ISSN 2175-6058
DOI: https://doi.org/10.18759/rdgf.v24i1.2161

# CHALLENGE TO GENERAL LAW OF DATA PROTECTION (GLDP) ENFORCEMENT OF INFORMATIVE SELF-DETERMINATION

## *DESAFIOS À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E A APLICAÇÃO DA AUTODETERMINAÇÃO INFORMATIVA*

Gabriela Buarque
Marcos Ehrhardt Júnior

## ABSTRACT

The present article approaches the paradigm of valuing consent to treat personal data as provided in the Brazilian General Law of data Protection (GLDP) due to confrontation with its effectiveness, based on informative self-determination. At this point, some insufficiencies of the model to the adequate adjustment in fundamental rights and in alternatives feasible to implement the idea of informative self-determination will be assessed based on the deductive methodology of literature review. It is pointed out that the merely formal consent cannot be enough to provide free consent protection due to cognitive limitations, asymmetry among powers, need of service usufruct, use of technical terms, time shortage and difficulty to manage future risks. On the other hand, some trends are highlighted to mitigate this insufficiency, be it through information systems such as *privacy by design, accountability,* offer of paid *premium* services without counterpart of the indiscriminate assignment of data and other contextual analyses.

**Keywords**: Data Protection. Consent. Informative Self-determination. Privacy. Consumer.

## RESUMO

O presente artigo aborda o paradigma de valorização do consentimento para o tratamento de dados pessoais estipulado na Lei Geral de Proteção de Dados, em confronto com sua efetividade sob o prisma da autodeterminação informativa. Nesse ponto, por meio de metodologia dedutiva de revisão bibliográfica, serão investigadas algumas insuficiências desse modelo para uma adequada tutela dos direitos fundamentais e as alternativas viáveis para efetivar a ideia de autodeterminação informativa. Aponta-se que o consentimento meramente formal pode ser insuficiente para a tutela do consentimento livre, em razão de limitações cognitivas, assimetria de poderes, necessidade de usufruto de serviços, uso de termos técnicos, escassez do tempo e dificuldade de gerenciamento de riscos futuros. Em contraponto, algumas tendências são indicadas para mitigar essa insuficiência, seja por meio de sistemas informacionais de *privacy by design, accountability,* oferta de serviços pagos *premium* sem a contrapartida da cessão indiscriminada dos dados e outras análises contextuais.


**Palavras-chave**: Proteção de Dados; Consentimento; Autodeterminação Informativa; Privacidade; Consumidor.

## INTRODUCTION

The Allegory of Plato's Cave exposed in "The Republic" teaches us that men are slaves of their own feelings: in the obscurity of the world of matter, which faces the perpetual becoming, they learn but shadows and vague reflexes. Education would have the initial goal of guiding the deviation of flashes of the becoming in favor of the immutable shapes of being.

Privacy policies, use conditions and terms within the context of Contemporary informational society oftentimes become merely formal mechanisms that keep us in obscurity about the management of platforms that host our personal data and our right to privacy. Consent, though, becomes a requirement lacking substantiality, which is featured by the mere mark of an "acceptance of terms and use conditions".

The aim of the present text is to reason about the challenges to put aside this panorama of vague reflexes and to enforce a paradigm of effective informative self-determination, by having in mind that the current mass and digital economy are boosted by the data monetization phenomenon.

The deductive methodology of literature review was adopted to investigate the idea of consent based on the General Law of Data Protection and on its effectiveness from the perspective of enforcing informative self-determination, as well as to highlight trends to make free and informed consent concrete.

## REGULATORY PANORAMA AND INFORMATIVE SELF-DETERMINATION

General Data Protection Regulation (GDPR) is a regulation used by the European Parliament, by the European Union Council and by the European Commission to reinforce and unify the protection of personal data to all individuals in the European Union by harmonizing data-privacy Bills all over Europe (MAGRANI, 2019, p. 102).

According to Eduardo Magrani, the push to great privacy protection derived from events related to information leaks and to the edition of general laws to protect data in foreign countries. Among them, one finds leaks by Edward Snowden[1], about espionage by the American government at world level, which reached State leaders, such as in Brazil (Dilma Rousseff, at the time) and in Germany (Angela Merkel), who presented to UN General Assembly a proposal listing rules to protect the right to privacy in the digital era (MAGRANI, 2019, p. 91).

GDPR principles and Law n. 13.709/18 (General Law of Data Protection – GLDP) are extremely similar; they start from the assumption of privacy protection in a democratic society (MAGRANI, 2019, p. 103), so that the European experience can bring along positive inflow to the construction of a data protection system in Brazil.

GLPD points out the essence of GDPR principles and highlights the European inspiration in the formulation of the Brazilian Legislative diploma. GLPD, in its art. 6, brings finality, adequacy, need, free access, data quality, transparency, security, non-discrimination, responsibility and accountability as its principles. Besides these principles, GLDP mentions, in its art. 6, lawfulness, loyalty, conservation limits, integrity and reliability.

Nevertheless, despite subtle differences, both normative diplomas are applicable to public and private entities that deal with personal data - by predicting rights attributed to holders whose data are processed. They discipline duties to agents who treat and set sections due to law disrespect.

From the mitigation viewpoint, finality and adjustment to data treatment principles - only data that were strictly necessary to the aims - were required to be collected. Moreover, agents will not be able to subject them to procedures aimed at other purpose rather than the previously informed one.

Document embodies relevance because data are the effective fuel of artificial intelligence based on the so-called Big Data. This expression can be conceptualized as a large set of data fed by sensory devices used in daily life and by the growing number of individuals connected to these technologies through digital networks (ITS RIO, 2016).

It is essential pointing out that the European experience is not limited to GDPR. Law n. 58/2019, in Portugal[2], aims at making sure, according to the national legal order, that the observance of regularity regarding people's data treatment and their circulation. In order to do so, it sets the creation, in its art. 4[3], of a national control authority, by also determining the duty of public and private entities to collaborate with such authorities.

The authority, among other attributions, based on art. 6[4], will have the competence to report - based on non-bond titles - legislative and regulatory measures concerning data protection, to inspect the respect to GLDP, to make available some criteria concerning the reliability of organisms set to monitor conduct codes and certifications.

Actually, the right to privacy, based on the contemporary context, puts aside the classic American concept of being the mere "right to be alone" by Samuel Warren and Louis Brandeis (1890), within a negative individual concept, in order to cover other control features over personal information, mainly in the digital society. Stefano Rodotá developed the concept of informative self-determination as fundamental right and he argues that the exercise of the right to privacy is, nowadays, mainly expressed through control over the flow of our personal information.

At this point,

> (...) coherently, due to change in the very definition of privacy, attention must be paid in secrecy to control. It means, first of all, that it becomes harder to individualize types of information from which citizens would be willing to fully 'get rid of', in order to definitely give up the control of moralities of its treatment and the activity of subjects who use it. This conception mainly depends on the perception that, even the apparently most emptied information, can, in case they are added to others, damage the interested party. And, it cannot be said that such a behavior is in conflict to the previously referred trend, according to which there are entire categories of personal information (such as those of economic content) whose outspread is timely or necessary: publicity and control are not contradictory terms, such as publicity and secrecy. It means confirming that the maximum circulation of economic-content information must allow interested parties to exercise a real control power over the exactness of such information by subjects who operate it and over the modalities applied to its use. Secondly, and most of all, the new situation determined by the use of computers to treat personal information makes it harder to consider citizens as simple "data providers", without having any control power. Actually, duty to provide data cannot be simply considered as counterpart of social benefits that, directly or indirectly, can be taken for granted by citizens. The collected information not just makes public and private organizations capable of planning and implementing their programs, but also allows the rise of new power concentrations or the reinforcement of existing powers; consequently, citizens have the right to the will to exert straight control over subjects whose provided information will grant growing plus-power (RODOTÀ, 2008, p. 36).

The sense of privacy as negative freedom undergoes a change that, nowadays, features it as an idea of positive freedom (SILVA, 2016, p. 102), i.e., the power by the individual to demand measures to ensure control over its data. It is important highlighting that the very concept of freedom has also been embodying resignifications; at this point, for example, according to José Afonso da Silva, freedom is the possibility of consistent coordination of means necessary to achieve personal happiness (SILVA, 2016, p. 103). It is based on this trajectory that GLPD ensures holders a whole series of rights, such as access to data, correction, elimination, portability, as well as to transparency regarding monetization, finality, storage mechanisms or to access by third parties.

Consent, though, becomes the very core of learning about the treatment given to personal data, nowadays. It works as core regulatory

instrument and the center of the practical legitimacy of this protective regime (MENDES; FONSECA, 2020, p. 509), the maximum sense of relevance when one finds out the rushed flow of information in the contemporary economy.

Accordingly, GLPD allows treating personal data through consent given by holders or, regardless consent, in case of some legal hypotheses, such as fulfilling the legal duty or conduction of public policies. Article 5, XII, of GLPD establishes that consent is the free, informed and unquestionable expression through which holders agree with the treatment of its personal data for a given end. Yet, it provides on sensitive data in the terms of art. 11; consent must be provided in a specific and underlined way. In case it regards children and adolescents, based on the terms of art. 14, it must be conducted in a specific way, with emphasis on consent granted by at least one of the parents or by the legal guardian.

Furthermore, controllers must not limit the participation of these holders in games, internet apps or in other activities to personal information supply, except for those strictly necessary for the activity. Consent will be invalid if information provided to holders has fake or abusive content, or if it was not previously introduced in a transparent, clear and unambiguous way (MODESTO, 2020, p. 45). Data collection must inform holders the information to be stored and what it is stored for; the unambiguous expression by holders is not enough, it is necessary having free consent.

The delimitation of what is effectively understood as "free", at this point, mainly depends on doctrinal, judge-made law efforts, and on the activity by the National Authority of Data Protection to conceptualize the referred undetermined legal concept. Thus, one can argue whether data supply is taken as free based on the hypothesis of free services, but that demand data transfer for their further use, i.e., a service that holders will only have access to after their consents for data collection and for sharing of such information (MODESTO, 2020, p. 46).

## THE PARADIGM OF CONSENT AND ITS CHALLENGES

Despite consent relevance as instrument to protect individual autonomy, it is possible arguing whether such fundamental is enough to safeguard privacy, given the new challenges posed by artificial intelligence, by big data domination, by behavioral publicity, by facial recognition and by other technologies that have been gaining the mainstream.

One of the most common data monetization practices lies on the driven and programed publicity, which is designed from the analysis of holders' personal information in order to receive services and products that meet their preferences. These tools allow drawing the niches of consumers whose profiles are, oftentimes, drawn through users' behavior in the web, based on their preferences, personal trends, musical taste, political positioning, and hobbies, among others.

This phenomenon is also boosted by the constant frantic sense that always encourages them in order to be in the virtual medium: there is always a message to send out, a picture to like or a notification to check on. Accepting the use and condition terms in any platform is now indispensable condition for the proper treatment of personal information after the enactment of the General Law of Data Protection.

In case of user's disagreement, it will be likely forbidden to use the provided service. This is the exchange guiding contemporary informational relationships and it stops us from reasoning about whether consent, is, after all, enough to the adequate protection of the treatment given to data. It is so, because the presence of these products and services in individuals' daily lives is so strong that it is difficult finding someone's will to give up all provided functionalities in exchange to preserving their privacy.

It is common for some internet users to observe benefits in advertisements, for example, Amazon's ability to suggest books that buyers may like based on their purchase background (MCDONALD; CRANOR, 2008, p. 566).

Furthermore, data are required by Public Administration and by the political, economic and social dynamics in the contemporary world; briefly, it makes the social cost of not providing required information unfeasible. Assumingly, many people not even check the existence of a

privacy policy or read the clauses and terms of data use; there is frequent sense of carelessness with personal information.

Exposure starts, then, to be voluntary, since, more and more, personal information, images and preferences are deliberately exposed on social networks such as Instagram and Twitter. This information can be further used by other people in other contexts. Exposure is encouraged by platforms themselves, since they, oftentimes, minimize the awareness of existing risks, mainly when it comes to children and adolescents.

Accordingly, usually, social exposure can lead to productive collective social values, such as sharing pleasant personal experiences, or they can help others to reach certain ends, a fact that encourages the personal resignation of personal privacy in favor of a given goal, visibility or professional success, besides the common cathartic feeling of being admired in social networks.

This practice, in its turn, leads to distortion of the very understanding of right to personality as inalienable and non-transferable right provided on art. 11 of the Civil Code, which sets the unfeasibility of voluntary limitation set to this legal interest. Yet, one can observe the process to turn the rights to personality into an asset. As for the specific case of privacy, these rights start to work as exchange currency to get several services and functionalities in the digital world, mainly in the informational market and in its vulnerabilities.

Thus, data embody a monetary profile. No wonder, when *Caesars Entertainment Operating Co.* declared bankruptcy in 2015, the main asset to the claim was customers' fidelity program, since it stored data from more than 45 million individuals (TODD, 2020). At this point, personal data "nowadays represent an important income source for businessmen; thus, even when there are merge and acquisition of organizations, data can be pointed out as one of the main sought assets, even more than personnel, intellectual property and facilities" (MODESTO, 2020, p. 41).

In light of the foregoing, data collection becomes the monetary fuel for those who explore it:

> A given organization can collect and treat its customers' data and, based on such information, customize the provided service or product sold to

> these same customers, thus, information is used as the means to facilitate and enhance this organization's transactions. On the other hand, this same businessman can collect and treat its customers' data and pass them out to a third party, by consideration, so that information becomes the very object of such a transaction (MODESTO, 2020, p. 41).

At this point, Laura Schertel and Gabriel C. Soares argue that, despite the importance of consent, assumptions that draw this paradigm, nowadays, emerge as not enough to ensure an effective and material regime, mainly, to ensure true control over holders' personal data flow (MENDES; FONSECA, 2020, p. 513).

Thus, it is argued that

> (...) the ideas of autonomy and individual empowerment embody, for several times, merely formal contours, if one disregards matters concerning the context of consent and treatment in question, such as dangers of the nature of the involved data. Based on such a scenario, consent becomes a convenient way to make data collection and use feasible without, however, "confronting it with the core values at stake". After all, in case it derives from a decision according to which the free will of a data holder is sensitively questioned, the ability to act of consenting to guarantee such ideas of autonomy and empowerment also becomes questionable (MENDES; FONSECA, 2020, p. 524).

This insufficiency would result from cognitive limitations of personal-data holders to assess the involved costs and benefits when it comes to the rights to personality, as well as to situations when there is no real freedom of choice by holders, such as those concerning "*take it or leave it*" and modern techniques to treat and analyze data based on big data, which avoid the whole value and use likelihood of this information to be fully measurable in case of consent granting (MENDES; FONSECA, 2020, p. 514).

With respect to cognitive limitations, it is possible arguing that oftentimes holders are not in the real position to assess costs and benefits involved in consenting; yet, several terms of use and privacy policies are not even read by users, because they are written with technical terms that are hard to be understood (MENDES; FONSECA, 2020, p. 514-516).

Similarly, it is important highlighting that privacy policies are hard to be read and that they do not support rational decision-making

(MCDONALD; CRANOR, 2008, p. 544); this feature is mainly boosted by the context of a society where time is becoming a scarce value for many people. Estimates show that the reading of a standard privacy policy in the most common websites demands approximately 12 minutes (MCDONALD; CRANOR, 2008, p. 555); consequences of an inappropriate data treatment, overall, use to be abstract and hard to be immediately transmitted.

Thus, privacy self-management faces a series of cognitive issues that become an effect barrier to its effectiveness, namely: (1) people do not read the privacy policies; (2) whenever they read them, they do not understand them; (3) whenever they read and understand them, most of the time they do not have previous knowledge enough to make an informed decision; (4) whenever they read, understand and can make an informed decision, their choice can be distorted due to several difficulties of decision-making (SOLOVE, 2020).

These challenges are incremented when one observes the aggregation issue, since, even when the individual makes a rational decision about sharing data of an isolated individual, these data can, in the future, be added to other set of information that starts showing sensitive facts about the person, after it is mined and combined (SOLOVE, 2020).

Damage evaluation issues are also highlighted, according to which, immediate benefits are many times prioritized, even when there is risk of future losses. Accordingly, the effect of aggregation evidences that privacy is a matter of long-term information management, whereas most consent to data collection, use and spread is bond to short-term benefits (SOLOVE, 2020).

Moreover, it is possible observing the frequent asymmetry of both powers and existing information between data holder and treatment agent, which conditions the process to enjoy a product or service to consent for personal information collection, based on the binary logic of *take it or leave it (*MENDES; FONSECA, 2020, p. 516).

Thus, one can question whether there is actually decision-making autonomy by holders, since their consent, oftentimes, is granted based on the social need of getting connected to other people or to use the platform for professional ends. It would concern a forced consent, a social imposition to indiscriminate data transfer, a fact that seems to make the

autonomy a pillar to seek enforcement through the General Law of Data Protection questionable.

It is essential evidencing the insufficiency of consenting to deal with challenges deriving from mass data collection and treatment (MENDES; FONSECA, 2020, p. 517), since they have the power to influence social, political and economic groups, besides to manipulate sharing processes. Furthermore, the use of criteria such as nationality, gender, political position, religion, age or sexual orientation can lead to a series of discriminations since they are related to the inner personality of each individual, besides reinforcing the process to stereotype groups and to chance social temper.

This difficulty is boosted when one observes that data flow faces a complex network of agents who use practices and operations for several purposes, a fact that makes it hard for data holders to fully understand all these elements (MENDES; FONSECA, 2020, p. 518). Thus, the impact of data protection must not just undergo the collection phase, but it must also assess generated effects based on these elements' treatment and aggregation, since such results can affect a whole series of fundamental rights involved in the social medium.

## TRENDS FOR FREE AND INFORMED CONSENT ENFORCEMENT

It is essential highlighting that indiscriminate consent, however, is not a unique peculiarity of the personal data issue. Consumers oftentimes are forced to adhere to mass contracts of health insurance, electric power supply, telephone supply and of other legal business that become essential in their daily lives and that do not open margin for clause changing or discussion, in the contemporary world.

After the rise of data monetization, this logic was transported to applications and to other services that only provide a given functionality after information collection - they do not provide any margin of negotiation for users. Thus, challenges posed by privacy self-management are quite relevant:

> (...) even well-informed and rational individuals cannot properly self-manage their privacy due to several structural problems. There are several entities collecting and using personal data to make it possible for this individual to manage its own privacy, in separate from each entity. Besides, several damages to privacy are the result of aggregation of data parts for a period-of –time, by different entities. It is virtually impossible for people to weigh about costs and benefits to disclose information or to allow its use or transfer without the understanding of potential uses, besides the limit of efficacy of the privacy self-management structure (SOLOVE, 2020).

Actually, it is important highlighting, yet, that art. 10 of GLDP provides that data treatment can happen, regardless of holders' consent, whenever it is necessary to fulfil legitimate interests by the controller or the third party, which are taken into consideration based on concrete situations that include, but that are not limited to, support and promotion of controllers' activities and protection - with respect to the holders - to the regular conduction of their rights and service supply that benefits them, by respecting the legitimate expectations and fundamental rights and freedoms.

Accordingly, it is also important highlighting that:

> Another point that the national authority must face lies on whether personal-data monetization may be done based on the controller's legitimate interest, since many business organizations have their greatest income source in this activity. However, this possibility will demand analysis based on concrete situations; it is on the hands of ANDP to set the qualified definition of legitimate-interest parameters to provide important subsidies for the concrete application of this open clause (MODESTO, 2020, p. 55).

Within this context, standards of objective good-faith, institutes of abuse of rights and vice of consent become relevant; they can be used to make feasible the analysis of concrete cases and the search for informative self-determination materialization. GLDP, in its art. 8, third paragraph, points out that personal-data treatment is forbidden based on vice of consent.

One of the propositions pointed out to facilitate the effectiveness of consent are *Privacy Enhancing Technologies (PET*s), which are technologies that reinforce the flow of right to informative self-determination and

privacy, such as cryptographies and control over access, according to which users are clarified and have domain over services and storage of their data (MENDES; FONSECA, 2020, p. 521).

The sense of accountability, which was understood as a set of practices that regard responsibility for ethics, duty, search for transparency and accountability for activities that are under development, as well as for the expression of their reasons and of their ways of conduction (GUTIERREZ, 2019, p. 85), when it comes to data protection - which is substantiated by the concept that accountability within a complex digital environment must be shared among all actors, but it cannot be limited to individual management of holders' only based on their consent (MENDES; FONSECA, 2020, p. 521).

One can question the possibility of adopting paid premium versions of certain services that were supposed to be provided for free – whose counterpart, overall, are users' personal data – by giving holders the option to pay a given value in order to use the service without data transfer (MODESTO, 2020, p. 47). Moreover, educational efforts with more evident warns and more options for consumers are good and tend to improve the effective exercise of privacy self-management.

Accordingly, it is relevant taking into consideration that some companies must develop a more effective transfer of their privacy policies to facilitate their understanding and to reduce the time needed for their reading. The isolated elaboration of privacy policies will not necessarily increase the necessary transparency in this sector, besides being a mechanism of limited practical use.

It does not mean abandoning the consent paradigm as protective instrument if one has in mind that such an idea is essential to adequate awareness of the use of personal data. However, it is essential assessing the effectiveness of valuing this fundamental as pillar of the data protection system in Brazil, if one takes into account the goals and the principles set for this same normative system.

Yet, the aim is not to determine a paternalist attitude to impair individual freedom and to make innovation markets unfeasible, but to materialize the sense of informative self-determination as effective mechanism that goes beyond a merely formal instrument.

Paternalism, in these cases, is not justified, since data use oftentimes determines social benefits, and it cannot be ignored. The absolute obstacle to data treatment, in number of cases, would lead to the disruption of new business models, and it also has hazardous social and collective effects - this is the reason why privacy self-determination is not a paradigm to be abandoned.

It is essential revisiting the concept of consent to add it to regulatory sets of involved actors. It does not mean, actually, embracing the much strict regulation and abandoning privacy self-management, but finding balance points that, from a weighing perspective, can ensure fundamental rights involved without the exacerbated sacrifice of respective interests.

One can start from the observation that consent is a concept that can embody several shades and that their approach, in the informational society's context, must understand these shades so that the debate about GLDP applicability can embody pragmatic and feasible parameters.

Understanding consumers' vulnerability, time shortage in the contemporary world and unfeasibility of having all privacy policy readers as expert in the management of information technology is a minimal perception that demands the adaptability of what we understand as free and informed consent. Thus, it is necessary putting aside the obsolete idea that the excessive valorization of a neutral sense of consent will solve all issues, since such perception pushes this concept to spheres that go beyond its factual limits.

It is essential developing a coherent approach of consent that corresponds to minimal ideas about how people make decisions about personal data to substantiate an idea of more significant privacy self-determination.

## FINAL CONSIDERATIONS

The dynamics related to personal-data treatment in the contemporary world is a phenomenon that leads to inflow in the very understanding of the General Law of Data Protection. At this point, the sense of consent determined by GLDP is in opposition to the pragmatic reality of the digital world, which sets the need of its reinterpretation and proper understanding.

The paradigm of data protection, with excessive and exclusive emphasis on consent, can bring insufficiencies concerning the adequate protection of the involved fundamental rights, be it due to cognitive limitations, asymmetry of powers, need of enjoying certain services, the use of technical terms, time shortage and the difficulty of managing future risks. Therefore, it is essential assessing the ways to turn informative self-determination into an effective paradigm that goes beyond a formal fiction.

Accordingly, some trends pointed towards the embodiment of a responsive treatment of free consent, be it through technology and through the design of informational systems of *privacy by design* and *accountability,* be it through paid premium services supply without counterpart of indiscriminate transfer of both data and other contextual analysis.

The understanding of this issue concerns the perception that there is no generic and universal formula that can be used in all cases, so that a balanced solution requires the analysis of concrete hypotheses and of involved parties.

It is not set by propositions that impair the freedom of involved parties, since such attitude is also harming to the development of innovation and to the rights to personality in the informational world. Actually, the idea is to seek the enforcement of the sense of self-determination by favoring the possibility of weighed and free choices made by individuals, and it goes beyond the merely formal consent.

## NOTAS

1 Edward Joseph Snowden is a systems analyst, former systems administrator for the US Central Intelligence Agency, and former contractor for the US National Security Agency, who disclosed a series of software of a Global Surveillance system of the American Agency, whose details, in synthesis, can be found in the book "Permanent Record" (2019) and in the movie "Snowden" (2016), by Oliver Stone.

2 The methodological cut that has selected the Portuguese diploma resulted from the attributes of similarities in provisions on the Brazilian legislation and from language proximity.

3 CNPD is an independent administrative entity that has legal personality of public right and authority of powers, it has administrative and financial data, that work along with the Congress. 2 – CNPD controls and inspects DGPR and the present law, as well as other legal and regulatory provisions when it comes to personal data protection in order to defend rights, freedoms and guarantees of singular people at personal data treatment scope. 3 – CNPD has independence to act in the prosecution of its duties and in the exercise of powers that are granted to it by law. 4 – CNPD members are subjected to the incompatibility regime established to those holding high public positions, and who during their offices in power cannot perform another activity, be it paid or not, except for teaching in higher education and investigation.

[4] Besides provisions in article 57 of GLDP, CNPD has the following attributions: a) report, in non-bond way, the legislative and regulatory measures regarding personal-data protection, as well as legal instruments under preparation, in European and foreign institutions concerning the same subject; b) Inspecting the respect to provisions in GLDP and to other legal and regulatory provisions concerning personal-data protection and the rights, freedoms and guarantee of holders' data, as well as correcting and punishing its disrespect; c) making available a list of treatments to be subjected to the evaluation of their impact on data protection, based on the terms of n. 4 of article 35 of GDPR, by equally defining criteria that allow decreasing the density of the sense of high risk provided in this article; d) elaborating and introducing to the European Committee for Data Protection, provided on GDPR, the projects of criteria for the accreditation of organisms to monitor conduct codes and certification organs, based on terms of articles 4 and 43 of GDPR, and ensuring the further publication of criteria, in case they are approved; e) Cooperating with the Portuguese Institute of Accreditation, I.P. (IPAC, I. P.), regarding the application of what is provided on article 14 of the present law, as well as on the definition of additional accreditation requirements, based on safeguarding GDPR application.

## REFERENCES

GUTIERREZ, Andriei. É possível confiar em um sistema de inteligência artificial? Práticas em torno da melhoria da sua confiança, segurança e evidências e accountability. In: FRAZÃO, Ana. MULHOLLAND, Caitlin**. Inteligência artificial e Direito**: Ética, Regulação e Responsabilidade*.* São Paulo: Thomson Reuters Brasil, 2019.

ITS Rio 2016. **Big Data in the Global South Project Report on the Brazilian Case Studies***.* Disponível em: https://itsrio.org/wp-content/uploads/2017/01/Big-Data-in-the-Global-South-Project.pdf. Acesso em: 3 nov. 2019.

MAGRANI, Eduardo*.* **Entre dados e robôs**: ética e privacidade na era da hiperconectividade**.** 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MCDONALD, Alecia M; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. **Journal of Law and Policy for the Information Society***,* v. 4, p. 543-568, 2008.

MENDES, Laura Schertel. FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais***.* V. 6, n. 2, p. 507-533, mai./ago. 2020.

MODESTO, Jessica. Breves considerações acerca da monetização de dados pessoais na economia informacional à luz da Lei Geral de Proteção de Dados Pessoais*.* **Revista de Direito, Governança e Novas Tecnologias.** V. 6, n. 1, p. 37/58, jan./jun. 2020.

RODOTÀ, Stefano*.* **A vida na sociedade de vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 36.

SILVA, José Afonso da. A liberdade no mundo contemporâneo. **Constituição, Economia e Desenvolvimento: Revista da Academia Brasileira de Direito Constitucional.** Curitiba, 2016, vol. 8, n. 14, jan./jun., p. 99-111.

SOLOVE, Daniel J. The Myth of the Privacy Paradox. **GWU Legal Studies Research Paper no. 2020-10, 2020**. Disponível em: Acesso em: 10 de março de 2020.

TODD, Steve. **O valor dos dados em um mundo impulsionado por informações**. Disponível em: https://canaltech.com.br/big-data/o-valor-dos-dados-em-um-mundo-impulsionado-por-informacoes-51425/. Acesso em: 5 nov. 2020.

WARREN, Samuel D. BRANDEIS, Louis D. **The right to privacy.** Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 20 out. 2020.

Recebido em: 15-9-2022
Aprovado em: 30-5-2023

**Gabriela Buarque**
Mestra em Direito pela Universidade Federal de Alagoas. Coordenadora do GT de Inteligência Artificial e Novas Tecnologias no Laboratório de Políticas Públicas e Internet (LAPIN). Advogada. Membra da Comissão de Inovação, Tecnologia e Proteção de Dados da OAB/AL. E-mail: gabrielabuarqueps@gmail.com

***Marcos Ehrhardt Júnior***
Doutor em Direito pela Universidade Federal de Pernambuco (UFPE). Mestre pela Universidade Federal de Alagoas (UFAL). Advogado. Professor de Direito Civil dos cursos de mestrado e graduação da Faculdade de Direito da Universidade Federal de Alagoas. Pesquisador Visitante do Instituto Max-Planck de Direito Privado Comparado e Internacional (Hamburgo/Alemanha). Líder do Grupo de Pesquisa Direito Privado e Contemporaneidade (UFAL). Editor da Revista Fórum de Direito Civil (RFDC). Diretor Regional Nordeste do Instituto Brasileiro de Direito Civil (IBDCIVIL). Membro do Instituto Brasileiro de Direito de Família (IBDFAM). E-mail: marcosehrhardtjr@uol.com.br

**Universidade Federal de Alagoas**
Av. Lourival Melo Mota, S/N,
Tabuleiro do Martins, Maceió - AL,
Cep: 57072-970