Revista ARACÊ
ISSN: 2358-2472

BRAZILIAN LEGAL MICROSYSTEM FOR THE "PROTECTION" OF PERSONAL DATA: A SUPPOSED EFFECTIVE GUARANTEE OF PRIVATE OWNERSHIP OF ONE'S OWN PERSONAL DATA

https://doi.org/10.56238/arev7n3-045

Submitted on: 02/07/2025 **Publication date:** 03/07/2025

Cleuler Barbosa das Neves[1] and Gisele Gomes Matos[2].

ABSTRACT

From a philosophical and historical reflection on privacy, adopting as an initial theoretical framework the formulations of Yuval Harari on the impacts of biotechnology and artificial intelligence, and as a legal framework the conceptualization of ownership proposed by Roberta Maia, using the dialectical-argumentative method, this article critically addresses the supposed effectiveness of the General Law for the Protection of Personal Data (LGPD) in Brazil regarding the guarantee of private ownership of personal data. From the literature review and the analysis of recent judgments, it was found that, although the LGPD proposes to protect the fundamental rights of freedom and privacy and the free development of the personality of the natural person, the achievement of this objective encounters significant obstacles even in the face of the constitutional recognition of the protection of personal data as a fundamental right (EC No. 115/2022). The results point to a relativization of the private ownership of personal data by exceptions and open concepts that confer greater power and discretion to the processing agents (controllers and operators), so that the expressiveness of the hypotheses of waiver of the consent of the data subject and the recurrent appeal to open concepts, such as "legitimate interest" and "legitimate purposes", are presented as an inversion of the protective paradigm. In the aforementioned cases of concrete application of the LGPD, the scenario reveals a tendency to shift a role theoretically directed to the holder of personal data, to economic agents, public and private, responsible for the processing of personal data. This finding reinforces the need to improve regulation and an effective supervisory and protective performance by the National Data Protection Authority (ANPD). Therefore, a more substantial balance is proposed between economic interests and the protection of the fundamental rights of the holders for the realization of the constitutional promise of primacy of the dignity of the human person to the detriment of a logic of the commodification of personal data and the submission of its holder to the condition of being a response in trade.

Keywords: General Data Protection Law. Constitutional principle protection. ADI 6.387. Functionalization of German Law. Legal nature.

[1] Dr. in Environmental Sciences
Institution: Federal University of Goiás (UFG)
Address: Goiânia - Goiás, Brazil
PPGDP/UFG productivity scholarship holder.
E-mail: cleuler@gmail.com
ORCID: https://orcid.org/0000-0001-8319-0257
Lattes: http://lattes.cnpq.br/3567330317986829
[2] Dr. in Law
Institution: University Center of Brasília (UNICEUB)
Address: Brasília - Distrito Federal, Brazil
Email: matosgisa@gmail.com
ORCID: https://orcid.org/0000-0001-7898-0473
Lattes: http://lattes.cnpq.br/0354770450063235

Revista ARACÊ
ISSN: 2358-2472

INTRODUCTION

Along with the "wonders" of the information society, there has been a belated concern with the problem of privacy, in the face of the collection, processing, storage, exploitation and disposal of personal data on such a scale that involves astronomical economic values, due to the large-scale application of processing to gigantic masses of personal data. As a result, the risk of violations of human rights is amplified (Rodotà, 2008, p. 6-7).

In this context of global expansion of the internet, which has metamorphosed ten times while a clumsy government bureaucracy has been buried by data (Harari, 2016, p. 327), the regulation of the "protection" of personal data by the General Data Protection Law (LGPD) emerged in Brazil, Law No. 13,709, of August 14, 2018), which, together with the Federal Constitution of 1988 (CF/1988), forms the Brazilian normative mainstay to respond to more than urgent social demands.

Later, in the context of the pandemic caused by Covid-19, Yuval Noah Harari (2020, p. 1) pondered on the risk of violations of human rights, warning that it is greater for modern Democratic States of Law, due to the power held by institutions, whether public or private, capable of monitoring everyone and at all times, by "ubiquitous sensors and powerful algorithms" used to "track, monitor and manipulate people", in addition to taking over citizens' data, in what he calls a dramatic transition in history from over-the-skin surveillance to under-the-skin surveillance.

In this scenario of a new oil mined in the clouds (Maia, 2019), one cannot disregard the need to ascertain who are the exploited (hyposufficient), the exploiters (hypersufficient) and what are the rights and obligations of both parties, which deserve more protection and vigilance by the State, whose presence is claimed whenever an environment of overexploitation or vulnerability is noticed, especially when it is a virtual, intangible environment, but whose effects jeopardize the foundation of the democracies themselves, built at the cost of so much effort by humanity.

Thus, the normative microsystem of the LGPD is taken as the object of research from a critical approach to the great pragmatic challenge on how to regulate the ownership of personal data in order to safeguard the Brazilian Democratic Rule of Law for the present and future generations, which is presented as "[...] a reality fragmented by the plurality of autonomous statutes" (Tepedino, 2000, p. 5), in a process of frank nomogenesis (Reale, 1996, p. 550-555), which needs to be better identified and investigated, in order to better

Revista ARACÊ
ISSN: 2358-2472

diagnose the current phenomenon of the reification of personal data (Honneth, 2018; Martins, 1998) and to position the country before the great pragmatic challenge of how to regulate the ownership of personal data in order to safeguard its Democratic Rule of Law for the present and future generations.

In view of this, this article has been structured in five topics.

Initially, concepts specific to the LGPD are operationalized, aiming at logical constructs through the conceptual articulation twinned by the legal microsystem of the "protection" of personal data and its articulation with concrete cases of judgments submitted to the scrutiny of the Judiciary.

Through a literature review, the debate on the state of the art in the constitutional, civil and criminal spheres and criminal procedure is addressed. Considering the general rule of private ownership of personal data, it is proposed to expand the list of constitutional principles and consider the legal recourse to open concepts and their implications that potentially limit the protection and guarantee of the personal freedoms of the holders of personal data.

In the context of the recognition of the fundamental right to personal data in Brazil, topic 4 addresses formal aspects of the cases judged by the STF (ADI 6.387 and related) and the contours of this recognition, with the presentation of four cases submitted to the scrutiny of the Judiciary (on the leakage of personal data by Facebook; Sincor and access by the taxpayer; Coaf and the sharing of data and information; and the collection of data and information by health operators and the genetic heritage of the users who hold their personal data), with the demonstration of the institutional variability that permeates the judgments of cases of violations of the right to the protection of personal data.

In topic 5, the functionalization of German Law is presented as a reference for limiting the collection and processing of personal data, addressing the paradigmatic German Census Law of 1983, articulating it with the judgment of ADI 6.387 and related, which gave rise to the recognition of the fundamental right to personal data.

In the last topic, the explanation about the legal nature of the right to the protection of personal data takes place from three perspectives: whether it is a real, obligatory or existential right; And from them, the extensiveness of the right to private property to the ownership of personal data is addressed as consistent with the expansion of constitutional protection to the holder of personal data, hyposufficient in the face of the mining, processing and exploitation of their personal data.

Revista ARACÊ
ISSN: 2358-2472

OPERATIONALIZATION OF LGPD CONCEPTS

HOLDER AND HIS "PROTAGONISM"

As a theoretical philosophical framework, the reflection promoted by Harari (2018, p. 107-111) regarding the rapid and profound impacts that the two main disruptive innovations already verified in the fields of biotechnology and information technology (development of Artificial Intelligences – AIs) are promoting in the way we already live in the twenty-first century was adopted.

A first outline for the urgent reflexive question is outlined by Harari (2018, p. 110) when he problematizes whether the ownership/ownership of data should be public or private: "[t]he private ownership of one's own data sounds more attractive than any of these options, but it is not clear what this means". Thus, the main dilemma presented by the philosopher is how to regulate the ownership/ownership of one's own data: private or public?

This author suggests starting from a historical-cultural point of view, by researching the millennial experience with the legal institute of real estate (or even movable property) and the last two centuries of experience with intangible property (trademarks, patents, industrial designs and utility models; non-transgenic and transgenic cultivars), to face the pragmatic challenge of how to regulate the private ownership/ownership of one's own data. This is because there is not much experience (Harari, 2018, p. 110) on the subject, related to a current phenomenon that continues at an increasingly accelerated technological pace of expansion.

Faced with the risks of submitting to a ruler who, despite having been elected, implements a centralizing regime guided by anti-democratic and even dictatorial practices (Levitsky; Ziblatt, 2018), the philosopher prefers that this property be private.

It does not, however, point out how it should be, evoking, as alluded to, the millennial historical-cultural experience of the regulation of private real estate property and also the most recent, since the beginning of modernity, the regulation of intangible property, as legitimate starting points for the construction of this necessary and urgent new model or mode of ownership/ownership over the data itself, especially those of the *under skin* type (terminology coined by Harari (2020) to designate a transition that he describes as dramatic, from surveillance on the skin, *over the skin*, to surveillance under *the skin*),[3]

[3] Unlike data collected by some form of registration – such as name, gender, height, weight, Individual Taxpayer Registration (CPF) number, address, registration of movable and immovable property, list of favorite movies or songs, etc. –, *under skin* data can contain information on body temperature, blood pressure, all medical imaging tests already performed (X-rays, ultrasounds, computed

Revista ARACÊ
ISSN: 2358-2472

given their high potential to result in the manipulation of the feelings and emotions of human people and the direction of their "choices".

The LGPD uses the titular denomination to characterize the "[...] natural person to whom the personal data that are the object of processing refers" (art. 5, V, Brazil, 2018a) and the notion of natural person is central to characterizing the data subject and its measurable attributes.

Maia (2020) clarifies that the use of the expression holder in the LGPD in relation to personal data, notably in its article 17,[4] would serve exactly to distinguish the subjective right of this individual as a genus of which the concept of owner is a species, since it is possible to be the holder of a right without necessarily being the owner (*propertization*) of an asset (material or immaterial), economically appreciable (Maia, 2019).

In fact, part of the doctrine considers the use of the term "owner" to qualify the natural person to whom the personal data subject to processing refers (article 5, V, of the LGPD), as it considers the proprietary perspective incompatible in matters that are directly linked to the dignity of the human person (Rodotà, 2008, p. 99 et seq. *apud* Souza; Silva, 2020, p. 253), in the name of an alleged and inappropriate reification of a right that, by its nature (*in re ipsa*), would be absolutely unavailable.

As mentioned, the questions proposed by Harari were adopted as a philosophical framework, while the meaning proposed by Roberta Maia is the one adopted as a theoretical framework, due to the existential regime of personal data protection, making the option for the use of the term ownership (corroborated, in topic 6, by the considerations about the legal nature of the right to personal data) while addressing, As a principled norm, the constitutional principle of private property as extendable to ownership, as well as its counterbalance established by the social function (topic 6.1).

Privacy and informational self-determination

In the historical understanding and evolution of the concept of privacy, despite the existence, in the American Supreme Court, of *older cases* (such as *Boyd v. United States*, from 1886, about the exposure of tax documents, and *Olmstead v. United*, from 1928, which involved a telephone interception), the reference work *The Right to Privacy* (Warren;

tomography, eye refraction) and even the genotype (DNA - Deoxyribonucleic Acid, the molecule that retains the hereditary genetic information of all living beings) and the phenotype (refers to the physical, morphological and behavioral characteristics).

[4] "Article 17. Every natural person is assured the ownership of his or her personal data and the fundamental rights of freedom, intimacy and privacy are guaranteed, under the terms of this Law." (Brazil, 2018a).

Revista ARACÊ
ISSN: 2358-2472

Brandeis, 1890), inserted in traditional modern legal theory and based on precedents of the *Common Law* tradition, allowed the establishment of a right to privacy of a personal nature, detached from the structure of the protection of property (Doneda, 2006, p. 275). In this sense, the legal protection granted to the right to privacy and to "*the right to be left alone" was consolidated*, which demanded an absentee posture on the part of the State.

Such pioneering is attributed to the fact that it glimpses the existence of a basic right to the protection of the person and the right to be alone. At first mentioned as a representation of the doctrinal creation of privacy (*privacy*), today the doctrine places it in the field of the general right of personality, as it encompasses an open list of protections that moves from the control of one's own body, through freedom of expression and reaching the control of personal information; demarcations that could not be defined in the context in which they arose (Ruaro; Rodriguez, 2011, p. 51), but which have become an important starting point for developing the idea of individual decision-making power over the publication of relevant information about the person himself.

This formal approach, embraced as a corollary of the framing of the right to privacy to a negative right of non-intervention, based on the conception of the right to privacy as an individual guarantee of state abstention in the individual private sphere (Ferraz Júnior, 1993), remained internalized in Brazil and was stamped in the jurisprudence of the Federal Supreme Court (STF), such as the judgment of Writ of Mandamus 21.729, [5] distributed in 1993 and judged in 1995, and RE 418.416,[6] distributed in 2004 and judged in 2006, in which the propositions of the national doctrine at the time, represented by the formulations of the jurist and philosopher of law Tércio Sampaio Ferraz Júnior, were evidenced.

It so happens that, after about two decades, marked by the rapid and profound impacts of technological transformations, notably the development of AIs, society has experienced a "process of inexorable reinvention of privacy" (Rodotà, 2008, p. 15), in which the right to privacy, by obvious and consequential, has undergone a (re)conceptualization.

As a milestone in this (re)conceptualization of the right to privacy, we point out the development of the concept of informational self-determination and the paradigmatic case of the German Census Law, of March 25, 1982 – BVerfGE 65, 1, "Census" (*Volkszählung*), which defined the contours given to the protection of personal data and which went beyond

[5] Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=1569577.
[6] Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2205705.

Revista ARACÊ
ISSN: 2358-2472

the mere constitutional protection of secrecy, projecting the general right of personality (Martins, 2005).

Also noteworthy is the definition by John L. Mills (2008), based fundamentally on the North American experience of *privacy*, who analyzed privacy from four prisms – *The Autonomy Sphere: The Personal Freedom to Make Decisions; The Personal-Information Sphere: Protecting Personal Data; The Personal-Property Sphere: Protecting Private Property; and The Control-of-Physical-Space Sphere: Protecting the Person* – which does not imply completeness (Ruaro; Rodriguez, 2011, p. 52-53).

In view of this, the LGPD brings respect for privacy and informational self-determination as foundations (art. 2, items I and II), "which should serve as an obstacle to the collection, sharing, and unbridled commercialization of personal data" (Silva, 2021, p. 207).

In fact, the Universal Declaration on Bioethics and Human Rights – which intersects ethical aspects of medicine, life sciences, and technologies associated with respect for human dignity, the protection of human rights, and fundamental freedoms – recommends, with maximum effort, respect for the privacy of individuals and the confidentiality of their information, which "should not be used or disclosed for purposes other than those for which it was collected or in line [...] with international human rights law" (art. 9, UNESCO, 2005).

As a guarantee given to citizens to control their own data, informational self-determination has been observed under a double dimension: subjective, as the citizen's right to negative freedom before the State; and objective, by establishing a State duty of protective action to guarantee the exercise and enjoyment of the fundamental right to the protection of personal data (Mendes; Fonseca, 2020).

Laura Schaetel Mendes and Danilo Doneda (2018, p. 22) consider the approval of the LGPD and the institutionalization of control and supervision mechanisms a milestone in the protagonism and empowerment of citizens. They also point out what they consider to be the three major innovations of the LGPD in relation to the protection of personal data, which make up the institution of an *ex ante model* for the protection of personal data, based: a) on the broad concept of personal data (considered as a projection of personality and, therefore, any treatment given to it can affect its personality and, therefore, any treatment given to it can affect its personality and, therefore, it has the potential to violate fundamental rights); b) the provision of legal support for any and all processing of personal

Revista ARACÊ
ISSN: 2358-2472

data; and c) in the flexibility of the system in the face of legitimate interest with the power to balance the rights of the holder.

To corroborate the assertion and the alleged claim of a leading role on the part of the holder of this personal data, Ana Frazão (2020, p. 98) indicates the following as objectives of the LGPD: a) to provide broad protection to citizens and to the most important existential situations that are affected by data processing; and b) to rescue the dignity of data subjects and their basic rights, related to informational self-determination.

In addition to privacy and its consectarian protection of intimacy, private life, honor and image, the centrality lies in informational autonomy and control over information, as well as in issues related to equality and freedom itself, whose protection is essential from the individual and social perspectives, considering that the foundations of democracy also depend on the regulation of data (Frazão, 2020, p. 124).

Currently, the so-called right to informational self-determination, an unfolding of the right to privacy, in which the individual has the right to control the collection, ownership, processing and transmission of data relating to his or her person, is considered a fundamental right (Doneda, 2006). In Brazil, the protection of personal data has already been recognized as a fundamental right (ADIs 6,387, 6,388, 6,389, 6,390 and 6,393, judged in 2020 and subject to specific topic 3.1; EC No. 115/2022), reinforcing aspects of the projection of the dignity of the human person.

In this environment, theorists point to the protection of personal data as an autonomous fundamental right and as an intention of the LGPD a protagonism on the part of the holder of this personal data (Doneda, 2011, p. 96; Frazão, 2020, p. 101 and 123; Mendes, Doneda, 2018, p. 22; Prestes *et al.*, 2021).

In this sense, if normative initiatives efficiently limit the power of public authorities and private sector actors towards their users; and, as it is an autonomous fundamental right, its holders are the individuals and legal entities that are the recipients of the "protection" against positive actions by the State and the private sector that, in any way, unjustifiably limit individual guarantees.

The LGPD contemplates a general rule that, a *priori*, points to an option for private ownership of one's own data (art. 7, I, and art. 11, I). However, the number of exceptional cases provided for the processing of data without the consent of the data subject (art. 7, II to XX, art. 11, II, paragraphs 'a' to 'g') and the use of open concepts such as, for example, "legitimate interest of the controller" and "legitimate purposes" (art. 10), calling into

Revista ARACÊ
ISSN: 2358-2472

question the scope of this "general rule", to the point of allowing an inquiry into the effective private option of this title, a central point of the philosophical premise from which the present study starts.

Analyzing the normative provisions of the LGPD, it is possible to identify an extensive list of situations in which the individual constitutional guarantees were limited, so that this somewhat romantic view that envisions this "protagonism" on the part of the data subject, conferred on him by the Law, is at least hasty[7].

In the Brazilian case, it seems that the legislation that bears in its epigraph the insignia of the "protection" of personal data, the LGPD, was much more concerned with the regulation of the way to exploit the data of the hyposufficient holder, giving primacy to the interests of the hypersufficient processor/operator, than with a concern with the effective protection of the hyposufficient holder of personal data. For this reason, the option to use the expressions "protagonism" and "protection", in quotation marks, is noted as a sign of the disvalue of the holder of personal data, both in the presumption of a "protagonism" and of an effective support given by the microsystem of "protection" of personal data.

PERSONAL DATA AND SENSITIVE PERSONAL DATA

In a circular movement to the conceptualization of data subject, the LGPD defines personal data as "[...] information related to an identified or identifiable natural person" (art. 5, I). Apparently, it equates the concept of data with that of information, a current and differentiated expression both in the field of Information Technology (IT) (Milagre; Santarém Segundo, 2015) and statistics (Barbetta, 2019; Lock *et al.*, 2017a, 2017b; Becker, 2015), in which information is extracted from data after it has been collected, ordered, stored, transformed, properly treated, visualized, explored, modeled, tested, and interpreted[8].

Because any information is legally included in the concept of personal data, it deserves extensive interpretation to achieve it, notably because in favor of the protection of hyposufficient holders (*thelos*) and because it is the duty of the Brazilian Democratic State of Law to defend consumers (art. 5, XXXII, CF/1988, combined with art. 18, § 8, and art. 45 of the LGPD).

[7] The pointing out of this list and the specific considerations in relation to the discredit of the holder of personal data in the processing of personal data and the use of open concepts such as "legitimate interest of the controller" and "public interest", as well as about the limitation of constitutional individual guarantees, will be topics addressed in specific articles.
[8] Cf. concepts of *wrangle* and *understand* data, in Wickam; Grolemund, 2017, p. 117; concepts of personal data and information and their overlaps, such as information in its "raw state" and so-called "useful" information, in Doneda, 2019, p. 135-138 and p. 154; a strong differentiation between data and information, in Becker, 2015, p. 35-38.

Revista ARACÊ
ISSN: 2358-2472

Thus, to define personal data, the broad meaning given by Stefano Rodotà, in his reference work on the subject, *Life in the surveillance society* (2008), is adopted, taking personal data as those

> [...] relating to an identified or identifiable natural or legal person capable of revealing information about their personality, affective relationships, ethnic or racial origin, or that refers to their physical, moral or emotional characteristics, their affective and family life, physical and electronic domicile, telephone number, assets, ideology and political opinions, religious or philosophical beliefs and convictions, physical or mental health status, sexual preferences or other similar conditions that affect their intimacy or informational self-determination (Rodotà, 2008, p. 6-7, footnote 23).

In view of this meaning, two classes of personal data are distinguished: sensitive personal data (article 5, II, LGPD[9]) and non-sensitive personal data (the others, by exclusion). The former encompass personal data whose analysis and use of the information extracted from them may, even if potentially, generate some type of discrimination not admitted (art. 6, IX, LGPD – principle of non-discrimination) by the legal system of a Democratic State of Law, such as the race, ethnicity, religion, political opinion, unionization, health or sex life of an individual, DNA, biometrics, etc.

Personal data – name, date of birth, eye color, Individual Taxpayer Registration (CPF) number, gender, ethnicity, height, weight, Body Mass Index (BMI), systolic and diastolic blood pressure, date and value of the last hundred purchases via the internet, net monthly income, daily and travel route, photographs of body image, DNA, etc. – are classified on a daily basis, categorized, measured and organized.

Since the genotype refers to genes and the phenotype to physical, morphological and behavioral characteristics[10], the concept of DNA is operationalized in more detail by the Glossary of Genomic and Genetic Terms, which contains the description of this molecule:[11]

> DNA is the chemical name of the molecule that contains genetic information in all living things. The DNA molecule consists of two strands that twist together to form a double helix structure. Each chain has a central part composed of sugars (deoxyribose) and phosphate groups. Attached to each sugar is one of the following 4 bases: adenine (A), cytosine (C), guanine (G), and thymine (T). The two chains are held together by links between the bases; adenine binds to thymine and cytosine to guanine. The sequence of these bases along the chain is what encodes

[9] "Article 5 For the purposes of this Law, the following shall be considered:
I - personal data: information related to an identified or identifiable natural person;
II - sensitive personal data: personal data on racial or ethnic origin, religious conviction, political opinion, membership in a union or organization of a religious, philosophical or political nature, data related to health or sex life, genetic or biometric data, when linked to a natural person;" (Brazil, 2018a).
[10] Available at: https://www.biologianet.com/genetica/diferenca-entre-genotipo-fenotipo.htm.
[11] Available at: https://www.genome.gov/es/genetics-glossary#P.

Revista ARACÊ
ISSN: 2358-2472

> the instructions for the formation of proteins and RNA molecules. (National Human Genome Research Institute, 2024).

The DNA molecule, in the form of a twisted ladder, in a double helix, has a complex structure, divided into functional units called genes – a portion of this molecule that has our genetic information, organized into chromosomes, located in the center of the eukaryotic cell. While DNA carries the cell's genetic code, ribonucleic acid (RNA), an intermediate molecule, converts that code into defined sequences of amino acids into proteins. Once the DNA, or RNA, is isolated, the material is extracted from any living organism, which can occur by different methods and types of samples. Practically any biological material contains DNA: the skin and mucous membranes, blood, semen, saliva, urine, feces, hair, etc.

TREATMENT, CONSENT AND EXAMPLE OF ADI 4.815 (BIOGRAPHEE AND BIOGRAPHER)

Of importance for the approach to the processing of personal data, the two types of normative sources arising from the European data protection model are differentiated, namely, the regulations prepared by the European Union and the national legislation separately, addressing relevant aspects for the understanding given to personal data by Brazilian legislation.

While the regulations of the European Union are presented in a perspective of Community Law, in which the cultural, commercial and institutional approximation of the States allows the delegation of part of their powers to the combined community of these states, with the binding power prevailing as to the result, being allowed, however, by each member state, the choice of the best way to achieve it; the separate national legislations, with their national data protection models, outline the initial guidelines for the protection of individual freedoms of their states (Machado, 2018; Martins, 2005).

Of the regulations made by the European Union, the so-called Directives, considered secondary sources or derived from Law (Ruaro; Rodriguez, 2010, p. 168), deserve to be highlighted: a) in view of its reception by the current *General Data Protection Regulation* (GDPR), EU 2016/679, [12] of April 27, 2016, in force since May 25, 2018; b) because they are precursors in the attempt to standardize the matter by the European

[12] Available in English and Portuguese, respectively: https://eur-lex.europa.eu/eli/reg/2016/679/oj; https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679 and https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679.

Revista ARACÊ
ISSN: 2358-2472

Parliament, without forgetting that previous documents from different entities dealt with the subject, without a standardizing character, such as: *European Convention on Human Rights* (Council of Europe, in 1950); *Fair Information Principles* (HEW – *Health, Education, Welfare* – Advisory Committee for Automated Data Systems, in 1973); *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, in 1980); *Convention No. 108 for the Protection of Individuals wiht regar to Automatic Processing of Personal Data* (European Parliament, 1981).[13]

The GDPR, a legal act of a secondary nature, valid for the European Union (EU) due to the prerogative conferred by the Treaty on the Functioning of the European Union (TFEU),[14] is the primary source of European Law because it contains fundamental rules regarding the objectives, organization and mode of functioning of the community, recognized as a provision with *status* and, as such, it can be invoked in the face of national norms that collide with the provisions of the European Union norms, in terms of fundamental guarantees, by provoking some type of judicial control.

In addition to maintaining the basis for the construction of personal data protection in Europe and the content of the right to personal data protection, the GDPR adopts a more global perspective on the protection of personal data, being considered a shift in the new model of data protection and regulatory equality by, among several other aspects, prioritizing the fundamental right to the protection of personal data over the economic interest of those responsible for processing – presenting notions of limitation of processing, definition of profiles, genetic and biometric data, control authority, among others (Machado, 2018, p. 90).

So much so that in the GDPR the protection related to the processing of personal data is a fundamental right, in a demonstration of the strengthening of traditional rights. In Brazil, recognition, as a fundamental right, was given in relation to the right to the protection of personal data (topic 4).

[13] Available in, respectively: https://www.echr.coe.int/Documents/Convention_ENG.pdf; https://course.ccs.neu.edu/csg256/handouts/01_fips.pdf; http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

[14] On the protection of personal data, Article 16 (ex Article 286 TEC): "1. Everyone has the right to the protection of personal data concerning him or her. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down rules on the protection of individuals with regard to the processing of personal data by the institutions, bodies, offices and agencies of the Union, as well as by Member States when carrying out activities falling within the scope of Union law, and on the free movement of such data. Compliance with these standards is subject to the control of independent authorities" (European Union, 2016).

Revista ARACÊ
ISSN: 2358-2472

For this reason, the GDPR is considered more assertive, as it has directed its protection to the processing of personal data, where, in fact, the remanufacturing of personal data takes place, from there it can be used for a multitude of situations and uses.

This regulation, in spite of having repealed Directive 95/46/EC,[15] in its consideration no. 9 maintains the objectives and principles of the Directive valid and is the most complete definition of the processing of personal data:

> [...] any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, communication by transmission, dissemination or otherwise making available, with alignment or combination, as well as blocking, erasure or destruction (Directive 95/46/EC, Art. 2). b).

As can be seen, the Directive chose not to differentiate the means by which data is processed, whether automated or not. It is, however, with the computerized processing of personal data that, in modern times, society expresses its concern and tries to ensure more protection for the data of its holders.

The concept of personal data processing brought by the LGPD in its article 5, X, practically reproduces the conceptualization of the GDPR and is a broad concept:

> [...] any operation carried out with personal data, such as those referring to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or control of information, modification, communication, transfer, dissemination or extraction. (Brazil, 2018a).

The concept of processing encompasses precisely an open enumeration of several typical IT operations that, once applied to a personal database, result in the extraction of relevant information, that is, it is a technological divider that separates data from information, adds informative value to personal data and, like the industry, transforms raw material (raw data) into an immaterial product (processed information), the latter of economic value many times greater than the former.

A prerequisite for the validity of this processing is the non-vitiated consent (art. 5, XII, and art. 8, § 3, LGPD), specific and informed, regularly issued by the holder of the personal data, under penalty of its nullity, in addition to civil liability for damages or unjust enrichment earned by controllers or operators (Maia, 2020).

[15] Available at: https://eur-lex.europa.eu/eli/dir/1995/46/oj.

Revista ARACÊ
ISSN: 2358-2472

From this point of view, the legal requirement of a "free, informed and unequivocal manifestation" is not satisfied with mere passive behavior, clearly demanding active behavior, given the high degree of autonomy granted to the data subject, who has the legal prerogative of having guaranteed his right to consent or not, since the concept of consent allows the data subject to decide on the restrictions on his right to protection of your own personal data.

In addition, there should be no doubt about the sufficiency of the information for the data subject, since the LGPD gives the holder the right to be informed of all circumstances related to the processing of their personal data, such as: the specification of which data will be processed; the identification of the handler, the form, purpose and consequences of the processing; the consequences of refusal of consent (if it prevents the business from being carried out); the destination of the processed data; its transfer for consideration to third parties.

In this sense, the understanding of the European Court of Justice was established, based on the GDPR, evidenced in judgments that refute the existence of an effective active behavior in consents through pre-validated options (standardized or adhesion contracts) on websites, as it is not possible to assess the exact degree of understanding, since it is not known whether the text in question, drafted in advance, has been read and understood (EUR-Lex, 2020).

There are also those who point to the impossibility of admitting a "nature" of negotiation for the consent of the holder of personal data (Tepedino; Teefé, 2020, p. 293), in those cases in which it is indispensable to regulate the application of processing by controllers-operators, on the same grounds that rights inherent to human dignity would touch the personality itself and that they would not have elements of content available.

However, there is a confusion here between the commercial unavailability of certain personality rights, such as the right to one's civil name, or to one's image (one's representation of oneself or one's reputation, the honor one intends to maintain before third parties) and the availability of some of one's attributes (one's biography, for example), according to the CF/1988, the infra-constitutional legislation and even the uses and customs in force in the national community as to its condition as a thing put into trade.

Revista ARACÊ
ISSN: 2358-2472

A striking example was the case of ADI 4.815,[16] in which the STF decided to waive the consent of the biographee, the copyright of the biographer, even when he uses the name, genealogy and other data and events that characterize the personality of the biographee. Once the data of the biographee's personality has been processed by the biographer, the latter becomes the owner of the literary work thus produced, which, despite containing several descriptive data of the biographee's personality, is undoubtedly put on the market and must respect all the copyright of its treater/author.

The object of the decision was only that the holder of the personal data would have no participation in the exploitation of the biographer's copyright, notably when this author processes a series of open data of the biographee, available to the general public or made available voluntarily by the biographee, such as photos, reports and *likes* on open social networks.

When the principles of the inviolability of the right to intimacy, privacy, honor and image (protection of private life) and freedom of thought and expression (literary artistic creation or scientific production) collide, the latter prevailed over the former, but not that there was an impediment to negotiate its participation in a case of authorized biography, without this representing the purchase and sale of his civil name or his human condition. If that were the case, in some part, the copyright law would have to be declared unconstitutional, since it could not take the names of living people as a starting point.

Not without reason there are several works that, in prestige to precaution, declare in their introduction: "This is a work of fiction and any relationship with real names or people is a mere coincidence", there precisely launched with the express objective of avoiding undue claims for compensation.

PROCESSING AGENTS: CONTROLLER AND PROCESSOR

With the massive circulation of personal data in commerce, there is, on the one hand, the hyposufficient figure of the holder and the accelerated expansion of the phenomenon of reification (Honneth, 2018; Martins, 1998; Neves, 2011) or *commodification* (Maia, 2020; Rodotà, 2008) or *commodity* (Schwartz, 2004), with protection legally equivalent to that of the consumer by the LGPD (art. 18, § 8, and art. 45). On the other hand, hypersufficient figures of controllers and operators, natural or legal persons, under

[16] Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4271057; *Link* to access the full content of the judgment: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=10162709.

Revista ARACÊ
ISSN: 2358-2472

public or private law, commonly appear, with the former being responsible for decisions on the processing of personal data and the latter for carrying out this processing on behalf of the former (art. 5, VI and VII, LGPD). In this context, the effective protection of the personal data of the underprivileged is contrasted with the fulfillment of the economic interest of the hypersufficient.

Still in reference to the GDPR and its influence on the LGPD, when it comes to the power conferred on the controller, among the new rights, the right to data portability, provided for in European legislation in its article 20, stands out as follows:

> Article 20. Right to data portability 1. **The data subject shall have the right to receive the personal data concerning him or her which he or she has provided to a controller**, in a structured, commonly used and machine-readable format, and the right to transmit such data to another controller without the controller to whom the personal data have been provided being able to prevent it, (a) the processing is based on consent given in accordance with Article 6(1)(a) or Article 9(2)(a) or on a contract referred to in Article 6(1)(b); and b) The processing is carried out by automated means. 2 When exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have personal data transmitted directly between controllers, where technically possible. 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. **This right does not apply to processing necessary for the performance of a task carried out in the public interest or to the exercise of official authority vested in the controller**. 4. The right referred to in paragraph 1 shall be without prejudice to the rights and freedoms of others (**highlighted**).

In a first analysis, the provision appears as a guarantee of the person interested in the control over his own data, insofar as it ensures the right to the recovery of his own data and obliges the service provider to provide them. It happens that, from protection to portability and recovery, there are points that unbalance the guarantor essence of the person interested in control over their own data, leading to the reflection of whether there is really effective protection of the data subject.

In the GDPR there are limitations to the scope of protection of the data subject, since the data covered by the right to portability and recovery: a) are only the personal data provided by the user to a data controller, excluding all data collected as part of *online* browsing and that have not been formally provided; b) this right does not apply to processing necessary for the exercise of functions of public interest or to the exercise of authority that the controller is vested with.

In the LGPD, in turn, among the rights of the holder is the possibility of "portability of data to another service or product provider, upon express request, in accordance with the

Revista ARACÊ
ISSN: 2358-2472

regulations of the national authority, observing commercial and industrial secrets" (art. 18, V, LGPD).

However, the proviso of paragraph 7 that "[t]he portability of personal data referred to in item V of the *caput* of this article does not include data that have already been anonymized by the controller" in itself mitigates the effective protection of personal data in the interest of the controller. Once anonymized, the data of the holder is remanufactured and no longer belongs to him, so that he himself cannot even carry out the portability, while the controller/operator becomes vested with the right to use, enjoy, enjoy the processed data and provide it to others, including for consideration.

Furthermore, as an example for reflecting on whether there is really effective protection of the personal data subject: a) the open concept "regulatory obligation" (article 7, II, LGPD), which may be invoked by the controller to waive the consent of the data subject, may be subject to infra-legal regulation by the National Data Protection Authority (ANPD), that, from an organ that is part of the Presidency of the Republic, pursuant to article 55-J, item XIII, of the LGPD, it became a special autarchy under the terms of Law No. 14,460, of October 25, 2022; b) the open concept of "legitimate interests of the controller" or of a third party (article 7, IX, of the LGPD) refers, by a circular argument, to the open concept of "legitimate purposes" of the same controller, to support the processing of personal data, which includes "support and promotion of the controller's activities", under the terms of article 10, item I, of the LGPD.

In this sense, and placing the legal provisions in the feasible horizon of the universe of all of us, holders of personal data, Nathalie Martial-Braz (2018, p. 104) highlights the possibility of repercussions on copyright and asks, with a pertinent example, whether an Instagram user has the guarantee of retrieval of his photo (his data) published in the application with the use of the filter offered by the service provider.

Strictly speaking, the interests of the controllers and operators of the data subject's data dispense with the agreement of the holder of the personal data in situations associated with the processing of personal data. There are also a series of situations outlined by open concepts such as "legitimate purposes" and "legitimate interest", clearly inserted in the LGPD with the *protection* of the rights of data controllers and operators, such as, for example, those aimed at the protection of industrial secrets (patents, utility models and other models for the protection of industrial property).

Revista ARACÊ
ISSN: 2358-2472

In this sense, the power conferred on the controller, who is responsible for decisions regarding the processing of personal data (article 5, VI, LGPD), highlights the discussion about what should ultimately justify acts of power within the scope of public law, which involves the aforementioned open concepts, which, in the final analysis, concern the supremacy of the public interest.

Such a concept, for democratic constitutionalism and from the nomological point of view, can be considered a technical impropriety in the face of fundamental principles such as the dignity of the human person, from the perspective that the entire legal system develops from it and that the very existence of the State is justified in it (Justen Filho, 1999, p. 100-126). Still, isonomy is of paramount importance as a basic reference in the proportionality of the relations between the public power (or to whom it confers powers, such as the controller in the LGPD) and the citizens (Binenbojm, 2014, p. 115-121), to the extent that evoking open concepts such as "legitimate purposes" is not sufficient to institute a unilateral privilege in the name of the mere allegation of public interest.

There is, moreover, the risk of manipulating citizens by these public or private agents with the power to process the data of a significant mass of holders, very clearly occupying and a hyposufficient position in the technological relations of mining and exploitation of their personal data when compared to the giants (Google, Twitter, Facebook, Instagram, Tik Tok etc.) and even the *start-ups*, given the technological irruption already experienced in this area. This occurs, notably, when technological advances are combined in the areas of information technology (*big data*, AIs, etc.), genetic engineering (collection, treatment, storage, and identification of genetic profiles on a large scale), and neuroscience (mapping of brain functions, extraction of mental reaction patterns, etc.).

The precise synchronization of *the data under skin*, when analyzed in a cross-and synchronized way with registration data and with access to artistic content (music, films, plays, etc.) and consumer goods (food, clothing, hygiene products, cosmetics, etc.) allows the animus to be measured with a high degree of accuracy of each of the millions of citizen-users (holders of this personal data, whether or not sensitive), such as their reactions of love or hate to *marketing* content, political propaganda or materials that convey Manichean ideological content.

This information extracted from it puts these thousands of citizen-users with "free" access to the countless applications made available to them, but exploits them information so valuable that they place them on the virtual shelves of the expressive business rounds

Revista ARACÊ
ISSN: 2358-2472

in which this information is bought and sold for *marketing* purposes or customized electoral propaganda, ideological enticements and other practices that denote a new situation of the human condition: the very conduct of each of the millions of human persons arranged on virtual shelves and counters, in a reduction of this singular attribute of the holders of personal data to the inescapable condition of a thing (Honneth, 2018).

This reification of the manipulated behaviors of human beings can be likened to their relaunch into servile condition, into captivity, without any possibility of manumission (Fanon, 1968; Honneth, 2018; Martins, 1998). Against this palpable possibility of a massive attack on civil liberties, the LGPD protected little or almost nothing.

The world-renowned case of *Cambridge Analytica*,[17] in which data from millions of Facebook users – personal identity, habits, preferences and contact networks – were violated and directed to specially adapted political advertising, has brought into question the risks of data concentration and the possibility of its manipulation by governments and corporations. This topic was even mentioned by Justice Luiz Fux in his statement of merit in ADI 6,387 (recognition of data protection as a fundamental right), where he highlighted the profitability of the use of personal data and warned of its misuse with the potential to harm privacy and democracy.

LITERATURE REVIEW AND STATE OF THE ART

In the validity of the Democratic Rule of Law and in line with its assumptions, the analysis of the CF/1988 shows, under the aspect of the protection of personal data, a complex of guarantees and fundamental rights listed as stony clauses in its article 5 – as recorded in the introduction, the Citizen Charter, in this article, item XII, brings the data from the angle of its secrecy.

Therefore, we enter the labyrinth of fundamental rights and guarantees applicable to the principled protection of personal data based on the review of the literature and the debate on the state of the art.

In order to expand the dialogue of this research with studies on the subject and so that, to some extent, it is reproduced and added to the research already carried out in the area (Creswell, 2010 *apud* Ferreira, 2021), the literature review and the debate on the state of the art and walk through institutes of:

[17] Documentary on the subject available at: https://www.netflix.com/br/title/80117542?trkid=13747225&s=a. Access to the news available at: https://www.bbc.com/portuguese/geral-43705839; https://www.bbc.com/portuguese/internacional-43461751; https://exame.com/tecnologia/cambridge-analytica-se-declara-culpada-por-uso-de-dados-do-facebook/.

Revista ARACÊ
ISSN: 2358-2472

a) Constitutional Law, such as and with emphasis on the principles enshrined in article 5, X, XII, XXII and LIV, of the CF/1988, which guarantee the right to privacy, to the confidentiality of data and to the private ownership of such data (extendable to ownership), also ventilated in the conformity analyses expressed in concrete cases submitted to judicial deliberation;
b) Civil Law, which, in addition to also addressing issues related to the aforementioned constitutional principles, innovates by articulating the debate on the protection of personal data with questions about the private ownership of these data;
c) Criminal Law and Criminal Procedure, insofar as it problematizes the conformation of criminal and procedural legislation to constitutional principles, such as due process of law, the prohibition of illicit evidence, the presumption of innocence and the limits of criminal identification of the civilly identified.

In view of the Brazilian microsystem of the "protection" of personal data and its intersection with the criminal control of crime, the literature review found that:

a) in the constitutional sphere, academic production has focused on the analysis of the constitutionality of current legislation (Campêlo, 2022; Rabelo, 2018; Silva, 2012; Trinity; Costa Neto, 2018), especially around Law No. 12,654/2012 (LAlteraLEP&LICCrim) and, more recently, Law No. 13,964/2019 (LPAC), mostly limited to the weighing of principles (Lima, 2020; Menezes, 2020; Netta, 2020; Serpa Júnior, 2017).

The importance of the control of constitutionality for the protection of fundamental rights, in the degree of institutionality and supremacy of the constitution, is well described and with a certain degree of universality.

Specifically regarding the legal regime of criminal identification, the parameters of normativity in Brazil are universal, such as intimacy, due process of law and proportionality of the State's response, portraits of constitutional guarantees in countries reputed as Democratic States of Law.

On the other hand, while this same legal regime and the state banks of genetic profiles are used in developed countries and in Brazil applauded as examples of investigative patterns, elucidation of crimes and identification of authors, here

Revista ARACÊ
ISSN: 2358-2472

contradictorily the argument of incompatibility of the legal regime of criminal identification and the national bank of genetic profiles (BNPG) is used.

Therefore, the criminal investigation with genetic profile data as a starting point is denied, under the pretext of the unconstitutionality of its provision and, ultimately, of the violation of the dignity of the human person, forgetting the universality taken as a premise, invoked here and there, evidence of an unsustainable level of hypocrisy that demands, for the invoked coherence of the beginning (invocation of universal normativity parameters), its application until the end (since the unconstitutionality of these aforementioned databases of genetic profiles from developed countries is not pointed out).

b) in Civil Law, privacy and the protection of personal data have been the object of focus by several scholars (Doneda, 2006, Frazão, 2020; Machado, 2018; Olive tree; Lopes, 2020; Ruaro, Rodriguez, 2011).

It is different who expands to the issue of ownership of one's own (Maia, 2013, 2019, 2020) and only more recently has there been a specific approach to data protection according to the guideline pointed out by Harari (2018), that is, from a perspective (a look) that privileges the private ownership/ownership of personal data, whether or not *under skin* (Maia, 2024).

c) at the intersection with the penal control of crime, the literature review revealed a vast production on the institutional arrangements within the scope of public policies for social security and defense, dealing with the administration of criminal justice, its institutions, state administration of conflicts, violence, criminality, police, prisons, homicides (Adorno, 1995; Fields; Alvarez, 2017; Cerqueira, 2014; Coast; Lima, 2018; Ferreira, 2021; Freire, 2009; File; Bueno; Mingardi, 2016; File; Misse; Miranda, 2000; File; Sinhoretto; Bueno, 2015; Oliveira, 2002; Soares, 2022; Soares, L. E., 2007; Suxberger; Lima, 2017; Zaluar, 1999).

In this sense, Campos and Alvarez (2017) consider that, from the 2000s onwards, researchers in the area have distributed their work into three axes of study, namely: a) studies on public security policies; b) studies on violence and sociability; c) investigations within the scope of a sociology of punishment.

In terms of themes and perspectives of approach, it focused on the first axis, because the present thesis addresses the consonance between public security policies and individual guarantees as a problem to be faced and better problematized.

Revista ARACÊ
ISSN: 2358-2472

On the other hand, regarding the legal regime of criminal identification through the collection, processing and storage of DNA of those criminally identified via judicial determination and of those convicted of certain serious crimes – a public policy adopted since 2012[18] and more recently evidenced in Law no.º 13.675, of June 11, 2018, called the Law of the Unified Public Security System (LSusp) – in the literature review, studies were found in the areas of health, bioethics and criminalistics (Beltrami, 2015; Bonaccorso, 2005; Carvalho, 2009; Garrido; Rodrigues, 2015; Giovanelli, 2022; Cardoso; Sato; Santiago, 2017; Oliveira, 2023; Rocha, 2017) and a few with mentions of Criminology (Borges; Birth, 2022; Raldi; Puhl, 2021).

In the field of Law, the discussion, eminently doctrinal, is more concerned with criminal identification and compulsory DNA extraction in the face of constitutional guarantees (Cardoso, 2022; Carvalho, 2014; George; Felix, 2014; Louzada; Rohden, 2022; Mahmoud; Moura, 2012; Macorin, 2018; Mariano Júnior, 2014; Mariú, 2018; Mateleto Filho, 2012; Menezes, 2020; Morais, 2020; Morgado, 2018; Nicolitt, 2013; Schiocchet, 2013, 2014; Schiocchet; Cunha, 2021; Sousa, 2018; Suxberger, 2015; Suxberger; Furtado, 2018).

The theme is considered little explored in terms of empirical research (Ataíde; Sousa, 2023; Brito; Bridges, 2020; Garrido; Costa, 2020; Minervino *et al*., 2019; Minervino *et al*., 2022; Silva Junior *et al*., 2019; Souza, 2019) and from the point of view of the institutional arrangement related to the national bank of genetic profiles (Garrido, 2018; Suxberger; Furtado, 2018).

In the universe of possibilities of genetic identification, the convergence of these areas presents the broadest and most complex criminal field compared to the context and scope of the development of the same theme in the civil area, focused on family and registry status and, consequently, patrimonial impacts, where the theme is facilitated by the rules of the burden of proof. In the criminal field, it is not only about predictive action (such as a conviction that gives rise to a genetic criminal identification that is considered more qualified and with the insertion in a genetic profile database), but also the comparison of traces, theoretical perspectives such as actuarial logic and tertiary prevention, etc., which result in more complex legal variables.

[18] By the changes brought about by Law No. 12,654, of May 28, 2012 (LAlteraLEP&LICCrim), which, in addition to including article 9-A of the LEP (Law No. 7,210, of July 11, 1984), providing for the genetic identification of those convicted of violent or heinous crimes; it also amended the Criminal Identification Law – LICCrim (Law No. 12,037, of October 1, 2009) to allow the collection of biological material to obtain the genetic profile when it is considered by the judge to be essential for police investigations (art. 3, IV, and art. 5, sole paragraph).

Revista ARACÊ
ISSN: 2358-2472

EXPANSION OF THE LIST OF CONSTITUTIONAL PRINCIPLES

The most complete principled list on the protection of personal data was observed in Doneda (2011, p. 103-105), who lists: the inviolability of intimacy, private life, honor and image of people (item X); freedom of expression (item IX); the secrecy of correspondence, communications and data (item XII); the right to information (art. 5, XIV); copyright (item XXVIII, with legislation updated and consolidated by Law No. 9,610, of February 19, 1998); access to information (item XXXIII, regulated by the Access to Information Law – LAI, Law No. 12,527, of November 18, 2011); the right to petition (item XXXIV); industrial property (item XXIX, regulated by Law No. 9,279, of May 14, 1996); the *habeas data* to know records or databases of the public power (item LXXII).

To this list are added other principles that are engraved as a stony clause in the current CF/1988 and are pertinent to the protection and guarantee of personal freedoms, considered the general rule of private ownership of personal data, which are:

- the right to property and the social function of property, which, extended by analogy to ownership, have repercussions on the regulation of the ownership of one's own data and impact on its general guidelines;
- due process of law, in its material or substantive and procedural or procedural dimensions (Nery Júnior, 2010, p. 83-87);
- the adversarial and the broad defense, observed even in administrative proceedings, an arena in which conflicts over personal data and processors/operators are dealt with under the judgment of the ANPD and also where the police investigation and the civil investigation are inserted (Nery Júnior, 2010, p. 221);
- the prohibition of evidence obtained by illegal means, especially for the control of the chain of custody in the collection, processing and storage of the DNA of those criminally identified by judicial order and of those convicted of certain serious crimes;
- the criminal identification of the civilly identified;
- The right to remain silent, which, based on a differentiation between data and information, gains relevance to prevent the State from using grounds built from a kind of "eloquent silence" to the detriment of those investigated or convicted.

Revista ARACÊ
ISSN: 2358-2472

PRINCIPLED PROTECTION OF PERSONAL DATA AND OPEN CONCEPTS: WHERE IS THE PROTECTION OF THE LGPD DIRECTED?

Still in the debate on the state of the art, Doneda (2011, p. 98-101), after a historical digression on what he calls the "generational progression" of important documents, such as the Strasbourg Convention and the Organization for Economic Cooperation and Development (OECD) Guidelines on the protection of personal data in Europe and North America, indicates a trend towards autonomy in the protection of personal data and its consideration as a fundamental right in various legal systems, concluding by the use of principiology as the backbone of generational progression in terms of personal data protection.

To this end, it points to the adoption of the principles of publicity or transparency; purpose; free access; accuracy; and physical security as a common core applied in important international documents, such as those mentioned above.

In the Brazilian system, which links the protection of natural persons (article 1) to their fundamental rights, the LGPD expressly and specifically brings principles for the processing of personal data in its article 6. Among them are those pointed out, by Doneda, as part of the principled backbone in the protection of personal data, in addition to the following six principles: adequacy, necessity, data quality, prevention, non-discrimination and accountability and accountability.

In fact, the LGPD brings principles expressed in its article 6, which refer to the processing of personal data. By analyzing them, it is possible to find principles applicable to it as a whole, such as the principles of purpose, security, responsibility, and accountability. In addition to these, from a systemic analysis, the right to property and the fulfillment of its social function are revealed as reflections of the constitutional provision.

For Frazão (2020, p. 101-104), this principled protection of the LGPD is an expression of a true autonomous fundamental right, with an emphasis on freedom and human dignity, capable of preventing the reduction of personal data to the merely patrimonial aspect by prioritizing its existential dimension, imposing a series of precautions and restrictions on data processing. Finally, it considers that the precepts of article 6 cannot be set aside even with the consent of the holder.

However, the principles listed in article 6 of the LGPD are already conceived and inserted in the microsystem of "protection" of personal data precisely under the assumption

Revista ARACÊ
ISSN: 2358-2472

that they may clash, so that a possible solution involves flexibility, with the search for the greatest application of all to the greatest extent possible (Alexy, 2008).

In an initial interpretation of article 6, there is nothing that privileges, a *priori*, a guarantee interpretation (protection of the individual freedoms of the holders of personal data). In this sense, principles can be weighed in such a way that processors and operators of personal data can and do act without the consent of the data subject.

While there is, in the LGPD, only article 1 as an express normative provision that guarantees the prevalence of secrecy that protects private life (engraved in the CF/1988), the same LGPD has several express normative provisions that industrial secrecy has to be considered (art. 6, VI; art. 9, II; art. 10, § 3; art. 18, V; art. 19, II, and § 3; art. 20, §§ 1 and 2), including in the decisions of the National Data Protection Authority (ANPD, art. 38; art. 48, § 1, III; art. 55-J, II and X).

If the LGPD aims to "[...] protect the fundamental rights of freedom and privacy and the free development of the personality of the natural person" (art. 1), if the legal discipline is the "protection of personal data" (art. 2) and if principiology is the backbone of the protection of personal data, the question arises: how to effectively guarantee the private ownership of personal data in the face of provisions using so many open concepts?

See:

a) the definition of the principle of purpose as "carrying out the processing for legitimate, specific, explicit and informed purposes to the data subject [...]" (art. 6, item I);

b) or even the hypotheses of waiver of consent in the processing of personal data:

1. "for the fulfillment of a legal or regulatory obligation by the controlling shareholder (art. 7, item II);
2. "necessary for the execution of public policies provided for in laws and regulations or supported by contracts, agreements or similar instruments (art. 7, item III);
3. "for the performance of studies by a research body, ensuring, whenever possible, the anonymization of personal data";
4. "when necessary for the execution of a contract or preliminary procedures related to a contract to which the data subject is a party, at the request of the data subject";
5. "for the regular exercise of rights in judicial, administrative or arbitration proceedings";

Revista ARACÊ
ISSN: 2358-2472

6. "for the protection of health, in a procedure carried out by health professionals or by health entities";
7. "when necessary to meet the legitimate interests of the controller or a third party, except in the case where fundamental rights and freedoms of the holder that require the protection of personal data prevail".

Faced with so many possibilities of processing personal data without the consent of its holder, the question arises: does the framework really guarantee the private ownership of personal data, as pointed out in the literature review?

The very legal concept of controller ("natural or legal person, under public or private law, who is responsible for decisions regarding the processing of personal data") and operator ("natural or legal person, under public or private law, who processes personal data on behalf of the controller") transfers to someone other than the holder of the personal data, the power to decide on the processing of data, often obtained without the consent of the data subject.

In addition, the figures of who are the controller and operator will vary according to each circumstance of personal data processing, especially in those listed among the hypotheses of waiver of consent under the use of open concepts.

The LGPD, even starting from the idea of the holder of personal data (art. 5, I and V) and understanding the individual as the holder of his or her own data, immediately subjects these data to the condition of "object of processing".

In addition, this processing operation (article 5, X) results in a new data, a new product, a new consumer good: the "processed" data, whose ownership is no longer in the domain sphere of that natural person from which the personal data was mined. Now, under the dominiality of controllers (article 5, VI, with decision-making power over data processing) and operators (article 5, VII, with power to process data on behalf of the controller), who can dispose of them as *a* response in trade.

Even subjecting both, the holders of personal data on the one hand and the controllers and operators on the other, to the inspection and judgment of the ANPD, there are numerous legal hypotheses in which the LGPD dispenses with consent as the first condition for access to the personal data of all of us. In other words, the LGPD itself treats this data, at its origin, as a shapeless mass subject to a wide mining capacity on the part of the processing agents: the controller-operator binomial.

Revista ARACÊ
ISSN: 2358-2472

Such considerations are put forward to rethink where the protection of the LGPD is really directed, much more in favor of the activities of controllers or even for the protection of commercial and industrial secrets than for the holder of personal data. Therefore, it is considered about the private option of personal data and the reasonableness and proportionality arising from the application of normative provisions that make use of general and open concepts (ANPD's arena of action) and represent a potential limitation of the individual freedoms of the holders of personal data, notably when the possibility of manipulating the preferences of countless citizens is envisaged, from his consumerist options to his "secret" vote.

PROTECTION OF PERSONAL DATA AS A FUNDAMENTAL RIGHT

The specific case of a rule that hypothetically, by the automated processing of the data of thousands of citizens, would jeopardize the power of each of us to decide for ourselves, about ourselves and how we intend to provide our own personal data to third parties, led to the recognition, by the Judiciary, of a fundamental right to the protection of personal data (and which later became part of CF/1988 via EC No. 115/2022), which privileges both the dignity of the data subjects themselves and their basic rights and protects the collective dimensions arising from this protection.

The risk situation referred to the terms of Provisional Measure No. 954, of April 17, 2020,[19] which provided for the sharing of citizens' personal data – specifically names, telephone numbers, and addresses – by telecommunication companies with the Brazilian Institute of Geography and Statistics (IBGE), to support official statistical production during the pandemic caused by Covid-19.

In practice, it was up to the STF, through concentrated control of constitutionality, to assess whether this Provisional Measure – by providing for the sharing of personal data of the entire universe of consumers, individuals or legal entities, of the country's telephone services, Fixed Switched Telephone Service (STFC) and Personal Mobile Service (SMP), with the IBGE during the public health emergency situation caused by Covid-19 – exceeded the limits outlined by the Constitution, especially regarding the right to privacy and its consectaries (protection of intimacy, private life, honor and image).

[19] Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. On this page it reads: "(See ADI No. 6387) (See ADI No. 6388) (See ADI No. 6390) (See ADI No. 6393)", without mentioning ADI 6389, which deals with the same issue.

Revista ARACÊ
ISSN: 2358-2472

The situation, which led to the processing of ADIs 6,387, 6,388, 6,389, 6,390 and 6,393[20] before the STF, has been considered a historic milestone in the recognition of a fundamental right to the protection of personal data (Estellita, 2023; Frazão, 2023; Mendes; Fonseca, 2020). This is because the conjuncture has become paradigmatic in the face of constant technological advancement, mass data processing and the insertion of the right to privacy in a dynamic and permanent protection, which has elevated the right to informational self-determination to the condition of a counterpoint in the scope of protection of the fundamental right to the protection of personal data not only in the case of ADIs, but for any specific context of collection, processing (processing and storage) or transmission of data by third parties, which may constitute a danger or violation to the holders of personal data.

Considering the relevance of ADIs 6,387, 6,388, 6,389, 6,390 and 6,393 in dealing with the protection of personal data as a fundamental right, the topic that follows them is dedicated to dealing with some of their procedural phases and entering into the content of their preliminary (monocratic) and merit (Plenary) decisions.

ADIs 6.387, 6.388, 6.389, 6.390 AND 6.393: FORMAL ASPECTS

These are ADIs proposed, respectively, by the Federal Council of the Brazilian Bar Association (CFOAB), the Brazilian Social Democracy Party (PSDB), the Brazilian Socialist Party (PSB), the Socialism and Liberty Party (PSOL) and the Communist Party of Brazil (PCdoB), legitimized under the terms of article 103 of the CF/1988, in view of Provisional Measure No. 954/2020, which provided for the sharing of data by telecommunication companies (fixed switched service and personal mobile) with the IBGE, for the purpose of supporting official statistical production during the pandemic (public health emergency situation caused by Covid-19, which is dealt with by Law No. 13,979, of February 6, 2020).

The arguments of the ADIs revolved around defects of formal unconstitutionality, due to the non-compliance with the constitutional requirements for the issuance of a provisional measure; and material, for violation of the dignity of the human person, intimacy, private life, honor and image of people, confidentiality of data and informational self-determination (art. 1, item III, and art. 5, items X and XII, CF/1988).

[20] Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165; https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895166; https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895168; https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895176; https://portal.stf.jus.br/processos/detalhe.asp?incidente=5896399.

Revista ARACÊ
ISSN: 2358-2472

The proposed actions were assessed and distributed to the Reporting Minister Rosa Weber, between April 20 and 22, 2020.

In ADI 6,387, proposed by the CFOAB, from which the other ADIs were distributed for prevention, the IBGE and the National Telecommunications Agency (Anatel) expressed their views on the data sharing procedure and the meaning of "official statistical production" to be carried out during the period of health emergency caused by Covid-19, as well as by the Attorney General's Office (AGU) and the Attorney General's Office (PGR), within a common period of 48 hours (Event 16).

The subpoenas of the entities are registered in the procedural progress of ADI 6.387:[21] respective letters in Events 17 to 20; Event 21, proof of PGR receipt; Events 36 and 37, with proof of AGU receipt; Event 38, with proof of IBGE receipt; Anatel's receipt receipt can be found in Events 122-124, with receipt date on 4.29.2020, after the Monocratic Decision of Event 53, which granted the precautionary measure.

Even before the manifestations of the aforementioned procedural subjects, the plaintiff reported, in Event 22, the publication of Normative Instruction No. 2, of April 17, 2020, by the IGBE, which is included in Event 23, considering the regulation given by the aforementioned normative instruction as generic and precarious regulation of the procedure for the direct sharing of personal data, reiterating the request for urgency in granting the requested injunction.

The AGU (Event 26) and the IBGE (Event 30), both for the rejection of the injunction request, as well as Anatel (Event 39), which limited itself to providing information.

On April 24, 2020, there is a Monocratic Decision in all ADIs, in which the Rapporteur, Justice Rosa Weber, granted the requested precautionary measure, *ad referendum* of the Plenary, to suspend the effectiveness of Provisional Measure No. 954/2020.

The determination was for the IBGE to abstain from requesting the data subject to Provisional Measure No. 954/2020 and, in the case of a request already made, the suspension of the request(s) with immediate communication to the telephone operator(s) (ADI 6,387, Event 53, ADI 6,388, Event 11, ADI 6,389, Event 15, ADI 6,390, Event 8, and ADI 6.393, Event 10).

[21] Available at: https://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5895165.

Revista ARACÊ
ISSN: 2358-2472

In ADI 6,387, the PGR expressed itself after the Monocratic Decision that suspended the effectiveness of Provisional Measure No. 954/2020: Event 77, with a petition for knowledge, and Event 102, with a statement of merit (Memorials).

The AGU and the IBGE, in Events 104 and 106, presented Memorials, in summary for proportionality and compliance with the public interest in favor of the constitutionality of Provisional Measure No. 954/2020, arguing for the dismissal of the requests).

The qualifications of the *Amicus Curiae* (Data Privacy, Event 61, Lapin, Events 80 and 90, IBGE representing AGU, Event 100, Interstate Federation of Workers and Researchers in Telecommunications Services (Fitratelp), Event 113, Aprocon, Event 125, IBDA, Event 136) were granted (Events 79 and 109) and, in Event 121, there is the certificate of initial judgment in Plenary on 5.6.2020, while, in Event 130, there is the judgment certificate with a decision that, by majority, on 5.7.2020, endorsed the precautionary measure granted to suspend the effectiveness of Provisional Measure No. 954/2020 (only Justice Marco Aurélio was defeated).

The entire content of the judgment, with 161 pages, can be found in Event 141. Justices Celso de Mello, Gilmar Mendes, Ricardo Lewandowski, Cármen Lúcia, Luiz Fux, Rosa Weber, Edson Fachin and Alexandre de Moraes voted with the Rapporteur, and Justice Marco Aurélio voted with the Rapporteur. There is the justified absence of Justice Luís Roberto Barroso, but with a vote presented following the rapporteurship.

On 11.17.2020, there is a new Monocratic Decision deeming ADI 6,387 (Event 144), 6,388 (Event 38), 6,389 (Event 36), 6,390 (Event 30) and 6,393 (Event 25) to be prejudiced, due to supervening loss of their object, extinguishing the proceedings without resolution of the merits. This is because Provisional Measure No. 954/2020, a contested rule, had its validity extinguished on 8.14.2020, and was not converted into law within the legal term (art. 62, §§ 3 and 7, CF/1988).

From the processing of the lawsuits, attention was drawn to the speed in the processing and judgment of ADIs 6,387, 6,388, 6,389, 6,390 and 6,393. This speed is very different, for example, from the procedure of RE 973.837[22], in which the constitutionality of article 9-A of the LEP and the identification of the genetic profile of those convicted of certain crimes are discussed, and which, therefore, involves the ownership of personal data. With recognized General Repercussion, it has been processed as such since 2016

[22] Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4991018. Object of specific study by researchers via exploratory documentary research and documentary analysis, whose intention is the publication in sequence to this article.

Revista ARACÊ
ISSN: 2358-2472

and has continued since 2019 without procedural momentum and without a determination to suspend the processing of all pending cases involving the matter discussed therein. With this inertia, the national database of genetic profiles continues to be increased with the collection, treatment and storage of DNA from criminally identified and convicted persons. In the last data available, from January 2024, it reached the mark of 242,185 genetic profiles in the BNPG and, of these, 178,608 genetic profiles of convicts, 73.75% of the BNPG.[23]

It also differs from the processing of ADI 5,545[24], which was processed without an injunction granted for almost seven years until the judgment on the merits, in 2023. The core of the ADI was in articles 1, final part, and 2, item III, of the Law of the State of Rio de Janeiro No. 3,990, of October 11, 2002[25], in which the proponent, the Federal Public Prosecutor's Office (MPF), via the Attorney General, considered a constitutional violation the obligation, for nursing homes, hospitals and maternity hospitals, to collect biological material from all mothers and children and subsequent identification by comparative DNA examination, when necessary, in cases of exchange or subtraction of newborns.

The relevant issue of the ownership of the data itself, called personal data by the LGPD/2018, presents a scope that, at least in theory, can be treated by a public controller as a result of the fulfillment of an obligation provided for by law (art. 11, II, 'a') or for the execution of a public policy (art. 11, II, b), notably, but not exclusively, in the protection of health (art. 11, II, 'f').

The case in question took care of analyzing whether the compulsory collection of biological material from parturients and neonates and its storage would violate the CF/1988, the fundamental rights to intimacy and privacy, as well as proportionality and reasonableness, in the dimension of the prohibition of excess, aggravated by the absence of prior consent, guarantee of confidentiality of the data and the prohibition of the use of these data for other purposes, different from the questioned legal prescription.

[23] Last updated on 24.2.2025, available at: https://app.powerbi.com/view?r=eyJrIjoiMGM0OGQwYzQtZWI3MC00NTkzLWJiNDAtNGM2YTgxMzA4OTNkIiwidCI6ImViMDkwNDIwLTQ0NGMtNDNmNy05MWYyLTRiOGRhNmJmZThlMSJ9. It is recorded that, in this *link*, the only public access not to the data, but to the information, the number of genetic profiles in the BNPG is updated monthly, accumulating the totals of each variable, so that, when accessed, there may be divergence between the month and the quantities mentioned, but it is decided to make the official source available.

[24] Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4998973. It is also the object of specific study by the researchers to analyze the merits of the Justices who participated in the vote in the Plenary and their argumentative theses, via exploratory documentary research and documentary analysis, whose intention is the publication in sequence to this article.

[25] Available at: https://leisestaduais.com.br/rj/lei-ordinaria-n-3990-2002-rio-de-janeiro-obriga-a-adocao-de-medidas-de-seguranca-que-evitem-impecam-ou-dificultem-a-troca-de-recem-nascidos-nas-dependencias-de-hospitais-publicos-ou-privados-casas-de-saude-e-maternidades-no-ambito-do-estado-do-rio-de-janeiro-que-possibilitem-a-posterior-identificacao-atraves-de-exame-de-dna-e-da-outras-providencias?q=3.990.

Revista ARACÊ
ISSN: 2358-2472

In this matter of protection and regulation of the ownership of personal data, the STF exercised the concentrated control of constitutionality in a process of its original jurisdiction and, unanimously, established the thesis of judgment of unconstitutionality of a state law that provides for the archiving of genetic materials of unborn children and parturients, in health units, in order to carry out comparative DNA tests in case of doubt (ADI 5.545, Plenary on 13.4.2023 and publication of the Full Content of the Judgment on 16.6.2023).

Having made these considerations, we then proceed to the analysis of the content of the preliminary and merit decisions rendered in the ADIs, focusing on the contours given to the fundamental right to the protection of personal data.

CONTOURS OF THE RECOGNITION OF THE FUNDAMENTAL RIGHT TO THE PROTECTION OF PERSONAL DATA

The contours of the fundamental right to the protection of personal data were drawn from the assessment of the scope of a rule that provided for sharing names, telephone numbers, and addresses of consumers of telephone concessionaires and the country's official statistical agency, in view of the limits outlined by CF/1988 and confirmed with the enactment of EC No. 115/2022, raising the protection of personal data to a constitutionally protected fundamental right.

In practice, it was up to the STF, via concentrated control of constitutionality (ADIs 6,387, 6,388, 6,389, 6,390 and 6,393), to assess whether Provisional Measure No. 954/2020, by providing for the sharing of personal data of the entire universe of consumers, individuals or legal entities, of the country's telephone services with the IBGE, during the Covid-19 pandemic, exceeded the limits set by the Constitution, especially regarding the right to privacy and its consectaries (protection of intimacy, private life, honor and image).

At the outset, Rapporteur Justice Rosa Weber highlighted the risk of handling personal data, by public or private agents, as a contemporary challenge to the right to privacy and data protection, pointing out principles not met by Provisional Measure No. 954/2020, especially purpose and transparency, despite its outstanding importance in the processing of personal data.

Another point raised was the lack of clarity regarding the need to share personal data and the pandemic caused by Covid-19, to the point of making it impossible to assess

Revista ARACÊ
ISSN: 2358-2472

the public interest that would justify the use and processing of personal data in light of the necessity, adequacy, and proportionality of the measure.

In addition, the vote informed the recent disclosure, by the IBGE, of a partnership with the Ministry of Health for the preparation of a version of the National Household Sample Survey (Pnad), with data collected by telephone contact for households, based on the information contained in its database, collected in the 2019 PNAD.

For the Reporting Minister, the unnecessity of the measure and the excess of sharing were magnified in the face of the situation, highlighting the following question: "if the PNAD is carried out with a sample of a little more than two hundred thousand households, I question: why share two hundred million telephone numbers, with the risks intrinsic to the manipulation of this data?" (ADI 6.387, Full Content of the Judgment, p. 26).

It also pointed out the lack of any measure to safeguard the protection of personal data in the event of unauthorized access and misuse of the data collected and processed, as well as a mechanism to guarantee confidentiality and anonymity, a situation aggravated by *the vacatio legis* of the LGPD at the time, which has accountability criteria, non-existent in Provisional Measure No. 954/2020.

The need for more transparency in the definition of the purpose and use of personal data was reiterated, along with the observation of the lack of security impact analysis of information prior to the collection and use of citizens' data, on the grounds that the fight against the pandemic does not constitute a general justification legitimizing the trampling of the fundamental guarantees enshrined.

In fact, the terms of Provisional Measure No. 954/2020 did not include the specific purpose of the use of the statistical research, its object, its scope, the procedure for making the data available, and how it would be used, being incompatible with the right to privacy because it does not have a precisely delimited purpose, not even the security procedures capable of avoiding risks of unauthorized access, misuse and leaks of information.

Although the decennial periodicity of the IBGE Population Census was public and general knowledge – which would take place in 2020 and would justify, to some extent, the sharing of names, telephone numbers and addresses of its consumers by telecommunications companies with the IBGE –, one month before the publication and effectiveness of Provisional Measure No. 954/2020 (4.17.2020), the IBGE itself announced the decision to postpone the Census to 2021 (3.17.2020) (IBGE, 2020).

Revista ARACÊ
ISSN: 2358-2472

Likewise, Provisional Measure No. 954/2020 left open the procedure for making the data available (article 2, paragraph 2), reserving for a subsequent act a measure whose provision in the Provisional Measure itself would bring credibility to the unilateral act of the then President of the Republic.

In fact, the arguments of disproportionality of the use of information shared over time (article 4 of MProv No. 954/2020: ([...] "*the IBGE Foundation may use the data for a period of thirty days, counted from the end of the public health emergency situation of international importance*") find shelter in the factual reality, since the pandemic caused by Covid-19 had its "end" announced by the World Health Organization (WHO) on 5.5.2023 (PAHO, 2023), three years and three months after the declaration of a global public health emergency. During this period, with MProv No. 954/2020 in force (and if converted into law, of course), all the data encompassed therein would be used for the purposes of an unspecified statistical production.

On the other hand, at the time and as a backdrop to the enactment of Provisional Measure No. 954/2020, there were the 2020 presidential elections. Although not openly mentioned, the center of the debate gravitated around the risk of concentrating citizens' personal data in the hands of political agents, so much so that arguments were aired around the establishment of a surveillance society, the collapse of democracy and the paving for autocratic regimes.

In the era of *fake news*, with the *Cambridge Analytica* scandal, with allegations of the misuse of Facebook user data with manipulation through algorithms in favor of Donald Trump's electoral campaign in the United States, in 2016, added to the very high consumption of social networks by Brazilians[26] and to the customized propaganda of social networks, the fight against deliberate disinformation, especially during election periods, requires measures to protect citizens and democracy itself.

INSTITUTIONAL VARIABILITY IN THE FACE OF VIOLATIONS OF THE RIGHT TO THE PROTECTION OF PERSONAL DATA

While the concern turned to protective measures against the State, citizens who use the same telephone lines, whose data would be shared with the IBGE, are bombarded daily with a multitude of calls and text messages by private companies offering products

[26] News of the time available at: https://www.redebrasilatual.com.br/blogs/blog-na-rede/pesquisa-revela-que-brasileiros-estao-entre-os-que-gastam-mais-tempo-nas-redes-sociais/; https://www.poder360.com.br/brasil/brasil-e-o-3o-pais-que-mais-usa-redes-sociais-no-mundo/; https://oglobo.globo.com/economia/tecnologia/noticia/2023/03/brasil-e-o-terceiro-pais-que-mais-consome-redes-sociais.ghtml.

Revista ARACÊ
ISSN: 2358-2472

and services, not knowing at what time their telephone numbers and, Therefore, your personal data became a commodity, *returned* to trade, without your specific authorization for such purpose and at the cost of monetization of third parties other than the holder of the data itself.[27] This point was even mentioned by Justice Marco Aurélio in his dissenting vote in ADI 6,387, which was not even touched on in the referendum on the Precautionary Measure.

The misuse of personal data cannot be disregarded, which places the citizen, the holder of his own data, in the condition of merchandise put into commerce by data leakage, such as those that occurred between 2018 and 2019 in accounts of Brazilian users of the giant Facebook and which reached more than 500 million users in the country.[28]

A look at the variability itself, which, in the application of the Law, allows the construction of alternatives with potential and even transformative power (Unger, 2004), would mobilize institutions in favor of the observation and construction of effective and lasting alternatives to the violations of the right to the protection of personal data today. Using documentary sources as examples, we can observe the contradictions and variability in the judgments of more recent cases involving the theme.

TJMG ACPs – Facebook and data leakage

The leak of data of millions of Facebook users in Brazil, such as name, phone number, e-mail, passwords and details of account transactions (cited in the vote of Justice Luiz Fux in ADI 6.387 and mentioned in item 2.4 to deal with the power in the hands of data processing agents, cf. Fornasier; Beck, 2020; Oliveira, 2021, Carvalho, 2022; Rodrigues, 2022), was the subject of a Public Civil Action (ACP) that was processed before the Court

[27] One of the researchers, for example, had her private phone number – acquired during the pandemic in 2020 for exclusively functional use, only for calls and WhatsApp messages for the subpoena of jurisdictions in the exercise of the activity of bailiff, without having provided it to any private registration, but only to the operator concessionaire of the mobile phone service – placed on the shelf of *res* put into commerce without her authorization, a situation perceived when consulting her name in a private database, paid for by the union entity that represents her professionally. As if that were not enough, through this same private telephone number made available in a private database and accessible by payment without her authorization, she was bothered with several offers of products and services. In fact, this database, fed with data provided solely and exclusively to a telephone concessionaire, still shows this telephone number as belonging to the researcher, who has already canceled it with the telephone operator more than a year ago.

[28] News of the time available at: https://www.jusbrasil.com.br/noticias/facebook-e-condenado-a-indenizar-a-brasileiros-por-vazar-dados-veja-como-pedir/1918363449; https://www1.folha.uol.com.br/mercado/2023/08/justica-manda-facebook-pagar-r-20-milhoes-por-vazamentos-de-dados-no-brasil-veja-como-pedir-indenizacao.shtml; https://www.otempo.com.br/tecnologia/facebook-e-condenado-a-indenizar-a-brasileiros-por-vazar-dados-veja-como-pedir-1.3099618; https://gauchazh.clicrbs.com.br/tecnologia/noticia/2023/08/facebook-e-condenado-a-pagar-r-5-mil-para-cada-usuario-do-brasil-prejudicado-por-vazamento-de-dados-clku333p800by01542x49l7ts.html; https://g1.globo.com/mg/minas-gerais/noticia/2023/08/11/apos-condenar-facebook-a-pagar-r-20-milhoes-por-vazamento-de-dados-justica-nega-pedidos-de-indenizacao-a-usuarios.ghtml.

Revista ARACÊ
ISSN: 2358-2472

of Justice of the State of Minas Gerais under numbers 5064103-55.2019.8.13.0024[29] and 5127283-45.2019.8.13.0024,[30] with appeals pending judgment.

Mentioned PCAs, distributed on 5.8.2019 and 7.16.2020, respectively, had a judgment on the merits on 7.24.2023, which includes the application of the LGPD and its scope in consumer protection, highlighting the importance of the rights of the data subject and, consequently, the demand for compliance with the duty of protection and information on how, when and under what conditions their personal data will be used, ensuring the citizen who is the holder of their own data the security of the effective protection of their personal data at all stages and even after the processing of the data. As a result, Facebook was sentenced, in each of the ACPs, to pay 10 million reais, as collective damages, and 5 thousand reais, as individual damages, to each of the users directly affected by the leak of their personal data.

It is interesting to note that in the sentences there is no mention of the recognition, by the STF, of the right to data protection as a fundamental right (ADIs 6,387 and related) nor EC No. 115/2022. In the same sense, in the judgment of the ADIs, there was no reference to the first of these cases of large improper sharing of data of millions of Brazilian citizens, already in progress at the time of the processing of the facts in the STF.

RE 673.707[31] and Topic 582[32] – Sincor and taxpayer access

In the judgment of ADI 6.387 and related matters, Justice Luiz Fux recalled the decision rendered in RE 673.707 in 2015, identifying in it an opening of the constitutional text to the recognition of the autonomy of the fundamental right to data protection (ADI 6.387, Full Content of the Judgment, p. 112), in view of the understanding adopted, by the *Habeas Data* for the purpose of accessing information included in the database of the Federal Revenue Service's Legal Account System (Sincor) (RE 673.707, Rel. Min. Luiz Fux, Full Court, judged on 6.17.2015, DJe 9.30.2015).

[29] Available at: https://pje-consulta-publica.tjmg.jus.br/pje/ConsultaPublica/DetalheProcessoConsultaPublica/listView.seam?ca=e733eaae91bf617bec30c59348e5aa21c3d2d35fb0f67868
[30] Available at: https://pje-consulta-publica.tjmg.jus.br/pje/ConsultaPublica/DetalheProcessoConsultaPublica/listView.seam?ca=1e14e1bd091b27dbec30c59348e5aa21c3d2d35fb0f67868
[31] Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4204594.
[32] Available at: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=4204594&numeroProcesso=673707&classeProcesso=RE&numeroTema=582.

Revista ARACÊ
ISSN: 2358-2472

The thesis established in Topic 582 was that *Habeas Data* constitutes "an adequate constitutional guarantee for the obtainment, by the taxpayer himself, of data concerning the payment of taxes contained in computerized systems to support the collection of the treasury administration bodies of state entities".

RE 1055941[33] and Topic 990[34] – Coaf and sharing of data and information

In the context of the sharing of data and information with the bodies responsible for criminal prosecution for criminal purposes, the General Repercussion of Topic 990 and RE 1,055,941 are pointed out as a reference process, in which the sharing of reports from the Council for the Control of Financial Activities (Coaf) was considered valid, without the need for prior judicial authorization in formally initiated proceedings.

From the public consultation to RE 1.055.941, recorded as a process in secrecy of justice, the procedural documents are not accessible due to[35] "Absence of electronic document or restricted viewing", but in the "Jurisprudence" option, the following [36] are made available: a) the decision to recognize the General Repercussion of the constitutional issue raised and the establishment of the topic, with the related manifestations (judgment on 4.12.2018 and publication on 4.30.2018); b) the Full Content of the Judgment of the judgment on the merits (judgment on 12.4.2019 and publication on 3.18.2021).

For a proper understanding of the constitutional controversy, Topic 990 (autonomous procedural category that arises with the judgment of the preliminary General Repercussion) and the thesis at the end established in the recognized General Repercussion are collated:

> Topic 990 - Possibility of sharing with the Public Prosecutor's Office, for criminal purposes, the taxpayer's bank and tax data, obtained by the Federal Revenue Service in the legitimate exercise of its duty to supervise, without prior authorization from the Judiciary. Description: Extraordinary appeal in which it is discussed, in the light of arts. 5, incs. X and XII, 145, § 1, and 129, item VI, of the Constitution of the Republic, the possibility of sharing with the Public Prosecutor's Office, for criminal purposes, the taxpayer's banking and tax data, obtained by the Federal Revenue Service in the legitimate exercise of its duty to inspect, without prior authorization from the Judiciary.
> General Repercussion. Topic 990. Constitutional. Criminal Procedure. Sharing of the FIU's financial intelligence reports and the full inspection procedure of the Federal Revenue Service of Brazil with criminal prosecution agencies for criminal

[33] Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5213056.
[34] Available at: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5213056&numeroProcesso=1055941&classeProcesso=RE&numeroTema=990.
[35] Available at: https://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5213056.
[36] Available at: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22RE%201055941%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true.

Revista ARACÊ
ISSN: 2358-2472

> purposes. No need for prior judicial authorization. Constitutionality recognized. Appeal granted to reinstate the conviction of the 1st degree. The national suspension injunction is revoked (article 1,035, § 5, of the CPC). Establishment of the following theses: 1. It is constitutional to share the financial intelligence reports of the FIU and the entirety of the inspection procedure of the Federal Revenue of Brazil – in which the levy of the tax is defined – with the criminal prosecution bodies for criminal purposes without prior judicial authorization, and the confidentiality of the information in **formally initiated proceedings must be safeguarded** and subject to subsequent judicial review; 2. The sharing by the FIU and the RFB referred to in the previous item must be done only through formal communications, with a guarantee of confidentiality, certification of the recipient and establishment of effective instruments for the investigation and correction of any deviations (**highlighted**).

Having established the previous guidelines by the STF, after more than four years, in 2024, the Superior Court of Justice (STJ), in *Habeas Corpus Appeals* (RHC) 188.838[37] and 187.335,[38] has been changing its position specifically in relation to the "formalized investigation", in judgments of May 21 and June 18 – for which the diction of article 926 of the Code of Civil Procedure (CPC) stands out: "The courts must standardize their jurisprudence and keep it stable, complete and coherent."

In May 2024, in RHC 188.838, in the specific case of sharing information in a preliminary procedure to the investigation, the Fifth Panel of the STJ signed an understanding that there is no need for prior judicial authorization or prior initiation of a police investigation for the sharing of reports from the Financial Intelligence Units (FIU) with criminal prosecution bodies for criminal purposes (Rapporteur Minister Ribeiro Dantas).

In June of the same year, the same Fifth Panel, in RHC 187.335, revised the position and no longer attributed legitimacy to the sharing before the initiation of the inquiry, considering the news of fact and the preliminary verification of the investigation prior to the investigation (Rapporteur Minister Reinaldo Soares da Fonseca, with Justice Ribeiro Dantas, rapporteur of RHC 188.838 being dissented

On the subject, Resolution No. 174, of July 4, 2017, of the National Council of the Public Prosecutor's Office (CNMP),[39] in its article 3, regulates the initiation and processing of the news of fact and authorizes the collection of preliminary information essential to deliberate on the initiation of the proper procedure, but prohibits the issuance of requests.

[37] Available at: https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroRegistro&termo=202303803910&totalRegistrosPorPagina=40&aplicacao=processos.ea.
[38] Available at: https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroRegistro&termo=202303359154&totalRegistrosPorPagina=40&aplicacao=processos.ea.
[39] Available at: https://www.cnmp.mp.br/portal/images/Resolucoes/Resoluo-174-1.pdf.

Revista ARACÊ
ISSN: 2358-2472

In addition, Resolution No. 181, of August 7, 2017,[40] of the CNMP, which provides for the initiation and processing of the criminal investigative procedure (PIC) under the responsibility of the Public Prosecutor's Office, object of ADI 5,793,[41] was recently judged on 6.28.2024, and an excerpt of the resolution that defines the PIC as "summary" and "unbureaucratic" (article 1 of the conceptual definition of the PIC) was considered unconstitutional. in the absence of authorization from the CF/1988 for the initiation of procedures of an abbreviated nature.

The situation narrated, analyzed from the perspective of institutional variability, is also observed in the absence of a criminal LGPD and the space lacking regulation in the face of the sharing of personal data involving taxpayers' banking and tax data with criminal prosecution agencies for criminal purposes, without the obligation of prior judicial authorization, in the face of a gap in a criminal LGPD that protects the processing of data in investigation and repression activities of criminal offenses (article 4, III, "d", of the LGPD provides for specific legislation, still pending).

In fact, the argument in ADI 6,387 and related provisions of *vacacio legis* of the LGPD, and the absence of validity of the liability criteria at the time, could be applied by analogy to a gap in a LGPD in the subject addressed. Moreover, it is necessary to have variability itself as a reference, for a logical and concatenated production, avoiding the multiplicity of disparate actions and judgments.

ADPF 1.175[42] – health and genetic heritage operators

As presented, Provisional Measure No. 954/2020, object of ADI 6,387 and related, was recognized as unconstitutional, denying the sharing of the names, telephone numbers and addresses of consumers of telephone concessionaires with the country's official statistical agency, which, from then on, would be available to public agents and at risk of manipulation of this personal data.

Now, in the public proceeding filed more recently on 06.04.2024, the interpretation to be given to Precedent No. 609/STJ is followed – "The refusal of insurance coverage, under the allegation of a pre-existing disease, is unlawful if there was no requirement for medical examinations prior to contracting or the demonstration of bad faith by the insured" –, questioned via the Allegation of Non-Compliance with a Fundamental Precept (ADPF)

[40] Available at: https://www.cnmp.mp.br/portal/images/Resolucoes/Resoluo-181-1.pdf.
[41] Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5288159.
[42] Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6945077.

Revista ARACÊ
ISSN: 2358-2472

1,175, whose injunction, requested to prevent the request for information about the genetic heritage, in view of the high degree of harm and threat to the fundamental precepts indicated, has not been considered so far (24.2.2025).

Of the fundamental rights and guarantees, ADPF 1,175 argues for the violation of the right to life, human dignity, health, privacy, economic protection of the consumer and the prohibition of inhuman and degrading treatment, with no express mention of the protection of personal data as a fundamental right, recognized in ADI 6,387 and related.

For the political party with national representation that proposed the demand, Precedent 609/STJ authorizes insurers and health plan operators to indiscriminately investigate the medical life of consumers, allowing the collection of sensitive personal data even before the pricing of the services to be provided.

This is because the obtaining of information on the genetic heritage of citizens takes place prior to the contracting of coverage, with which insurers and health plan operators start to count on the unilateral definition of prices and conditions of the services provided to a range of more than 51 million Brazilian citizens.

It is important to highlight the difference between pre-existing diseases or injuries (DLP), which must be informed in a health declaration prior to hiring, and genetic mutations, considered variations in the DNA sequence, which may or may not lead to medical limitations, and do not qualify as diseases.

In the clarifications provided by the STJ, reference is made to: arts. 422, 765 and 766 of the Civil Code, article 51, IV, of the Consumer Protection Code and twelve precedents of the STJ on the matter,[43] in a demonstration of observance of the variability itself, expected in the construction of alternatives to violations of the right to the protection of personal data, to be observed in the development of this ADPF by the STF.

In order to monitor this process from the aspect of institutional variability, the decision of the aforementioned ADI 5.545 will be considered,[44] in which the so-called "genetization of life" was addressed to deal with the appropriation of genetic information, the power of those who hold this information (scientific, political, strategic and even warlike, whose mention is found in the Summary of the judgment on the merits) and the risk of

[43] REsp 1.230.233/MG, Third Panel, judged on 5/3/2021; AgRg in AREsp 330.295/RS, Third Panel, judged on 2/10/2015; AgRg in AREsp 429.292/GO, Third Panel, judged on 3/5/2015; AgRg in AREsp 353.692/DF, Third Panel, judged on 6/9/2015; AgRg in REsp 1.299.589/SP, Third Panel, judged on 9/1/2015; AgInt in AREsp 868.485/RS, Third Panel, judged on 8/22/2017; AgInt in AREsp 177.250/MT, Fourth Panel, judged on 10/23/2012; EDcl in AREsp 237.692/SC, Fourth Panel, judged on 6/18/2013; AgInt in AREsp 826.988/MT, Fourth Panel, judged on 5/17/2016; AgInt in REsp 1.359.184/SP, Fourth Panel, judged on 12/6/2016; AgInt in REsp 1.280.544/PR, Fourth Panel, judged on 5/2/2017; AgInt in AREsp 767.967/RS, rapporteur Min. Raul Araújo, Fourth Panel, judged on 8/3/2017.

[44] Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4998973.

Revista ARACÊ
ISSN: 2358-2472

social categorization evaluated in its exclusively genetic dimension (potential aptitude of the development of a genetic disease), exemplified by the conduct of health insurance.

FUNCTIONALIZATION OF GERMAN LAW AS A REFERENCE FOR LIMITING THE COLLECTION AND PROCESSING OF PERSONAL DATA

On the other hand, part of the argument of the vote of some Justices (Luiz Fux, Ricardo Lewandowski and Gilmar Mendes), in ADI 6.387 and related, was based on the functionalization of International Law (Suxberger, 2015) and dedicated to the invocation of the German experience with the 1983 Census Law, which provided, in addition to data collection as a profession, housing and place of work, the possibility of cross-referencing, transmitting and comparing the data obtained with data from other public records, such as those of the civil registry, in addition to the imposition of a fine in case of failure to fill out the form for statistical purposes, which contained about 160 questions, some of them of an intrusive nature, about the professional aspirations and even the religious and political practices of each citizen (Doneda, 2006, p. 192; Machado, 2018, p. 69).

This dialogue of cuts has been expressive within the scope of the STF in important decisions in matters of fundamental rights, such as HC 82.424/RS,[45] ADI 3.112[46] and ADI 3.510[47] (Neves, 2014) and, in the case of ADI 6.387 and related, the invocation of German jurisprudence as a paradigm appears in the single votes of the Justices, but also in the summary of the ruling, as part of the *ratio decidendi*.

The decision of the German Constitutional Court pointed to the protagonism of citizens with regard to their personal data and recognized the right to informational self-determination, precepts contained in the LGPD. Notwithstanding the protection constitutionally recognized in Germany, and introduced into the Brazilian legal system, it differs from the Brazilian case whose object was MP No. 954/2020, given its breadth, previously summarized.

When dealing with the German Census Law, Justice Gilmar Mendes, in his vote in ADI 6.387, summarizes that, with the collection and cross-referencing of data from the German Census, the possibility of "creating a comprehensive and detailed picture of the respective person – a personality profile – even in the intimate area; the citizen becomes a true 'transparent person'" (ADI 6.387, Entire Content of the Ruling, p. 102). Although

[45] Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2052452.
[46] Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2194197.
[47] Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2299631.

Revista ARACÊ
ISSN: 2358-2472

constitutional, the German Census Law of 1983 had several provisions declared null and void, "notably those involving comparison and exchange of data, as well as the competence to transmit data for the purposes of administrative enforcement" (Schwabe; Martins, 2005, p. 234).

Regarding the universe of data to be made available based on MP No. 954/2020, in Brazil, this broad possibility cannot be envisioned, given that the sharing of personal data would only cover personal data of name, telephone number, and address.

The core of the Brazilian question referred to the concrete possibility of forming a "personality profile" by listing the names, telephone numbers and addresses of its consumers, individuals or legal entities.

The relevance of the judgments has even been compared with the historical relevance of the judgment by the German Constitutional Court, in 1983, on the German Census Law – BVerfGE 65, 1, "Census" (*Volkszählung*), which dealt with the fundamental right to self-determination over personal data in the face of state interventions.

The paradigmatic German judgment dealt prominently with the right to privacy, the rights to the protection of personal data and informational self-determination, recognizing their autonomy and the individual's capacity for self-determination with their personal data, as a form of expression of the free development of personality (Martins, 2005).

The crux of the German issue referred to the concrete possibility of forming a "complete personality profile" by processing information on citizens, such as their profession and places of work and residence (Martins, 2005). In this case, a greater dimension of data collection is observed compared to the Brazilian case of Provisional Measure No. 954/2020.

In the German case of 1983 and in the Brazilian case of 2020, the limitation on the collection and processing of personal data prevailed, with the high point being the proportionality for the hypotheses of relativization of the asserted fundamental right to informational self-determination.

The German Court declared the partial unconstitutionality of the rule due to its vagueness and amplitude, which made it possible to cross-reference collective data with other public records, as well as to transfer them to other administrative bodies (Martins, 2005). The Brazilian Court, on the other hand , suspended the effectiveness of Provisional Measure No. 954/2020 for not meeting the basic principles of privacy, also considering it to be unjustified vague and broad, aggravated by the lack of definition of a specific purpose

Revista ARACÊ
ISSN: 2358-2472

and the mention of the transfer of information; all in prestige to the protection of personal data.

LEGAL NATURE OF THE RIGHT TO THE PROTECTION OF PERSONAL DATA

To point out what is most in line with the fundamental right to the protection of personal data, its legal nature is addressed: whether it is a real right (direct and absolute legal relationship) or an obligatory right (indirect and relative legal relationship), in addition to its patrimonial character (obligatory or real) or existential (Maia, 2013).

Roberta Maia (2019, 2020) is absolutely right regarding the use of the expression ownership that the LGPD (art. 17) reserved for the subject of law (holder) of personal data, denoting that she opted for the genus of which property is a species. And also its conclusion by inserting it as a patrimonial legal situation (of Private Obligation Law), highlighting peculiar characteristics such as erga *omnes enforceability* and patrimoniality, which have always been considered as typical and exclusive of Real Rights (Maia, 2013, 2020; Tepedino, 2006, 2011).

One could see some similarity between this new obligatory private right to personal data and the already known *propter rem* obligations (Neves, 2011, p. 189-191; Pereira, 2010, p. 38-42) and obligations with real effectiveness (Costa, 1993, p. 112-115; Pereira, 2010, p. 38-42). As with real rights and these two hybrid obligations in relation to the thing (Pereira, 2014, p. 338) object of their legal relations, the erga *omnes enforceability* of the holder's potestative right to terminate the assignment of right over his or her non-sensitive personal data interferes with them and, thus, can be invoked against third parties, which encompasses the entire chain of succession of controllers and operators through which this personal data navigates or is stored (Neves; Matos, 2023), at any time (art. 8, § 5, LGPD), even those subsequent, in which the holder does not appear as a contracting party (Maia, 2013).

More appropriate than looking at this new private right to personal data from the point of view of property and, thus, inquiring about its ambulatoriness and right of sequelae (Tepedino, 2006, p. 141), is to inquire "[...] whether it is a direct, immediate and absolute legal relationship or a mediate and relative legal relationship, since real rights are no longer the only category that fits into the first option" (Maia, 2020, p. 146).

But it could not be said that the obligations of controllers and operators in relation to the personal data on which they regularly apply their processing would arise from a "thing"

Revista ARACÊ
ISSN: 2358-2472

object of real right, since this concept of *res* is appropriable, although it can be extended to immaterial objects (example: the work, in the authorial property; trademarks, patents, utility models and industrial designs, in industrial property; cultivar, in relation to the rights of the breeder), is typical of goods subject to dominiality. Furthermore, as already seen, the private right to personal data is of the strain of patrimonial legal situations (obligatory rights), and it is more appropriate to see this personal data as an immaterial object of this unique obligatory legal relationship, as it is direct, immediate and absolute with this virtual object (Maia, 2020).

In addition, the possibility that personal data may have economically appreciable content is not excluded (Neves; Matos, 2023), such as their *trade-off* in exchange for the "free" use of an application (Maia, 2019, p. 681) and, therefore, be considered patrimonial, now in another sense: they can integrate the patrimony – the set of assets, rights and obligations of economic value belonging to an individual or legal entity (Pereira, 2010, p. 329-341) – of its holder and of those controllers and operators to whom they are regularly assigned for lawful processing purposes (notably the information extracted from them), although there are extra-patrimonial or existential rights linked to the same right to non-sensitive personal data, such as freedom, intimacy, and privacy, all of which are located in the field of fundamental personality rights (Maia, 2020).

As for the capacity for mutation, the field of Real Rights, closed in its world of closed numbers (Maia, 2013), subject to the rule of the reservation of law in the strict sense (Tepedino, 2006, p. 143) or this reservation as to the legal figures that can be registered (art. 167, Law No. 6,015 of December 31, 1973), regardless of its real or obligatory nature (Maia, 2013, p. 294; Tepedino, 2011, p. 228-231), has changed very little over time when compared to the innovative impulse that the openness to sign atypical contracts by the contracting parties has provided to the field of Obligation Law (Maia, 2013, 2020). In this sense, it is more in line with new rights, such as the private right to personal data, notably the patrimonial portion of this right, subject to an accelerated mutation, both in its genesis and reproduction and in the market conditions of the selection of success cases, quickly replicated in the form of massive adhesion contracts.

Revista ARACÊ
ISSN: 2358-2472

PRIVATE OWNERSHIP OF PERSONAL DATA AND THE PRINCIPLE OF PRIVATE PROPERTY (EXTENDED TO OWNERSHIP) AND ITS SOCIAL FUNCTION

The analysis of the ownership of one's own data according to the guideline pointed out by Harari (2018), that is, from a perspective (a look) that privileges the private ownership of personal data, whether or not *under skin*, in the light of contemporary constitutionalism and the CF/1988, highlights, without discarding the others, the principle of private property and its social function, extended to the title.

Until then not treated in the national literature (Doneda, 2006; Frazão, 2020; Machado, 2018; Olive tree; Lopes, 2020; Ruaro, Rodriguez, 2011), with the recent publication of Roberta Maia (2024), property began to be treated as an instrument of protection for the person, taking into account the historical meaning of the right to property as a minimum patrimonial sphere of the individual and, at the same time, as an instrument of social inclusion.

As exposed, Harari (2018, p. 110) suggests starting from a historical-cultural point of view in facing the challenge of how to regulate the private ownership of one's own data.

Following this philosophical framework, and taking the point of view of private property, a historical foreshortening arising from the literature review goes back to a context of a property right resulting from a millennial historical evolution idealized to encompass the goods then available, the corporeal things. In that context, it was affirmed in the Declaration of the Rights of Man and in the United States Constitution of 1776, representing a first-generation fundamental right and a break with the medieval model of "excess property".

Throughout the twentieth century, such a transformation took place, to the point of being placed at the service of the pursuit of constitutional objectives and as an instrument for the promotion of personality in its multiple attributes (Maia, 2024). In this sense,

> [...] the **property status** becomes twofold, ceasing to be a power of exclusion and **becoming the right not to be excluded from access to goods**. There are, therefore, two **antagonistic biases** to be accommodated throughout **the exercise of the right to property**: one exclusionary, capable of allowing the control of the use, enjoyment, and disposal of goods by non-proprietary third parties, and the other **of access**, which should **transform it into an effectively universal right, in opposition to the historical view of property as a privilege of the few** (Maia, 2024, p. 142, was highlighted).

In Brazil, the context that takes as its scope the arable land and the rural real estate, from the time it is put on the market, can be described as a game: a) that starts from the King's hereditary concessions (e.g., letters of sesmarias, subject to the penalty of

Revista ARACÊ
ISSN: 2358-2472

commission and becomes vacant to the Crown or the Empire); b) it oscillates towards absolute private appropriation at the end of the Empire (Land Law No. 601/1850; Mortgage Law on rural property, Law No. 1,237/1864) and throughout the Old Republic (Civil Code, CC/1916); c) to move to a period of resumption of public ownership of assets that are of interest to common purposes (e.g., the 1934 Water Code, mining subsoil in the CF/1934, the Continental Shelf, etc.); d) to incorporate the principle of social function (Charter of Punta Del Leste, ET/1964, CF/1988 and CC/2002), which imposes on the owner a list of duties inspired by the teleological achievement of some purpose recognized as of a social nature.[48]

In this historical-cultural game, there was a dematerialization of corporeal things and a virtualization of a wide range of objects (digital assets) from innovative and disruptive business formats (Maia, 2024), which demanded a greater scope of property rights, especially after contemporary constitutionalism, with the identification of hyposufficient (such as the consumer) and the search for normative provisions that envisioned their protection, still pending social effectiveness today.

However, the LGPD does not notice this clear identification of a hyposufficiency in the individual of the holder of their own personal data, by seeking the protection of their individual rights and guarantees, including the recognition of their right of private ownership over their own data.

It can be seen that the treatment reserved for them in the face of the power granted to the controller-operator binomial is all referred to open concepts, which can be applied by this same hyper-sufficient binomial.

As if that were not enough, controllers/operators are entitled to invoke the fulfillment of some social function and at all times invoke the protection of their confidential intangible property (commercial and industrial secret), as immaterial as that of the personal data that they can mine without the prior consent of their holders and without any mining state grant.

This mining, almost without any control, reserves a last hope, deposited in the power of a central superauthority, the ANPD, which will perhaps observe prudence and its duty of necessary express motivation (art. 15 and 489, § 2, CPC) when faced with decisions that

[48] Such as, for example, in relation to rural property (art. 186, CF/1984): 1) its rational and adequate use (impediments to mere speculative appropriation, which does not excel in the productivity of goods for quantitative and qualitative food security of the national collectivity); 2) exploitation in order to conserve and preserve the environment (a heritage of all, from the present to future generations); 3) observance of the regulation of labor relations (rural employee, agricultural or livestock parcel worker, rural tenant, as impediments to the overexploitation of people considered hyposufficient); 4) promotion of the social well-being of rural landowners and these workers: social security, rural module, family property, etc. (Braga, 1991, p. 96-113; Neves, 2011, p. 116-128).

Revista ARACÊ
ISSN: 2358-2472

will necessarily have to weigh the collision between the principle of private ownership of personal data (extending to ownership) and the degree of public and private interference; Had it not been for the police power all deposited in its hands, it could not decide outside the due administrative legal process.

Not that the ownership of personal data cannot be protected, from now on, or even limited to it due to the fulfillment of the social function on the part of the controllers-operators who become the owner by applying any processing to a plexus of mined personal data.

However, in view of the long *vacatio legis* on such a pressing subject to which the LGPD (2018) was submitted until May 2021 (excluding the ANPD), it was enough to invoke the individual rights and guarantees of article 5 of the current CF/1988 to resolve the collisions of principles during this implicit period of mining, processing, and negotiation of personal data in open commercial circulation. We all undergo a reification (Honneth, 2018; Martins, 1998), resulting from the exploitation of a significant portion of the precarious human condition in the disruptive technological present.

This mandatory collision of principled norms already inserts, in the FC/1988, a tension, so that private property is not absolute, entailing reasonable and proportional limitations and serving to combat the abuse of the right to be a property owner (such as, for example, expropriation/sanction for the purposes of agrarian reform). The starting point, then, is the freedom to be a private owner/holder (minimum patrimonial sphere), weighted by the fulfillment of its social function (social inclusion).

For the processing of personal data, there is no constitutional obstacle to the characterization of the freedom to be a private owner/holder as another strain of the right to property (extended to ownership). On the contrary, treating them as a right to property of their holders expands this constitutional protection (Neves; Matos, 2023).

Once the right to property is combined with its inescapable social function, fundamental rights and guarantees of the current CF/1988, will serve to protect the holder of his own personal data, today a hyposufficient one made available to giants that daily mine, process and exploit his personal data, taking commercial advantage and claiming his property rights and protection of industrial or commercial secrecy over "his processed personal data".

In fact, a concrete appropriation in the face of those who cannot even claim their condition of expropriation results in a complete absence of tutelage by the State in this

Revista ARACÊ
ISSN: 2358-2472

already immolated human condition. In this context, on the one hand, the indispensable protection of individual freedoms, including from the perspective of the protection of the ownership of one's own (personal) data, and, on the other hand, the protection of freedoms of expression (defense of non-violent or intolerant ideologies in the democratic political arena), intellectual property (artistic production, such as the production of unauthorized biographies; exploitation of the image of people who inadvertently donate their property, by accepting the conditions imposed uniformly by "free" applications) and industrial property (industrial secrets of data processing algorithms that train AIs to manipulate human behavior in favor of *marketing* interests, including agencies specializing in advertisements and political campaigns, notably *outsiders*).

Not without reason, the then Governor of the state of Pernambuco decreed (Decree No. 49,265, of August 6, 2020[49]) the intention to enjoy part of this power to also dispose of personal data, as if the power to legislate on this matter had been concurrent (art. 24, items V and IX, CF/1988) and as if he were only acting in the exercise of common material competence reserved to the states, to the Union and the municipalities (art. 23, CF/1988), without any concern about the production of normative acts outside the due legislative process, produced outside the democratic arena, which is not justified even in times of pandemic.

In order to include the protection of personal data among the fundamental rights and guarantees, and to establish the exclusive competence of the Union to legislate on the protection and processing of personal data, by the Proposed Amendment to the Constitution (PEC) No. 17/2019,[50] the need for a derived constitutional legislative amendment was ventilated so that the right to the protection of personal data would be treated as a fundamental right and culminated in the amendment of the CF/1988 via Constitutional Amendment No. 115/2022.

Without forgetting the importance of being included as a fundamental right in the CF/1988, according to the GDPR guideline, but looking at this protection from the perspective of the right to property and its counterpoint, the fulfillment of its social function, both the right to property and the fulfillment of its social function, are already inscribed as stony guarantees expressly declared as a fundamental right of all in the CF/1988.

[49] Available at: https://www.lai.pe.gov.br/facepe/wp-content/uploads/sites/29/2021/07/DECRETO-No-49-265-DE-6-DE-AGOSTO-DE-2020.pdf
[50] Available at: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757 and https://www25.senado.leg.br/web/atividade/materias/-/materia/135594.

Revista ARACÊ
ISSN: 2358-2472

In addition, both PEC No. 17/2019 and EC No. 115/2022 focused on the inclusion, as a private legislative competence of the Union, of the enactment of laws such as the LGPD, already enacted since 2018. However, this same exclusive legislative competence of the Union already derives from article 22 of the CF/1988, in which the Union legislates on information technology (item IV), statistical system (item XVIII) and public records (item XXV). It is also worth mentioning the provision of concurrent legislative competence to enact laws such as those provided for in items V (production and consumption) and IX (technology) of article 24, also of the current CF/1988, since personal data are subject to extraction, processing, use and negotiation by an immeasurable range of computer systems (e.g., DataPrev, SerPro, Electronic Invoice with the State Treasury Secretariats, etc.), statistical (IBGE, Mauro Borges Institute – IMB, etc.) and public records (National Multibiometric and Fingerprint Bank, Genetic Profile Database, National Civil and Criminal Identification System, etc.).

CONCLUSION

The *constitutional status* conferred on the protection of personal data as a fundamental right by Constitutional Amendment No. 115/2022, widely conceived as a reflection of international interaction and as the last piece to compose a microsystem for the "protection" of this fundamental right, in this study was used for a critical approach to this new oil mined in the clouds (Maia, 2019), focusing on the vulnerability of citizens in the face of the exploitation and manufacture of your personal data, in the LGPD called personal data processing.

This view is important for the protection of individuals (private sphere), society (social purposes) and the Democratic Rule of Law itself (public sphere), before those who come to hold the power of data, whose dimension of action is still undefined, given the cyclical movement of successive processing to which personal data can be subjected and the consequent dissemination of citizens' information.

From the historical understanding and evolution of the concept of privacy, it is understood the insertion, in the LGPD, of respect for privacy and informational self-determination as foundations and guarantee to citizens for control over their own data. However, the same law that brings these protections in its foundations and the insignia of the "protection" of personal data, excepted several hypotheses for the processing of the personal data of the holder with the waiver of his consent (art. 7, II to XX, art. 11, II,

Revista ARACÊ
ISSN: 2358-2472

paragraphs 'a' to 'g') and resorted to several open concepts, such as "legitimate interest of the controller", "legitimate purposes", "legal or regulatory obligation", "necessary for the execution of public policies" or "for the performance of studies by a research body", which point much more to the regulation of the form of exploitation of the data of the hyposufficient holder than to the protection of his interests.

Therefore, it was decided to use the expressions "protagonism" and "protection" in quotation marks, given the disvalue of the holder of personal data in an effective "protagonism" and in the de facto protection of the "protection" of their personal data, mitigated by the figure of controllers and operators responsible for the processing of personal data, natural or legal persons, of public or private law with different interests in personal data.

The power of processing the data of a mass of holders brings with it the risk of manipulation of citizens, given the capacity of AIs, *big data*, and data mining by giants such as Google, Twitter, Instagram, Tik Tok, etc., exemplified by the *Cambridge Analytica* scandal and the data leak of millions of Facebook users. This spillage of citizens' data demonstrated their status as merchandise put on trade and, in Brazil, convictions in public civil actions are pending judgment (appeals filed).

In terms of violations of the right to the protection of personal data, contradictions and variability have been observed in recent court judgments, in cases in which the processing agents alternate, via public or private entities, but the citizens who are the holders of personal data always remain in the condition of being exploited, including in the face of the appropriation of their genetic information. such as the aforementioned ADPF 1,175, which deals with the indiscriminate investigation of the medical life of consumers of insurance and health plans, with the collection of their sensitive personal data even before pricing and contracting services.

Of these cases submitted to the judgment of the Judiciary, reference to the models and institutions of other States was observed as a constant, such as the German Census Law, brought as a paradigm for the judgment of ADI 6,387 and related by the STF, in 2020, about Provisional Measure No. 954/2020, which provided for the sharing of names, e-mails and addresses by telephone concessionaires with the IBGE and culminated in the recognition of the protection of personal data as a fundamental right.

Notwithstanding its general recognition as a paradigm in the protection of personal data and the coincidence with the Brazilian case of the prevalence of the limitation on the

Revista ARACÊ
ISSN: 2358-2472

collection and processing of personal data, having as a high point the proportionality for the hypotheses of relativization of the affirmed fundamental right to informational self-determination, the core of the German question referred to the concrete possibility of forming a complete personality profile, of much greater scope than the collection and processing of the names, e-mails and addresses of Brazilian citizens.

The LGPD's reservation for the use of the expression ownership for the subject of personal data rights was followed by Roberta Maia's (2020, 2019) understanding of its legal nature and the option for the genus of which property is a species. From its insertion as a patrimonial legal situation, it was recognized the possibility that personal data may have economically appreciable content and, therefore, be considered patrimonial in the sense that it can be part of the assets of its holder (Neves; Matos, 2023) and also of the processing agents whose personal data were regularly transferred for lawful processing purposes, without forgetting the existential regime of personal data protection and the off-balance sheet or existential rights linked to non-sensitive personal data, such as freedom, intimacy and privacy, all of which are located in the field of fundamental personality rights (Maia, 2020).

Recognizing this character of personal data, and in order to face the pragmatic challenge of how to regulate the ownership of personal data, the ownership of the data itself was related to the principles of private property and its social function, extended to ownership as an instrument of protection to the person, taking into account the historical meaning of the right to property as a minimum patrimonial sphere of the individual and, at the same time, as an instrument of social inclusion.

Despite the normative advance of a legal microsystem of data "protection" in the Brazilian legal scenario, the regulation of the ownership of this data is crossed by the interests of the processing agents (controllers and operators). In view of this, it is alerted to the risk of weakening the constitutionally recognized fundamental right to the protection of personal data and a critical revisit of the personal data protection microsystem is suggested, to be seen under vigilance, especially regarding the hypotheses of waiver of the consent of the holder.

Revista ARACÊ
ISSN: 2358-2472

REFERENCES

1. Adorno, S. (1995). Violência na sociedade brasileira: Um painel inconcluso em uma democracia não consolidada. Revista Sociedade e Estado, 10(2), 299–342. Available at: https://periodicos.unb.br/index.php/sociedade/article/view/44055/33673 (Accessed June 20, 2023).

2. Ataíde, M. C. F., & Sousa, M. M. (2023). Revisão sistemática dos indicadores de eficácia em bancos de DNA forenses. Revista Brasileira de Segurança Pública, 17(1), 166–187. https://doi.org/10.31060/rbsp.2023.v17.n1.1527 Available at: https://revista.forumseguranca.org.br/index.php/rbsp/article/view/1527 (Accessed March 20, 2023).

3. Barbetta, P. A. (2019). Estatística aplicada às Ciências Sociais (9th ed., 3rd rev. reprint). Florianópolis: Editora da Universidade Federal de Santa Catarina.

4. Becker, J. L. (2015). Estatística básica: Transformando dados em informação (1st ed.). Porto Alegre: Bookman. Available [for professors] at: https://viewer.bibliotecaa.binpar.com/viewer/9788582603130/capa (Accessed February 5, 2021).

5. Beltramini, L. S. (2015). Identificação por DNA de agressores sexuais no Rio Grande do Sul: Caracterização da melhor sistemática para obtenção de perfil genético autossômico com finalidade de confronto em banco de DNA criminal [Master's dissertation, Pontifícia Universidade Católica do Rio Grande do Sul]. Porto Alegre.

6. Binenbojm, G. (2014). Uma teoria do Direito Administrativo: Direitos fundamentais, democracia e constitucionalização (3rd rev. and updated ed.). Rio de Janeiro: Renovar.

7. Bonaccorso, N. S. (2005). Aplicação do exame de DNA na elucidação de crimes [Master's dissertation, Universidade de São Paulo]. São Paulo.

8. Borges, C. M. R., & Nascimento, D. S. (2022). O reflexo da seletividade do sistema de justiça criminal na composição dos bancos de perfis genéticos. Revista da Faculdade de Direito da UFRGS, 50, 150–182. https://doi.org/10.22456/0104-6594.124895 (Accessed August 24, 2024).

9. Brasil. Presidência da República. (1984). Lei n.º 7.210, de 11 de julho de 1984. Institui a Lei de Execução Penal. Brasília: Presidência da República. Available at: http://www.planalto.gov.br/ccivil_03/leis/l7210.htm (Accessed June 2, 2020).

10. Brasil. Presidência da República. (1988). Constituição da República Federativa do Brasil: Promulgada em 5 de outubro de 1988. Available at: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm (Accessed September 15, 2019).

11. Brasil. Presidência da República. (1990). Lei n.º 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República. Available at: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm (Accessed August 31, 2024).

Revista ARACÊ
ISSN: 2358-2472

12. Brasil. Presidência da República. (2002). Lei n.º 10.406, de 10 de janeiro de 2002. Código Civil. Brasília: Presidência da República. Available at: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm (Accessed August 31, 2024).

13. Brasil. Presidência da República. (2012). Lei n.º 12.654, de 28 de maio de 2012. Altera as Leis nºs 12.037, de 1º de outubro de 2009, e 7.210, de 11 de julho de 1984 – Lei de Execução Penal, para prever a coleta de perfil genético como forma de identificação criminal, e dá outras providências. Brasília: Presidência da República. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12654.htm (Accessed June 2, 2020).

14. Brasil. Presidência da República. (2018a). Lei n.º 13.675, de 11 de junho de 2018. Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública. Brasília: Presidência da República. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm (Accessed August 24, 2024).

15. Brasil. Presidência da República. (2018b). Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm (Accessed June 2, 2020).

16. Brasil. Presidência da República. (2019). Lei n.º 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Brasília: Presidência da República. Available at: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm (Accessed June 2, 2020).

17. Brasil. Supremo Tribunal Federal. (n.d.). Ação de Descumprimento de Preceito Fundamental (ADPF) 1.175. Relator: Ministro Dias Toffoli. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6945077 (Accessed August 26, 2024).

18. Brasil. Supremo Tribunal Federal. (n.d.). Ação Direta de Inconstitucionalidade 4.815. Relatora: Ministra Cármen Lúcia. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4271057 (Accessed May 15, 2023).

19. Brasil. Supremo Tribunal Federal. (n.d.). Ação Direta de Inconstitucionalidade 6.387. Relatora: Ministra Rosa Weber. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165 (Accessed May 15, 2023).

20. Brasil. Supremo Tribunal Federal. (n.d.). Mandado de Segurança 21.729. Relator: Ministro Marco Aurélio. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=1569577 (Accessed August 24, 2024).

21. Brasil. Supremo Tribunal Federal. (n.d.). Recurso Extraordinário 418.416. Relator: Ministro Sepúlveda Pertence. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2205705 (Accessed August 24, 2024).

Revista ARACÊ
ISSN: 2358-2472

22. Brasil. Supremo Tribunal Federal. (n.d.). Recurso Extraordinário 673.707. Relator: Ministro Luiz Fux. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4204594 (Accessed August 29, 2024).

23. Brasil. Supremo Tribunal Federal. (n.d.). Recurso Extraordinário 1.055.941. Relator: Ministro Dias Toffoli. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5213056 (Accessed August 29, 2024).

24. Brito, A. F., & Pontes, A. P. (2020). Identificação humana por DNA através do banco nacional de perfis genéticos e a quantificação de amostras armazenadas. Revista Brasileira de Criminalística, 9(2), 76–84. http://dx.doi.org/10.15260/rbc.v9i2.328 Available at: https://revista.rbc.org.br/index.php/rbc/article/view/328 (Accessed March 19, 2023).

25. Campêlo, R. V. C. (2022). Análise da (in)constitucionalidade da extração compulsória de DNA de condenados por crimes dolosos ou aqueles determinados em lei como hediondos [Undergraduate thesis, Universidade Federal do Rio Grande do Norte]. Available at: https://repositorio.ufrn.br/handle/123456789/46800 (Accessed November 12, 2023).

26. Campos, M. S., & Alvarez, M. C. (2017). Políticas públicas de segurança, violência e punição no Brasil. In S. Miceli & C. B. Martins (Eds.), Sociologia brasileira hoje (pp. 143–201). São Paulo: Ateliê Editorial.

27. Cardoso, J. F., Sato, M. O., & Santiago, R. M. (2017). Organização e funcionamento do banco de dados de perfil genético do Paraná. Revista Saúde e Desenvolvimento, 11(7). Available at: https://www.revistasuninter.com/revistasaude/index.php/saudeDesenvolvimento/article/view/655 (Accessed March 19, 2023).

28. Cardoso, T. M. P. (2022). Identificação por perfil genético para fins criminais: Reflexões sobre as modificações trazidas pela Lei n.º 13.964/2019. Boletim Científico ESMPU, 21(58).

29. Carvalho, S. P. M. (2009). Avaliação da qualidade do DNA obtido de saliva humana armazenada e sua aplicabilidade na identificação forense em odontologia legal [Master's dissertation, Universidade de São Paulo]. Available at: https://www.teses.usp.br/teses/disponiveis/25/25141/tde-02062009-105931/pt-br.php (Accessed August 24, 2024).

30. Carvalho, L. C. C. (2014). A utilização de exames de DNA como forma de garantia de direitos fundamentais no processo penal [Undergraduate thesis, Universidade de Brasília].

31. Carvalho, R. A. (2022). Os eventuais impactos das redes sociais na qualidade democrática: Estudo de caso sobre o escândalo de dados Facebook/Cambridge Analytica [Undergraduate thesis, Universidade Federal da Paraíba].

32. Cerqueira, D. R. C. (2014). Causas e consequências do crime no Brasil. Rio de Janeiro: BNDES.

Revista ARACÊ
ISSN: 2358-2472

33. Costa, A. T. M., & Lima, R. S. (2018). Estatísticas oficiais, violência e crime no Brasil. BIB, 2(84), 81–106. https://doi.org/10.17666/bib8403/2018 Available at: https://bibanpocs.emnuvens.com.br/revista/article/view/437/415 (Accessed June 21, 2023).

34. Costa, J. B. (1993). Arrendamento rural: Direito de preferência (1st ed.). Goiânia: AB.

35. Council of Europe. (1981). Convention n. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (Accessed July 24, 2020).

36. Creswell, J. W. (2010). Projeto de pesquisa: Métodos qualitativo, quantitativo e misto (M. Lopes, Trans.; D. Silva, Tech. Rev.). Porto Alegre.

37. Doneda, D. C. M. (2006). Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar.

38. Doneda, D. (2011). A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Joaçaba, 12(2), 91–108.

39. Estellita, H. (2023). O legado de Rosa Weber na proteção da privacidade e tratamento de dados pessoais. Jota. Available at: https://www.academia.edu/107697818/O_legado_de_Rosa_Weber_na_prote%C3%A7%C3%A3o_da_privacidade_e_tratamento_de_dados_pessoais (Accessed February 18, 2024).

40. European Parliament and of the Council. (1995). Directive 95/46/EC. Available at: https://eur-lex.europa.eu/eli/dir/1995/46/oj (Accessed June 7, 2020).

41. European Union. (n.d.). Convenção Europeia dos Direitos do Homem. Available at: https://www.echr.coe.int/documents/d/echr/convention_por (Accessed August 31, 2024).

42. European Union. (2016). Diretiva (EU) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Jornal Oficial das Comunidades Europeias, 119. Available at: https://eur-lex.europa.eu/legal-content/PT/TXT/html (Accessed September 15, 2021).

43. European Union. (1950). European Convention on Human Rights. Available at: https://www.echr.coe.int/Documents/Convention_ENG.pdf (Accessed July 24, 2020).

44. European Union. European Court of Human Rights. (n.d.). Antonio Peruzzo against Germany and Uwe Martens against Germany. Applications nos. 7841/08 and 57900/12. Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-121998%22]} (Accessed August 31, 2024).

45. European Union. European Court of Human Rights. (2008). S. and Marper vs. The United Kingdom (Applications nos. 30562/04 and 30566/04). Available at: https://www.echr.coe.int/d/reports_recueil_2008-v?p_l_back_url=%2Fsearch%3Fq%3Dmarper (Accessed May 15, 2014).

46. Fanon, F. (1968). Os condenados da terra. Rio de Janeiro: Editora Civilização Brasileira.

Revista ARACÊ
ISSN: 2358-2472

47. Ferraz Júnior, T. S. (1993). Sigilo de dados: O direito à privacidade e os limites à função fiscalizadora do Estado. Revista dos Tribunais. Available at: https://www.revistas.usp.br/rfdusp/article/view/67231 (Accessed February 25, 2022).

48. Ferreira, C. T. (2021). Política penitenciária nacional (1976-2018): Arranjos institucionais e instrumentos de produção estatística [Doctoral dissertation, Fundação Getulio Vargas].

49. Fornasier, M. O., & Beck, C. (2020). Cambridge Analytica: Escândalo, legado e possíveis futuros para a democracia. Revista Direito em Debate, 29(53), 182–195. https://doi.org/10.21527/2176-6622.2020.53.182-195 Available at: https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033 (Accessed February 10, 2024).

50. Frazão, A. (2020). Objetivos e alcance da Lei Geral de Proteção de Dados. In G. Tepedino et al. (Eds.), A lei geral de proteção de dados pessoais e suas repercussões no Direito brasileiro (pp. 97–125). São Paulo: Revista dos Tribunais.

51. Frazão, A. (2023). O Direito constitucional à proteção de dados: Reflexões sobre as contribuições do voto da Ministra Rosa Weber na ADI 6.387. In M. E. G. T. Rocha et al. (Eds.), Ela pede vista: Estudos em homenagem à Ministra Rosa Weber (pp. 153–127). São Paulo: Thoth Editora.

52. Freire, M. D. (2009). Paradigmas de segurança no Brasil: Da ditadura aos nossos dias. Revista Brasileira de Segurança Pública, 5, 100–115.

53. Garrido, R. G., & Rodrigues, E. L. (2015). O Banco de Perfis Genéticos brasileiro três anos após a Lei n.º 12.654. Revista de Bioética y Derecho, 35, 94–107. https://dx.doi.org/10.1344/rbd2015.35.14284

54. Garrido, R. G. (2018). Crítica científica de “Investigação criminal genética – banco de perfis genéticos, fornecimento compulsório de amostra biológica e prazo de armazenamento de dados” – Apontamentos sobre a inconstitucionalidade da Lei 12.654/2012. Revista Brasileira de Direito Processual Penal, 4(2), 809–842. https://doi.org/10.22197/rbdpp.v4i2.122 (Accessed May 21, 2024).

55. Garrido, R. G., & Costa, B. R. N. (2020). O banco nacional de perfis genéticos: Uma análise da efetividade e eficiência. Revista Duc In Altum Cadernos de Direito, 12(27). https://doi.org/10.22293/2179-507x.v12i27.1308 Available at: https://revistas.faculdadedamas.edu.br/index.php/cihjur/article/view/1308/944 (Accessed April 19, 2023).

56. Giovanelli, A. (2022). A construção do laudo pericial ao longo do tempo: As disputas de poder no âmbito da persecução penal. Research, Society and Development, 11(3), 1–14.

57. Guedes, G. P., & Felix, Y. (2014). A identificação genética na Lei n.º 12.654/2012 e os princípios de direito processual penal no estado democrático de direito. Revista de Estudos Criminais, 12(53), 157–179.

58. Harari, Y. N. (2016). Homo Deus: Uma breve história do amanhã. São Paulo: Companhia das Letras.

Revista ARACÊ
ISSN: 2358-2472

59. Harari, Y. N. (2018). 21 lições para o século 21 (1st ed.). São Paulo: Companhia das Letras.

60. Harari, Y. N. (2020, March). The world after coronavirus. Financial Times. Available at: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75 (Accessed April 6, 2020).

61. Honneth, A. (2018). Reificação: Um estudo da teoria do reconhecimento (R. Melo, Trans.). São Paulo: Editora Unesp.

62. Justen Filho, M. (1999). Conceito de interesse público e a "personalização" do direito administrativo. Revista Trimestral de Direito Público, 26, 115–136.

63. Levitsky, S., & Ziblatt, D. (2018). Como as democracias morrem (R. Aguiar, Trans., 1st ed.). Rio de Janeiro: Zahar.

64. Lima, R. S., Sinhoretto, J., & Bueno, S. (2015). A gestão da vida e da segurança pública no Brasil. Revista Sociedade e Estado, 30(1), 123–144. Available at: https://www.scielo.br/j/se/a/GXvgpX8S3K9dFzL4GMCky7G/?lang=pt (Accessed June 20, 2023).

65. Lima, R. S., Bueno, S., & Mingardi, G. (2016). Estado, polícias e segurança pública no Brasil. Revista Direito GV, 12(1), 49–85. Available at: https://www.scielo.br/j/rdgv/a/k8CfD9XbDpJ8vzyfJqXP3qN/?format=pdf&lang=pt (Accessed June 20, 2023).

66. Lima, R. K., Misse, M., & Miranda, A. P. M. (2000). Violência, criminalidade, segurança pública e justiça criminal no Brasil: Uma bibliografia. Revista Brasileira de Informação Bibliográfica em Ciências Sociais – BIB, 50, 45–123. Available at: https://app.uff.br/riuff/handle/1/10294 (Accessed June 21, 2023).

67. Lock, R. H., et al. (2017a). Estatística: Revelando o poder dos dados (A. M. L. Farias & V. R. L. Flores, Trans.). Rio de Janeiro: LTC.

68. Lock, R. H., et al. (2017b). Statistics: Unlocking the power of data (2nd ed.). Hoboken, NJ: Wiley.

69. Louzada, L. C., & Rohden, A. L. M. (2022). Bancos de Perfis Genéticos para fins de investigação criminal no Brasil. São Paulo: Associação Data Privacy Brasil de Pesquisa.

70. Machado, F. I. S. (2018). Privacidade e proteção de dados pessoais na sociedade da informação: Profiling e risco de discriminação [Master's dissertation, Pontifícia Universidade Católica do Rio Grande do Sul].

71. Macorin, P. S. C. (2018). A utilização do banco de dados de perfis genéticos na persecução criminal: Uma abordagem sobre os direitos de personalidade e o princípio da não autoincriminação. Revista Brasileira de Ciências Policiais, 9(1), 91–108. Available at: https://periodicos.pf.gov.br/index.php/RBCP/article/view/517 (Accessed May 15, 2023).

72. Mahmoud, M. A. H., & Moura, M. T. R. A. (2012). A Lei 12.654/2012 e os direitos humanos. Revista Brasileira de Ciências Criminais, 20(98), 339–358.

Revista ARACÊ
ISSN: 2358-2472

73. Maia, R. M. M. (2013). Teoria geral dos direitos reais. São Paulo: RT.

74. Maia, R. M. M. (2019). Vivendo nas nuvens: Dados pessoais são objeto de propriedade? In G. Tepedino & J. B. Menezes (Eds.), Autonomia privada, liberdade existencial e direitos fundamentais (pp. 669–697). Belo Horizonte: Fórum.

75. Maia, R. M. M. (2020). A titularidade dos dados pessoais prevista no art. 17 da LGPD: Direito real ou pessoal? In G. Tepedino, A. Frazão, & M. D. Oliva (Eds.), Lei geral de proteção de dados pessoais: E suas repercussões no Direito brasileiro (2nd ed., pp. 127–152). São Paulo: Thomson Reuters Brasil.

76. Maia, R. M. M. (2024). A propriedade como instrumento de proteção da pessoa: Nota sobre a tutela do adquirente de bens digitais. In J. B. Menezes & F. N. Barbosa (Eds.), A prioridade da pessoa humana no Direito Civil-Constitucional: Estudos em homenagem a Maria Celina Bodin de Moraes. Indaiatuba, SP: Editora Foco. Available at: https://www.google.com.br/books/edition/A_Prioridade_da_Pessoa_Humana_no_Direito/TO3xEAAAQBAJ?hl=pt-BR&gbpv=1&printsec=frontcover (Accessed March 21, 2024).

77. Mariano Júnior, A. R. (2014). A (des)regularização da obtenção do material biológico no processo penal brasileiro. Revista Magister de Direito Penal e Processual Penal, 11(63), 78–92.

78. Mariú, P. R. (2018). A busca pela equidistância entre garantismos: Identificação criminal de perfis genéticos e análise da constitucionalidade do art. 9-A da Lei de Execuções Penais no Recurso Extraordinário n.º 973837/MG. Revista do Ministério Público do Rio de Janeiro, 70, 209–223. Available at: https://www.mprj.mp.br/servicos/revista-do-mp/revista-70/pags-209-223 (Accessed May 25, 2024).

79. Martial-Braz, N. (2018). O direito das pessoas interessadas no tratamento de dados pessoais: Anotações da situação na França e na Europa. Revista de Direito, Estado e Telecomunicações, 10(1), 85–108. https://doi.org/10.26512/lstr.v10i1.21501 Available at: https://periodicos.unb.br/index.php/RDET/article/view/21501 (Accessed August 27, 2024).

80. Martins, J. S. (1998). O cativeiro da terra (7th ed.). São Paulo: Hucitec.

81. Martins, L. (Ed.). (2005). Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. BVerfGE 65, 1, “Recenseamento” (Volkszählung) (B. Hennig et al., Trans.). Montevidéu: Fundação Konrad Adenauer.

82. Mateleto Filho, W. (2012). O direito à não autoincriminação no processo penal contemporâneo. Belo Horizonte: Del Rey.

83. Mendes, L. S., & Doneda, D. (2018). Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): O novo paradigma da proteção de dados no Brasil. Revista de Direito do Consumidor, 120, 555–587. Available at: https://www.academia.edu/42740879/Coment%C3%A1rio_%C3%A0_nova_Lei_de_Prote%C3%A7%C3%A3o_de_Dados_lei_13_709_2018_o_novo_paradigma_da_prote%C3%A7%C3%A3o_de_dados_no_brasil (Accessed February 18, 2024).

Revista ARACÊ
ISSN: 2358-2472

84. Mendes, L. S., & Fonseca, G. C. S. (2020). STF reconhece direito fundamental à proteção de dados: Comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. Revista de Direito do Consumidor, 130, 471–478. Available at: https://edisciplinas.usp.br/pluginfile.php/7695208/mod_resource/content/1/1%20-Revista%20dos%20Tribunais%2C%20v.%201%2C%20p.%2035%2C%202019.pdf (Accessed February 18, 2024).

85. Menezes, L. J. P. S. (2020). A Lei n. 12.654/2012 e sua controvérsia constitucional: Uma análise sobre o Banco Nacional de Perfis Genéticos e a obrigatoriedade na coleta de DNA [Undergraduate thesis, Universidade Federal Rural do Semiárido].

86. Milagre, J., & Santarém Segundo, J. E. (2015). A propriedade dos dados e a privacidade na perspectiva da Ciência da Informação. Encontros Bibli – Revista Eletrônica de Biblioteconomia e Ciência da Informação, 20(43), 47–76. https://doi.org/10.5007/1518-2924.2015v20n43p47 Available at: https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2015v20n43p47/29945 (Accessed February 10, 2021).

87. Minervino, A. C., et al. (2019). Increasing convicted offender genetic profiles in the Brazilian National DNA Database — Legislation, projects and perspectives. Forensic Science International: Genetics Supplement Series, 7, 575–577. https://doi.org/10.1016/j.fsigss.2019.10.095 (Accessed March 19, 2023).

88. Minervino, A. C., et al. (2022). Projeto de coleta de amostra de condenados – Interação nacional e cumprimento legal em prol da justiça. Revista Brasileira de Ciências Policiais, 13(8), 53–70. https://doi.org.br/10.31412/rbcp.v13i8.930 (Accessed March 18, 2023).

89. Morais, L. S. (2020). Direito à privacidade no sistema regional europeu de direitos humanos. Revista de Direito Brasileira, 25(10), 200–220. Available at: https://www.indexlaw.org/index.php/rdb/article/view/3902 (Accessed May 25, 2024).

90. Morgado, C. O. (2018). Coleta do material biológico como forma de identificação criminal: Lei 12.654/12 e o princípio nemo tenetur se detegere [Undergraduate thesis, Universidade Federal de Uberlândia].

91. Nery Júnior, N. (2010). Princípios do processo na Constituição Federal (10th rev., expanded, and updated ed.). São Paulo: RT.

92. Netta, E. T. M. (2020). A ampliação do rol compulsório do Banco Nacional de perfis genéticos à luz da colisão entre a garantia da não autoincriminação e o direito à produção de provas [Undergraduate thesis, Universidade Federal da Paraíba].

93. Neves, C. B. (2011). Águas doces no Brasil. Rio de Janeiro: Descubra.

94. Neves, C. B., & Matos, G. G. (2023). E-commerce dos dados pessoais e a LGPD: Abordagem de uma lacuna à luz da teoria do ordenamento jurídico de Bobbio. Constituição, Economia e Desenvolvimento: Revista da Academia Brasileira de Direito Constitucional, 15(28). Available at: https://www.abdconstojs.com.br/index.php/revista/article/view/461/311 (Accessed January 9, 2023).

Revista ARACÊ
ISSN: 2358-2472

95. Neves, M. (2014). Do diálogo entre as cortes supremas e a Corte Interamericana de Direitos Humanos ao transconstitucionalismo na América Latina. Revista de Informação Legislativa, 51(201), 193–214. Available at: https://www12.senado.leg.br/ril/edicoes/51/201/ril_v51_n201_p193.pdf (Accessed October 20, 2024).

96. Nicolitt, A. L. (2013). Banco de dados de perfis genéticos (DNA). As inconstitucionalidades da Lei 12.654/2012. Boletim do IBCCRIM, 245, 15–16.

97. Oliveira, A. S. S., et al. (2002). Das políticas de segurança pública às políticas públicas de segurança. São Paulo: Ilanud.

98. Oliveira, M. A. B., & Lopes, I. M. P. (2020). Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In G. Tepedino et al. (Eds.), Lei geral de proteção de dados pessoais e suas repercussões no Direito brasileiro (pp. 53–81). São Paulo: Revista dos Tribunais.

99. Oliveira, L. C. (2021). O uso de dados pessoais na Era Digital como forma de manipulação social e ameaça à democracia: Um estudo de caso da Cambridge Analytica [Undergraduate thesis, Pontifícia Universidade Católica de Goiás].

100. Oliveira, A. A. B. (2023). Abordagem bioética no estabelecimento e no significado para a sociedade sobre o uso de perfis genéticos na identificação criminal [Doctoral dissertation, Universidade de Brasília].

101. OPAS – Organização Pan-Americana da Saúde. (2023). OMS declara fim da emergência de saúde pública de importância internacional referente à Covid-19. Available at: https://www.paho.org/pt/noticias/5-5-2023-oms-declara-fim-da-emergencia-saude-publica-importancia-internacional-referente (Accessed August 25, 2024).

102. Pereira, C. M. S. (2010). Instituições de Direito Civil: Teoria Geral das Obrigações (23rd rev. and updated ed., G. C. N. Gama, Ed.). Rio de Janeiro: Forense.

103. Pereira, C. M. S. (2014). Instituições de Direito Civil: Introdução ao Direito Civil; Teoria Geral de Direito Civil (27th rev. and updated ed., M. C. B. Moraes, Ed.). Rio de Janeiro: Forense.

104. Prestes, M. V. P., et al. (2021). Lei Geral de Proteção de Dados n.º 13.709/2018: Apontamentos sobre sua contextualização como marco legal no Brasil. Research, Society and Development, 10(12). http://dx.doi.org/10.33448/rsd-v10i12.20906 Available at: https://rsdjournal.org/index.php/rsd/article/view/20906 (Accessed February 18, 2024).

105. Rabelo, J. G. (2018). A coleta compulsória de material biológico para obtenção de perfil genético: Uma análise do Recurso Extraordinário n.º 973.837 e da Lei n.º 12.654 à luz de Dworkin [Undergraduate thesis, Universidade de Brasília]. Available at: https://bdm.unb.br/handle/10483/21989 (Accessed August 24, 2024).

106. Raldi, A. P. S., & Puhl, E. (2021). Banco de dados de DNA sobre o prisma da criminologia crítica. Revista Científica Eletrônica Academia de Direito, 3, 124–142. Available at: http://www.periodicos.unc.br/index.php/acaddir/article/view/3184/1550 (Accessed March 19, 2023).

Revista ARACÊ
ISSN: 2358-2472

107. Reale, M. (1996). Filosofia do Direito (17th ed.). São Paulo: Saraiva.

108. Rocha, W. S. (2017). Isolamento, preservação de local de crime e utilização do exame de DNA na identificação criminal: Uma proposta de padronização para o Estado do Tocantins [Master's dissertation, Universidade Federal da Bahia].

109. Rodotá, S. (2008). A vida na sociedade de vigilância: A privacidade hoje. Rio de Janeiro: Renovar.

110. Rodrigues, F. T. (2022). Sociedade civil global e os direitos digitais: A emergência de arranjos institucionais no âmbito da governança da internet a partir do caso Cambridge Analytica (CA). Revista Perspectiva: Reflexões Sobre a Temática Internacional, 15. Available at: https://seer.ufrgs.br/index.php/RevistaPerspectiva/article/view/124492 (Accessed January 9, 2024).

111. Ruaro, R. L., & Rodriguez, D. P. (2010). O direito à proteção de dados pessoais: Uma leitura do sistema europeu e a necessária tutela dos dados sensíveis como paradigma para um sistema jurídico brasileiro. Direitos Fundamentais e Justiça, 11, 163–180. Available at: https://dfj.emnuvens.com.br/dfj/article/view/438/315 (Accessed May 12, 2024).

112. Ruaro, R. L., & Rodriguez, D. P. (2011). O direito à proteção de dados pessoais e a privacidade. Revista da Faculdade de Direito – UFPR, 53, 45–66.

113. Schiocchet, T. (2013). A regulamentação da base de dados genéticos para fins de persecução criminal no Brasil: Reflexões acerca do uso forense do DNA. Revista Novos Estudos Jurídicos, 18(3), 518–529. https://doi.org/10.14210/nej.v18n3.p518-529 Available at: https://periodicos.univali.br/index.php/nej/article/view/5137 (Accessed December 31, 2021).

114. Schiocchet, T. (2014). Reflexões jurídicas acerca da regulamentação dos bancos de perfis genéticos para fins de investigação criminal no Brasil. In H. Machado & H. Moniz (Eds.), Bases de dados genéticos forenses: Tecnologias de controlo e ordem social (pp. 67–102). Coimbra: Coimbra Editora.

115. Schiocchet, T., & Cunha, A. S. (2021). Desmistificando o DNA: Análise dos argumentos difundidos na arena jurídica sobre perfis genéticos no Brasil. Revista da Faculdade de Direito UFPR, 66(3), 9–32. http://dx.doi.org/10.5380/rfdufpr.v66i3.74361 Available at: https://revistas.ufpr.br/direito/article/view/74361 (Accessed December 31, 2021).

116. Schwabe, J., & Martins, L. (Eds.). (2005). Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Berlim: Konrad-Adenauer-Stifung E.V. Available at: http://www.kas.de/wf/doc/kas_7738-544-4-30.pdf (Accessed July 24, 2020).

117. Schwartz, P. M. (2004). Property, privacy, and personal data. Harvard Law Review, 117(7), 2056–2128. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=721642 (Accessed February 10, 2021).

118. Serpa Júnior, W. S. (2017). A recusa do investigado ao fornecimento de material biológico nos casos previstos pela Lei 12.654/2012 [Undergraduate thesis, Universidade de Brasília].

Revista ARACÊ
ISSN: 2358-2472

119. Silva, M. S. (2012). Análise da constitucionalidade da Lei n.º 12.654/12, que prevê a coleta de perfil genético como forma de identificação criminal e dá outras providências [Undergraduate thesis, Centro Universitário de Brasília]. Available at: https://repositorio.uniceub.br/jspui/handle/235/4344 (Accessed March 19, 2023).

120. Silva, J. L., Emmendoerfer, M. L., & Cunha, N. R. S. (2020). Análise documental ilustrada em administração pública: Uma proposta operacional (re)aplicável. Teoria e Prática em Administração, 10(2), 23–41. https://doi.org/10.21714/2238-104X2020v10i2-51394 (Accessed August 25, 2024).

121. Silva, V. A. (2021). Direito Constitucional brasileiro (1st ed., 1st reprint). São Paulo: Editora da Universidade de São Paulo.

122. Silva Junior, R. C., et al. (2019). Geolocation of the Brazilian National DNA Database matches as a tool for improving public safety and the promotion of justice. Forensic Science International: Genetics Supplement Series, 7, 549–551. https://doi.org/10.1016/j.fsigss.2019.10.086 Available at: https://www.fsigeneticssup.com/action/showPdf?pii=S1875-1768%2819%2930424-X (Accessed March 19, 2023).

123. Soares, J. R. A. B. (2022). Política Nacional de Segurança Pública e Defesa Social: Análise da aderência dos planos estaduais de segurança pública e das capacidades estatais [Master's dissertation, Universidade de Brasília].

124. Soares, L. E. (2007). A Política Nacional de Segurança Pública: Histórico, dilemas e perspectiva. Estudos Avançados, 61, 77–98.

125. Sousa, S. S. (2018). Coleta de perfil genético e investigação criminal: Identificação criminal ou meio de prova, à luz do princípio da constitucionalidade? Revista de Direito de Polícia Judiciária, 2(3), 113–149. Available at: https://periodicoshom.pf.gov.br/index.php/RDPJ/article/view/554 (Accessed May 7, 2024).

126. Souza, M. B. (2019). Uma análise acerca da (in)constitucionalidade e da operacionalização da coleta de perfis genéticos de acordo com a Lei nº 12.654/2012 [Undergraduate thesis, Universidade Federal do Rio de Janeiro].

127. Suxberger, A. H. G. (2015). A funcionalização como tendência evolutiva do Direito Internacional e sua contribuição ao regime legal do banco de dados de identificação de perfil genético no Brasil. Revista de Direito Internacional, 12(2), 649–665. https://doi.org/10.5102/rdi.v12i2.3708

128. Suxberger, A. H. G., & Lima, J. W. F. (2017). O processo penal e a engenharia de controle da política criminal. Revista Brasileira de Políticas Públicas, 7(1).

129. Suxberger, A. H. G., & Furtado, V. T. M. M. (2018). Investigação criminal genética – Banco de perfis genéticos, fornecimento compulsório de amostra biológica e prazo de armazenamento de dados. Revista Brasileira de Direito Processual Penal, 4(2), 809–842. https://doi.org/10.22197/rbdpp.v4i2.122

Revista ARACÊ
ISSN: 2358-2472

130. Tepedino, G. (2000). Código Civil, os chamados microssistemas e a Constituição: Premissas para uma reforma legislativa. In G. Tepedino (Ed.), Problemas de Direito Civil-Constitucional (pp. 1–16). Rio de Janeiro: Renovar.

131. Tepedino, G. (2006). Temas de Direito Civil. Tomo II. Rio de Janeiro: Renovar.

132. Tepedino, G. (2011). Comentários ao Código Civil: Direito das Coisas (arts. 1.196 a 1.276) (A. J. Azevedo, Coord.). São Paulo: Saraiva.

133. Tepedino, G., & Teefé, C. S. (2020). Consentimento e proteção de dados pessoais na LGPD. In G. Tepedino et al. (Eds.), A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro (pp. 281–318). São Paulo: Revista dos Tribunais.

134. Trindade, B. R., & Costa Neto, J. (2018). Banco Nacional de Perfis Genéticos: Exame de constitucionalidade à luz da dignidade humana. Revista Brasileira de Ciências Policiais, 9(1), 175–211. https://doi.org/10.31412/rbcp.v9i1.515 Available at: https://periodicos.pf.gov.br/index.php/RBCP/article/view/515 (Accessed May 15, 2023).

135. UNESCO – Organização das Nações Unidas para a Educação, a Ciência e a Cultura. (2005). Declaração Universal sobre Bioética e Direitos Humanos. Available at: https://bvsms.saude.gov.br/bvs/publicacoes/declaracao_univ_bioetica_dir_hum.pdf (Accessed June 18, 2024).

136. Unger, R. M. (2004). O Direito e o futuro da democracia. São Paulo: Boitempo.

137. União Europeia. (2016). Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Jornal Oficial das Comunidades Europeias, 119. Available at: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN (Accessed September 15, 2021).

138. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220. Available at: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf (Accessed May 15, 2020).

139. Zaluar, A. (1999). Um debate disperso: Violência e crime no Brasil da redemocratização. São Paulo em Perspectiva, 13(3), 3–17.