee of controlling the flow of their data in society".
MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 176.

This is the main direction given by the LGPD to regulating the processing of personal data by public institutions. In that sense, the law expressly determines that public entities and bodies are transparent regarding operations involving personal data. On the one hand, pursuant to art. 23, I, proactive action is required, through the dissemination of "clear and up-to-date information on the legal provision, purpose, procedures and practices used to carry out these activities, in easily accessible sources, preferably on their websites". On the other hand, when requested by titleholders, entities and public bodies must provide information about the processing of their personal data and adopt the appropriate measures, pursuant to art. 18 of the LGPD.

As demonstrated, these transparency obligations have met with strong resistance in the public sector. Thus, for example, the veto to art. 28 of the LGPD was justified on the grounds that the "unrestricted publicity" envisaged in the norm could make essential activities of the public authority unfeasible. Similarly, an audit carried out by the TCU identified a high number of public organizations that do not have a privacy policy and are not prepared to meet the requests of data subjects.[33]

Allied to this, and despite its close connection with the principle of transparency, the LGPD has been interpreted in the opposite direction, that is, as a law that strengthens and expands the secrecy of administrative practices. This can be seen in some recent cases, in which the new protection legislation of personal data was used as justification by public authorities to deny access to certain information, much of which are of obvious public interest, such as the registration of visitors to the Planalto Palace and voucher payments of compensation sums to civil servants.[34]

LGPD demands from public entities and bodies, in line with the guidance of the ANPD, "a position of caution and risk analysis regarding the disclosure of personal information".[35] However, this does not mean confusing or limiting the protection of personal data to the broad attribution and unrestricted confidentiality of information collected by the State.

As provided for in LAI (art. 31, paragraph 3, V), personal information may be disclosed, among other hypotheses, whenever necessary "for the

---

33 Cf. a Seção 2 anterior, "Vetos e vigência da LGPD".

34 ARCOVERDE, Léo; RAMOS, Maria Vitória; ZANATTA, Rafael. Transparência sob ataque. Folha de S.Paulo, 4 nov. 2021. Available at: https://bit.ly/3Nwy6ci. Accessed on: 2 Nov. 2022.

35 BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. Tratamento de dados pessoais pelo poder público (guia orientativo). Brasília: jan. 2022. Available at: https://bit.ly/3gXPEBR. Accessed on: 2 Nov. 2022.

protection of the general and overriding public interest". In this regard, the STF decided that the information relating to the remuneration of civil servants is of collective and general interest, so that it can be legitimately disclosed by public bodies and entities, especially in order to facilitate the control of the social role of the State.[36]

Similarly, in response to the consultation made by the *Ministério do Trabalho e Previdência*, the ANPD demonstrated in favor of the possibility of disclosure of lists of beneficiaries of aid paid to taxi drivers and autonomous freight carriers. At the time, the ANPD considered that the disclosure of such personal data, as it is associated with the execution of a specific public policy, "is consistent with the pursuit of the public interest, mentioned in art. 23 of the LGPD", with the proviso that it must be limited to "data necessary to comply with the principle of publicity and the provisions of LAI", and that beneficiaries be informed, in compliance with the principle of transparency – that "their names will be disclosed".[37]

In another case, the ANPD maintained that "the LGPD did not establish anonymization as a technical condition for public disclosure […] of personal data by public entities and bodies". Thus, even with the "possible identification of the subjects" or if there is "some degree of risk of identification", the LGPD admits the disclosure of personal data "when necessary to meet, for example, legal determinations, public interest and the right of access to information [...], as long as the safeguards are adopted".[38]

Thus, although secrecy is a necessary protective measure in certain circumstances, particularly when determined by law or in relation to sensitive data, such as relating to health, it can be stated that public authorities have a double duty of dissemination regarding operations carried out with personal data.

---

[36] BRASIL. Supremo Tribunal Federal. Suspensão de Liminar nº 623. Rel. min. Ares Britto. 10 jul. 2012.

[37] BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. Nota Técnica nº 92/2022/CGF/ANPD. Available at: https://bit.ly/3DDNpeV. Accessed on: 3 Nov. 2022.

[38] In the case in question, Inep had suspended the disclosure of certain information about educational censuses that were traditionally posted on the internet. Such restrictive measures were adopted based on a technical study, according to which there would be a risk of identification of data subjects, despite the technical means used to protect their identity and ensure statistical secrecy. BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. Nota Técnica nº 46/2022/CGF/ANPD. Available at: https://bit.ly/3WN8ivW. Accessed on: 29 Dec. 2022. In a sense similar to that of ANPD, see BRASIL. Controladoria- Geral da União. Nota Técnica nº 1136/2022/CGAT/DTC/STPC. Available at: https://bit.ly/3Q46dJR. Accessed on: 29 Dec. 2022.

First, they should actively divulge information about treatment of data and respond to the requests presented by those in question. In this case, transparency is a necessary and direct assumption for subjects to exercise control over the flow of personal data within the public sector. Second, there is a duty, under certain circumstances, to disclose personal data, observing the applicable precautions and restrictions, whenever this measure is necessary to serve the public interest and preponderant to ensure the right of access to information. In this case, transparency is linked, more broadly, to the exercise of democratic control of the performance of institutions and administrative authorities, a guarantee that is also promoted by the LGPD and compatible with the right to the protection of personal data.

It is important to mention that this reading is supported by the decision rendered by the STF in the judgment of ADPF nº 695 and ADI nº 6649. According to the rapporteur minister's vote, the principle of transparency imposes on the public administration the obligation to ensure a "level of sufficient control for prospective verification of the legality of the treatment of data". More specifically, this guarantee unfolds into a "duty to provide minimum conditions to ensure control of the way the State handles personal data". Furthermore, the linking of this duty of transparency to principles of management of public health and fundamental rights implies that any intentional transgression "will involve the accountability of the state official for an act of administrative impropriety".[39]

In the same decision, the STF declared unconstitutional the composition of the *Comitê Central de Governança de Dados* (CCGD), a body established by Decree no. 10.046/2019, with authority to establish guidelines and parameters for the sharing of personal data within the scope of the federal public administration. According to the vote of the rapporteur, the effective guardianship of the right to privacy demands that the competent institutions be formed "from a plural and democratic composition, open, to some extent, to constant dialogue with civil society."[40] The composition of the CCGD did not meet this requirement, since the body was made up only of representatives of the Executive Branch, without independence or guarantees against undue influence. The agency therefore was insular and hostile to any proposal of democratic opening and pluralization of

[39] BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 695. Voto do relator, ministro Gilmar Mendes. 15 set. 2022, p. 27 e 69.

[40] Ibid., p. 61.

the debate", which could lead to "an authentic dismantling of the pillars structuring the LGPD".[41]

Given this scenario, it is concluded that, although privacy is usually identified with the notion of secrecy, at odds with the principle of transparency, the protection of personal data, as established by the LGPD and ratified by the STF, is more related to the idea of control by the subject of the use of information and, more generally, about the performance of public authorities and institutions. Thus, the LGPD has not revoked or amended the LAI and not established any rules on the attribution of secrecy to personal information held by the State. So, the legal provisions dealing with the right of access to information and the right to data protection are "systematically compatible with each other", so that there is no need to speak of an antinomy between these norms.[42]

This is a fundamental point, especially in the public sector, as personal data constitute a source of power, in that the more knowledge about a person, the more power wielded. As Carissa Véliz points out, "Privacy matters because the lack of it gives power over you to others".[43] In the same sense, Daniel Solove argues:

> Privacy is a limit on the power of government and business. When it comes to personal data, knowledge is power. Personal data is involved in many important decisions about people's lives. It can readily be used to affect reputations, shape decision-making and influence behavior. In the wrong hands, personal data can be used to cause serious harm to people.[44]

---

41 Ibid., p. 62. In compliance with the decision of the STF, the President of the Republic established Decree no. 11.266, November 25, 2022, which reworded Decree no. 10.046/2019, to include, among the members of the CCGD, two representatives of "social organizations with proven performance in the area of personal data protection" (art. 22, IX). Also, the possibility of participation in the CCGD by representatives of the Conselho Nacional de Justiça, do Senado Federal and the Câmara dos Deputados, as guest participants (art. 22, § 4º).

42 According to Statement No. 4, of March 10, 2022, by the Comptroller General of the Union: "the LAI, Law no. 14.129/2021 (Lei de Governo Digital) and Law no. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais — LGPD) are systematically compatible with each other and harmonize the fundamental rights of access to information, privacy and protection of personal data, with no antinomy between their devices". BRASIL. Controladoria-Geral da União. Enunciado nº 4, de 10 de março de 2022. Available at: https://bit.ly/3NwDkEW. Accessed on: 3 Nov. 2022.

43 VÉLIZ, Carissa. Privacy is power: why and how you should take back control of your data. Londres: Corgi Books, 2021. p. 56.

44 SOLOVE, Daniel. The myth of the privacy paradox. The George Washington Law Review, v. 89, n. 1, jan. 2021. p. 38. Available at: https://bit.ly/3FMNCyR. Accessed on: 5 Nov. 2022.

Thus, recognizing the existence of a political dimension to the right to protection of personal data implies conceiving privacy beyond the secrecy-transparency binary, refuting simplistic interpretations of LGPD, which improperly use it as a basis for attributing unrestricted secrecy to information of obvious public interest. As Stefano Rodota highlights:

> This set of indications obliges us to review the commonly used schemes adopted in terms of privacy; and presents some paradoxes. The first stems from the fact that the expansion of protection of the private sphere, of the subjects whose data is collected, with the attribution to them of direct powers of control, determined a greater transparency in the sphere of information collection, whether public organs or private organizations. Privacy rules, designed to ensure opacity and confidentiality for the individual, become the means for a greater social transparency.[45]

In short, although the attribution of secrecy to personal data is necessary in certain circumstances, the right to data protection is constituted as a legal barrier to the power exercised by public authorities and institutions. In other words, it is a guarantee that promotes control of the flow of personal information, imposing on authorities the duty of publicity, ensuring the existence of mechanisms for participation and accountability, responsive to the interests of citizens and civil organizations.

It reaffirms, therefore, the existence of an intrinsic connection between the protection of personal data, transparency and the exercise of political liberties. After all, as Neil Richards points out, there is no democracy without privacy and protection of personal data, since these rights constitute "an essential source of political power for citizens in relation to the State", which "drives the development of ideas and policy expression" and "enables them to act as autonomous citizens".[46]

---

45 Stefano Rodotà, A vida na sociedade da vigilância, op. cit., p. 129.
46 RICHARDS, Neil. Why privacy matters. Nova York: Oxford University Press, 2022. p. 132.

Conclusion

In Brazil, the processing of personal data by the public authorities was based, traditionally, on two well-known administrative practices. On the one hand, recourse to discretionary prerogatives, immune to social control and jurisdiction, allowed authorities and public institutions to deal with personal data, compulsorily collected from citizens, with wide margin of decision, as if this data were a kind of "property", whose "owner" was the State. On the other, the amplitude of these prerogatives was reinforced by the opacity of operations involving personal data and the absence of effective mechanisms for participation and accountability to society.

With the advent of the LGPD, these two administrative practices were put in check. As opposed to administrative discretion, the new law started to demand a detailed motivation of the operations, which must be supported by a legal hypothesis, linked to specific purposes and limited to strictly necessary data, in addition to observing other principles and rules provided for in the standard. As a counterpoint to the opacity and culture of secrecy, the LGPD joined the LAI in demanding greater transparency and the mechanisms to respond to requests from data subjects.

Resistance to these rules arose during the processing of the LGPD in the National Congress, where the data protection legislation was identified as an obstacle to efficiency, innovation and regular provision of public services. With some variations, similar arguments have been used to justify vetoes to LGPD provisions and to postpone, more than once, their validity. Likewise, general purposes, accompanied by measures not altogether transparent and without adequate motivation, served as the basis for controversial initiatives, such as the issuance of digital student portfolios, the sharing of data from telecommunications services with the IBGE and the provision of data from drivers, to attend Abin's "intelligence activities".

As demonstrated here, these arguments were expressly rejected by recent decisions of the STF. The Constitutional Court recognized that the right to protection of personal data imposes limits on the actions of authorities and public institutions, under the terms of the LGPD. To guarantee the subject control over the flow of their personal information, the right to protection of personal data assumes a relevant political dimension, associated with the democratic control of authorities and public institutions. Thus, in order to contain the risks of deviations, the search for efficiency and innovation in the public sector must be reconciled with the guarantees of transparency,

participation of civil society, definition of specific purposes and motivation of administrative decisions.

Despite the relevance of established legal parameters, it is necessary to recognize that the decisions of the STF are only a first step along the way to establishing a culture of data protection in the public sector. It is certain that the future will see increasing digitization of services, continuous innovation and the search for of greater efficiency in state actions. But it is also true that these new challenges cannot be used as a pretext to sustain old administrative practices. After all, more and more, confidence in public institutions presupposes the effective protection of personal data.

References

ABREU, Jacqueline; MASSARO, Heloisa; LAGO, Lucas. As políticas de privacidade de apps do governo. *InternetLab*, maio, 2018. Available at: https://bit.ly/2ZtuQWE. Accessed on: 18 Oct. 2022.

ARCOVERDE, Léo; RAMOS, Maria Vitória; ZANATTA, Rafael. Transparência sob ataque. *Folha de S.Paulo*, 4 nov. 2021. Available at: https://bit.ly/3Nwy6ci. Accessed on: 2 Nov. 2022.

BINENBOJM, Gustavo. *Uma teoria do direito administrativo*: direitos funda mentais, democracia e constitucionalização. 2. ed. Rio de Janeiro: Renovar, 2008.

BOBBIO, Norberto. *O futuro da democracia*. São Paulo: Paz e Terra, 2000.

BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. *Tratamento de dados pessoais pelo poder público (guia orientativo)*. Brasília: jan. 2022. Available at: https://bit.ly/3gXPEBR. Accessed on: 2 Nov. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. *Nota Técnica nº 46/2022/CGF/ANPD*. Available at: https://bit.ly/3WN8ivW. Accessed on: 29 Dec. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. *Nota Técnica nº 92/2022/CGF/ANPD*. Available at: https://bit.ly/3DDNpeV. Accessed on: 3 Nov. 2022.

BRASIL. Controladoria-Geral da União. *Enunciado nº 4, de 10 de março de 2022*. Available at: https://bit.ly/3NwDkEW. Accessed on: 3 Nov. 2022.

BRASIL. Controladoria-Geral da União. *Nota Técnica nº 1136/2022/CGAT/DTC/STPC*. Available at: https://bit.ly/3Q46dJR. Accessed on: 29 Dec. 2022.

BRASIL. Ministério da Educação. *Política de privacidade do aplicativo ID Estudantil*. 2020. Available at: https://bit.ly/38FDG80. Accessed on: 18 Oct. 2022.

BRASIL. Presidência da República. *Mensagem de Veto nº 451, de 14 de agosto de 2018*. Available at: https://bit.ly/2N6fp0T. Accessed on: 14 Oct. 2022.

BRASIL. Presidência da República. *Mensagem de Veto nº 288, de 8 de julho de 2019*. Available at: https://bit.ly/2CkTYqE. Accessed on: 14 Oct. 2022.

BRASIL. Presidência da República. *Medida Provisória nº 959, de 29 de abril de 2020*. Exposição de Motivos nº 00168/2020. Available at: https://bit.ly/30RKHRb. Accessed on: 14 Oct. 2022.

BRASIL. Senado Federal. *Projeto de Lei nº 1.027/2020*. Available at: https:// bit.ly/2NfDoe1. Accessed on: 14 out. 2022.

BRASIL. Supremo Tribunal Federal. *Suspensão de Liminar nº 623*. Rel. min. Ares Britto. 10 jul. 2012.

BRASIL. Supremo Tribunal Federal. *Suspensão de Liminar nº 1.103*. Rel. min. Cármen Lúcia. 2 maio 2017.

BRASIL. Supremo Tribunal Federal. Mandado de Segurança nº 36.150. Rel. min. Roberto Barroso. 10 dez. 2018.

BRASIL. Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387. Rel. min. Rosa Weber. 24 abr. 2020.

BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 695. Manifestação do advogado-geral da União. 20 jun. 2020.

BRASIL. Supremo Tribunal Federal. Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental nº 695. Rel. min. Gilmar Mendes. 24 jun. 2020.

BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 695. Voto do relator, Ministro Gilmar Mendes. 15 set. 2022.

BRASIL. Tribunal de Contas da União. Acórdão nº 13842/2022. Relator ministro Augusto Nardes, TCU/Plenário, 21 jun. 2022. Available at: https://bit.ly/3MyEYFv. Accessed on: 15 out. 2022.

DIAS, Tatiana; MARTINS, Rafael. Documentos vazados mostram que Abin pediu ao Serpro dados e fotos de todas as CNHs do país. *The Intercept*, 6 jun. 2020. Available at: https://bit.ly/2B6uSvy. Accessed on: 2 Nov. 2022.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

LEMOS, Ronaldo. Privacidade vale também para governo. *Folha de S.Paulo*, 16 abr. 2018. Available at: https://bit.ly/2NcpvwV. Accessed on: 14 Oct. 2022.

MARIZ, Renata. MEC quer acessar dados sigilosos de alunos para emitir nova carteirinha estudantil. *O Globo*, 16 maio 2019. Available at: https://glo.bo/2H1Odgu. Accessed on: 18 Oct. 2022.

MACHADO, Jorge; BIONI, Bruno. A proteção de dados pessoais nos programas de Nota Fiscal: um estudo de caso do 'Nota Fiscal Paulista'. *Liinc em Revista*, Rio de Janeiro, v. 12, n. 2, p. 350-364, nov. 2016.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECO NÔMICO. *Vectors of digital transformation.* OECD Digital Economy Papers, n. 273, Jan. 2019. Available at: https://bit.ly/3fDfbQx. Accessed on: 6 Nov. 2022.

PALACIOS Y OLIVARES, Guillermo. Revoltas camponesas no Brasil escravista: a "Guerra dos Marimbondos" (Pernambuco, 1851-1852). *Almanack Braziliense*, n. 3, p. 9-39, maio 2006. Available at: https://bit.ly/3TG0Zow. Accessed on: 23 Oct. 2022.

RICHARDS, Neil. *Why privacy matters*. Nova York: Oxford University Press, 2022.

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

SOLOVE, Daniel. The myth of the privacy paradox. *The George Washington Law Review*, v. 89, n. 1, p. 1-51, jan. 2021. Available at: https://bit.ly/3FMNCyR. Accessed on: 5 Nov. 2022.

SOPRANA, Paula. Governo quer lei de proteção de dados que tira responsabilidade do Poder Público. *O Globo*, 11 abr. 2018. Available at: https://glo.bo/3d75ym1. Accessed on: 14 Oct. 2022.

URUPÁ, Marcos. Congresso derruba vetos na LGPD. *Teletime*, 25 set. 2019. Available at: https://bit.ly/3rXjlFy. Accessed on: 14 Oct. 2022.

VARGAS LLOSA, Mario. *A guerra do fim do mundo*. Rio de Janeiro: Alfaguara, 2008.

VÉLIZ, Carissa. *Privacy is power*: why and how you should take back control of your data. Londres: Corgi Books, 2021.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: MENDES, L.; DONEDA, D.; SARLET, I.; RODRIGUES JR., O. (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 271-288.

ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. Nova York: Public Affairs, 2019.