The right to personal data protection in Brazil: The formation of a new fundamental right

Rodrigo Brandão

Abstract: This article describes the path taken to recognize personal data protection as an autonomous fundamental right in Brazil. It begins by analyzing how the Brazilian Constitution of 1988, in response to the indiscriminate processing of personal data by information agencies during the military regime, particularly safeguarded privacy. This protection was manifested through creating a legal remedy (habeas data), which was later replicated in other Latin American countries. However, the initial optimism was frustrated by the limited effectiveness of habeas data and a restrictive jurisprudence that confined privacy to protecting intimate and communication-flow data. The scenario begins to change in the second decade of the 21st century, with Brazilian jurists recognizing the fundamental right to data protection. Subsequently, the Supreme Federal Court's jurisprudence and a constitutional amendment formally incorporated it into the catalog of fundamental rights, reinforcing its effectiveness: safeguarding its core in the face of not only ordinary laws but also constitutional amendments, immediate applicability irrespective of legislative regulation, and prima facie priority when conflicting with other constitutional principles. Despite these advancements, Brazilian law still has a long way to go to define the essential aspects of the fundamental right to personal data protection, particularly delineating its scope, subjective and objective dimensions, and parameters for conflict resolution with other fundamental rights.

A. Privacy protection in the 1988 Constitution: frustrated optimism

The 1988 Brazilian Federal Constitution contains several provisions to safeguard different aspects of private life. The central provision is Article 5, Section X: "The intimacy, private life, honor, and image of individuals are inviolable, ensuring the right to compensation for material or moral damage resulting from their violation." Additionally, the Brazilian constitu-

tional tradition, initiated in the imperial Constitution of 1824[1] to protect the inviolability of the home[2] and the confidentiality of communications,[3] has been maintained.

A highly relevant innovation was the creation of habeas data, a procedural instrument designed for issues related to public databases containing personal information.[4] Some authors have derived a corresponding substantive right to access and rectify personal data from this new legal action.[5]

This was a clear response from the 1988 Brazilian Constitution to the use of personal information by the Brazilian military regime's security agencies, revealing its concern with the risks posed by public entities' broad processing of personal data.[6] This innovation had a notable influence in Latin America, given the typical scenario of overcoming military dictatorships where similar abuses were committed by "information communities."[7][8]

Despite the 1988 Constitution's favorable stance on privacy, a restrictive position regarding its scope initially prevailed, particularly concerning protecting personal data. Notably, the previous constitutional order's restrictive

---

1 Article 179.

2 Article 5º, XI, Brazilian Federal Constitution, 1988.

3 Article 5º, XII, Brazilian Federal Constitution, 1988.

4 Article 5º, LXXII, Brazilian Federal Constitution, 1988.

5 PERTENCE, Sepúlveda. Dois instrumentos de garantia de direitos: habeas corpus, ação popular, direito de petição, mandado de segurança individual e coletivo, mandato de injunção e habeas data. Seminário sobre Direito Constitucional. Série Cadernos do CEJ. Brasília: Conselho da Justiça Federal, 1992, p. 54.

6 Luís Roberto Barroso argues that these entities have become involved in ordinary politics, delving "into a murky terrain of persecutions against adversaries, often operating on the fringes of marginality." He asserts that "the community of information has become a parallel and aggressive power, which, at times, surpasses institutional political power, resorting to illicit means for condemnable ends." BARROSO, Luís Roberto. A viagem redonda: habeas data, direitos constitucionais e provas ilícitas. In: WAMBIER, Teresa Arruda Alvim (coord.). Habeas Data. São Paulo: Ed. RT, 1998.

7 It is the case, for example, in Colombia, Paraguay, Peru, Argentina, Ecuador, Venezuela, and Chile.

8 Before the 1988 Constitution, the states of Rio de Janeiro and São Paulo had advanced laws on the subject, as they provided for the right to access and rectify personal data, the linking to specific purposes, and the requirement of informed consent. Clémerson Merlin Cléve attributes to José Afonso da Silva the proposal for creating habeas data, which was already part of the draft Constitution prepared by the Afonso Arinos Commission. In this, the proposal was innovative, as it provided for a material right to the protection of personal data not only with the prerogatives of access and rectification but also with the prohibition of storing information about "political activities and private life." CLÈVE, Clèmerson Merlin. Habeas data: some reading notes. Habeas Data. WAMBIER, Teresa Arruda Alvim (ed.). Habeas Data. São Paulo: RT, 1998, p. 75.

orientation was maintained, indicating that obtaining personal information would be guided by the secrecy/access dichotomy, and the guarantee of secrecy would depend essentially on the connection of personal data to intimate issues.[9] Data related to specific individuals but not linked to their private lives would not be covered by constitutional protection.[10]

Also, only data in the flow of communication, not stored data, would be subject to protection. This position prevailed in the Brazilian Supreme Federal Court (STF) in the judgment of RE n. 418416-8/SC[11] when its rapporteur, Justice Sepúlveda Pertence, stated that Article 5, Section XII, of the 1988 Constitution, by explicitly referring to the "secrecy of telegraphic communications data" linked the terms "communications" and "data" in a way that protected only the secrecy of data in transit, not the data itself.[12][13]

---

9 DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados. 3. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 269.

10 STF (Supreme Federal Court), Full Bench, Case No. 418416-8/SC, Rapporteur Justice Sepúlveda Pertence, judgment on May 10, 2006. Indeed, the explicit codification of the fundamental rights to privacy and private life led to the interpretation that intimate information would be subject to legal protection, but not other information related to specific individuals. Thus, the possibility of third-party use of such information depended on its content, that is, its connection to privacy. Furthermore, the protection of privacy was essentially achieved through secrecy, i.e., the prohibition of third parties capturing and using such information rather than regulating the terms under which its processing would be permissible.

11 It was an extraordinary appeal filed against the judgment of the Santa Catarina Court of Justice that upheld the criminal conviction under Article 203 of the Penal Code: "to frustrate, through fraud or violence, a right secured by labor legislation.".

12 The theoretical foundation relied upon the influential article by Tércio Sampaio Ferraz Jr., who, in summary, considered that the term "data" referred to in Article 5, XIII, should be interpreted as "computer data," in line with the proposal of Manoel Gonçalves Ferreira Filho based on the premise that it was an innovation of the 1988 Constitution prompted by the evolution of information technology. Thus, confidentiality would be linked "to communication, in the interest of privacy," as confirmed by the literal wording of the provision, establishing a connection between the terms "data" and "communications." Therefore, "what violates the freedom to withhold thought is entering into someone else's communication, causing what should stay between private subjects to pass into the domain of a third party legitimately. FERRAZ JR., Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Cadernos de Direito Constitucional e Ciência Política. Rt 1/77, 82. The article was also published in the Revista da Faculdade de Direito da Universidade de São Paulo, vol. 88, pp. 447, 1993.".

13 This guidance was reiterated, among others, in the case HC 91867/PA, where the legality of the conduct of police officers who, during the defendant's arrest on the spot, seized mobile phones and analyzed call records was being examined. It was found that the data on phone calls did not connect with "any constitutionally protect-

There is no doubt that the secrecy of intimate information and communication of personal data is an element that composes the scope of protection of the rights to privacy and confidentiality of communications. However, due to individuals being recognized in various spheres through profiles created from the collection and automated processing of their data, it seems clear that denying constitutional protection to personal data in general (including those stored or not directly related to intimate matters) poses severe risks to the free development of personality and, consequently, to the principle of human dignity in its autonomy aspect.

Another frustration occurred with the limited practical effectiveness of habeas data, contrasting with its symbolic impact beyond national borders. Several factors led to this result: first, the emphasis on the procedural aspect (creating a new constitutional action) and silence on the material dimension (subjective right to access and rectify personal data) must meet contemporary needs in addressing the issue. Second, the need for prior administrative requests and the cautious acceptance of the new institute by the courts, among other factors, significantly limited its effectiveness even for its typical purposes (access and rectification of personal information in public databases), let alone addressing contemporary challenges in the information society.

B. The beginning of the recognition in legal doctrine of the fundamental right to personal data protection

In international treaties and national constitutions, the express recognition of an autonomous fundamental right to personal data protection is still in its early stages. In this regard, Ingo Sarlet points out that "there is no express provision for a corresponding human right in the UN international system, as well as in the European and Inter-American Conventions, so that, for now, it is only possible to deduce such a right as implicitly enshrined through the work of the judicial bodies that oversee the interpretation/ap-

ed value," being a "mere numerical combination (that) in itself means nothing, just a phone number." Furthermore, following the cited precedent, it was stated that "the clause in Article 5, XII, of the Constitution cannot be interpreted to protect data as a record, registry deposit. Constitutional protection is for the communication 'of data' and not the 'data.'" Supreme Federal Court (STF), 2nd Panel, HC 91867/PA, Rapporteur Justice Gilmar Mendes, judgment on April 24, 2012, rapporteur's vote p. 9.

plication of treaties, which, by the way, still occurs to a large extent in the case of constitutions."[14]

In Brazilian law, even before Constitutional Amendment (EC) No. 115/2022 and paradigmatic judgments of the Supreme Federal Court (STF), some authors had already spoken in favor of the autonomy of the right to personal data protection about privacy. For example, Ingo Sarlet emphasizes that the scope of protection of the former is broader than that of the latter, as it would encompass all data that allows the identification of a specific person. Furthermore, he recognizes it as a materially fundamental right because "it does not pose a greater difficulty in demonstrating its relevance to the individual sphere of each person and to the collective interest (of organized society and the State), of the values, principles, and fundamental rights associated with the protection of personal data and protected by it. In this sense, he highlights, among others, the principle of human dignity, the right to free development of personality, and the right to privacy."[15]

In the same vein, Laura Schertel Mendes notes that, given the extensive protection of personality and private life, it makes no sense to exclude the protection of personal data from its scope, as nowadays privacy is much more at risk due to the massive and automated collection of personal data than by "traditional methods," such as paparazzi and sensationalist newspapers.[16]

As early as 2011, Regina Linden Ruaro, Daniel Piñeiro Rodriguez, and Brunize Finger advocated for the autonomy of the right to data protection, arguing that privacy had emphasized "exclusively individual protection

14 SARLET, Ingo. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, LAURA Shertel; DONEDA, Danilo; SARLET, Ingo; RODRIGUES JR., Otávio Luiz (org), Coordenador Executivo BIONI, Bruno. Tratado de Proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 26.

15 SARLET, Ingo. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, LAURA Shertel; DONEDA, Danilo; SARLET, Ingo; RODRIGUES JR., Otávio Luiz (org), Coordenador Executivo BIONI, Bruno. Tratado de Proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 28/9.

16 MENDES, Laura Shertel: Habeas Data e autodeterminação informativa: os dois lados de uma mesma moeda. In: MENDES, Laura Shertel; ALVES, Sérgio Garcia; DONEDA, Danilo. Internet e Regulação. São Paulo: Saraiva, 2021, p. 309.

instruments," while advances in data processing make it imperative to enhance the State's duties to protect the individual.[17]

These doctrinal contributions were crucial for the Supreme Federal Court to begin recognizing that, even before being formally enshrined in the 1988 Constitution, protecting personal data already constituted an implicit fundamental right autonomous about privacy.

C. New perspectives in the jurisprudence of the Supreme Federal Court

The beginning of a new phase in the jurisprudence of the Supreme Federal Court (STF), more attuned to contemporary needs in personal data protection, can be considered with the judgment of RE No. 673,707. It originated as a habeas data filed to ensure access to information from the Corporate Checking Account System of the Federal Revenue Service (SINCOR).[18] On this occasion, the Brazilian Supreme Court overturned the decision of the 1st Region Federal Court of Appeals, which had denied the existence of a duty for the Federal Revenue to provide "complex, burdensome, and general information from a non-public registry. "Instead, the STF considered that taxpayers have the right to access information stored in a database managed by the Federal Revenue to preserve "the status of their name, business planning, investment strategy, and especially the recovery of wrongly paid taxes."

Beyond the result itself, it is noteworthy that the rapporteur defined the habeas data's object broadly, based on an equally comprehensive concept of databases, "understood in its broadest sense, encompassing everything related to the interested party, whether directly or indirectly." Thus, it aligned with the concept of personal data as any information referring to a specific individual. Moreover, Justice Gilmar Mendes envisioned the possibility of the case becoming "the starting point for a revitalization of habeas data

17 RUARO, Regina Linden, RODRIGUEZ, Daniel Piñeiro, FINGER, Brunize. O Direito à Proteção de Dados e a Privacidade. Revista da Faculdade de Direito - UFPR, Curitiba, n. 53, p. 45/67, 2011, p. 10.

18 Supreme Federal Court (STF), Full Bench, Appeal Number: RE 673,707, Rapporteur: Justice Luiz Fux, Date of Judgment: June 17, 2015. Publication: DJe (Electronic Justice Diary) on September 30, 2015.

in a broader perception, beyond procedural issues, turning towards the recognition of a fundamental right to informational self-determination."[19]

This new phase was consolidated with the paradigmatic judgment of ADIs 6387, 6388, 6390, and 6393,[20] in which the interim decision of the rapporteur, Justice Rosa Weber, was endorsed by the majority of STF members to suspend the effectiveness of Provisional Measure No. 954/2020.

According to Article 2: "telecommunications companies providing Fixed Switched Telephone Service (STFC) and Personal Mobile Service (SMP) must make available to IBGE, electronically, the list of names, telephone numbers, and addresses of their consumers, individuals or legal entities." This provision mandated telecommunications companies to provide a pervasive set of data about their service users to the Brazilian Institute of Geography and Statistics (IBGE), "for the official statistical production, to conduct non-face-to-face interviews within the scope of household surveys" (Article 2, § 2).

Despite the formal limitations of the provisional measure,[21] Justice Rosa Weber considered that "such information, related to the identification – actual or potential – of a natural person, constitutes personal data and, in this measure, falls within the scope of protection of constitutional clauses ensuring individual freedom (Article 5, caput), privacy, and the free development of personality (Article 5, X and XII). Its manipulation and treatment, therefore, must observe, at the risk of harm to these rights, the limits outlined by constitutional protection. Derivatives of the rights of personality, respect

19 In this context, as Laura Schertel Mendes aptly pointed out, "if the Constitution provides habeas data as a procedural guarantee available to the individual to access or correct data concerning them, it is logical to assume that there is a substantive right supporting this procedural guarantee: the fundamental right to data protection or the right to informational self-determination, to use the terminology of German law." MENDES, Laura Shertel: Habeas Data e autodeterminação informativa: os dois lados de uma mesma moeda. In: MENDES, Laura Shertel; ALVES, Sérgio Garcia; DONEDA, Danilo. Internet e Regulação. São Paulo: Saraiva, 2021, p. 305.

20 "Supreme Federal Court (STF), Full Court, Rapporteur Justice Rosa Weber, Judgment on May 7, 2020."

21 Article 3 aimed to establish limitations on the use of such data, safeguarding its confidential nature (i), its connection to the purpose above (ii), the prohibition of its use as evidence in administrative, fiscal, or judicial proceedings (iii), its availability to other public entities (§ 1), and, after its use, the obligation to disclose the situations in which the data were used and a report on the impact on the protection of personal data (§ 2). On the other hand, Article 4 provided that once the emergency situation resulting from the coronavirus pandemic was overcome, the information would be eliminated.

for privacy, and informational self-determination were stated in Articles 2, I, and II of Law No. 13,709/2018 (General Data Protection Law) as specific foundations of personal data protection regulation."

Justice Luís Roberto Barroso stated that the case involved a typical case of balancing constitutional principles: on one side, statistics as a tool aimed at providing reliable data for the conception and implementation of public policies; on the other side, privacy, "which is the right that every person has to have an area of their life that is not accessible, either to the State or to other people, except, possibly, by their own will."

He emphasized initially that objective and reliable data are essential for the development of public policies by the state and for economic growth (given that valuable contemporary companies mainly have data processing as their primary asset). Although the "internet industrial revolution" with the notable expansion of capturing and processing personal data, has provided "great advantages," especially in communication, it has also brought "serious risks and threats," such as disinformation campaigns, defamation, hate speech, deepfakes, robotized digital militias, hacking, misuse of data for political purposes, etc.

Despite assigning enormous importance to data, he considered that, since the provisional measure did not provide security elements regarding the precautions for its sharing and there was no prior debate about what those measures would be, there was a significant risk of misappropriation of this data, leading to privacy damage.

In his significant vote, Justice Gilmar Mendes also advocated for the autonomy of the fundamental right to protect personal data. In his words: "The affirmation of the autonomy of the fundamental right to the protection of personal data - it must be said - is not contingent on mere theoretical enchantment but rather on the inescapable need to assert fundamental rights in contemporary democratic societies. It also recognizes the dual dimension of this right because it involves, from a subjective perspective, the protection of the individual against the risks that threaten their personality in the face of the collection, processing, use, and circulation of personal data, and, from an objective perspective, the attribution to the individual of the guarantee to control the flow of their data."

Similarly, Justice Luiz Fux acknowledged that "the protection of personal data and informational self-determination are autonomous fundamental rights, which involve specific legal protection and scope of application. These rights are derived from the integrated interpretation of the guarantee of the inviolability of intimacy and private life (Article 5, X), the principle

of human dignity (Article 1, III), and the procedural guarantee of habeas data (Article 5, LXXII), all provided for in the 1988 Federal Constitution."

The decision is relevant for several reasons, notably the recognition of the right to informational self-determination due to individual freedom, privacy, and the free development of personality. Additionally, the Court stated that the Head of the Executive Branch needed to demonstrate that the measure would be necessary to protect a legitimate public interest, not even providing minimal clarification on how and for what purpose this massive amount of data would be used.

Despite formally establishing its "secrecy" and prohibiting sharing with other public agencies, it "does not present technical or administrative mechanisms capable of protecting personal data from unauthorized access, accidental leaks, or misuse," failing to adequately protect the mentioned fundamental rights, which were aggravated by the non-enforcement of the General Data Protection Law (LGPD) at the time.

Finally, note that the inherent exceptionality of the pandemic raised debates about the relativization of privacy standards.[22] The Supreme Court's decision, by rejecting the generic argument of the "state of sanitary exception" and by requiring concrete measures to safeguard the right to personal data protection, demonstrated faithful compliance with its role as the guardian of fundamental rights, which is especially important and challenging in crisis contexts such as the COVID-19 pandemic.

D. The Material and Formal Foundations of the Fundamental Right to Data Protection

On February 10, 2022, the National Congress approved Constitutional Amendment Project (PEC) No. 17/2019, which became Constitutional Amendment (EC) No. 115/2022, as follows:

> "Art. 1 The twelfth item of article 5 of the Federal Constitution shall be amended to read as follows:
> 'Article 5 (...)
> XII – the confidentiality of correspondence and telegraphic, data, and telephone communications is inviolable, except, in the latter case, by judicial order, in the situations and the manner established by law for

22 VÉLIZ, Carissa. Privacidade é poder: por que e como você deveria retomar o controle de seus dados. 1. ed. São Paulo: Editora Contracorrente, 2021, p. 74/5.

criminal investigation or criminal procedural instruction, as well as the right to the protection of personal data, including in digital media.'
Art. 2 The heading of article 22 of the Federal Constitution shall be amended to include the following item XXX:
'Article 22 (...) XXX – **protection and processing of personal data**.' (Emphasis added) [23] "

The constitutional amendment, besides granting exclusive competence to the Federal Union to legislate on 'the protection and processing of personal data,' included the right to the protection of personal data in the list of Article 5 of the Brazilian Constitution, which contains the list of fundamental rights. There is no doubt that it is formally a fundamental right in Brazil. This innovation is essential to bring certainty to the application of the constitutional effectiveness inherent in the legal regime of fundamental rights to the protection of personal data, even though the doctrinal and jurisprudential orientation presented in the previous topics, which considered it a material fundamental right, seems correct.

Indeed, Article 5, paragraph 2 of the Brazilian Constitution contains an opening clause in the constitutional catalog of fundamental rights, as it recognizes the material fundamentality of other rights 'arising from the regime and principles adopted by it or from international treaties in which the Federative Republic of Brazil is a party.' Despite doctrinal controversies about the substantive requirement for identifying these 'other rights,' the right to personal data protection fulfills the main criteria, especially the constitutional relevance of its content to the community. It cannot be entirely left to regulation by the ordinary legislator,[24] and its indispensability for protecting the dignity of the human person is evident.[25] This is crucial in the face of the relevance of protecting personal data for individual autonomy against oppressive measures by public and private entities.

Therefore, its material fundamentality seems clear. This conclusion is reinforced when analyzing the concern of the 1988 constituent in safeguarding privacy (Article 5, X), particularly personal data in public databases, with the provision of habeas data in Article 5, LXXII. Furthermore, recog-

23 SARLET, Ingo Wolfgang. A Eficácia dos Direitos Fundamentais. 9. ed. Porto Alegre: Livraria do Advogado, 2009, p. 90/156.
24 ALEXY, Robert. Teoría de los derechos fundamentales. Madrid: Centro de Estudios Constitucionales. 1997.
25 ANDRADE, José Carlos Vieira. Os direitos fundamentais na constituição portuguesa de 1976. 2. ed. Coimbra: Almedina, 2001.

nizing the autonomy of this right concerning privacy is significant in the current context of the information society.[26] There is no doubt about the proximity between these rights and overlapping areas in their scopes, which is common when dealing with fundamental rights.

This is evident not only in cases of access and processing of sensitive personal data (e.g., philosophical and religious beliefs, health, sexual orientation etc.), but also in cases of personal data that, although not initially exposing the private life of the holder (civil identification document, profession, marital status etc.), when processed extensively by artificial intelligence tools to create 'profiles' of their holders,[27] captured by internet usage surveillance tools, and used for purposes other than those that led to their capture, may raise excessive exposure of the individual's private life.

The image of continuous monitoring of the individual - at home by voice assistants, computers, and 'smart' appliances, and on the street by cameras, sensors, and Wi-Fi networks - highlights the privacy risks. The formation of these digital profiles or 'digital dossiers' and the circumstance of the natural person being somewhat hostage or stigmatized by a kind of 'digital biography' indicates that the right to know and rectify personal data in these databases is more directly connected to the general clause of personality protection and the dignity of the human person as autonomy than to privacy. It aims to safeguard the person's ability to make free decisions. It does not seek to protect the secrecy of intimate information but only the accuracy of personal data processed in an automated manner.

On this point, Stefano Rodotà clarifies that privacy traditionally has been attributed a negative and static dimension, guided by the possibility of the holder denying third parties' access to intimate information. The right to personal data protection does not follow this logic of secrecy, as it recognizes the possibility of third-party collection and processing of personal data, providing, however, powers to the data subject to ensure control measures over these activities.[28]

---

26 Manuel Castells argues that contemporary society is characterized by "a new informational mode of development, in which the source of productivity lies in knowledge generation technology, and information and knowledge are the central actors in economic production." CASTELLS, Manuel. A sociedade em rede. 3. ed. São Paulo: Paz e Terra, 2000.

27 SOLOVE, Daniel. The Digital Person: technology and privacy in the informational age. New York: New York University Press, 2004, p. 3.

28 RODOTÁ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. (org. Maria Celina Bodin de Moraes). Rio de Janeiro: Renovar, 2008.

Thus, although it has close connections with privacy, the right to protect personal data plays autonomous and relevant roles in the current information society. The perception of how the formation of digital profiles implies the 'categorization of people' that radically conditions their economic and existential opportunities indicates that the massive collection of personal data can lead to a 'data dictatorship,'[29] diminishing individual freedom. Damages can also be caused by equality, as algorithms may reproduce biases of those who conceived them, further reduce opportunities for disadvantaged groups, and promote arbitrary distinctions between people.

The Chinese social credit system is an example of how indiscriminate data collection can be oppressive to citizens. It involves using big data for the massive collection of personal data, and its application to all areas of life, guided by moral standards of credibility. As Carissa Vèlez explains, 'Good actions earn you points, and bad actions make you lose points. Buying diapers earns you points. Playing video games, buying alcohol, or spreading fake news makes you lose points.'[30] The significant repercussions in the lives of citizens - advantages or disadvantages in waiting lists, prices of public and private services, access to work and credit, have even led to the prohibition of millions of Chinese citizens buying air and high-speed train tickets and the installation of cameras at home doors for the government to check if people complied with quarantine during the pandemic - make evident the risk to individual freedom.

The protection of freedoms presupposes a certain degree of ignorance about human behaviour. This draconian scenario of authoritarian regimes helps make even more evident the risks generated by the massive collection of data for categorizing people based on digital profiles, even in democratic societies. This phenomenon can restrict access to relevant economic and existential opportunities and establish unreasonable discriminations between people based on mechanisms that are not transparent outside public and private entities that collect and process them (or their respective agents with powers of command over such activities).

The exponential development of these technological mechanisms for collecting and processing personal data and the multiple economic and political uses that technological evolution has allowed have made information,

29 MAYER, Jonathan; NARAYANAN, Arvind. Do not track universal web tracking opt-out. IAB Internet Privacy Workshop Position Paper, Nov. 2010.

30 VÉLIZ, Carissa. Privacidade é poder: por que e como você deveria retomar o controle de seus dados. 1. ed. São Paulo: Editora Contracorrente, 2021, p. 87.

which has always represented a source of power and wealth, the main asset of contemporary societies. In this context, the affirmation of a fundamental right to the protection of data, autonomous concerning privacy, freedom, and other fundamental rights, fulfills the notable function of making any activity of collecting and processing personal data a restriction to the respective fundamental right, raising the need for special justification in the light of its reinforced constitutional effectiveness.

As in other countries, particularly in the European context, the 'recognition' of this new fundamental right in Brazil was the result of a rich contribution between members of civil society, law professors, and judges who paved the way for its subsequent recognition by the legislator (in the Brazilian case, by a constitutional amendment, which positively distinguished our experience by formally linking the protection of this right to the constitutional sphere and the reinforced effectiveness of fundamental rights).

The power of public and private entities benefiting from the massive use of personal data, the lack of transparency in data collection and processing methods, and the high political and economic value of this data in today's information society reveal that recognizing the formal and material foundations of the right to data protection, while crucial, is only the first step on a challenging path.

It will be the task of Brazilian legal doctrine to develop the scope of protection, the subjective and objective dimensions, and the horizontal effectiveness of this fundamental right, among other elements inherent in the grammar of fundamental rights. Courts, particularly the Supreme Federal Court, will face complex issues regarding its practical application, revealing a tension between, on one side, public and private entities interested in the massive processing of personal data for various purposes (national security, efficiency in providing public services, creating new businesses, profit, etc.), and on the other, individuals (and public and private actors supporting their cause) interested in preserving some control over the management and use of their data.

Striking a balance between protecting human dignity, freedom, equality, and transparency in data management in the face of free enterprise, economic development, and preserving trade secrets will take a lot of work. This challenge is also felt by lawmakers, as evidenced by the approval of laws such as “Lei Geral De Proteção de Dados” (LGPD, Law No. 13.709/2018, our General Data Protection Law) and the intense debates in the National Congress on combating misinformation and hate speech on the internet

and regulating artificial intelligence. Although challenging, this is a doctrinal, jurisprudential, and legislative agenda and an essential political debate for preserving human dignity in the face of the challenges posed in Brazil by the overwhelming pace of digitization in the 21st century.