The Right to Personal Data Protection – A Procedural Right

Rafael Tedrus Bento

TABLE DES MATIERES

Résumé

Cet article vise à définir le concept de droit à la protection des données à caractère personnel. À cet égard, il est important d'examiner les exigences formelles du droit à la protection des données à caractère personnel, à savoir le sujet, le contenu et l'objet. Ainsi, le domaine juridique devrait bénéficier grandement de cette recherche, notamment en raison du débat intense entourant la mise en œuvre du système mondial de protection des données à caractère personnel. En outre, ce travail académique cherche à identifier les modèles normatifs et les caractéristiques du droit fondamental en question. Il se situe donc dans le domaine de la dogmatique juridique. Pour répondre à ces questions, cette étude propose une exploration de la conception de la protection des données personnelles, en analysant ses origines et le développement de sa conception jusqu'à aujourd'hui. Il s'agit donc d'une étude de l'évolution de la compréhension de ce droit. Ainsi, nous pouvons définir les objectifs de cette thèse comme suit : (i) élucider la construction du droit à la protection des données personnelles, en considérant les exigences intrinsèques du droit subjectif fondamental ; (ii) identifier les exigences de propriété, d'objet et de contenu du droit subjectif actuel. Pour répondre à ces questions, cette étude sera structurée comme suit. Dans la première partie, un bref historique de la discussion sur le droit à la protection des données à caractère personnel et des sujets fréquemment liés sera fourni. Dans la deuxième partie, une analyse plus détaillée des concepts de vie privée, d'information et de protection des données personnelles sera présentée.

Abstract

This article aims to identify the concept of the Right to Personal Data Protection. In this regard, it is important to examine the formal requirements of the right to personal data protection, namely, subject, content, and object. Thus, the legal field stands to benefit greatly from this research, particularly given the intense debate surrounding the implementation of the global system for the protection of personal data. Furthermore, this academic work seeks to identify normative patterns and characteristics of the fundamental right in question. It is therefore situated within the field of legal dogmatics. To address these issues, this study proposes an exploration of the conception of personal data protection, analyzing its origins and the development of its conception to the present moment. It is, therefore, a study of the evolution of the understanding of this right. Thus, we can define the objectives of this thesis as follows: (i) To elucidate the construction of the right to personal data protection, considering the intrinsic requirements of the fundamental subjective right; (ii) To identify the requirements of ownership, object, and content of the current subjective right. To seek answers to these questions, this study will be structured as follows. In the first section, a brief history of the discussion on the right to personal data protection and frequently related topics will be provided. In the second part, a more detailed analysis of the concepts of privacy, informational self-determination, and the pursuit of an understanding of the right to personal data protection will be conducted. In the third stage, an examination of legislation and examples of jurisprudence in the United States of America will be undertaken. In the fourth part, an analysis of the scope and limits

of this fundamental right will be conducted, as well as an exploration of the understanding of the creation of due informational process and its connection to the right to personal data protection. In the fifth and final section, the "procedural" dimension of the right to personal data protection will be examined, with the aim of understanding the subjective and objective dimensions of the right, the potential essence of the right to personal data protection, and whether the right can be considered instrumental/procedural to ascertain whether the hypotheses described above are equivalent to the right pursued here.
Keywords: Personal Data Protection; Fundamental Right; Informational Self-Determination; Due Informational Process.

Introduction

The importance of determining the contours of this right has been renewed by events and debates brought forth in the 21st century, especially after 2010. Data leaks and public and private

scandals, such as those revealed in the episode of unauthorized data sharing between Facebook and Cambridge Analytica[1], make clear the timeliness of the discussion on personal data protection. Websites make available the history of personal data exposed irregularly around the world.[2] In his 2023 State of the Union address, President of the United States of America, Joe Biden, criticized the practices of personal data collection by Big Tech and the use of targeted ads to young users.[3] A society constantly surveilled and monitored, individuals identified in the minutiae of their personal lives, the power of personal data controllers renewed and multiplied with automated data collection.[4] Furthermore, approximately 65% of the world's GDP has been linked to the perspective of cross-border flows of personal data.[5]

All these factors lead to the same question being constantly and insistently repeated: after all, what does it mean and what are the limits of the right to personal data protection? The exercise of reflection by this work proves necessary as it provides an opportunity to revisit key concepts of the personal data protection regime, serving as anticipation of legal and practical problems common to all nationals or internationals who propose to address this matter.

In this regard, it is important to examine the formal requirements of the right to personal data protection, namely, subject, content, and object.[6] Thus, the legal field stands to gain from this research, especially given the intense debate regarding the implementation of the national system for personal data protection. Furthermore, this academic work seeks to identify normative patterns and characteristics of the fundamental right in question. It is therefore situated within the field of legal dogmatics. It should be noted that we use the term, as defined by Tércio Sampaio Ferraz Júnior, namely, "legal dogmatics as a means of legal work concerned with the identification of

---

[1] Isaak, J. and Hanna, M. J. (2018) "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," *Computer*, 51(8), pp. 56–59.

[2] Fell, J. *et al.* (2023) "See your identity pieced together from stolen data," *ABC News*, 17 May. Available at: https://www.abc.net.au/news/2023-05-18/data-breaches-your-identity-interactive/102175688 (Accessed: February 19, 2024).

[3] *State of the union 2023* (2023) *The White House*. Available at: https://www.whitehouse.gov/state-of-the-union-2023 (Accessed: February 19, 2024).

[4] Zuboff, S. (2019) *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019*. London, England: Profile Books.

[5] Leighton, L. (2013) "No title," in, pp. 1–1.

[6] Ferraz Júnior, T. (1993) "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado," *Revista da Faculdade de Direito, Universidade de São Paulo*, 88.

normative patterns and their respective evaluation and systematization."[7] Legal dogmatics is a way to facilitate legal understanding to society, simplifying complexity and seeking to stabilize society.[8]

Thus, we can define that the objective of this article is to expose the construction of the right to personal data protection, regarding the essential requirements of the subjective right. It is reaffirmed, therefore, that it is not seeking a complete analysis of personal data protection, but merely an attempt to construct the history of this right.

1. **Contours of the Privacy Concept**

This chapter will address the study of personal data protection and its intersections with the right to privacy. The right to privacy has emerged in countries worldwide in differents dimensions. The term "privacy" is used to refer to many different human values, including control over personal information, fairness, personal security, financial security, peace and tranquility, autonomy, integrity against commodification, and reputation.[9]

The interactions between these values and different types of information technology are complex; therefore, interventions aimed at protecting these values vary in their effectiveness and timing.[10] Privacy is used to describe many different human values. The strongest sense of privacy can be discussed as control over access to personal information, which people use to shape their personalities and roles in society.[11]

The presence of information and communication networks in social, legal, and political environments has determined awareness and the need to conceive the values and rights of individuals as universal guarantees for their integral development by virtue of their essential

---

[7] Ferraz Júnior, T. (1993) "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado," *Revista da Faculdade de Direito, Universidade de São Paulo*, 210.

[8] Ferraz Júnior, T. (1993) "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado," *Revista da Faculdade de Direito, Universidade de São Paulo*, 200.

[9] Rigaux, F. (1991) "La liberté de la vie privée," *Revue internationale de droit comparé*, 43(3), pp. 539–563. doi: 10.3406/ridc.1991.2290.

[10] Finn, R. L. *et al.* (2013) *European Data Protection: Coming of Age*. Org.; London: Springer.

[11] Doneda, D. (2019) *Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados*.

dignity.[12] As a result of the phenomenon of datafication, which is the existence of a digital biography, which is a logical and expected result of the extension of the person through their data.[13]

In this sense, personal data not only characterize themselves as an extension of the person (subjectivity) but also influence this relational perspective of the person (intersubjectivity). The protection of personal data is instrumental for the person to freely develop their personality.[14]

The strong and growing demand for transnational alignment of regulations on privacy and data protection aims primarily to create equitable rules in an increasingly globalized world, with the intention of abstaining individuals from possible "tax havens", places where there would be no discipline of protection rights, which would enable unregulated commerce.[15]

It is important to consider, however, that beyond this bit capture of the human being, there is their classification and segmentation based on such information. True stereotypes are created that stigmatize a subject before their peers. This factor is crucial for calibrating a series of decisions that influence the course of their own lives.[16]

Automated decisions[17] based on such stereotypes of people are already a reality, and are even the subject of explicit approach by the European Union Regulation (GDPR).[18] Specifically the item 22(3), in the cases outlined in subparagraphs “a” and “c,” grants individuals subject to automated decisions the right to have their rights, freedoms, and legitimate interests safeguarded. Precisely, this includes the right to obtain human intervention from the responsible party, express their viewpoint, and contest the decision.

---

[12] Silva, L. L. (no date) *Globalização das Redes de Comunicação: uma reflexão sobre as implicações cognitivas e sociais*.

[13] Solove, D. J. (2005) “The digital person and the future of privacy,” in *Privacy and Technologies of Identity*. New York: Springer-Verlag, pp. 3–13.

[14] Solove, D. J. (2005) “The digital person and the future of privacy,” in *Privacy and Technologies of Identity*. New York: Springer-Verlag, pp. 3–13.

[15] Bennett, C. (no date) *Regulating Privacy, Data protection and public policy in Europe and the United States*.

[16] Solove, D. J. (2005) “The digital person and the future of privacy,” in *Privacy and Technologies of Identity*. New York: Springer-Verlag, pp. 3–13.

[17] Renato Leite Monteiro defined the term as follows: "The concept of automated decision-making can be constructed here as a result of processing personal data, without significant involvement of a human operator, computationally or otherwise, that produces or can produce effects on the individual and whose processing of the data in question allows for other possible outcome. (Monteiro, R. (no date) *Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de Dados do Brasil. 385f. Tese Doutorado. Programa de Pós-Graduação em Filosofia do Direito e Teoria Geral do Direito*).

[18] Pariser, E. (2012) *Filter Bubble: Wie wir im Internet entmündigt werden*. Translated by U. Held. Munich, Germany: Hanser.

As can be observed, the GDPR[19] - more specifically in articles 13(2)(f), 14(2)(g), 15(1)(h) and 22(3) - does not explicitly or bindingly establish a "right to explanation," despite mandating practices and rights related to transparency and the right to review.[20] The notion of a right to explanation has been supported by some scholars based on a holistic interpretation of the regulation's text, particularly through a systematic reading of Articles 13, 14, 15, and 22, as well as Recital 71[21]. Although Recital 71 is not legally binding, it explicitly broadens the safeguards of Article 22(3) by stipulating a "right to explanation" in the context of automated decisions. Articles 13 and 14 encompass a set of transparency obligations, while Article 15 establishes a right of access.[22] Together, these provisions require that meaningful information be provided about the existence of automated decision-making, including profiling. Thus, the right to explanation in the GDPR would be derived from the rights and guarantees against being subject to automated decisions (Article 22(1) and (3)), as well as from the notification and information duties of controllers and the right of access (Articles 13-15).[23]

In summary, proponents assert unequivocally that the GDPR, by establishing the right to information regarding the logic behind automated decision-making processes, clearly grants a right to explanation. This right should be interpreted to enable data subjects to exercise their rights as outlined in the regulation and the broader legal framework.[24] Conversely, opponents argue that the

---

19 JANSSEN, J. H. N. means for 'white-boxing' the black-box?: research into the ability of the 'right to explanation' about decisions based solely on automated decision-making of Articles 13(2)(f), 14(2)(g), 15(1)(h) and 22(3) of the General Data Protection Regulation, as well as of current explanation methods, to solve the legal problems arising from algorithmic decision-making. JANSSEN, J. H. N. (2012) *The right to explanation:* (Masters Thesis in Law and Technology) — Universiteit van Tilburg, Tilburg, 2019.

20 SELBST, A. D.; POWLES, J. (2017) Meaningful Information and the Right to Explanation. *International Data Privacy Law*, v. 7, n. 4, p. 233-242.

21 "In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child."

22 CASEY, B.; FARHANGI, A.; VOGL, (2018) R. Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise. In: *Berkeley Technology Law Journal*, v. 34, p. 145-189.

23 GUNST, H. (2017) *The Right to Explanation and the Right to Secrecy* – Reconciling Data Protection and Trade Secret Rights in Automated Decision-making. 2017. Dissertation (Masters Thesis in Law) – Faculty of Law, University of Helsinki.

24 WACHTER, S.; MITTELSTADT, B.; FLORIDI, L. (2017) Why a Right to Explanation of Automated Decision Making Does Exist in the General Data Protection Regulation. *In: International Data Privacy Law*, vol. 7, n. 2, maio 2017, p. 76–99.

absence of the term “explanation” in the binding text of the GDPR precludes the definitive affirmation of such a right.[25]

It is the practice known as profiling, in which an individual's personal data forms a profile about them for making numerous decisions.[26] Everything is calibrated based on these stereotypes, including the content accessed on the Internet.

Eli Pariser reports that there is a bubble that - like an invisible filter - directs everything from the user's interaction with other people on a social network to accessing and searching for information on the web.[27]

The information society prints a new dynamic and new challenges for the protection of the human person, starting with the monetization of their personal data. Such data, in addition to consolidating a new form of extension of the person, begin to interfere in their own relational sphere, requiring specific standardization that dogmatically justifies the autonomy of the right to the protection of personal data and the unfolding of its legal protection.[28]

And, for this, it is necessary to seek the concepts of these rights to verify which aspects of their regulation and how the application of these rights can occur. According to the parameters set out by Rachel L. Finn and others, privacy is treated by various aspects, but it is possible to select seven (seven) subspecies, which although they have aspects of convergence, highlight unique aspects in the defense of privacy, these are (i) privacy of the person, (ii) privacy of behavior and action, (iii) privacy of personal communication, (iv) privacy of data and image, (v) privacy of thoughts and feelings, (vi) privacy of location and space, and (vii) privacy of association (including group privacy).[29]

Although these seven types of privacy may overlap, they are discussed individually because they provide different aspects through which the practical aspects of this right can be visualized.

The privacy of the person encompasses the right to keep the functions and characteristics of the body private (such as genetic codes and biometrics). The human body has a strong symbolic

---

[25] SELBST, A. D.; POWLES, (2017) J. Meaningful Information and the Right to Explanation. *International Data Privacy Law*, v. 7, n. 4, p. 233-242.

[26] Rubinstein, I., Lee, R. D. and Paul, M. (no date) *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*

[27] Pariser, E. (2012) *Filter Bubble: Wie wir im Internet entmündigt werden*. Translated by U. Held. Munich, Germany: Hanser.

[28] Doneda, D. (2019) *Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados*.

[29] Finn, R. L. *et al.* (2013) *European Data Protection: Coming of Age*. Org.; London: Springer.

dimension because of the integration of the physical body and the mind and is intrinsic to the cultural values of society.[30] It is thought that the privacy of the person leads to individual feelings of freedom and helps support a well-adjusted democratic society.[31]

The notion of privacy of behavior and action includes sensitive issues such as sexual preferences and habits, political activities, and religious practices.[32] However, the notion of privacy of personal behavior pertains to activities that occur in public space as well as in private space. It is necessary, therefore, to make a distinction between casual observation of the behavior of nearby people in a public space, with the systematic recording and storage of information about these activities. The ability to behave in public or private space without actions being monitored or controlled by others contributes to the development and exercise of autonomy and freedom of thought and action.[33]

Privacy of communication aims to prevent the interception of communications, including mail interception, use of directional microphones, telephone or wireless communication interception, or recording and access to email messages.[34] This right is recognized by many governments, as telephone wiretaps or other communication interceptions must be supervised by an independent judicial authority. This aspect of privacy benefits individuals and society itself because it allows and encourages the free discussion of a wide range of views and options and enables growth in the communications sector.[35]

The category of privacy of personal data includes, but is not limited to, image capture, as they are considered a type of personal data by the European Union as part of the General Data Protection Regulation (2016/679) - especially Recitals 14, 51, article 9(1) .[36] This privacy of data and image includes concerns about ensuring that individuals' data is not automatically available to other individuals and organizations, in order to limit the exercise of control over that data.

---

[30] Mordini, E. (2011) *Whole body imaging at airport checkpoints: The ethical and political context*.

[31] Finn, R. L. *et al.* (2013) *European Data Protection: Coming of Age*. Org.; London: Springer.

[32] Allen, A. L. (no date) *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*.

[33] Rigaux, F. (1991) "La liberté de la vie privée," *Revue internationale de droit comparé*, 43(3), pp. 539–563. doi: 10.3406/ridc.1991.2290.

[34] Poscher, R. (2017) "The right to data protection: A no-right thesis," in Miller, R. A. (ed.) *Privacy and Power*. Cambridge: Cambridge University Press, pp. 129–142.

[35] Raab, C. (2011) *Protecting Information Privacy. Equality and Human Rights Commission Research Report series*.

[36] Coppel, P. (2020) *Information Rights: A Practitioner's Guide to Data Protection, Freedom of Information and other Information Rights*.

Transparency about data control increases trust in the reliability, accountability, and privacy practices of the entities managing the data. It signifies a commitment to openness and fairness, reassuring individuals that their personal information is not being misused or exploited. This transparency cultivates a sense of security and confidence, strengthening the relationship between individuals and data controllers while empowering individuals to exercise greater autonomy over their data in relation to the controller..[37]

Like privacy of thoughts and feelings, this aspect of privacy has social value, as it deals with the balance of power between the State and the individual. New technologies have the potential to impact people's privacy of thoughts and feelings. People have the right not to share their thoughts or feelings or to have those thoughts or feelings revealed.[38]

Privacy of thought and feeling can be distinguished from privacy of the person, in the same way that the mind can be distinguished from the body.[39] Similarly, we can distinguish between thought, feelings, and behavior, since thought does not automatically translate into behavior, just as one can behave without thinking.

According to the conception of privacy of location and space, individuals have the right to move in public spaces without being identified, tracked, or monitored.[40] This conception of privacy also includes the right to be alone and the right to privacy in private spaces such as home, car, or office. This conception of privacy has primary social value.[41] When citizens are free to move through public space without fear of identification, monitoring, or tracking, they experience a feeling of living with freedom.[42]

The final type of privacy, namely, association privacy (including group privacy), concerns the right of people to associate with whom they wish without being monitored.[43] This has long been recognized as desirable for society, as it promotes freedom of expression, including political speech,

---

[37] Paul and Gutwirth, S. (2009) *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*.

[38] Rigaux, F. (1991) "La liberté de la vie privée," *Revue internationale de droit comparé*, 43(3), pp. 539–563. doi: 10.3406/ridc.1991.2290.

[39] Finn, R. L. *et al.* (2013) *European Data Protection: Coming of Age*. Org.; London: Springer.

[40] Mordini, E. (2011) *Whole body imaging at airport checkpoints: The ethical and political context*.

[41] Allen, A. L. (2000) *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*.

[42] Finn, R. L. *et al.* (2013) *European Data Protection: Coming of Age*. Org.; London: Springer.

[43] Bellanova, R., Hart, D. E. and Paul, G. (2011) "The German Constitutional Court Judgment."

freedom of worship, and other forms of association.[44] Society benefits from this type of privacy in that a wide variety of interest groups will be promoted, which can help ensure that marginalized voices are heard.

One may question what the difference is between location and space privacy and behavior privacy. Location privacy means that a person has the right to travel through physical space, to travel where they want without being tracked and monitored.[45] Behavior privacy means that the person has the right to behave as they wish, as long as the behavior does not harm another person.[46]

Association privacy differs from behavior privacy because it is not only about groups or organizations (e.g., political parties, unions, religious groups, etc.) that we choose to belong to, but association privacy also relates to groups or profiles over which we have no control, for example, DNA testing may reveal that we are members of a particular ethnic group or a particular family.[47] Association privacy is directly related to other fundamental rights, such as freedom of religion, freedom of assembly, etc., of which behavior and action privacy is a step forward.

The primary concept of privacy was strictly linked to intimate matters, the right to secrecy, confidentiality, and isolation, thus it could be defined as a right of negative exercise, i.e., the person has the right not to be invaded in their intimacy.[48] The right to privacy, therefore, also concerns interference with bodily integrity, home, and correspondence.

It is important to note that in 1960, William L. Prosser summarized the 04 (four) types of privacy harms that can cause harm to the person, namely, (i) intrusion into the plaintiff's seclusion; (ii) public disclosure of embarrassing private facts about the plaintiff; (iii) publicity that places the plaintiff in a false light in the eyes of the public; (iv) appropriation, for the defendant's advantage, of

---

[44] Hildebrandt, M. (2020) *Law for computer scientists and other folk*. London, England: Oxford University Press.

[45] Mordini, E. (2011) *Whole body imaging at airport checkpoints: The ethical and political context*.

[46] Kokott, J. and Sobotta, C. (2013) "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR," *International data privacy law*, 3(4), pp. 222–228. doi: 10.1093/idpl/ipt017.

[47] De Andrade, N. N. (2011) *Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization*.

[48] Bible, J. D. and McWhirter, D. (1992) *Privacy as a constitutional right: Sex, drugs, and the right to life*. Westport, CT: Praeger.

the plaintiff's name or likeness.[49] Indeed, this definition is used by most existing Courts in the United States of America to the present day.[50]

In the so-called "golden age of privacy" (the second half of the 19th century), privacy followed a path to perform the function of a right considered a prerequisite for the exercise of other fundamental freedoms, such as freedom of expression and freedom of thought, at a time when there was a growth in classical legal liberalism thought.[51]

Subsequently, it was seen that personality rights, including the concept of privacy, entered legal systems, receiving, in this context, the designation of public freedoms. The main declarations that dealt with the subject, in chronological order, were the Magna Carta (1215), the Bill of Rights (1689), the American Declaration of the Rights and Duties of Man and the Universal Declaration of Human Rights (1948).[52]

It is worth mentioning that privacy has always been considered and studied in cases related to the upper (wealthy) classes of society at that time, as in the case called "Affaire Rachel", which clearly has a causal nexus with the greater social connotation that the wealthy social classes had at the time and the society's knowledge of their right to privacy. To better explain the case, it is worth remembering that in 1858, the right to privacy was recognized for the first time in France, in case law, when the Séné Court recognized, to the family of a deceased actress, the right not to publish her image, on her deathbed.[53]

Furthermore, privacy began to be exercised positively by society, as a result of the detachments of the generations of fundamental rights[54], the change in the relationship between citizen and State and between citizen and companies[55], as well as the advancement of technological development, causing a greater flow of information globally and broadly. Note that privacy had its

---

[49] Prosser, W. L. (1960) “Privacy,” *California law review*, 48(3), p. 383. doi: 10.2307/3478805.

[50] Solove, D. J. (2010) *ProsserProsser's priv's privacy law: A mixacy law: A mixed legacy ed legacy*, *Gwu.edu*. Available at: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2104&context=faculty_publications (Accessed: February 19, 2024).

[51] Doneda, D. (2019) *Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados*.

[52] Dworkin, R. M. (1986) *A Matter of Principle*. London, England: Oxford University Press.

[53] Sampaio, J. A. L. (1998) *Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte*. Del Rey Books.

[54] Bobbio, N. (1 outubro 2018) *ESTADO, GOBIERNO Y SOCIEDAD: por una teoria general de la politica*. 2nd ed. Fondo de Cultura Economica.

[55] Bonavides, P. (2008) *Curso de Direito Constitucional*. 22nd ed. Malheiros Editores.

first mention in international declarations in 1948 when drafting the American Declaration of the Rights and Duties of Man, approved by the newly created Organization of American States, and the Universal Declaration of Human Rights, approved by the United Nations.[56]

In the European Union, the Charter of Fundamental Rights of the European Union addresses the topic in its article 7, specifically on the right to "respect for private and family life".[57] Indeed, privacy is considered a fundamental human right.[58] Therefore, true privacy is a product of personal responsibility. It is protected by remaining silent, refusing to interact, and keeping to oneself what is one's own concern. As a practical example, we refer to the judgments in cases C-293/12 and C-594/12 (Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources) addressed the balance of rights concerning data collection and retention by Member States. This precedent is pivotal and warrants careful analysis for the consolidation of this right within the Union. The controversy revolved around Directive 2006/24/EC, which obligated Member States to enact laws requiring internet and telecommunications providers to retain metadata of all their customers for up to two years, for law enforcement and public security purposes. The data retained under Directive 2006/24/EC could reveal personal information such as identity, time, location, and frequency of communication, enabling precise conclusions about individuals' private lives, including residence, movements, and social circles.[59] The Court was asked to examine the validity of Directive 2006/24/EC in light of Articles 7, 8, and 11 of the Charter of Fundamental Rights of the European Union, which concern privacy, data protection, and freedom of expression. In its decision, the Court emphasized that the essence of the right to privacy was respected since the Directive did not allow access to the content of communications. It also stated that this norm did not affect the essence of the right to personal data protection, as the Directive prescribed certain principles of data protection and security, such as technical and organizational measures against accidental or unlawful destruction, accidental loss, or alteration of data.[60]

---

[56] Doneda, D. (2019) *Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados*.

[57] Carta D O S Direitos Fundamentais, da U. E. (no date) *7.6.2016 Jornal Oficial da União Europeia C 202/389*, *Europa.eu*. Available at: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR (Accessed: February 19, 2024).

[58] Anderson, D. A. (1998) *The failure of American privacy law*, *Utexas.edu*. Available at: https://law.utexas.edu/faculty/publications/1999-The-Failure-of-American-Privacy-Law (Accessed: February 19, 2024).

[59] BOEHM, Franziska; COLE, Mark D. (2014) *Data retention after the judgement of the Court of Justice of the European Union*. Wayback Machine.

[60] Case C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung and others*. Decision on April 8th 2014.

The right to be left alone was defined in the United States in 1888 by American jurist Thomas Cooley and later solidified by Samuel Warren and Louis D. Brandeis, according to the article titled "Right to Privacy," which depicted the right to privacy in the face of photographic activity, in 1890. Through this facet of privacy, what is called in English zero-relationship is defended, that is, the total absence of interaction or relationship with the other.[61]

The United States of America provide reflective protection against violations of the right to privacy since neither its Constitution nor the Amendments to the U.S. Constitution of 1791 (known as the Bill of Rights) explicitly referred to the right to privacy. However, the Supreme Court of the United States has interpreted articles of the Bill of Rights as safeguards of an individual's right to privacy, notably based on the Fourth Amendment.[62]

The first relevant case to bring this interpretation to the American Constitution was the ruling of Griswold v. Connecticut, 381 U.S. 479 (1965), by the Supreme Court. This right to privacy has been the justification for decisions involving a wide range of civil liberty cases, including Pierce v. Society of Sisters, 268 U.S. 510 (1925), which invalidated a 1922 Oregon initiative that required compulsory public education; Roe v. Wade, 410 U.S. 113 (1973), which authorized abortion in Texas and restricted the state's excessive powers over this act; and Lawrence v. Texas, 539 U.S. 558 (2003), which struck down a sodomy law in Texas and thereby eliminated the state's powers to criminalize acts of same-sex and consenting adults.[63]

In this regard, we see the distinguished Pontes de Miranda affirming, in the 1970s, that privacy would be the fundamental basis of personal life, since there is only the right to protect private life, as there is the freedom to express it, starting from the individual will. For this significant author, the right to value intimacy would be the right to remain in reserve from the public, not to let others intrude on their private life.[64]

In a study dedicated to the origins of the privacy concept, Daniel J. Solove observed that this right was strictly linked to the protection of intimate matters, the right to secrecy, confidentiality, and isolation. Therefore, in its origin, it is an individual right of a negative nature, which recognizes

---

[61] Warren, S. D. and Brandeis, L. D. (1890) “The right to privacy,” *Harvard law review*, 4(5), p. 193. doi: 10.2307/1321160.

[62] Beaney, W. M. (1966) “The right to privacy and American law,” *Law and contemporary problems*, 31(2), p. 253. doi: 10.2307/1190670.

[63] Beaney, W. M. (1966) “The right to privacy and American law,” *Law and contemporary problems*, 31(2), p. 253. doi: 10.2307/1190670.

[64] de Miranda, F. C. P. (1 janeiro 2000) *Tratado de direito privado*. 1st ed. BOOKSELLER.

the person the faculty not to be invaded in what concerns solely and exclusively to personal sphere and private life.[65]

This exclusivist conception dates to the well-known article by Samuel Warren and Louis Brandeis, in which the authors argue for the existence of a common law principle that protects privacy from unauthorized intrusions, including theft and physical appropriation, and that does not equate to private property: the inviolability of personality and privacy, or privacy.[66] In this sense, Solove recalled that the U.S. Supreme Court - decades after the publication of Warren and Brandeis' article - debated a classic case about citizens' privacy.[67]

The case known as Olmstead v. United States established that government wiretapping was not a violation under the Fourth Amendment of the U.S. Constitution since it could not be considered a physical trespass into the home. However, Justice Brandeis dissented, stating that the framers of the Constitution "conferred, as against the government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men".[68]

To this aspect of privacy, the paradigm to be followed was the absence of communication between a person and others, taking the right marked by exacerbated individualism.[69] Therefore, except for rare exceptions[70], the right to personal data protection has not yet been recognized by federal legislation in the United States of America, resulting in the guidance that "Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information can generally be freely transmitted".[71]

Despite these facts, Daniel J. Solove recalls that the U.S. Supreme Court expounded an important conceptualization for privacy in the case Planned Parenthood v. Casey, in which it was indicated that the most intimate and personal choices a person can make throughout life, namely,

---

[65] Solove, D. J. (2009) *Understanding Privacy*. London, England: Harvard University Press.

[66] Solove, D. J. (2009) *Understanding Privacy*. London, England: Harvard University Press.

[67] Warren, S. D. and Brandeis, L. D. (1890) “The right to privacy,” *Harvard law review*, 4(5), p. 193. doi: 10.2307/1321160.

[68] *OLMSTEAD et al. v. UNITED STATES. GREEN et al. v. SAME McINNIS v. SAME* (no date) *LII / Legal Information Institute*. Available at: https://www.law.cornell.edu/supremecourt/text/277/438 (Accessed: February 19, 2024).

[69] Solove, D. J. (2009) *Understanding Privacy*. London, England: Harvard University Press.

[70] Among them, it is noteworthy to mention the FCRA (Fair Credit Reporting Act), aimed at regulating the privacy of consumer information.

[71] *U.S. West, Inc. v. Federal Communications Commission* (1999) *UNITED STATES COURT OF APPEALS FOR THE TENTH CIRCUITS*. Available at: https://cite.case.law/f3d/182/1224/ (Accessed: February 19, 2024).

choices centered on personal dignity and autonomy, are central to freedom, protected by the Fourteenth Amendment.[72]

Another important decision of the American Supreme Court occurred in 1967[73] when it was decided that once a person exposes their personal data to third parties, such as banks or other services, the latter do not have a reasonable expectation of privacy regarding government access. The following year, Alan Westin characterized privacy as the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others.[74]

In this sense, all classes were subject to having their privacy infringed or affected by entities and institutions. The theorist Robert Post argued that privacy is not just a set of restrictions on society's rules and norms. Instead, privacy constitutes an attempt by society to promote civility.[75]

Note that privacy is not simply a way to free individuals from social control; it is itself a form of social control that emerges from society.[76] Therefore, privacy has social value; it is not simply an external restriction on society but rather an internal dimension of society. When the law protects the individual, it does so not only for the individual's sake but for the sake of society.

Emergence of Informational Self-Determination

Gerrit Hornung and Christoph Schnabel state that the idea of protecting personal data was introduced in the ruling of the well-known case of the German Census Act of 1983[77], which involved an attempt to census the population. The purpose of the collection was: a) to gather statistical information, such as population growth, demographic density, and economic activities, among others; b) to compare them with data stored in public records; and c) to send them, when necessary, to public authorities.

---

[72] Solove, D. J. (2009) *Understanding Privacy*. London, England: Harvard University Press.

[73] *Katz v. United States, 389 U.s. 347 (1967)* (no date) *Justia Law*. Available at: https://supreme.justia.com/cases/federal/us/389/347 (Accessed: February 19, 2024).

[74] Westin, A. F. (1970) *Privacy and Freedom*. London, England: Bodley Head.

[75] Post, R. C. (2001) *Three concepts of privacy*, *Yale.edu*. Available at: https://openyls.law.yale.edu/bitstream/handle/20.500.13051/1114/Three_Concepts_of_Privacy.pdf?sequence=2&isAllowed=y (Accessed: February 19, 2024).

[76] Hornung, G. and Schnabel, C. (2009) "Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention," *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

[77] Martins, L. (2005) *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão*.

The German Constitutional Court declared the nullity of the legal provisions that provided for the comparison and transmission of the collected data to public authorities and recognized the existence of a right to informational self-determination, understood as the right of the individual to protect themselves against the collection, storage, use, and disclosure of their personal data, carried out unlimitedly, a right that could only be restricted in case of a public interest, based on constitutional grounds.[78]

It is worth remembering that in 1977, the Federal Republic of Germany created its first law on informational self-determination, which had the specific purpose of protecting individuals against interference in the use of their personal data, a norm directed exclusively against state action that would negatively interfere (through unauthorized individual data collection) or positively interfere (preventing individuals from using the data as they please) in the individual self-determination of personal data.[79] The fundamental assumption of such legislative creation was the existence of an asymmetrical power and knowledge relationship between the data collecting entity (the State) and the subjects subjected to the data collection activity (private individuals, holders of the fundamental right).[80]

This legislation had two assumptions. First, with the establishment of the welfare state and the consequent increase in state functions, the collection of personal data became necessary for the organization of public functions, especially for the provision of public services efficiently and promptly.[81] Data collection, in this sense, was conceived as a means of protecting the user of public services, who has the right to continuity and quality of the public activity provided by the State or by concessionaires of these services.[82]

Second, for the realization of such activities, public bodies began to create large databases, in which information related to personal characteristics and habits began to be cataloged in a

---

[78] Hornung, G. and Schnabel, C. (2009) "Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention," *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

[79] Martins, L. (2005) *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão*.

[80] Hornung, G. and Schnabel, C. (2009) "Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention," *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

[81] Buchner, B. (2020) *Informationelle Selbstbestimmung im Privatrecht*. JCB Mohr (Paul Siebeck). doi: 10.1628/978-3-16-158031-4.

[82] Dimoulis, L. M. D. (2020) *Teoria Geral Dos Direitos Fundamentais*. Nova Edição[a]. Revista dos Tribunais.

centralized and systematic manner.[83] The control power resulting from this accumulation of information was the trigger for the creation of a shield of protection of personal freedom.[84]

Without the guarantee that their actions would not be influenced by holders of personal information and that access to essential services would not be limited based on personal information, individual freedom and spontaneity would be chilled by the individuals themselves, who would control their actions by foreseeing possible damages that could result from them.[85] The protection of personal data thus emerges as a doubly instrumental right: not only does it protect individual freedom against unauthorized and excessive intrusions by the State - as is the case with all other fundamental rights, but it also ensures that all other fundamental rights are exercisable.

Such as freedom of expression, artistic freedom, freedom of movement, and freedom of assembly, are exercised and realized without the holders of these rights feeling threatened by an omnipresent and omniscient observer: the State.[86] Therefore, defending the protection of personal data was seen as synonymous with defending democracy and, conversely, those who opposed this right were identified as supporters of authoritarianism.[87]

This construction of apocalyptic and antigovernmental ideas took on dramatic political and social contours in the context of the trial of the constitutionality of the 1983[88] census law. Amid protests against the arms policy of the early 1980s, the slogan arose: "Down with the census."[89] It was the same State that harmed the environment, concentrated wealth, aligned itself with the combat policy established by the North Atlantic Treaty Organization, which now, surreptitiously, demanded that citizens provide data.[90] And if it, the State, is capable of carrying out such atrocious actions, what will it do with the data collected from the population?

---

[83] Vesting, T. (2003) *Das Internet und die Notwendigkeit der Transformation des Datenschutzes*.

[84] Hornung, G. and Schnabel, C. (2009) “Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention,” *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

[85] Bull, H. P. (2013) *Netzpolitik: Freiheit und Rechtsschutz im Internet*. 1st ed. Baden-Baden, Germany: Nomos.

[86] Britz, G. (2010) *Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts*.

[87] Vesting, T. (2003) *Das Internet und die Notwendigkeit der Transformation des Datenschutzes*.

[88] Simitis, S. (2000) *Das Volkszählungsurteil Oder Der Lange Weg Zur Informationsaskese*.

[89] Buchner, B. (2020) *Informationelle Selbstbestimmung im Privatrecht*. JCB Mohr (Paul Siebeck). doi: 10.1628/978-3-16-158031-4.

[90] Hoffmann-Riem, W. (1998) *Informationelle Selbstbestimmung in der Informationsgesellschaft*.

It was for all these reasons that the census law concentrated the anger and fury of an entire generation formed by the constant and present threat of socialism and nuclear war: the threat of sudden destruction, caused by an enemy that is not even known.[91] Encouraged by state governments opposed to the expansion of federal power, more than four hundred protests were held against the census law, many of which called for a widespread popular uprising and even civil insurrection against the census law.[92] The response of the German Constitutional Court to this situation of widespread social turmoil was simply the creation of the "Magna Carta of Personal Data Protection": a decision that states that there is no data without legal value since, after all, no matter how small the personal information is, when aggregated with other data, it can be the basis for the creation of informational profiles that replace concrete individuality.[93]

Another landmark decision in the evolution of the position on this right and its horizontal effectiveness concerning private life refers to decision BVerfGE 84, 192, of the year 1991. In the case, there was the signing of a lease contract with a person who had been legally incapacitated - partially - since 1963, due to "mental deficiency." At first, this factor was not disclosed, and there was an addendum signed by this person's guardian. Due to the lack of information provided, the lessors requested the termination of the contract. After going through the ordinary instances, the case was deliberated by the Constitutional Court. In this sense, the Court ruled that there was no general incapacity, but only partial, and that the lease obligations by this person were duly fulfilled. Therefore, and in the face of a stigmatizing disease, there would be no reasoned justification for the necessary disclosure of their legal incapacity, even more so "if the claimant had to disclose their legal incapacity without examining the question of whether their contractual opponent has a protected interest (...) it would be almost impossible for them to rent a space."[94]

This second decision brings two important points to the discussion on informational self-determination. First, it states that there is effectiveness of the right in the context of relations between individuals (horizontal effectiveness) since its application to an eminently private dispute was possible. Second, it refers to this as the instrument capable of protecting the individual from

---

[91] Hornung, G. and Schnabel, C. (2009) “Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention,” *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

[92] Hoffmann-Riem, W. (1998) *Informationelle Selbstbestimmung in der Informationsgesellschaft*.

[93] Martins, L. (2005) *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão*.

[94] Axel Tschentscher, L. L. M. (1991) BVerfGE 84, 192 - Offenbarung der Entmündigung, Unibe.ch. Available at: https://www.servat.unibe.ch/dfr/bv084192.html (Accessed: February 19, 2024).

apparent or fictitious consent due to power imbalances with the other party, thus reaffirming its scope alongside the right to personality. Thus, we result in specific judicial control over contracts that regulate the processing of personal data.

For this reason, every data subject now has the right to know "who, where, how, and for what purpose their data has been used." Only in this way can individuals have the possibility of knowing who holds their data, which aspects of their personality have been identified and collected, and, finally, why the State and private entities have become interested in their lives and what purpose is sought by the collection of this personal data.

At first glance, there are problems in this construction, starting with the assumption that people's personality can somehow be developed in a completely aseptic environment, without social interaction and without the daily transfer of data that arises from social contact and communication.[95] Therefore, society and the State cannot be expected to provide what they cannot offer: complete transparency regarding the use and destination of all data collected daily from all citizens of a country. After all, just as it is not possible to determine in advance whether information is true or false, it is not possible to foresee completely and determinedly what personal data will be used for.

This would simply mean the extinction of any possibility of implementing public policies and the consequent extinction of essential public services for the population.[96] Therefore, American jurisprudence until today considers the right to data protection to have a very limited character, as "even though we may feel uncomfortable knowing that our personal information circulates the world, the fact is that we live in a free and open society, where information must flow freely."[97]

This is exactly why legislation has focused on identifying the due informational process, that is, as we can see in the personal data protection law, there is express authorization for the shared use of data for the execution of public policies, demanding shortly thereafter, however, that the cases be informed in which, in the exercise of their competences, they carry out the processing of personal data, providing clear and updated information about the legal provision, the purpose, the procedures, and the practices used for the execution of these activities, in easily accessible vehicles, preferably on their websites.

---

[95] Martins, L. (2005) *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão*.

[96] *U.S. West, Inc. v. Federal Communications Commission* (1999) *UNITED STATES COURT OF APPEALS FOR THE TENTH CIRCUITS*. Available at: https://cite.case.law/f3d/182/1224/ (Accessed: February 19, 2024).

[97] Hornung, G. and Schnabel, C. (2009) “Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention,” *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

From this point of view, it is verified that for the state act, it is necessary to comply with the principle of purpose and the linked administrative act, requiring legal authorization, for the provision of updated and efficient public services.[98]

In the Census decision, it was said as precisely as mysteriously, that every citizen has the right to "know who, how, when, and by what means their personal information reaches the knowledge of third parties."[99] This conclusion has two normative foundations - articles 1 (dignity) and 2 (freedom in a general sense), both of the Basic Law of Bonn - which, when combined, lead, in the understanding of the Court, to the conclusion that people have the right to develop their personality fully and without constraints imposed by the State or by society; and also a factual foundation that lies in the sudden development of automated databases, capable of mapping in detail all aspects of individual behavior.[100]

Combined with the constant fear of state political persecution and popular dissatisfaction with German foreign and energy policy[101], these foundations led to the creation of this new fundamental right: informational self-determination.[102]

This right provides the basis for contemporary general personal data protection codes. The preventive and accessory nature of the right to informational self-determination can help to contribute to a better understanding of transatlantic differences in personal data protection standards.[103]

A systematic preemptive right to personal data protection, which provides protection against mere potential harm, does not easily fit into this legal tradition. As Navarro defines: "Data are personal and their protection ensures the self-determination of personality."[104] The informational

---

98 Hornung, G. and Schnabel, C. (2009) “Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention,” *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

99 Martins, L. (2005) *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão*.

100 Hornung, G. and Schnabel, C. (2009) “Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention,” *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

101 Honnige, C., Kneip, S. and Lorenz, A. (eds.) (2011) Verfassungswandel Im Mehrebenensystem. 2011th ed. Wiesbaden, Germany.

102 Hornung, G. and Schnabel, C. (2009) “Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention,” *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

103 Isaak, J. and Hanna, M. J. (2018) “User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection,” Computer, 51(8), pp. 56–59.

104 Ana Maria Neves de Paiva. O direito fundamental à autodeterminação informativa (2012).

self-determination of the individual requires active participation from the data subject and, consequently, greater control over the flow of their personal information, constituting an active right and necessary participation of the individual in relation to its terms.

On a macro level, in order to develop more regulations and mechanisms for governing personal data and to avoid their misuse, it is necessary to develop a clearer view of the fundamental issue of personal data ownership; that is, to whom the data belong and which aspects of that ownership can be waived or contracted under what circumstances and which aspects can never be contractually waived.

It is worth noting that the German Federal Constitutional Court continues to defend this right to this day. In February 2023, the Court issued a decision considering that §25a(1) of the Public Security and Order Act for the Hesse region (Hessisches Gesetz über die öffentliche Sicherheit und Ordnung – HSOG) and §49(1) of the Police Data Processing Act for the Hamburg region (Hamburgisches Gesetz über die Datenverarbeitung der Polizei – HmbPolDVG) are unconstitutional. These provisions authorized the police to process personal data stored through automated data analysis (Hesse) or automated data interpretation (Hamburg). The provisions violate the general right to personality (Art. 2(1) together with Art. 1(1) of the Basic Law (Grundgesetz – GG) in its manifestation as the right to informational self-determination because they do not contain sufficient thresholds for interference. According to the Court, these laws allow for the subsequent processing of stored data through automated data analysis or interpretation in certain cases, subject to case-by-case evaluation, when necessary, as a precautionary measure to prevent specific criminal acts. Given the particularly broad wording of the powers, in terms of data and methods in question, the grounds for interference fall far short of the constitutionally required threshold of identifiable danger.[105]

These decisions by the German Federal Constitutional Court align with the European framework of fundamental rights protection, including both the European Union (EU) and the European Convention on Human Rights (ECHR). Firstly, they reflect the principles enshrined in the Charter of Fundamental Rights of the European Union, particularly concerning the right to privacy and data protection (articles 7 and 8). The Court's rulings emphasize the importance of safeguarding individuals' rights to informational self-determination and protecting personal data against

---

[105] Bundesverfassungsgericht, 1. Senat (2023) Bundesverfassungsgericht - Entscheidungen - Regelungen in Hessen und Hamburg zur automatisierten Datenanalyse für die vorbeugende Bekämpfung von Straftaten sind verfassungswidrig, Bundesverfassungsgericht. Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html;jsessionid=4C277453C112811049FBC9244433D0C5.1_cid507 (Accessed: February 19, 2024).

unjustified interference by state authorities. Secondly, these decisions resonate with the jurisprudence of the European Court of Human Rights (ECtHR) regarding the right to privacy under Article 8 of the European Convention on Human Rights. The ECtHR has consistently emphasized the need for any interference with privacy rights to be proportionate, necessary, and subject to adequate safeguards.[106] Consequently, the European Court of Human Rights (ECtHR) has consistently demanded that the interception of communications be authorized by a law that is particularly precise. As elucidated by the Court, clear and detailed regulations are indispensable, especially given the continuous advancement of technology in this field. Specifically, domestic legislation must provide citizens with sufficient clarity regarding the circumstances and conditions under which public authorities are permitted to employ such measures.[107]

In this context, the German Constitutional Court's rulings underscore the significance of establishing clear legal thresholds for state interference with personal data, in line with the principles of proportionality and necessity. They highlight the importance of ensuring robust safeguards against arbitrary or excessive intrusion into individuals' privacy rights, thus contributing to the broader European framework of fundamental rights protection.

To this extent, the German court continues to indicate that legal provisions must indicate the grounds for interference in a proportional manner in light of the seriousness of the interference and the provisions, always based on respect for the right to informational self-determination.[108] We emphasize that this is a decision not only of individual but also of collective scope.

This will be important to contain current practices of companies that determine, through non-negotiable terms, that they can do whatever they please with users' personal data. It remains crucial that, with all technological promises innovations worth for a greater good, we do not lose sight of the ethical principles that keep us human. In general, humanitarian and development

---

[106] For example, in the case of *Kruslin v France* (1985), it was underscored that actions such as tapping and intercepting telephone conversations constitute significant intrusions into private life and correspondence. (Case of Kruslin v. France. Application no. 11801/85. Judgment 24 April 1999).

[107] 1) Case of Zakharov v. Russia. Application no. 47143/06. Judgment 4 December 2015; 2) Case of Iordachi and Others v. Moldova. Application no. 25198/02. Judgment 10 February 2009; 3) Case of Podchasov v. Russia. Application no. 33696/19. Judgment 13 february 2024; 4) Case of Nejdet Şahin and Perihan Şahin v Turkey. Application no. 13279/05. Judgment 20 October 2011; 5) Case of Rekvényi v Hungary. Application no. 25390/94. Judgment 20 May 19999; 6) Case of Hashman and Harrup v UK. Applicattion no 25594/94. Judgment 25 November 1999.

[108] Bundesverfassungsgericht, 1. Senat (2023) *Bundesverfassungsgericht - Entscheidungen - Regelungen in Hessen und Hamburg zur automatisierten Datenanalyse für die vorbeugende Bekämpfung von Straftaten sind verfassungswidrig*, *Bundesverfassungsgericht*. Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html;jsessionid=4C277453C112811049FBC9244433D0C5.1_cid507 (Accessed: February 19, 2024).

communities need to adopt a more rigorous and transparent approach to data protection and innovation.

2. **Regulatory Landscape in the United States of America**

The right to personal data protection refers to the legal framework that regulates the collection, use, and storage of personal information. It is designed to protect individuals from having their personal information misused or manipulated. It is based on the principle that individuals have control over their personal information and that organizations have a responsibility to handle it responsibly.[109]

There appear to be two types of personal data protection regulatory systems existing in various countries.[110] There is the comprehensive personal data protection system, which is broad and general ("omnibus"), with the action of a central and uniform authority, with concern for the regime in general. On the other hand, the second system is restricted and limited ("sectional"), opting for the absence of a global regimen but focusing on specific areas and according to the sensitivity of that area and its actors, both private and public. In most cases, there is no general authority for control.

In particular, it is noted that the choice of the omnibus system emphasizes the following principles: (1) limits on data collection, also called data minimization; (2) data quality principle; and (3) notification, access, and correction rights for the individual. In the system chosen by the United States of America, however, there has been a reinforcement of the concept of notification of data processing practices and consent of the affected party for processing. Certain principles, only recently being incorporated into specific legislation - and more forcefully into state legislation - which are already present in countries that adopt omnibus systems, such as (4) personal data processing carried out according to a legal basis; (5) regulatory supervision by an independent data protection authority; (6) enforcement mechanisms, including restrictions on exporting data to countries lacking sufficient privacy protection; (7) limits on automated decision-making; and (8) additional protection for sensitive data.

In the case of the United States of America, the right to personal data protection is governed by a combination of federal and state laws, as well as specific sectoral regulations, with no single

---

[109] Lynskey, O. (2014) Deconstructing data protection: the “added-value” of a right to data protection in the EU legal order. International and Comparative Law.

[110] Newman, A. P. (2008) Protectors of Privacy: Regulating Personal Data in the Global Economy.

authority with enforcement and control power, but with several bodies responsible, each in its specific category.[111]

Driven by the consumer protection movement, Congress passed the Fair Credit Reporting Act (FCRA) in 1970, which provides a set of basic rights guaranteed to citizens of that country (examples of rights include: right to information about credit report, right to obtain credit score for free, right to dispute incomplete and inaccurate information, right to consent to the transmission of information to potential employers). Furthermore, the Privacy Act can be indicated as the discipline on personal data protection, especially and solely focused on the use and sharing of personal data by federal government agencies of the United States. The S. 3418, commonly referred to as the "1974 Privacy Act," was enacted on December 31, 1974. This law is characterized as a comprehensive code of fair information practices that seeks to regulate the collection, maintenance, use, and dissemination of personal information by agencies of the Federal Executive Branch.[112]

Moreover, in the idea of sectoral regulation, in 1974[113], the "U.S. Privacy Protection Study Commission" was designated, which delved into the question of applying regulations to the private sector.[114] It is also noted that at the federal level, in 1996, the Personal Data Protection Act with a special focus on the health sector was promulgated, namely the Health Insurance Portability and Accountability Act (HIPAA), which applies to healthcare providers and organizations.[115] The Federal Trade Commission (FTC) also has the authority to regulate personal data protection and enforce laws against unfair or deceptive practices.[116] The Children's Online Privacy Protection Act

---

[111] Guidi, G. (2017) Modelos regulatórios para proteção de dados pessoais. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio.

[112] Waller, S. (2011) “Consumer protection in the United States: an overview. European Journal of Consumer Law, rotection in the United States: an overview,” European Journal of Consumer Law.

[113] UNITED STATES. CONGRESS. SENATE. COMMITTEE ON GOVERNMENT OPERATIONS (1974) Legislative history of the Privacy Act of 1974, S. 3418 (Public Law 93-579) source book on privacy, https://tile.loc.gov/storage-services/service/ll/llmlp/lh_privacy_act-1974/lh_privacy_act-1974.pdf. Available at: https://tile.loc.gov/storage-services/service/ll/llmlp/LH_privacy_act-1974/LH_privacy_act-1974.pdf (Accessed: February 19, 2024).

[114] Solove, D. J. and Hartzog, W. (2014) “The FTC and the New Common Law of Privacy,” Columbia Law Review, 114, pp. 583–676.

[115] UNITED STATES. (1977) Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission transmitted to President Jimmy Carter, https://epic.org/privacy/ppsc1977report/c1.htm. Available at: https://epic.org/privacy/ppsc1977report/c1.htm (Accessed: February 19, 2024).

[116] *Health insurance portability and accountability act of 1996 (HIPAA)* (2022) *Cdc.gov*. Available at: https://www.cdc.gov/phlp/publications/topic/hipaa.html (Accessed: February 19, 2024).

(COPPA) is a federal law that applies to websites and online services that collect personal data from children under 13 years of age.[117]

At the state level, 13 (thirteen) states have already passed specific laws on the subject. The states of California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia have their own legislation to regulate aspects of personal data protection, at least in the consumer field.

Basically, the right to personal data protection in the United States is governed by a combination of federal and state laws, especially regarding consumer protection. These laws grant individuals the right to know what personal data is being collected about them, request its deletion, and opt-out of the sale of their personal data. They also impose obligations on organizations to handle personal data responsibly and ethically.[118]

Furthermore, in the regulatory field, the Federal Trade Commission (FTC) is a United States government agency whose primary function is antitrust law enforcement (non-criminal) and promotion of consumer protection, being one of the most active agencies in regulating and enforcing regulations on the subject. The FTC itself has drafted a report with guidelines for companies and data subjects, and its guidelines are for processing to follow 3 (three) core principles[119]: (i) Privacy by Design; (ii) Simplified Consumer Choice, and; (iii) Transparency.

An example of a legal case involving personal data protection that was decided by the Supreme Court of the United States is Carpenter v. United States (2018).[120] In this case, the defendant, Timothy Carpenter, was convicted of several robberies. The government used his cellphone location data, obtained from his cellphone carrier without a warrant, as evidence against him. The defendant argued that the warrantless collection of his cellphone location data violated his rights under the Fourth Amendment against unreasonable searches and seizures.[121]

---

[117] Solove, D. J. and Schwartz, P. M. (2023) *Information privacy law*. 8th ed. Aspen Publishing.

[118] Solove, D. J. and Schwartz, P. M. (2023) *Information privacy law*. 8th ed. Aspen Publishing.

[119] *Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers* (2012) *Federal Trade Commission*. Available at: https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers (Accessed: February 19, 2024).

[120] Tokson, M. (2018) "The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021," *Havard Law Review*, 135, pp. 1791–1851.

[121] U.S. SUPREME COURT (2017) *Carpenter v. United States*, *Supremecourt.gov*. Available at: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf (Accessed: February 19, 2024).

The Supreme Court ruled in favor of Carpenter, holding that the warrantless collection of his cellphone location data was a violation of his rights under the Fourth Amendment.[122] The Court stated that geolocation data involves a "comprehensive chronicle of a person's physical presence compiled every day, every moment, over several years."[123] The Court's decision is significant because it recognizes that individuals have a reasonable expectation of privacy in the location data of their cellphones and that this information is protected by the Fourth Amendment of the country. This case highlights the importance of data protection rights and the need for the government to obtain a warrant before collecting personal information to respect individuals' privacy rights.

Finally, it is worth noting that the United States of America currently has a valid legal basis for data transfer by the European Union after long controversy. Let's go through the history. In 2016, the European Union adopted an adequacy decision called the EU-US Privacy Shield, which allowed the transfer of personal data from the European Union to that country. In this multilateral agreement, the United States Department of Commerce and the European Commission established a set of principles and safeguards to be guaranteed by companies adhering to the agreement to enable the transfer of personal data of individuals located in the European Union to companies located in the United States.[124] However, in the case known as Schrems II, the Court of Justice of the European Union declared this instrument null and void, as the adequacy of the Privacy Shield as a valid legal basis for international data transfer was not recognized.

The Court's decision to invalidate the EU-US Privacy Shield was directly tied to the fundamental right to protection of personal data guaranteed by the European Union. This right is enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (CFREU), which safeguards individuals' privacy and data protection. Additionally, Article 16, § 1 of the Treaty on the Functioning of the European Union (TFEU) reinforces the importance of protecting personal data within the EU legal framework. In the Court's view, the surveillance programs implemented by the United States government were deemed to disproportionately violate individuals' privacy and data protection rights as guaranteed by the GDPR. This disproportionate violation of fundamental rights, as understood by the Court, necessitated the invalidation of the Privacy Shield agreement, which was intended to facilitate international data transfers while ensuring adequate protection of personal data.

---

[122] Kerr, O. S. (no date) “An Equilibrium-Adjustment Theory of the Fourth Amendment,” *Havard Law Review*, 125.

[123] Kerr, O. S. (no date) “An Equilibrium-Adjustment Theory of the Fourth Amendment,” *Havard Law Review*, 125.

[124] *Implementing decision - 2016/1250 - EN - EUR-Lex* (no date) *Europa.eu*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG (Accessed: February 19, 2024).

This ruling underscored the fundamental importance of the principle of proportionality in European Union law, particularly within the realm of safeguarding fundamental rights as enshrined in Article 52, § 1 of the Charter of Fundamental Rights of the European Union. Throughout various rulings, the Court has consistently emphasized the significance of reasonableness (proportionality) in the measures implemented, always with the aim of ensuring the protection of rights delineated in the Charter.[125] This principle requires that any action taken by public authorities, including those related to data protection and privacy, be proportionate to the intended objective and not exceed what is necessary to achieve that goal. In the context of international data transfers, the Court's application of the proportionality principle reflects its commitment to upholding the rights and values enshrined in EU law while addressing the complex challenges posed by global data governance and surveillance practices.

In effect, by not clearly foreseeing the limitations of the powers granted to intelligence services, the surveillance programs end up allowing public authorities to carry out excesses, which are not limited to what is strictly necessary to ensure national security, as provided for in the GDPR. However, it's important to note that the CJEU did uphold the validity of the European Commission's standard contractual clauses for data transfers to the USA in the same ruling. This decision was significant as it provided a clear pathway for organizations to continue conducting cross-border data transfers while ensuring compliance with the GDPR's stringent data protection standards. By validating the SCCs, the CJEU acknowledged their role as a robust legal mechanism for safeguarding personal data when transferred to third countries. The CJEU's decision regarding the SCCs underscored their importance as a flexible and adaptable tool for facilitating international data transfers, offering organizations a viable alternative to the now-defunct Privacy Shield framework. This validation provided much-needed reassurance to businesses and individuals alike, offering a practical solution to the complex challenges posed by global data flows in the digital age.

In this regard, the European Commission initiated a new process to adopt a decision of adequacy of the EU-US Data Privacy Framework, called the Adequacy Decision for the EU-US Data Privacy Framework, which sought to foster transatlantic data flows and address the concerns

---

[125] 1) Case C-301/06. Ireland v. European Parliament and Council of the European Union. Judgment 10 February 2009; 2) Case C-293/12 and C-594/12. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e others. Judgment 08 April 2014; 3) Case C-207/16. Ministério Fiscal. Judgment 02 October 2018; 4) Case C398/15. Câmara de Comércio, Indústria, Artigianato and Agricoltura di Lecce v. Salvatore Manni. Relator M. Ilešič. Judgment 09 March 2017; 5) Case C-136/17. GC e outros v. Commission nationale de l'informatique et des libertés (CNIL). Judgment 24 September 2019; 6) Case C-360/10. Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV. Judgment 16 February 2012; 7) Case C-275/06. *Digital Promusicae v. Telefónica de España SAU*. Judgment 29 January 2008.

raised by the Court of Justice of the European Union in the above decision, which was approved by the European Commission in 2023.

The European Commission approved the request after the publication of Executive Order No. 14086 by the Federal Government of the United States of America and supplemented by the Regulation approved by the Department of Justice of that country ("EO 14086" and "AG Regulation").

As provided in the Executive Order and the Department of Justice Regulation, the Data Protection Review Court will be created, which will be the Independent Authority, with powers of binding decision on the Federal Government, to which individuals from the European Union may submit complaints, free of charge, to the so-called Civil Liberties Protection Officer of the US Intelligence Community, and, in the second instance, individuals will have the right to appeal the decision to the newly created Data Protection Review Court.

The Court (or Authority) will be composed of members chosen by individuals not affiliated with the government of the United States of America, appointed based on their previous qualifications and who can only be dismissed for serious misconduct and cannot receive instructions from the Government for making their decisions. Thus, the Court (or Authority) will have powers to investigate complaints from Union individuals, including obtaining information from intelligence agencies of the United States of America and may adopt binding corrective decisions.

Following this, companies based in the United States of America will be able to self-certify their entry into the EU-US Data Privacy Framework, committing to comply with a detailed set of privacy obligations, such as deleting personal data when it is no longer necessary for the purpose for which it was collected and ensuring the continuity of protection, in accordance with the terms of Executive Order No. 14086.

Finally, it is worth noting that the European Union already had an Adequacy Decision with the United States of America, regarding the protection of personal information related to the prevention, investigation, detection, and repression of crimes. Decision 2016/920 is dated 2016 and aims to establish principles and guarantees regarding the protection of personal data transferred for the purpose of criminal law enforcement between the United States, on the one hand, and the European Union and its Member States, on the other. The objective is to ensure a high level of protection of this data and, thus, enhance cooperation between the Parties. Although not constituting the legal basis for the transfer of personal data to the United States, the agreement complements,

when necessary, the guarantees regarding data protection provided for in existing or future agreements, concerning data transfer or in national provisions authorizing such transfers.

3. **Subjective and Objective Dimensions of the Right to Personal Data Protection**

Fundamental rights generally have a dual dimension, namely the subjective and objective.[126] In its subjective condition, the right to personal data protection can be understood as a set of heterogeneous and subjective defensive positions (negative), but it also assumes the condition of a right to provisions, whose object consists of the principle of accountability and accountability. That is, when referring to the subjective dimension of the right, one will be faced with the rights attributed to that right, its effective application in the life of each human being. And in the present case, as already specified in the above topic, the rights attributed to the data subject are the subjective legal positions of this right being studied here. Thus, the aim is to elucidate and clarify the realization, thus ensuring the double function of such a right as a negative (defense) and positive (provisional) right.

Regarding the objective dimension, we must evaluate the three instances of this dimension, namely, (i) effectiveness; (ii) protection duties; (iii) procedures to guarantee and enforce the right.[127]

Regarding the topic of effectiveness, it must be observed that the protection of personal data is of special interest in caring for the human being in the face of private actors, since it is these actors who produce content – especially on the World Wide Web – capable of generating eventual restrictions/ injuries to this right. Thus, there must be control over restrictions on fundamental rights in the sphere of private relations, including preventively, considering especially the legislative options of that nation.

---

[126] Sarlet, I. (2018). *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado*.

[127] Regarding the objective dimension, Ingo Sarlet stated: "the paradigmatic assertion of the Federal Constitutional Court is always recalled, according to which fundamental rights are not limited to the primary function of being subjective rights for the defense of the individual against acts of public authority, but also constitute evaluative decisions of a juridical-objective nature of the Constitution, with effectiveness throughout the legal system, providing guidelines for legislative, judicial, and executive bodies. However, it is also worth recalling that the objective perspective of fundamental rights does not represent a mere 'flip side' of the subjective perspective, but rather means that autonomous function is granted to norms that provide subjective rights, which transcends this subjective perspective and, moreover, leads to the recognition of normative contents and, therefore, distinct functions for fundamental rights." (Sarlet, I. (2018). *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado*).

Regarding the second topic, protection duties, these are especially focused on the protection that the State must safeguard, including preventively, not only against the Public Power (internal and external) but also against attacks by individuals. In relation to the right to the protection of personal data, we can identify that the edition of state legislation and its system of material and procedural guarantees was the main protective milestone of the protection duties.

Regarding the third item, procedures to guarantee and enforce the right, it is already identified that the above item brings the state regularization of its protection and effectiveness attempt. However, delving into the topic at hand here, we can see that the principle of data protection from the conception of processing systems ("privacy by design") to the creation of means to contain defects in operations ("privacy by default") are the final definers of this topic, as practical ways of executing and processing personal data safely and reasonably by third parties.[128]

In this way, the creation of the two dimensions of the right to the protection of personal data is verified, with its foundation to reinforce the legal regime and translate the right, especially focused as a fundamental guarantee.

Furthermore, defining the protection of personal data as a fundamental right and having a rule system to regulate it leads to postulating what may be the essence of this right to personal data protection, being certain that this topic seeks to elaborate the vision on the essence of the right to personal data protection.[129] Understanding the essence, at least in our view, of a right has the advantage of better considering the specificities of each right and the legal and political context in which it was developed.[130] The distinction between the protection of personal data and substantive rights lies in their respective nuances and essential elements. While personal data protection focuses on safeguarding individuals' privacy and controlling the use of their data, substantive rights encompass a broader spectrum of rights, including intellectual property rights like copyright. Copyright, as a form of intellectual property right, indeed presents complexities in its categorization. It intersects with the right to protection of personal data in various contexts, such as in the digital environment where data privacy and copyright considerations often overlap. However, it's important to note that copyright primarily pertains to the protection of creative works and expressions, rather than personal data specifically. Regarding its classification as a substantive right,

---

[128] Waldman, A. E. (2018). Privacy, notice, and design. *Stanford Technology Law Review*, *21*, 160–161.

[129] Lenaerts, K. (2019). Limits on Limitations: The Essence of Fundamental Rights in the EU. *German Law Journal*, *20*, 779–793.

[130] Dawson, M. E., & Orla E Muir, E. (2019). What is the Added Value of the Concept of the “Essence” of EU Fundamental Rights? *German Law Journal*, *20*, 763–778.

copyright is typically considered as such due to its role in protecting the intellectual creations of individuals or entities. However, its precise categorization can vary depending on legal frameworks and interpretations within different jurisdictions.[131] In the context of EU law, the framework for copyright protection is indeed multifaceted and not entirely unified, which can complicate its relationship with the right to protection of personal data.[132] The intersection between these legal domains underscores the need for careful consideration and balanced approaches to address the complex challenges arising from technological advancements and evolving legal landscapes.).[133] If these attributes represented the essence of data protection, their comparison would not be allowed, which does not seem to be the case. In this sense, we can understand the protection of personal data as, at a systemic level, checks and balances in which they are embodied to express society's stance towards the processing of personal data by third parties.[134]

Thus, we will study the essence of the right to the protection of personal data to collaborate with the research and updating of this essential topic for legal studies. The essence of the protection of personal data is to safeguard the rights and freedoms of individuals with respect to the processing of their personal data. This includes protecting individuals from possible harms that may arise from the improper handling of their personal data, such as discrimination, identity theft, or reputational harm.

Laws and regulations for the protection of personal data establish a framework for the collection, storage, and use of personal data and establish specific rules and procedures that organizations and governments must follow to ensure that personal data are treated fairly and securely, and respect individuals' privacy rights. This includes, among other things, requirements for organizations to obtain informed consent before collecting personal data, provide individuals with clear and concise information about how their personal data are being collected, used, and shared, and notify individuals and authorities in case of data breaches.

---

[131] HUGENHOLTZ, P. Bernt; VAN VELZE, Sam C. (2016) *Communication to a new public?* Three reasons why EU copyright law can do without a ‘new public’. International Review of Intellectual Property and Competition. p. 797-816.

[132] APLIN, Tanya. (2005) *Copyright law in the digital society*. Oxford: Hart.

[133] PORCEDDA, Maria Grazia. **On Boundaries – Finding the Essence of the Right to the Protection of Personal Data.** *In* LEENES, Ronald. (org.) *Data Protection and Privacy – The Internet of Bodies.* Hart Publishing. PP. 277 – 312. 2018. P. 289.

[134] Brkan, M. (2016). The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors? *Maastricht Journal of European and Comparative Law*, *23*(5).

The protection of personal data also includes rights for individuals, such as the right to access, rectify, or erase their personal data and the right to object to the processing of their personal data. In this way, the essence of the protection of personal data is to ensure that personal data are treated responsibly, transparently, and legally and safeguard the rights and freedoms of individuals with respect to their personal data.

Robert Alexy, commenting on the theory of spheres developed by the German Constitutional Court, clarifies that there are three spheres of protection, with varying and decreasing intensities. (i) The sphere, said to be lower, protected absolutely, and by legislation, fully, comprising the most secret matters that should not be known to others due to their extremely reserved nature; (ii) The expanded private sphere, which consists of matters that the individual brings to the knowledge of another trusted person, excluding the rest of the community, which can be known by the individual himself or the community at large; (iii) The sphere of communication, with the least intensity, comprising matters that the individual brings to the knowledge of everyone, which can be known by the individual himself or by everyone in the community.[135]

With the current portrayal of the subject, Maja Brkan depicts possible interferences with fundamental rights as concentric circles, where, in the outermost layer, there is no interference with the right and then - progressing towards the center - justified interference, unjustified interference, serious interference, and interference with the essence of the right. The distinction between interferences is particularly significant in light of the debate surrounding the relationship between balancing (proportionality sensu lato) and the essence of fundamental rights.[136]

A relativizing stance admits the possibility of compressing the essence of a fundamental right to safeguard another fundamental right, an absolute stance constructs essence and proportionality as mutually exclusive concepts. To explain better, theorizing the essence of the right to personal data protection is significant regardless of adhering to an exclusive or integrative stance. In the first case, it identifies unacceptable interferences regardless of the relative nature of the right to data protection; in the second, it allows for mitigating the gradation of interference based on the realization or assessment of the balancing test.

In this sense, Takis Tridimas and Giulia Gentile argue that there are three ways to analyze the essence of a right. First, the essence can be seen as an inviolable core in which interference

---

[135] Alexy, R. (1997). *Teoria dos derechos fundamentales. Trad. Ernésto Garzón Valdés. Madrid: Centro de Estudios Constitucionales*.

[136] Brkan, M. (2016). The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors? *Maastricht Journal of European and Comparative Law*, *23*(5).

cannot be legitimately interfered with a limit whose compression cannot be justified by compelling/ superior reasons. In this sense, the essence acts as an additional limit and identifies the type of interference with a right that cannot be legitimized by proportionality.[137]

Secondly, they continue to assert that the concept of essence can be seen, through the lens of a relative stance on interference itself, from the parameter of the most serious interference that one has on a right. It focuses, therefore, on the legal interest that the right seeks to protect and identifies the essence as the part of the right that is necessary to provide effective protection to that interest. In this conception, the essence is violated whenever the imposed limitations prevent its exercise and deprive it of any legal protection.

A third view of the essence is the limit beyond which an interference with the right leads to its extinction.

Returning to Brkan's teachings, the essence of a fundamental right suffers interference if (1) the interference threatens the very existence of that right, whether for all rights holders or for a specific right holder or group of rights holders; and (2) if there are no compelling reasons for such interference.

The principle that the essence of a right is violated when its existence is questioned without compelling reasons for restriction, thus introducing considerations of proportionality, finds illustration in various rulings of the Court of Justice of the European Union (CJEU). Here are some examples: In Case C-301/06, Ireland v. European Parliament and Council of the European Union (Judgment 10 February 2009), the legality of data retention laws and the balance between privacy rights and security interests were examined. Similarly, in Case C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Kärntner Landesregierung e.a. (Judgment 08 April 2014), the validity of EU data retention directives and their compliance with fundamental rights were at the forefront. In Case C-207/16, Ministério Fiscal (Judgment 02 October 2018), the proportionality of national legislation imposing tax penalties and its impact on the right to property were discussed. Another case, C 398/15, Câmara de Comércio, Indústria, Artigianato and Agricoltura di Lecce v. Salvatore Manni (Judgment 09 March 2017), examined the compatibility of Italian legislation on immovable property auctions with EU law, focusing on the right to property. Furthermore, in Case C-136/17, GC and Others v. Commission nationale de l'informatique et des libertés (CNIL) (Judgment 24 September 2019), the balance between the right to privacy and the right to freedom of expression in the context of internet search

---

[137] The Essence of Rights: An Unreliable Boundary? (2019). *German Law Journal. PP*, *20*.

engine delisting requests was deliberated. Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV (Judgment 16 February 2012), dealt with the balance between copyright protection and the rights of internet service providers regarding user-generated content. Lastly, Case C-275/06, Digital Promusicae v. Telefónica de España SAU (Judgment 29 January 2008), examined the balance between the right to copyright protection and the right to privacy in the context of disclosing internet user data for civil proceedings.[138]

Following such a structure and the framework of personal data protection described above, this topic argues that a violation of the essence of the right to personal data protection is a strong enough compression to threaten the very existence of the system of checks and balances on which the right to data protection is based, when there are no compelling reasons for doing so.

The first part of the test determines the presence of an interference in the essence of the right, which occurs when the very existence of the right is questioned for rights holders (objective interference in the essence) or for a specific rights holder (subjective interference in the essence). The second part of the test defends the exclusive position, which conceives interference with the essence of the right as unjustifiable by balancing and - conversely - does not consider interference with the right as compression of its essence in all cases where it can be justified, by reference to compelling reasons (i.e., balancing). Thus, Brkan's test to determine an interference in the essence of a fundamental right is particularly interesting considering the conception of the right to personal data protection outlined in this thesis.

Personal data protection is not an absolute right, so it can be legitimately compressed by other primordial rights; it can also be illegitimately usurped, which would result from the balancing test favoring personal data protection over the other conflicting right. In EU law, no fundamental right is considered absolute. Instead, each right must be balanced and articulated with other fundamental rights using the principle of proportionality. This principle requires that any restriction or limitation on a fundamental right must be necessary and proportionate to achieving a legitimate aim. Therefore, in cases where personal data protection conflicts with other rights, such as freedom of expression or national security, a careful balancing exercise is required to ensure that the restrictions placed on personal data protection are justified and proportionate to the competing interests at stake.[139]

---

[138] Dalla Corte, L. (2020). *Safeguarding data protection in an open data world: On the idea of balancing open data and data protection in the development of the smart city environment*.

[139] POLAKIEWICZ, Jörg. (2003) Profiling – the Council of Europe's Contribution. *In:* GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul; POULLET, Yves (org.). *European data protection:* coming of age. London: Springer, p. 367-377. p. 372.

A violation of the essence of the right to personal data protection would exist, therefore, in cases where the interference with the right challenges, explicitly or implicitly, society's choice to have a legal framework for the processing of personal data. Think of all the ways in which the system of checks and balances on which personal data protection is based can be practically eradicated by neglecting, exploiting, or misinterpreting the provisions of derivative law that are not directly mentioned in art. 5th, LXXIX, of the CF/88 or defined as "fundamental" by the STF, such as perhaps the provisions on transfers of personal data to third countries or international organizations.

Limitations on the right to personal data protection should be the exception, not the rule. Thus, the essence of the system of checks and balances on which data protection is based - the "fundamental right to a rule" regulating the processing of personal data - should be seen as the collective decision to generally allow the processing of personal data because of its promises while at the same time regulating it because of its dangers. An interference with the essence of the right to personal data protection is therefore different from a regular interference, regardless of how serious. While the former harms part of the system of checks and balances of personal data protection, the latter questions and jeopardizes the very functioning and legitimacy of the collective stance on data processing as a whole and, ultimately, its deeper roots: the rule of law and democracy. Drawing a parallel with copyright in the EU legal order, where exceptions or limitations are strictly construed, underscores the gravity of interfering with the core principles of personal data protection. Just as exceptions to copyright are carefully circumscribed, limitations on the right to personal data protection should be approached with caution and reserved for truly exceptional circumstances.[140]A right to a permissive and procedural rule, allowing - and still channeling - an activity as fundamental to modern society as it is possibly dangerous. The *sui generis* emergence of personal data protection is linked to technological development and its constitutionalization to the growing importance of secondary legislative framework. Lorenzo Dalla Corte brings the notion that the right to personal data protection has the idea of proceduralism, which he defines as "a theory that justifies rules, decisions, or institutions by reference to a valid process, as opposed to being morally correct according to a substantive account of justice or goodness."[141]

---

[140] HUGENHOLTZ, P. Bernt; VAN VELZE, Sam C. (2016) *Communication to a new public?* Three reasons why EU copyright law can do without a ‘new public’. International Review of Intellectual Property and Competition. p. 797-816.

[141] Dalla Corte, L. (20020. *Safeguarding data protection in an open data world: On the idea of balancing open data and data protection in the development of the smart city environment*.

Given the heterogeneity of the rights and principles underlying the fundamental right, its formal (and practical) differentiation from privacy, and its procedural/instrumental and permissive nature, this thesis argues that the most coherent conceptualization of the right to personal data protection is of a system of rules and principles that regulate the processing of personal data by virtue of its potential impacts on individuals and society.

The essence of the right to personal data protection has been framed as the collective and social choice to have a system of checks and balances regulating the processing of personal data. The violation of the essence of the right to data protection can be defined as a compression strong enough to threaten the very existence of such a system of checks and balances when compelling reasons do not exist, regardless of which specific component of the right is compressed.[142]

Personal data protection is a non-homogeneous set of rules and norms whose content hardly fits into a unitary logic. Technological development, the spread of informatics, and the rampant datafication of society have led to the development of a sui generis right that no longer equates to privacy - if it ever did - but to something different, new, and still in flux, which was then elevated to the status of a fundamental right.

Personal data protection is a response to the power and information asymmetries that exist between those who control the means of data processing and the individuals to whom this data refers and responds to a recent need for protection that has emerged in parallel with advances in information technologies and their role in contemporary society.

In a way, the justification for the elevation of personal data protection to the status of a fundamental right should not be sought in the conceptual autonomy or systematic coherence of the heterogeneous array of rights and principles that constitute personal data protection. On the contrary, it is the constitutionalizing of personal data protection as an autonomous fundamental right that helps delineate its substance.

The seemingly inconsistent set of rights and principles underlying personal data protection, in the face of its explicit constitutionalizing by the Charter and assuming the democratic legitimacy of the underlying legislative process, creates a pragmatic system of protection that should be seen as the embodiment of such choice.

The conceptualization of the right to personal data protection serves the purpose of explicitly delineating how it expresses a defined social stance regarding the processing of personal data. More importantly, recognizing the conceptual autonomy of personal data protection and its links to the

---

[142] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019*. Profile Books.

advancement of computing technology and thus modern society could promote the development of the right, to its full potential.

Procedural rights refer to the legal process and procedures that individuals and organizations must follow to have their rights protected and respected. These procedures aim to ensure fairness, impartiality, and transparency in legal proceedings and decision-making processes. Examples of procedural rights include the right to a fair trial, the right to be informed of the charges against you, the right to legal representation, the right to summon and examine witnesses, the right to appeal a decision, and the right to access court records.[143]

Procedural rights are important because they ensure that individuals and organizations are not subjected to arbitrary or discriminatory treatment by the state or other authorities. They also provide a means for individuals and organizations to challenge decisions that may negatively affect them and seek redress for any violations of their rights.

The most coherent construction of personal data protection is simply the fundamental right to have a set of rules regulating the processing of personal data. The value of personal data protection lies, in a way, in the existence of a system of rules and norms applicable to the processing of personal data, regardless of its connection to concepts such as privacy, or the secrecy and confidentiality of information.

The fundamental right to personal data protection has emerged therefore and response to the rampant digitization of society and the increasing importance of information (personal) processing. Its core, whose content depicts a heterogeneous range of rights and principles of personal data protection.

A right to a rule, therefore, its logic is closer to due process than privacy. This dimension of the right may have already been observed since the early discussions about this normative innovation.[144] In 1973, in a study prepared for the United States Department of Health, Education, and Welfare, the main aspects and foundations for the proper processing of citizens' data, especially aimed at the three areas of that Department, were dissected.

This study elaborated in the 1970s serves as a basic parameter for understanding this right, and it is seen that the reasons for its study and presentation are paramount to understanding the growing concern about the harmful consequences that may result from the uncontrolled application of computer and telecommunications technology for the collection, storage, and use of personal

---

[143] Carnelutti, F. (1999). *Instituições do processo civil. Trad. Adrián Sotero de Witt Batista. Campinas: Servanda*.

[144] Docksey, C. (2015). *Articles 7 and 8 of the EU Charter: Two Distinct Fundamental Rights. in GROSJEAN, Alain (org.) Enjeux européens et mondiaux de la protection des données personelles*.

data about citizens. In fact, the Secretary of Health, Education, and Welfare of the United States at the time of the study emphasized the public interest in establishing rules and principles for the care of personal data:

The study carries with it the primordial idea of transparency to the public regarding the treatment of personal data and its purpose, including its sources, its uses, and the justification for retaining it. Furthermore, the study records that it is based on five basic principles that would have legal effect as safeguard requirements for automated systems of personal data, namely:

> "- There should be no systems for maintaining records of personal data whose very existence is secret.
> - There must be a way for an individual to find out what information about him is in a record and how it is used.
> - There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent;
> - There must be a way for an individual to correct or alter a record of identifiable information about him.
> - Any organization that creates, maintains, uses, or discloses records of identifiable personal data must ensure the reliability of the data for the intended use and must take precautions to prevent the misuse of the data."[145]

Moreover, the study itself delves into the need to protect identifiable or identified personal data of human beings, and with care to protect data, even if made available in anonymized form.

The essence of the system of checks and balances on which data protection is based—the "fundamental right to a rule" regulating the processing of personal data—should be seen as the collective decision to generally allow the processing of personal data because of its promises, while at the same time regulating it because of its dangers. An interference with the essence of the right to personal data protection is therefore ultimately an affront to the rule of law and the dignity of the human person. Substantive rights, on the other hand, refer to the actual rights and freedoms to which individuals and organizations are entitled under the law. These rights are designed to protect and safeguard the interests and well-being of individuals and organizations. Examples of

---

[145] *Records, computers and the rights of citizens*. (n.d.). ASPE. Retrieved February 20, 2024, from https://aspe.hhs.gov/reports/records-computers-rights-citizens

substantive rights include the right to life, liberty, and security of the person; the right to freedom of expression, religion, and assembly; the right to property, the right to privacy, the right to education, and the right to fair and equal treatment under the law.

Substantive rights are important because they provide the basis for the ability of an individual or organization to live a full and meaningful life and to fully participate in society. They also provide an important check against the arbitrary or discriminatory use of power by the state or other authorities.

Thus, the role of substantive law is to confer legality on citizens, that is, to make them guarantors of positive legal norms for their protection. Pérez Luño refers to this idea of the dignity of the human person, as well as the demands and needs linked to the conquest of freedom and equality, from which human rights derive. These essential rights have a foundation that predates positive law, that is, preliminary and basic in relation to it. It is therefore clear that the reference to provisions on personal data protection stands out as a procedural system of heterogeneous checks and balances that gradually dissociates from the logic of privacy.[146]

Conclusion

Thus, we can outline the main aspects of personal data protection as follows: the subject is any natural person, from that country or foreign, resident, or transient in that country or region. The content is the specific faculty attributed to the subject, which may be the faculty to deal with their data by others, or to resist them, or to dispose of, enjoy, or handle their personal information. Personal data protection, as a right, has as its content the faculty to constrain others to respect it and to resist the violation of what is proper to it, that is, the vital situations that, as they concern only the individual, they wish to keep for themselves, sheltered by their sole and discretionary decision. The object is the protected good, which may be *a res* (a thing, not necessarily physical, in the case of real rights) or an interest (in the case of personal rights). In the right to personal data protection, the object is, succinctly, informational self-determination.

The subject can be clearly verified in the legal text, since the legislator himself affirmed that the data subject is the person to whom the data refer and not the person who collected them. Moreover, protection must be limited to subjects with identifiable data or identified individuals. When data is disclosed, as an example, in statistical form, reasonable precautions must be

---

[146] Luño, A.-E. (2005). *Derechos Humanos, Estado de Derecho y Constitución. 9*.

considered, with the aim of fulfilling the obligation not to disclose data that can be traced back to specific individuals.

However, it is worth mentioning the existence of literature in an extensive sense, which guarantees legal entities a personal data protection equivalent to that of natural persons, which refers to the proposition that personal data protection has an instrumental nature, also serving (but not only and not necessarily) to safeguard privacy. In any case, even though we adhere to the position, for now, the legislation determines that the right to personal data protection is held only by natural persons. Furthermore, for the record, legal entities and even other entities can be holders of fundamental rights, compatible with their condition.

Still on this point, even though personal data protection as such is guaranteed only to natural persons, the same does not occur with the ownership of the right to informational self-determination, which, although also controversial, has been, at least in some legal orders — as is the case in Germany — equally attributed to legal entities.

We see that, through these two concepts, there is a great differentiation of object and objective. While the right to privacy seeks to defend the individual's intimacy and private (and family) life, the right to personal data protection is the protection of personal data itself, its use, its collection. Although it protects the individual, since it protects the individual from the search of third parties for collected and organized information that can describe, identify, qualify, and standardize such person and their life, this defense of the individual should be understood as a mediate objective.

Furthermore, it is reaffirmed that transparency about how personal data is processed is the key to the proper functioning of the market. Data subjects must know when and how their personal data is being collected and used and be able to decide whether and how to participate; and they must have access to companies' information on how they are collecting, storing, and using it, so they can select the company that best meets their preferences.

However, given the scale and complexity of personal data processing practices, it is argued that such transparency will not be sufficient to guarantee effective protection of personal data. It is suggested that the principle of controller/processor responsibility should play a more effective role in ensuring effective control over personal data. This accountability is a form of collective approach in that it strengthens the individual in relation to the controller/processor.

Indeed, individuals are recognized rights and protective instruments – such as the right to be forgotten, simplified access to data, the right to portability, and the right to know when data has been hacked. Data controllers and processors, on the other hand, are required to follow the principle

of data protection from the design of processing systems ("privacy by design") to the creation of means to contain defects in operations ("privacy by default"). The object of the right to data protection is to protect personal data, which is any information that can be used to identify an individual, such as name, address, or biometric data. Personal data can be confidential, such as health information or information about an individual's political or religious opinions, or may not be confidential, such as information about an individual's name and address.

The right to data protection aims to ensure that personal data is collected, used, and stored in a way that respects individuals' privacy rights and that personal data is accurate, complete, and up to date. Data protection laws are designed to give individuals control over their personal data, including the right to access, correct, delete, and object to the use of their personal data for certain purposes.

The right to data protection also imposes obligations on organizations that collect and process personal data, such as obtaining explicit consent from individuals before collecting their personal data, informing them about how the data will be used, and providing them with the ability to control their personal data. Organizations must also implement appropriate technical and organizational measures to protect personal data against unauthorized access, alteration, or destruction.

Thus, the objective of the right to data protection is to protect personal data and ensure that it is collected, used, and stored in a way that respects individuals' privacy rights, giving individuals control over their personal data, including the right to access, correct, delete, and object to the use of their personal data for certain purposes, and also imposing obligations on organizations that collect and process personal data, such as obtaining explicit consent, informing individuals about data usage, giving them control over their personal data, and implementing appropriate measures to protect personal data against unauthorized access, alteration, or destruction.

Therefore, the principle of purpose, the principle of adequacy, the principle of necessity, the principle of free access, the principle of data quality, the principle of transparency, the principle of security, the principle of prevention, the principle of non-discrimination, and the principle of accountability and accountability are thus constitutive elements of the right to personal data protection, and not additional conditions. Still, regarding the content, it is noteworthy that it is identical to that of informational self-determination, which is a decision right, whose object would be the care of data and information related to a particular person.

Finally, it is worth mentioning that according to the legislation, there is no differentiation between the terms "information" and "data", but rather, if there is the identification of a natural

person. Nevertheless, it is always worth remembering that academia has already clarified the exactness of each of these terms.

Thus, it is concluded that the right to personal data protection should be understood as a new right to personality, since these same data influence the individual's projection and their relational sphere with the world.

The Right to Personal Data Protection is a new right, which mainly arises from the incessant search for personal data by States and Private Companies in the need to monetize, turning them into highly profitable raw material and product. As Shoshana taught us, surveillance capitalism is primarily based on the expropriation of the most basic human rights, such as autonomy and freedom, through the extraction, prediction, and sale of people's data.

In this scenario, the elevation of the Right to Personal Data Protection to a fundamental right serves as a systemic defense of checks and balances that are embodied to express society's stance in the face of personal data processing. Thus, the recognition of a subjective right of constitutional scope.

By this corollary, the Right to Personal Data Protection can be defined as an instrumental/ procedural and substantive right. Data protection is primarily a transparency tool, but sometimes its substantive provisions restrict the possibility of processing personal data or establish limits on the types of processing that can be done on personal data. Personal data protection is intended to enable a wide range of rights and freedoms, such as privacy. Being a right that aims to provide proactive and structural protection of the rights and freedoms that may be affected by the processing of personal data.

Repeat. The principle of purpose, necessity, free access, data quality, transparency, security, prevention, non-discrimination, accountability, and accountability are constitutive elements of the right to personal data protection. Nevertheless, it is worth emphasizing that these elements are not unique to constitute the right. The right is dynamic and constitutes a synthetic representation of the social stance that has developed over the years, in response to the diffusion and importance that the processing of personal data has acquired since the turn of the century.

Data protection can be considered both a substantive and procedural right. Substantive data protection refers to the protection of an individual's personal information, including rights of access, rectification, or erasure of personal data and the right to object to the processing of their personal data. It also includes the right to privacy, which is the right to control who has access to personal information and for what purpose it is used.

Procedural data protection refers to the processes and procedures that organizations and governments must follow to ensure that personal data is collected, stored, and used in compliance with data protection laws and regulations. This includes requiring organizations to have clear and transparent privacy policies, obtain informed consent before collecting personal data, and notify individuals and authorities in case of data breaches.

Thus, it refers to a combination of substantive and procedural rights. Substantive rights ensure that individuals have control over their personal information and procedural rights ensure that organizations and the government follow specific procedures to protect personal data.

Therefore, to understand the essence and logic of a right, one can also start from its violation: a violation of purpose specification or rights of access and rectification, or the control of the independent authority, does not necessarily equate to a violation of the essence of the right to personal data protection itself. It is explained that personal data protection is intended to enable information sharing: there would be no need for this if there were a general prohibition on disclosing personal data, and the law rarely prohibits the processing of personal data, but obliges processors and operators to meet requirements, to do so legally. This permissive conception of the right to personal data protection as a transparency tool is consistent with its procedural nature.

In this sense, it is recalled that in many circumstances of modern life, an individual may wish to waive part of that control or make their personal data available to the public and/or private organization that offers a desirable service/product to them. In this vein, the sharing of personal data for a benefit is not inherently unfair, as long as both parties have clarity and transparency about the terms of this exchange and comply with the law. As elaborated in this thesis, the implications of the right to personal data protection in today's world have ramifications in virtually all other existing rights. The right to personal data protection can identify and be applied to transatlantic sharing of personal data, mass surveillance, mass collection and/or retention of data, by the State or private companies, as well as in cases of monitoring and filtering electronic communications to prevent copyright infringements, to the transmission of personal data on a website accessible to anyone on the internet. In contrast, copyright protection primarily concerns the safeguarding of intellectual property rights, particularly in creative works and expressions. Acts such as copying, distributing, or reproducing copyrighted material without authorization constitute copyright infringement. While the right to personal data protection focuses on safeguarding individuals' privacy and controlling the use of their personal data, copyright protection pertains to the protection of creators' rights over their intellectual creations. The two legal concepts operate in distinct domains, with personal data protection primarily concerned with privacy rights and data control, while copyright protection

revolves around intellectual property rights and the prevention of unauthorized use or reproduction of creative works.

Individual control over personal data is desirable from a conceptual perspective. It is fundamental for individual self-development and can help minimize power and information asymmetries. Individual control should not, therefore, be absolute. Instead, it is suggested that individual control over personal data should function as a starting point for the analysis of personal data processing: individuals should have control over their personal data unless there is a legally accepted third-party interest in processing. Thus, personal data processing must ensure compliance with principles and safeguards for respecting individuals' rights. Implicit in this framework is, therefore, a reconciliation of the rights of data subjects with the interests of those processing personal data and of society, more generally.

However, the burden of proof falls on the data controller responsible for demonstrating the limitations on the data subject's right. This is justified based on the subjective dimension, which seeks precedence over the interests of personal data controllers. The starting point in the application should be individual control over personal data, as it does not require the data subject to demonstrate a legitimate reason to object and instead requires the controller to justify the need/ purpose of processing, especially when dealing with sensitive personal data.

Thus, it can be affirmed that the right to personal data protection has acquired the attribute of a fundamental right and is fully applied to the constitutional-legal regime, in both material and formal senses: 1) it has become an integral part of formal constitutionality, with normative status superior to supranational legal order; and, finally, and most importantly, 2) its essence is endowed with immediate applicability (direct) and directly binds the actors.

It is concluded, therefore, that the Right to Personal Data Protection is a fundamental right, with the characteristic of an instrumental/procedural right, which serves as a transparency tool, designed to provide safeguards to the individual whenever their personal data is processed. Personal data protection is also a procedural/instrumental right, insofar as it hardly protects a specific interest, but serves the objectives pursued by other substantive fundamental rights, such as human dignity and/or privacy. Time and reflection will serve as a process of adjusting the law in 21st-century society. It is certain, therefore, that national legislation and the Supreme Court hold defined rules and norms that allow protecting the individual citizen and society, with authorities, society, and the judiciary dealing with arbitrary or abusive practices in the coming decades, which we may observe in future academic work that allows for a comprehensive overview of the subject in daily practice.

The right to personal data protection, therefore, is a fundamental right to the protection of the human person and their dignity with the foundations of the legal and normative bases of the due informational process in the face of existing conflicts in the information society and the era of surveillance capitalism.

The tectonic movement of creation, modification, and assimilation of personal data protection has deeply impacted the legal landscape, triggering a frenzy among scholars, authorities, and the curious. Suddenly, capitalism has transformed into surveillance capitalism, and pandemic-fighting mechanisms have become instruments of privacy invasion. Artificial intelligence emerges as the last frontier of a wave of new opinions, all based on cyber-legal concepts, turning data protection into a battleground where there is no middle ground: either one accepts the collection and secondary sharing of personal data, even without the consent of the data subject, or activities come to a standstill. In this context, data protection, its logic, and discourse have presented discouraging results.

Similar problems arise regarding fundamental concepts of the data protection system. The law should require a purpose in the collection, but reality responds with the increasing combination of databases, often in an automated way, making this legal requirement illusory. The law should determine that processing should use the minimum necessary data, while reality contradicts, with the global volume of processed data increasing exponentially every year. The most concerning result is that the data protection system does not work in practice, generating bureaucratic problems and legal conflicts on a global scale.