ADMINISTRAÇÃO DE EMPRESAS EM REVISTA

Submetido em: ***22/07/2023***
Aprovado em: ***24/09/2023***
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

PERSONAL DATA PROTECTION: A CHANGING CONCEPT IN THE UNITED STATES, GERMAN-EUROPEAN, AND BRAZILIAN MODELS

PROTEÇÃO DE DADOS PESSOAIS: UM CONCEITO EM MUDANÇA NOS MODELOS DOS ESTADOS UNIDOS, ALEMANHA-EUROPA E BRASIL

LUCAS CATIB DE LAURENTIS
Professor da Pontifícia Universidade Católica de Campinas, Faculdade de Direito, coordenador e membro do corpo docente permanente do Programa de Pós-Graduação stricto sensu em Direito (PPGD). lucas.laurentiis@gmail.com. https://orcid.org/0000-0001-5596-6695

RAFAEL TEDRUS BENTO
Doutorando em Direito Constitucional pela Pontifícia Unidades Católica de São Paulo (PUCSP), Mestre em Direitos Humanos e Desenvolvimento Social pela Pontifícia Universidade Católica de Campinas (PUCCAMP), com período integrado ao Mestrado em Direito da União Europeia da Universidade do Minho (UMinho), em 2021, Especialista em Direito Empresarial pelo INSPER, Especialista em Direito do Trabalho pela Pontifícia Unidades Católica de São Paulo (PUCSP), Graduação em Direito pela Pontifícia Universidade Católica de Campinas (PUCCAMP). rafaeltedrus@gmail.com. ORCID: 0000-0003-2677-5595

CARLO JOSÉ NAPOLITANO
Professor Associado da Universidade Estadual Paulista – UNESP, Departamento de Ciências Humanas e do Programa de Pós-Graduação em Comunicação, da Faculdade de Arquitetura, Artes, Comunicação e Design, Bauru/SP, Livre-Docente em Direito à Comunicação, Pós-Doutor pelo Departamento de Direito do Estado, da Faculdade de Direito, da Universidade de São Paulo, Doutor em Sociologia pelo Programa de Pós-Graduação em Sociologia da Faculdade de Ciências e Letras, UNESP/Araraquara, membro do grupo de pesquisa Mídia e Sociedade/CNPq, coordenador da linha de pesquisa Direito à Comunicação. e-mail: carlo.napolitano@unesp.br. CV: http://lattes.cnpq.br/4413410311464411. https://orcid.org/0000-0002-6328-6398

FLÁVIA PIVA ALMEIDA LEITE
Professora Assistente Doutora da Universidade Estadual Paulista – UNESP, Departamento de Ciências Humanas de Bauru e do Programa de Pós-Graduação em Direito da UNESP - Franca. e-mail: flavia.leite@unesp.br. https://orcid.org/0000-0002-8994-6198.

TATIANA STROPPA
Doutora e Mestre em Direito pelo Programa de Pós-graduação – Instituição Toledo de Ensino, professora de Direito Constitucional e de Direito Processual Constitucional do

ADMINISTRAÇÃO DE EMPRESAS EM REVISTA

Submetido em: ***22/07/2023***
Aprovado em: ***24/09/2023***
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

Curso de Direito do Centro Universitário de Bauru (ITE-SP) e da Faculdade Iteana de Botucatu, advogada, e-mail: tatianastroppa@hotmail.com. https://orcid.org/0000-0002-3456-7588

ABSTRACT:

Objective: This article aim to describe and analyse three different models of regulating the personal data protetion, the American, the German-European, and the Brazilian models.

Methodology: This text is based on a review of national and foreign literature and documentary research.

Results: The article provides some critical considerations regarding the effectiveness of the personal data protetion in all this models.

Contributions: The main contribution of this text is to present and analyze the evolution of the concept and the right to personal data protection in three different legal models, considering that there are normative provisions, however, with low effectiveness.

Keywords: Fundamental right; Personal data protection; American law; German-European law; Brazilian law.

RESUMO:

Objetivo: Este artigo tem como objetivo descrever e analisar três diferentes modelos de regulação da proteção de dados pessoais, o americano, o alemão-europeu e o brasileiro.

Metodologia: Este texto baseia-se em uma revisão da literatura nacional e estrangeira e pesquisa documental.

Resultados: O artigo traz algumas considerações críticas sobre a efetividade da proteção de dados pessoais em todos esses modelos.

Contribuições: A principal contribuição deste texto é apresentar e analisar a evolução do conceito e do direito à proteção de dados pessoais em três diferentes modelos jurídicos, considerando que existem dispositivos normativos, porém, com baixa efetividade.

Palavras-chave: Direito fundamental; Proteção de dados pessoais; direito americano; Direito alemão-europeu; Direito brasileiro.

1 INTRODUTION

More than concepts or words. Data protection, privacy, cybersecurity, consent, big data or artificial intelligence have become expressions of order, indicating the place and

ADMINISTRAÇÃO DE EMPRESAS EM REVISTA
Submetido em: **22/07/2023**
Aprovado em: **24/09/2023**
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

assumptions of those who speak and apply these concepts; signs of a way of thinking that prioritizes the security of the individual in a world of growing uncertainty, generated by the constant exchange of information and the multiplication of means of data collection and behavioral surveillance, whether state or private; In short, they are indicative of a new era in which legal concepts are supplanted, often colonized, by terminology from the computer sciences, engineering and even the language sciences, which dictate the development of a whole range of articles, books, theses, lectures and experts.

The production on data protection is titanic and torrential, much like the debates, the theses, the comments, and, of course, the challenges to be faced by anyone who, in some way, dares to venture into the new and unknown world of personal data protection.[1]

Here, we propose an overview of some central aspects of different models of personal data protection, some of which are already well-known to the Brazilian public. However, this is not purely a speculative or comparative endeavor, not only because, as will be indicated later, these models have points of interconnection in what many might call an international dialogue of legal systems[2], but also and above all because we adopt here the theoretical assumption, with practical implications, that legal concepts are not generated in a vacuum, much less conceived and applied within a territory or jurisdiction in isolation or in isolation.[3]

Thought, whether legal or not, knows no physical or imaginary boundaries, and therefore, it is not possible to think about "Brazilian data protection" without considering what the fundamental or human right to data protection is, what it has been, and what is

[1] Among others: BRITZ, G.. Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts. In: HOFFMANN-RIEM, W.. *Offene Rechtswissenschaft*. Tübingen: Mohr Siebeck, 2010; BUCHNER, B.. *Informationelle Selbstbestimmung im Privatrecht*, Tübingen: Mohr, 2006; VESTING, T.. Das Internet und die Notwendigkeit der Transformation des Datenschutzes. In: LADEUR, K. H. (Hrsg.). *Innovationsoffene Regulierung des Intertet*, Baden-Baden: Nomos, p. 155-190, 2003; ALBERS, M.. *Informationelle Selbstbestimmung*, Baden-Baden: Nomos, 2005; BULL, H. P.. *Informationelle Selbstbestimmung – Vision oder Illusion*?, MohrSiebeck: Tübingen, 2009; LADEUR, K. H. Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?.In: *Die Öffentliche Verwaltung*, p. 45-55, 2009; PITSCHAS; R. Informationelle Selbsbestimmung zwischen idgitaler ökonomie und internet, *DuD*, n. 139, p. 146 e ss, 1998; HOFFMANN-RIEM, W.. *Informationelle Selbstbestimmung in der Informationsgesellschaft - Auf dem Wege zu einem neuen Konzept des Datenschutzes*, AöR, v. 123, n. 4, p. 513-540, 1998; POSCHER, R.. The Right to Data Protection. In: MILLER, R. (org.), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair*. Cambridge: Cambridge University Press. P. 129–142, 2017; LYNSKEY, O.. *The Foundations of EU Data Protection Law*. Oxford University Press, Oxford, 2015; RODOTÀ, S.. *A vida na sociedade da vigilância*: A privacidade hoje. Rio de Janeiro: Renovar, 2008; TZANOU, M.. *The fundamental right to data protection*, Oxford: Hart Publishing, 2017.

Submetido em: **22/07/2023**
Aprovado em: **24/09/2023**
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

expected of it in the United States or on the "old continent." Especially in a hyperconnected world with a high flow of information and data in all directions across the globe, it is indeed no longer possible to think of rights such as freedom of expression, privacy, or data protection based on isolationist concepts that separate national thought and law from international parameters of human rights protection and international trade regulation.[2]

With the aim of providing an overview of some central aspects of different models of personal data protection, based on a review of national and foreign literature and documentary research, the text begins with the place that was the origin of the right, often seen as synonymous with, or the ancestor of, personal data protection: privacy, born in the United States of America. Subsequently, we present the German-European model of data protection and the Brazilian model. Finally, an analysis of the evolution of the right to personal data protection is presented, concluding that despite the existing legal regulation, its effectiveness is a problem.

2 NORTH AMERICAN MODEL OF PROTECTION

As well-known as it is misunderstood, the text by Samuel Warren and Louis Brandeis, written in 1890 and still relevant, (BRANDEIS; WARREN, 1890) lays out the foundations and understanding of privacy and, consequently, personal data protection in American law.

The foundations or roots of this right appear early in the well-known article: the protection of the right to liberty and property, which, based on the evolution of common law, must be periodically renewed and reinterpreted, especially in light of progress. In this case, the progress referred to by the authors has two dimensions: one is socio-economic, and the other is rooted in technology.

From a social and economic perspective, the interpretative renewal proposed by the authors is rooted in the transformation of American society. It shifted from a rural and extractive society, where individuals and families were separated by vast spaces with few

[2] Learn more about the subject, at the OECD guidelines on personal data protection: G20/0ECD Principles of Corporate Governance. Paris: *OECD Publishing*, 2015.

Submetido em: **22/07/2023**
Aprovado em: **24/09/2023**
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

places for social interaction (sparse encounters mostly occurred in churches or religious gatherings).

Industrialization and the development of international trade altered this structure, creating urban concentrations and intensifying contact between different groups and classes.[3] This structural change was accompanied by a technological revolution: the invention of the camera, which made it possible to preserve the capture of moments, situations, and actions that were previously forgotten over time.

This led to the emergence of a new form of communication: the penny press, yellow journalism, or tabloid media, which specialized in disseminating unusual facts about the lives of celebrities and politicians, fake news, and everyday gossip. While, on one hand, the audience from lower social classes satisfied their thirst for entertainment and leisure with these publications, the wealthier classes began to harbor a growing aversion towards these media outlets and everything they represented.

That's what happened to Louis Brandeis, a successful lawyer from a wealthy French-descendant family, who, after hosting a party at his home, had his image published alongside acquaintances and family members.[4]

The conclusion of Warren and Brandeis' work reflects this situation and marks the authors' stance in the face of society's encroachment on the sphere of personal secrecy: "The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery." (BRANDEIS; WARREN, 1890, p. 196).

The "fundamental right"[5] that arises from this realization is one of the most significant and enduring innovations in the history of American constitutional law: the right "to be let alone," viewed as the prerogative of its holder to withdraw from the public eye and, in doing so, prevent the intrusive gaze of the government and society from encroaching upon the space guaranteed by privacy. The consequences of this right have been as extensive as they have been controversial. Coupled with the Fourth Amendment

[3] In the same sense, regarding the social roots that led to the emergence of Privacy, learn more at: FREEDMAN, W.. *The right to privacy in computer age*, New York: Quorum Books, 1987.
[4] On the context of the elaboration of the article by Warren and Brandeis, see HOFSTADTER, S.; HOROWITZ, G.. *The right to privacy*, New York: Central Books, 1967.

Submetido em: **22/07/2023**
Aprovado em: **24/09/2023**
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

of the U.S. Constitution (equal protection under the law and due process), it not only protects certain spaces (workplaces, universities, schools, and residences) from the intrusion of state authorities but also limits these authorities' access to personal information transmitted or accessed through interindividual means of communication (telephone, mail).[5]

This does not mean that the protection provided by privacy in American law is broad and exhaustive. On the contrary, whether the information accessed and disclosed is in the public domain or because the treatment or collection of data occurred by private agents, the effectiveness of the fundamental right to privacy is automatically set aside. In these latter scenarios, for the holder to have the right to access or retain data processed by third parties, it is necessary for subconstitutional legislation to specify the limits and content of this right, which has already occurred in known cases but with limited scope. Among these, one can mention the Health Insurance Portability and Accountability Act of 1996, the Electronic Communications Privacy Act and the Fair Credit Reporting Act, the Privacy Act, de 1974, the Computer Fraud and the Abuse Act, finally, the Digital Millennium Copyright Act).

As a result, websites and internet portals that "data mine" their users or use malicious tools to access browsing data or even personal information of their users can operate without fear in the American virtual territory. Despite the efforts of the Obama administration (2009/2017), the logic of the market still prevails when it comes to controlling the flow of information in the virtual environment[6] in the United States. In Europe, the situation is different.

3 GERMAN-EUROPEAN MODEL OF DATA PROTECTION

The year 1977 was when the Federal Republic of Germany enacted its first law on the protection of personal data, which had the specific purpose of 'protecting individuals

[5] In both situations, the U.S. Supreme Court requires the presence of probable cause and that the means employed in searching for information be "reasonable" for access to personal information to be considered valid, which generally means that the search must be supported by a judicial warrant: Winston v. Lee 470 U.S. 753 (1983).

Submetido em: **22/07/2023**
Aprovado em: **24/09/2023**
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

against interference in the use of their personal data' (GERMANY, BDSG, 2017), a regulation exclusively aimed at state actions that negatively interfere (through unauthorized individual data collection) or positively interfere (by preventing individuals from using data as they please) with individual self-determination over personal data.[6]

The premise behind such legislative creation was the existence of an asymmetric relationship of power and knowledge between the data-collecting entity (the State) and the subjects subjected to data collection activities. This resulted in two consequences.

Firstly, with the establishment of the welfare state and the subsequent increase in state functions, the collection of personal data became a necessary activity for the organization of public functions, particularly for the efficient and timely provision of public services.[7] Data collection, in this sense, was conceived as a means of safeguarding the users of public services, who have the right to the continuity and quality of public services provided by the State or by service concessionaires.[8]

Secondly, for the execution of these activities, public agencies began to create extensive databases in which information related to personal characteristics and habits started to be cataloged in a centralized and systematic manner. The control power resulting from this accumulation of information was the catalyst for the creation of a shield called the protection of personal freedom.

Without the assurance 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 constrained by individuals themselves (chilling effect), as they would control their actions in anticipation of potential harm that could result from them.[9]

[6] For the distinction between these scenarios of intervention in fundamental rights, learn more at: MARTINS, L.; DIMOULIS, D.. *Teoria geral dos direitos fundamentais*, São Paulo: RT, 2014.
[7] Identifying this function of data collection.: BUCHNER, B.. *Informationelle Selbstbestimmung im Privatrecht*, Tübingen: Mohr, 2006. Similar: RODOTÀ, S.. *A vida na sociedade da vigilância*: A privacidade hoje. Rio de Janeiro: Renovar, 2008.
[8] Verify, in this regard, what is provided in article 6 of Law 13,460/ 2017, which deals with the defense of the interests of users of public services and specifically addresses the right to access personal data collected by providers of these services.
[9] In contrast, asserting that this assumption is illusory: BULL, H. P.. *Netzpolitik: Freiheit und Rechtsschutz im Internet*, Baden-Baden: Nomos, 2013.

Submetido em: **22/07/2023**
Aprovado em: **24/09/2023**
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

Personal data protection thus emerges as a doubly instrumental right: it not only protects individual freedom against unauthorized and excessive intrusions by the State, as is the case with all other fundamental rights[10], but it also ensures that all other fundamental rights, such as freedom of expression, artistic freedom, freedom of movement, and freedom of assembly, can be exercised and realized without the holders of these rights feeling threatened by an omnipresent and omniscient observer: the State.

Advocating for data protection was therefore seen as synonymous with defending liberal democracy, and conversely, those who opposed this right were identified as proponents of authoritarianism.

This narrative took on dramatic political and social dimensions in the context of the constitutional review of the 1983 census law (*Volkszählungsentscheidung*).

Amidst protests against the militaristic policies of the early 1980s, the slogan "Down with the census" emerged. It was the same state that harmed the environment, concentrated wealth, and aligned with the policies enforced by the North Atlantic Treaty Organization (NATO), now surreptitiously demanding that citizens provide their data. And if the State, capable of committing such heinous actions, what will it do with the data collected from the population? It was for all these reasons that the census law concentrated the anger and fury of an entire generation shaped by the constant and looming threat of socialism and nuclear war: the threat of sudden destruction caused by an enemy whose identity isn't even known.

Encouraged by state governments opposed to the expansion of federal power, more than four hundred protests were held against the census law, with many of them calling for a widespread popular uprising and even civil insurrection against the census law.[10]

The response of the German Constitutional Court to this situation of widespread social upheaval was simply the creation of the Magna Carta of data protection[11]: a decision that states that there is no data without legal value, after all, no matter how small the personal information may be, when aggregated with other data, it can be the basis for

[10] For a precise description of the events that led to this uprising, learn more at: BUSCH, A.; JAKOBI, T.. Die Erfindung eines neuen Grundrechts. Zu Konzept und Auswirkungen der,“informationellen Selbstbestimmungg“. In: HÖNNIGE, C.; KNEIP, S.; LOREN, A. (ed.), *Verfassungswandel im Mehrebenensystem*, VS Verlag für Sozialwissenschaften, 2011.

Submetido em: **22/07/2023**
Aprovado em: **24/09/2023**
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

the creation of informational profiles that replace concrete individuality. For this reason, every data subject now has the right to know "who, where, how, and for what purpose their data has been used." (ALEMANHA, BVerfGE, 65/1, 1983). Only in this way would individuals have the opportunity to know who holds their data, which aspects of their personality have been identified and collected, and, in short, why the State has become interested in their lives and what purpose is sought by the collection of this data. Data is personal, and its protection ensures the self-determination of personality.This idea spread at the European level, with two consequences.

The first of these consequences is the overcoming of the linkage of data protection to privacy. This is because the violation of the duty to protect data occurs primarily when the State or individuals act surreptitiously, monitoring or collecting personal data without the authorization or consent of its owners. Such actions represent an attack on democracy itself and, therefore, on the condition of being a citizen. The fundamental right to personal data protection then acquires its own distinct functions, quite different from its North American origin: while privacy protects the sphere of secrecy and intimate life, data protection establishes procedural duties designed to create mechanisms of control and greater transparency in the procedures for the collection and storage of information linked, whether actually or potentially, to data subjects.[11]

The second consequence is related to the creation of typical or specific situations that give rise to the duty of data protection for the data subject. Even when adopting a broad conception of personal data, according to which any information that potentially identifies the data subject can be considered as personal data, the Court of Justice of the European Union was forced to establish a complex system of restrictions on this right, lest it turn data protection into a limitless right: In order for information to be considered personal data, it is necessary to assess whether, considering the technical and financial resources available at the time of processing, the controller had the means to identify the data subject[12]. With these modifications and characteristics, the fundamental right to data protection has arrived in Brazil.

[11] In this vein, among others, developing these categories with analytical rigor: TZANOU, M.. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right, *International Data Privacy Law*, 2013, Vol. 3, n. 2, p. 88-99.

ADMINISTRAÇÃO DE EMPRESAS EM REVISTA
Submetido em: **22/07/2023**
Aprovado em: **24/09/2023**
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

4 BRAZILIAN MODEL OF PERSONAL DATA PROTECTION

Since the promulgation of the 1988 Constitution, the provision that guarantees "data secrecy" in Article 5, XII (BRAZIL, 1988) has generated debate and interpretative confusion. First, it's due to the use of the term "data," which in a broad sense could mean any and all information (BASTOS; MARTINS, 1989, Vol. 2, p. 73); secondly, because when the provision uses the restrictive term "in the last case," it is not clear whether this "case" encompasses all the previously mentioned forms of communication (telegraphic, data, and telephonic) (STRECK, 2013, p. 292), or if the exception is only directed to one of these modalities (telephonic) (QUEIROZ, 2018). In short, it is not clear whether what is protected are data in transit during communication (data communication) (DONEDA, 2011), or if archived (static) data would also be protected by inviolability (FERRAZ JR, 1993).

The legislator's response to this series of uncertainties was to create a general law to address the matter, the General Data Protection Law, Federal Law No. 13,709/2018 (BRAZIL, 2018), followed by a Constitutional Amendment, Amendment No. 115, of 2022 (BRAZIL, 2022), both treating the protection of personal data as an autonomous fundamental right, whether in relation to the right to informational self-determination or in relation to privacy or freedom of expression (Art. 2, LGPD).

The similarities with the European data protection system are evident: beyond the explicit and debatable citation[12] of informational self-determination as one of the foundations of the Brazilian personal data protection regime, the core of the system, found in the definition of personal data (Art. 5, I, LGPD) and the legal bases for processing (Art. 7, LGPD), literally replicate the provisions found in the European General Data Protection Regulation, articles 4 and 7 (EUROPEAN PARLIAMENT, 2016).[13]

As a result, what we have is the importation of solutions (including the definitions and limits of data processing acts constructed by the jurisprudence of the Court of Justice of the European Union), but also the problems, with the most prominent one being the absolutization of data protection in relation to the protection of other fundamental rights. Some of these topics and issues will be addressed in the next section.

ADMINISTRAÇÃO DE EMPRESAS EM REVISTA
Submetido em: **22/07/2023**
Aprovado em: **24/09/2023**
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

5 AN ANALYSIS OF THE EVOLUTION OF THE RIGHT TO PERSONAL DATA PROTECTION

The tectonic movement of creating, modifying, and assimilating personal data protection has had a profound impact on Brazilian law, causing a frenzy among scholars, authorities, and the curious. Suddenly, capitalism has become surveillance capitalism, pandemic control mechanisms have become instruments of privacy invasion, and artificial intelligence presents itself as the latest frontier in a wave of new opinions, all based on foreign and cyber-legal concepts, turning data protection into a new battlefield where there is no middle ground: either it is admitted that the collection and secondary sharing of personal data will occur, even without the consent of the data subject, or public policies will not be implemented. At this point, data protection, its logic, and discourse have presented rather discouraging results.

Firstly, despite all efforts to reconstruct and define its requirements, the primary legal basis, the data subject's consent, has never been truly effective. This is not only because users of the most effective data collection systems (social networks, purchasing mechanisms, various streaming services) do not have sufficient knowledge to understand the terms of use and the conditions and purposes of data collection operations linked to them, but also, and above all, because they do not have the time to do so. After all, who wants to read lengthy technical documents that deal with the conditions and scenarios for data sharing when users can simply click the "I agree" button?

The opposite hypothesis – simplifying the language of consent terms – is accompanied by the obvious loss of meaning in these documents, which, to mirror the technicality of the data protection world, need to be genuinely technical. At the crossroads between Scylla, which says everything without anyone understanding anything, and Charybdis, which says little or almost nothing so that everyone understands something, the legal basis of consent remains as it has always been: without function or effectiveness (KOOPS, 2014).

Submetido em: **22/07/2023**
Aprovado em: **24/09/2023**
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

Similar problems arise with central concepts and ideas in the Brazilian and European data protection systems. The law commands: there must be a purpose in the act of collection (Art. 6, I, LGPD); to which reality responds: the growing combination of databases, often occurring automatically, makes this legal requirement illusory. The law mandates: the processing operation must use the minimum necessary data to achieve the intended purpose (Art. 6, II, LGPD); and reality retorts: year after year, the volume of data processed globally increases exponentially – in 2020, it was 60 Zettabytes (10^{21}), with projected growth to 180 Zettabytes by 2025 (STATISTA, 2023).

As these problems arise, the most serious consequence is that the data protection system as a whole doesn't work effectively in practice but creates bureaucratic issues and legal conflicts on a global scale. We can only hope that these problems can be minimized, even though the effectiveness of the system remains precarious.

REFERENCES

ALBERS, M.. *Informationelle Selbstbestimmung*. Baden-Baden: Nomos, 2005.

ALEMANHA. BDSG. *Bundesdatenschutzgesetz*, de 30 de junho de 2017. Disponível em: http://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html. Acesso em: novembro de 2023.

ALEMANHA. *Bundesverfassungsgericht*. BVerfGE 65, 1 – Volkszählung. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83. Alemanha, 15 de dezembro de 1983. Disponível em: http://www.servat.unibe.ch/dfr/bv065001.html. Acesso em: novembro de 2023.

BASTOS, C. R.; MARTINS, I. G. da S.. *Comentários à Constituição Brasileira*. São Paulo: Saraiva, 1989, t. 2.

BRANDEIS, L.; WARREN, S.. The right to privacy. *Harvard Law Review*, vol. 4, 1890, p. 193-220.

BRASIL. *Lei Geral de Proteção de Dados Pessoais, Lei Federal n. 13.709/2018. 2018*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em novembro de 2023.

Submetido em: **22/07/2023**
Aprovado em: **24/09/2023**
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

BRASIL. *Emenda Constitucional n. 115, de 10 de fevereiro de 2022*. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais. Acesso em novembro de 2023.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em novembro de 2023.

BRITZ, G.. Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts. In: HOFFMANN-RIEM, Wolfgang. *Offene Rechtswissenschaft*. Tübingen: Mohr Siebeck, 2010.

BUCHNER, B.. *Informationelle Selbstbestimmung im Privatrecht*. Tübingen: Mohr, 2006.

BULL, H. P.. *Informationelle Selbstbestimmung – Vision oder Illusion*?. MohrSiebeck: Tübingen, 2009.

BULL, H. P.. *Netzpolitik: Freiheit und Rechtsschutz im Internet*. Baden-Baden: Nomos, 2013.

BUSCH, A.; JAKOBI, T.. Die Erfindung eines neuen Grundrechts. Zu Konzept und Auswirkungen der,"informationellen Selbstbestimmungg". In: HÖNNIGE, C.; KNEIP, S.; LOREN, A. (ed.), *Verfassungswandel im Mehrebenensystem*, VS Verlag für Sozialwissenschaften, 2011.

COLLEY, L.. *The gun, the ship, and the pen*. New York/London: Liveright Publishing, 2021.

DONEDA, D.. A proteção de dados como um direito fundamental. *EJJL*, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

FERRAZ JR., T. S.. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista Da Faculdade De Direito, Universidade De São Paulo*, n. 88, p. 439-459, 1993.

FREEDMAN, W.. *The right to privacy in computer age*. New York: Quorum Books, 1987.

HOFFMANN-RIEM, W.. Informationelle Selbstbestimmung in der Informationsgesellschaft - Auf dem Wege zu einem neuen Konzept des Datenschutzes. *AöR*, v. 123, n. 4, p. 513-540, 1998.

HOFSTADTER, S.; HOROWITZ, G.. *The right to privacy*. New York: Central Books, 1967.

KOOPS, B. J. The trouble with European data protection law. *International Data Privacy Law*, v. 4, n. 4, p. 250-261, 2014

Submetido em: **22/07/2023**
Aprovado em: **24/09/2023**
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

LADEUR, K. H. Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?. In: *Die Öffentliche Verwaltung*, p. 45-55, 2009.

LYNSKEY, O.. The Foundations of EU Data Protection Law. *Oxford University Press*, Oxford, 2015.

MARTINS, L.; DIMOULIS, D.. *Teoria geral dos direitos fundamentais*. São Paulo: RT, 2014.

PARLAMENTO EUROPEU. *REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: novembro de 2023.

PITSCHAS; R., Informationelle Selbsbestimmung zwischen idgitaler ökonomie und internet. *DuD*, n. 139, p. 146 e ss, 1998.

POSCHER, R.. *The Right to Data Protection*. *In* MILLER, R. (org.), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair*. Cambridge: Cambridge University Press, p. 129–142. 2017.

QUEIROZ, R. M.. Privacidade, criptografia e dever de cumprimento de ordens judiciais por aplicados de trocas de mensagens. *Revista dos Tribunais*, Caderno Especial - A Regulação da Criptografia no Direito Brasileiro, vol. 1, p. 13 -26, 2018.

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

STATISTA. *Quantidade de dados criados, consumidos e armazenados 2010-2020, com previsões para 2025*. 2023. Disponível em: https://www.statista.com/statistics/871513/worldwide-data-created/. Acesso em: 30 maio. 2022.

STRECK, L.. Comentários Art. 5º, XII, CF, in: CANOTILHO, J.J.; MENDES, G.; SARLET, I.; STRECK, L.. (Coords.). *Comentários à Constituição do Brasil*. São Paulo: Saraiva/Almedina, 2013, p. 292

TZANOU, M.. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 2013, Vol. 3, No. 2, p. 88-99.

TZANOU, M.. *The fundamental right to data protection*, Oxford: Hart Publishing, 2017.

ADMINISTRAÇÃO DE EMPRESAS EM REVISTA

Submetido em: ***22/07/2023***
Aprovado em: ***24/09/2023***
Avaliação: Double Blind Review e-
e-ISSN: 2316-7548

VESTING, T.. Das Internet und die Notwendigkeit der Transformation des Datenschutzes. In: LADEUR, Karl-Heinz (Hrsg.), *Innovationsoffene Regulierung des Intertet*, Baden-Baden: Nomos, p. 155-190, 2003.