DISRUPTIVE INNOVATIONS AND PERSONAL DATA PROTECTION: NEW CHALLENGES FOR THE LAW

Valter Shuenquener de Araujo [1],
Daniel Calil [2]

ABSTRACT

Disruptive technological innovations interfere in the regulatory framework of public services and in the execution of economic activities. Therefore, they demand a new regulatory conformation that is able to absorb new demands and to allow competition between economic agents. In this context, the protection of personal data has evolved significantly nationally and internationally, which is why this subject should be deeply researched. The research is qualitative, bibliographic and descriptive of jurisprudence, doctrine and of the positive law.

Keywords: Technologic innovation. Disruptive innovation. Data Protection Law. Privacy. Fundamental rights.

INOVAÇÕES DISRUPTIVAS E A PROTEÇÃO DE DADOS PESSOAIS: NOVOS DESAFIOS PARA O DIREITO

RESUMO

As inovações tecnológicas disruptivas interferem na formatação jurídica do modelo de prestação de serviços públicos e na execução de atividades econômicas e, assim, reclamam uma nova configuração regulatória que seja capaz de absorver as novas demandas e viabilizar a competição entre os concorrentes. Nesse contexto, a proteção de dados pessoais tem evoluído significativamente em âmbito nacional e internacional, razão pela qual sua pesquisa merece maior aprofundamento. A pesquisa é qualitativa, bibliográfica e descritiva da jurisprudência, doutrina e do direito positivo.

PALAVRAS-CHAVE: *Inovação tecnológica. Inovação disruptiva. Lei de Proteção de Dados. Privacidade. Direitos fundamentais.*

1. INTRODUCTION

In the 21st century, the expansion of the use of new technologies, not only among individuals, but also by the Public Administration, arouses debates about the best regulatory design to be adopted for each economic activity or public service. One of the problems that has arisen in the regulation of new technologies is the protection of

[1] Doutor em Direito Público pela UERJ. KZS pela Ruprecht-Karls Universität Heidelberg. Professor Associado da Universidade do Estado do Rio de Janeiro e Conferencista da EMERJ. Professor do Programa de Pós-Graduação em Direito da UERJ (PPGD). Mestre em Direito Público pela Universidade do Estado do Rio de Janeiro.

[2] Possui graduação em Direito pela Universidade Presbiteriana Mackenzie (2006). Assessor Jurídico da Tribunal de Contas do Município de São Paulo.

personal data, which has recently been shaped by the decision of the US Supreme Court[3], the new European legislation on the subject[4] and, at the national level, by virtue of the treatment provided to the matter by Law 13,709/18.[5]

In this context, there is a need to strike a balance between the normative incentive for innovation and for the liability it causes. If, on the one hand, disruptive innovations and the adoption of new technologies can lead to the reduction of public expenditure, to the increase of the public services quality and can make the Public Administration more transparent, on the other hand, its uncritical and unbridled application may conflict with fundamental rights. In this way, given the risks that disruptive innovations can offer, especially to the protection of personal data, there is a pressing demand for legal and regulatory mechanisms for risk prevention and control.

Faced with the unbridled use of new technologies today, the protection of personal data has become a fundamental measure, and is permeated by risks, for example, regarding the formation of a *Big Data*. The complexity of the thematic is such that the definitions about this phenomenon of data accumulation are very different from each other, which is why there are those who classify them into four groups, according to the focus presented by each concept: (i) data attributes, (ii) technology needs, (iii) overcoming limits, (iv) social impact.[6] A *Big Data* concept that seeks to reconcile its main elements is that of an "*information asset characterized by such a volume, speed and variety that it requires specific technology and analytical methods for its transformation into value.*"[7]

In this context, it can be stated that there are at least three problems concerning the relationship between the *Big Data* analysis and the protection of personal data:

(a) data life cycle management;

(b) privacy and data security, and

(c) data representation.[8]

Firstly, because of the media profusion from which the data are originated and their unlimited quantity, traditional storage technologies are insufficient to deal with such a large volume, thus raising the demand for efficient data analysis mechanisms able to determine which should be archived or discarded. In addition, another relevant aspect is related to data privacy. Despite the legal rules and normative guidelines intended to provide the security of such information, it is difficult to specify which data

[3] Case Carpenter v. United States No. 16,402, 585 U.S. (2018). Decision of June 22, 2018.
[4] General Data Protection Regulation (GDPR) 2016/679. This is a legislative act applicable to both the European Union and the European Economic Area.
[5] General Law on Data Protection, dated August 14, 2018.
[6] MAURO, Andrea de; GRECO, Marco; GRIMALDI, Michele. A Formal Definition of Big Data Based on its Essential Features. Library Review, Vol. 65 Iss: 3, pp.122 – 135. 2016, https://doi.org/10.1108/LR-06-2015-0061.
[7] MAURO, loc. cit.: "On the whole, we argue that the definition for Big Data should refer to its nature of 'Information asset', a clearly identifiable entity not dependent on the field of application. Therefore, the following consensual definition is proposed: "Big Data is the Information asset characterized by such a High Volume, Velocity and Variety to require specific Technology and Analytical Methods for its transformation into Value." Such a definition is compatible with the usage of terms such as "Big Data Technology" and "Big Data Methods" when referring directly to the specific technology and methods cited in the main definition.
[8] TAYLOR-SAKYI, Kevin. Big Data: Understanding Big Data. 2016. Available at: https://www.researchgate.net/publication/291229189_Big_Data_Understanding_Big_Data. Access in: march, 4th 2018.

demand greater protection and to ensure that there are no failures in these systems. Finally, it can be said that the collected data are presented in different types (texts, numbers, graphs), as well as their "semantics, organization, granularity and means of accessibility"[9] are also different, so that their representation is, also, an obstacle to an effective selection and data protection.

In this way, there is a clear need for research and construction of legal systems and regulatory environments to safeguard personal data that are exposed and accumulated due to new technologies.

2. PRIVACY AS A FUNDAMENTAL RIGHT

Privacy is one of the most important and relevant values in the light of the Brazilian Constitution, being characterized as a fundamental right in its article 5th, item X. Thus, it is a fundamental clause and, therefore, not subject to the action of the derived constituent power that tends to abolish its protection core.

Despite the *status* of fundamental right and all legal protections arising from this circumstance, there is no doctrinal consensus on the scope of privacy protection with respect to, for example, the protection of personal data. As an example, Tércio Sampaio Ferraz conceptualizes the right to privacy as:

> A fundamental subjective right, whose holder is any person, physical or juridical, Brazilian or foreign, resident or in transit in the country; whose content is the ability to constrain others to respect and to resist the violation of what is proper to them, that is, of the vital situations which, by their being concerned with him, wish to maintain for themselves, under their sole and discretionary decision; and whose object is the moral integrity of the holder.[10]

In contrast to this comprehensive concept, Gilmar Mendes understands that:

> The right to privacy, in a narrower sense, leads to the individual's claim not to be the focus of third-party observation, not to have their affairs, personal information and particular characteristics exposed to third parties or the general public.[11]

The distinctions between concepts are justified not only by the terminological problems involved, given the similarity with the protection, also at the constitutional level, of the intimacy and even of the right to honor and to the image, but also by the

[9] HU, H, 2014. Toward Scalable Systems for Big Data Analytics: A Technology Tutorial, 1, 658-659, 665: "semantics, organization, granularity, and means of accessibility"

[10] FERRAZ JÚNIOR, Tércio Sampaio. Secrecy of data: the right to privacy and limits to the state's oversight function. Cadernos de Direito Constitucional e Ciência Política, n. 1, São Paulo: Revista dos Tribunais, 1992. P. 77.

[11] MENDES, Gilmar Ferreira. BRANCO, Paulo Gustavo Gonet. Course of Constitutional Law. 13ª ed. rev. e atual. – São Paulo: Saraiva Educação, 2018. P. 287.

current scenario of technological development. New challenges for the legal protection of that right arises at all times, mainly due to the difficulty of legal norms to keep up with economic and social transformations.

Recognizing the difficulty to solve the diversity of problems related to the extent of the private life protection, Ingo Sarlet makes the following observations:

> The notion, developed by sectors of the doctrine and by German constitutional jurisprudence, that one can distinguish between three spheres (the so-called theory of spheres) within the right to privacy, an intimate sphere (which is the essential and intangible nucleus of the right to privacy and privacy), a private sphere (which refers to non-confidential or restricted aspects of the individual's family life, professional and commercial life, and can be weighed against other legal goods) and a social sphere (where image and word rights, but no longer to privacy and intimacy) has been criticized as insufficient to account for the diversity of cases involving the protection of privacy.[12]

From another point of view, emphasis should be placed on the idea that the fundamental right to privacy is also related to other values protected by the Brazilian legal system, such as bank secrecy, fiscal secrecy, home inviolability and confidentiality of communications. In fact, the latter hypothesis, foreseen in article 5th, item XII,[13] of the 1988 Constitution, is currently much debated. In addition, the protection of user's personal information on the most different platforms, whose procurement and management, often not expressly authorized, as in mobile applications, is closely related to the protection of privacy and personal data.

In this sense, Gilmar Mendes points out that:

> The secrecy of communications is not only a corollary of the guarantee of the free expression of thought; also expresses traditional aspects of the right to privacy and privacy. The breach of confidentiality of communication means frustrating the right of the issuer to choose the recipient of the content of his communication.[14]

Therefore, the privacy protection, in spite of the divergences as to its scope, due to the constitutional entrenchment of this value and its relation with other rights provided in the constitutional level, reveals the importance of the topic and the relevance of its discussion from the new technologies' perspective. It serves, therefore, as a

[12] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Course of Constitutional Law. 6ª ed – São Paulo: Saraiva, 2017. P. 446 e 447.

[13] Art. 5º, XII - the secrecy of correspondence and telegraphic communications, data and telephone communications is inviolable, except in the latter case, by court order, in the cases and in the form established by law for the purpose of criminal investigation or criminal procedural instruction.

[14] MENDES, Gilmar Ferreira. BRANCO, Paulo Gustavo Gonet. Course of Constitutional Law. 13ª ed. rev. e atual. – São Paulo: Saraiva Educação, 2018, p. 298.

foundation for normative systems that seek to realize this protection, as will be explained below.

3. INNOVATION AND THE PERSONAL DATA PROTECTION

In contemporary law, the protection of privacy and personal data suffers the direct influx of the increasingly frequent and intense social impact of innovations. As an example, Uber and Airbnb, two of the leading joint-stock companies,[15] have tripled the value of their business in recent years.[16] Among the several factors that have supported this growth, we can mention the flexibility offered to the contractors, the easiness of workers entry, the existing regulatory mismatch in relation to the activity, the innovative character of the (disruptive) technology and the operational efficiency.[17] There are also estimates that sharing cars and rooms, collective financing, personal services and streaming audio and video will reach $ 335 billion (global revenue) by 2025.[18]

The economic impact of these economic activities is such that various sectors are affected. There are, for example, changes in the labor market, which now has more temporary and alternative options, all members and resulting from the so-called *gig economy*.[19] In the current digital age context, there is a greater flow of workplaces and an increase of short-term jobs, which is justified by the possibility of companies saving financial resources and maintaining a balance of costs, since they do not need to rent spaces for the performance of their business and do not need the traditional hiring of personnel.[20] In this way, the expansion of digital platforms creates "*innovative employment options and democratizes the employment process*".[21]

Another relevant economic repercussion that comes up from disruptive technological innovations is that "*people postpone the decision to buy new cars in cities after using options like Uber, Ola (Indian tour company) or Lyft*."[22] The revolutionary character of the results of these new business models is recognized by Patrizia Grifoni and Alessia D`Andrea in the following terms:

> the economy of sharing and collaboration could have the same impact on the Western economic model (based mainly on capitalism) as the incorporation

[15] GÖRÖG, Georgina. The Definitions of Sharing Economy: A Systematic Literature Review. Available at: https://doi.org/10.26493/1854-4231.13.175-189. Access in: march, 8th 2019. P. 183: "The term "sharing economy" refers to the activity of sharing underutilized assets with the help of technology."
[16] YARAGHI, Niam; RAVI, Shamika. The Current and Future State of the Sharing Economy. Brookings India IMPACT Series No. 032017. March 2017, p. 8.
[17] YARAGHI, *ibidem*, p. 8 – 15.
[18] HAWSKSWORTH, J. and VAUGHAN, R. The Sharing Economy—Sizing the Revenue Opportunity. Pricewaterhouse-Coopers, 2014.
[19] "The gig economy involves the exchange of labour for money between individuals or companies via digital platforms that actively facilitate matching between providers and customers, on a short-term and payment by task basis." LEPANJUURI, Katriina; WISHART, Robert; CORNICK, Peter. The Characteristics of those in the Gig Economy. Final Report. Department for Business, Energy & Industrial Strategy. UK Government. Fev/2018, p. 4. Available at: https://assets.publishing.service.gov.uk/government/ uploads/system/uploads/attachment_data/file/687553/ The_characteristics_of_those_in_the_gig_economy.pdf. Access in: 08/03/2019.
[20] YARAGHI, Niam; RAVI, Shamika (2017). "The Current and Future State of the Sharing Economy," Brookings India IMPACT Series No. 032017. March 2017, p. 20.
[21] YARAGHI, *ibidem,* p. 21.
[22] YARAGHI, *ibidem*, p. 22.

> of mass production, from the organization of labor to the nature of the social contract in a capitalist society.[23]

Thus, it is uncontroversial that new technologies, and especially shared economies, have significant effects in today's society, and stimulate a growing appeal for digital tools and innovative applications. From the consumers perspective, the choice of technological innovations can be explained not only by the economic advantages, but also by the greater certainty about the contracted product or service, as well as greater security and confidence, due to the evaluation and classification policies,[24] if compared to the traditional options available in the market.

However, there are several risks involved in these new technologies, such as those related to exposure, management and control of personal data, which, because of these innovations, tend to accumulate exponentially. In Comparative Law, an example that demonstrates the relevance of guardianship of personal data in the midst of the new technologies is the one pertinent to the recognition of the "right to forget" by the European Court of Justice, which has recognized the responsibility of the Internet search engine operators due to the need of privacy protection. In this sense, the judgment of case *C-31/12, Google Spain SL, Google Inc. Vs. Spanish Data Protection Agency (AEPD), Mario Costeja González*:

> a processing of personal data such as that at issue in the main proceedings by the operator of a search engine is liable to significantly affect the fundamental rights to respect for privacy and the protection of personal data when searching through that engine is carried out from the name of a natural person, since this treatment allows any surfer to obtain, with the results list, a structured overview of the information about that person, which can be found on the Internet, to many aspects of their private life and which, without such a search engine, could not or could hardly have been related, and thus to establish a more or less detailed profile of the person concerned. respect of the rights provided for in those provisions and provided that the conditions laid down therein are effectively fulfilled, the operator of a search engine is obliged to remove from the list of results, following a search carried out from the name of a person, links to other web pages published by third parties and containing information about that person, also in the case of that name or that information not be previously or simultaneously erased from these web pages, that is, if applicable, even when its publication on those pages is, in itself, lawful.[25]

The new guidelines of the courts, such as the one mentioned above, which arise in the face of new technologies do not, however, hinder the demand for new

[23] GRIFONI, Patrizia; D'ANDREA, Alessia. Sharing Economy: Business Models and Regulatory Landscape in the Mediterranean Areas. International Business Research; Vol. 11, No. 5; 2018. P. 64.

[24] WALLENSTEIN, Judith; SHELAT, Urvesh. Hopping Aboard the Sharing Economy. Available at: https://www.bcg.com/publications/2017/strategy-accelerating-growth-consumer-products-hopping-aboard-sharing-economy.aspx. Access in: 04.11.2018.

[25] Case C-31/12, Google Spain SL, Google Inc. vs. Spanish Agency for Data Protection (AEPD), Mario Costeja González. Available at: <http://curia.europa.eu>. Accessed March 4, 2019.

regulatory models for the protection of personal data. Besides, in this context, it is possible that the regulatory framework of an activity achieved by disruptive innovations, such as in the case of search engines, is also influenced by other factors, such as self-regulatory practices, in order to maximize the effectiveness of legal protection. In this sense, Patrícia Baptista and Clara Keller:

> Google Inc. has been acting as a true decision maker when it comes to ensuring privacy on the network. Since the European Court of Justice recognized about two years ago the right to forgetfulness and set the responsibility of the search tool on data protection, Google began to examine thousands of requirements for the suppression of search results. And, with very low transparency, he decided to stay or withdraw these results. [...] European regulatory authorities, on the other hand, admit that the system adopted has worked well, that the number of challenges to the company's decisions is not significant and that the regulatory bodies would not have the technical, financial and personnel resources to deal with the nearly 1.4 million applications submitted since the TJCE ruling.[26]

Therefore, it is evident that the regulatory challenges in this area are the most diverse, either because of the non-adaptability of traditional regulatory models or because of the uncertainty about the efficiency of the new regulatory systems. The innovations effects on worker protection, discrimination between economic agents, damage to local communities, threats to consumer safety and harmful anti-competitive practices can also be highlighted.[27] All these problems spread in an environment of profound regulatory asymmetry, where perplexity with what is new has not yet given way to the emergence of secure legal norms.

Thus, in view of the expansion of new technologies and the insufficiency of traditional regulatory and legislative models, the theme of personal data protection makes it imperative to research by effective methods in the treatment and control of personal data. In this context, it is of crucial relevance to evaluate the recent experiences of Comparative Law in relation to the subject. This is justified because, just as the popularization of new technologies is gaining worldwide expression, the data treatment regulation controlled by large business groups also becomes an international issue.

It must be considered that if, on the one hand, there are risks arising from the spread of new technologies, on the other hand, the dissemination, especially by the State, of qualified and adapted regulation is crucial for a society progress.[28] Thus, the possibility of adopting regulatory alternatives capable of extracting the greatest possible benefits from disruptive innovations should be evaluated.

---

[26] BAPTISTA, Patrícia F., KELLER, Clara. Why, when and how to regulate new technologies? The challenges brought by disruptive innovations. RDA – Revista de Direito Administrativo, Rio de Janeiro, v. 273, p. 126.
[27] STEMLER, Abbey. The Myth of the Sharing Economy and its Implications for Regulating Innovation. Emory Law Journal. Vol. 67:197, p. 203.
[28] WIENER, Jonathan B. The regulation of technology, and the technology of regulation. Technology in Society 26, 2004, p. 496.

In this perspective, especially in the face of the need for personal data protection, the challenge that arises is how existing legal systems must "*address these innovations, given their broad but sometimes inert legislation*."[29]

Therefore, it is necessary to analyze the current stage of interaction between new technologies and their respective regulation, in order to investigate the advantages and disadvantages in the adoption of certain normative treatment concerning the protection of personal data. For this reason, we will analyze the Carpenter v. United States 585 U.S., *General Data Protection Regulation*, in force in Europe, and Law No. 13,709 / 18.

4. CASE CARPENTER V. UNITED STATES 585 U.S.

Timothy Carpenter had his cell phone number apprehended by police and prosecutors in the wake of robberies at RadioShack and T-Mobile stores and obtained court orders to track location data of suspected cell phones, including Carpenter was included. With the data provided, the prosecutors had 12,898 user location points, which meant an average of 101 points per day and thus sufficient to prove the crime. In turn, the defense argued that the collection of these data would violate the Fourth Constitutional Amendment,[30] since it would require a warrant based on a probable cause, having only been satisfied the standard least demanding of reasonable grounds.[31]

Firstly, because of a revolution in the telecommunications service, the US Supreme Court had to revisit its old jurisprudence that supported the access to customer data from telephone operators. In the *Carpenter v. United States 585 U.S. (2018)*, there was thus the overruling of the preceding precedent *Smith v. Maryland, 442, U.S. 735 (1979)*. In short, it had been established that the use of a dialed numbers registry does not constitute a violation of the "legitimate expectation of privacy", since the numbers would be available and would already be registered by the telephone company.[32] Thus, considering that the registration device was installed on the property of the telephone company and at its central offices, there would be no violation of the Fourth Amendment, since there would be no expectation of privacy regarding the registrations of dialed telephone numbers.[33]

In general, in the *Carpenter v. United States* case, the court understood that the provision of data, as has been possible with modern applications and handsets, could pose a great threat to the fundamental right of privacy. Therefore, no more support would be given to the thesis of "*lack of privacy expectation over documents delivered to third*

[29] CORTEZ, Nathan. Regulating disruptive innovation. Berkeley Technology Law Journal. Berkeley, n. 29, p. 175-228, 2014. p. 184. No original: "The contemporary challenge, then, is how existing agencies can confront these innovations given their broad but sometimes inert statutory frameworks".

[30] Amendment IV - Constitution of the United States of America: "The right of the people to the inviolability of their persons, houses, papers and assets against arbitrary search and seizure shall not be infringed; and no warrant shall be issued except by evidence of guilt confirmed by oath or declaration, and particularly by the description of the place of the search and the indication of the persons or things to be apprehended."

[31] FREIWALD, Susan. SMITH, Stephen. The Carpenter chronicle: a near-perfect surveillance. Harvard Law Review. 205. P. 217.

[32] Smith v. Maryland, 442 U.S. 735 (1979): We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not "legitimate." The installation and use of a pen register, consequently, was not a "search," and no warrant was required. Available at: <https://www.loc.gov/>. Accessed March 4, 2019.

[33] Smith v. Maryland, 442 U.S. 735 (1979): Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner obviously cannot claim that his "property' was invaded or that police intruded into a "constitutionally protected area." Available at: <https://www.loc.gov/>. Access in March 5, 2019.

parties".[34] Indeed, what prevailed was the understanding that location records derived from cellular devices, by reason of their unique and revealing nature, are not subject to the third-party doctrine of the *United States v. Miller (1976)* and *Smith v. Maryland (1979)*" cases,[35] according to which an individual would have no legitimate privacy expectation concerning information that he voluntarily transmits to third parties.[36]

The *Carpenter v. United States* case therefore addressed the constitutional compatibility of "*long-term clandestine tracking by a single powerful device capable of near-perfect surveillance*"[37] when faced with the guarantee of the Fourth Amendment of the US Constitution. The constitutionality analysis of the mentioned tracing included not only an exam on whether the technique employed was (a) hidden, (b) continuous, (c) indiscriminate and (d) intrusive, although such factors were not explicitly listed,[38] but also an assessment of the application relevance to the case of the third-party doctrine.

It was understood, therefore, that since the information obtained by cell phone tracking revealed exhaustive details of Carpenter's location, unlike the cases in which the previous precedent was based, involving not so advanced technology, there would be, in this new reality, a significant and inappropriate extension of the circumstances legitimated by the third party doctrine.[39] Therefore, a technological innovation turned a prevailing judicial understanding completely inappropriate, especially because it was grounded on older equipment.

The lesson from the foreign experience is that even if "*the legislative and judiciary powers adapt law to the new technology to ensure that the proper balance between security and freedom is maintained*,"[40] they do not do it efficiently. Thus, there is a need for a dynamic and flexible state regulation and interpretation of technological innovations. Otherwise, outdated decisions and norms will prevail and they will not be able to understand what the new already is.

5. GENERAL DATA PROTECTION REGULATION [GDPR] FROM EUROPEAN UNION

Since May 2018, the General Data Protection Regulation (GDPR) has been in force in Europe, which, in addition to the protection of personal data, guarantees greater clarity and specificity regarding the requirements for the consent to the collection and

[34] CASAGRANDE, **Cássio**. Is your cell phone an electronic anklet? No, says the US Supreme Court. American constitutional court restricts search of location data to telephone companies.Available at: https://www.jota.info/opiniao-e-analise/colunas/o-mundo-fora-dos-autos/o-seu-celular-e-uma-tornozeleira-eletronica-nao-diz-a-suprema-corte-dos-eua-06072018. Accessed December 26, 2018.

[35] FREIWALD, Susan. SMITH, Stephen. The Carpenter chronicle: a near-perfect surveillance. Harvard Law Review. 205. P. 218.

[36] PRICE, Michael W. Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine. Journal of National Security. Law & Policy, vol. 8: p. 247-299, 2016, p. 265: "under an aggressive reading of the third-party doctrine, the Fourth Amendment would not guarantee the privacy of any personal data held by any private company. This would include virtually all records of electronic communications, web browsing activity, and cloud data, to name just a few examples".

[37] FREIWALD, Susan. SMITH, Stephen. The Carpenter chronicle: a near-perfect surveillance. Harvard Law Review nº 205, 2018, p. 217.

[38] *Ibidem* p. 219.

[39] *Ibidem* p. 224.

[40] *Ibidem* p. 205.

processing of such data, as well as portability and the suppression of data.[41] The normative treatment conferred by the GDPR also establishes requirements regarding data security and protection concerning those responsible for its treatment. One of the highlights are the ones the provisions of the GDPR apply. There are four main addressees:

> (a) data subjects,[42] who are natural persons, whose data are processed;
>
> (b) controllers,[43] which are usually companies that define the destination and means of processing personal data;
>
> (c) processors,[44] entities that treat personal data on behalf of controllers, in a hierarchical relationship, and[45]
>
> (d) data protection authorities.

Traditionally, in the North American system, with a liberal matrix, it is believed that data subjects are more responsible than natural persons, who should be critical and make conscious choices regarding the exposure and treatment of their data. However, in the system implemented by GDPR at a European level, there is a broader scope of responsibility for controllers, even in the case of breaches perpetrated by processors, the former being, in principle, responsible since they must guarantee, in accordance with the provisions of the GDPR, that processors are competent and responsible.[46]

Under another approach, there is, as far as the scope of the GDPR is concerned, an emphasis on its extraterritoriality. As can be inferred from the analysis of its article 3,[47] the GDPR applies to all companies processing personal data of data holder's resident in the European Union, irrespective of the location of the company. The GDPR also applies to the processing of personal data by controllers and processors in the EU,

---

[41] LEMOS, Ronaldo *et al*. GDPR: the new personal data protection legislation in Europe. What will change in the international business environment? And what are the effects on Brazilian citizens and entities? Available at: <//www.jota.info/opiniao-e-analise/artigos/gdpr-dados-pessoais-europa-25052018>. Accessed March 4, 2019.

[42] Article 4, paragraph 1, of the GDPR: "Personal data" refers to any information relating to an identified or identifiable natural person ("data holder"); an identifiable natural person is one that can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more specific factors of physics, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[43] Article 4, paragraph 7, of the GDPR: "Controller" means the natural or legal person, public authority, agency or other body that, individually or jointly with others, determines the purposes and means of the processing of personal data; If the purposes and means of such processing are determined by the law of the Union or the Member State, the controller or the specific criteria for their appointment may be laid down in Union or Member State law.

[44] Art. 4, § 8, of GDPR: "Processor" is a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

[45] HOOFNAGLE, Chris Jay, VAN DER SLOOT, Bart & BORGESIUS, Frederik Zuiderveen. The European Union general data protection regulation: what it is and what it means, Information & Communications Technology Law, 28:1, 65-98, 2019, p. 73.

[46] HOOFNAGLE, 2019, *loc. cit*.

[47] Article 3. Territorial scope.

1. This Regulation shall apply to the processing of personal data carried out in the context of the activities of an establishment of a controller or a subcontractor located within the territory of the Union irrespective of whether the processing occurs within or outside the Union.
2. This Regulation shall apply to the processing of personal data of holders resident in Union territory by a controller or subcontractor not established in the Union where the processing activities relate to:

(a) the supply of goods or services to such data holders in the Union, irrespective of the requirement that data holders make a payment;

(b) control of their conduct, provided that such conduct takes place within the Union.

3. This Regulation shall apply to the processing of personal data by a controller established not in the Union but in a place where the law of a Member State applies under public international law.

regardless of whether processing takes place in the EU. Furthermore, GDPR achieves the processing of personal data of data holders in the EU and is done by someone not established in the EU, when the activities concern: (a) offering goods or services to EU citizens (regardless of payment be necessary) and (b) monitoring of behavior in the EU. Finally, non-EU companies processing EU citizens' data also have to nominate a representative in the EU.[48]

The importance of GDPR is therefore not only due to the fact that it has provided more adequate data protection that proliferate with technological innovations, but also because of the potential to "*lead to a large-scale (but not total) harmonization of data protection law across the European Union*"[49] and to generate "*global impact by restricting cross-border data transfers, directly regulating the conduct of many non-EU organizations, and, importantly for our discussion here, influencing data protection legislation around the world.*"[50]

However, now that the standard has already come into effect and produces its effects, the risks and implementation difficulties involved are evident:

> Even before the data are being processed, both data controller and data processor need to have in place a lot of policies which makes them compliant with the regulation. Yet, it is difficult to predict what will happen at every step of data processing. The steps include new rights to be respected, joint responsibilities and mandatory notifications, as a consequence, the company or public entity will be on alert (…) all the time. A lot of uncertainties, a lot of documents and many departments are involved by the GDPR. Finding the right interpretation of definitions and legal interpretations is not easy.[51]

Other problems resulting from the immediate implementation of the GDPR relate to the duty nature of the data protection and to the uncertainty of such liability range. In the European Union, there is still some difficulty regarding the precise delimitation of the term "appropriate protection", since "*The European rules impose a duty to implement appropriate technical and organizational security measures. This is an 'obligation of means'. The actors are not obligated to provide a perfect security. The meaning of 'appropriate' depends on the context.*"[52] Thus, despite the uniformity proposal in the law field of data protection at European level, there could still be great discretion on the part of the national courts because:

[48] GDPR Key Changes. An overview of the main changes under GDPR and how they differ from the previous directive. Available at: < https://eugdpr.org/the-regulation/>. Accessed March 4, 2019.
[49] KUNER, Christopher. JERKER, Dan. The GDPR as a chance to break down borders. International Data Privacy Law, Volume 7, Issue 4, p. 231–232, 1st November 2017, p. 231.
[50] KUNER, 2017, p. 231.
[51] DODE, Albi. The challenges of implementing General Data Protection Law (GDPR). 14th International Conference in "STANDARDIZATION, PROTYPES AND QUALITY: A MEANS OF BALKAN COUNTRIES' COLLABORATION", September 21 - 22, 2018, Tirana, Albania. Available at: https://www.researchgate.net/publication/327829348 _The_challenges_of_implementing_General_ Data _Protection_Law_GDP R/download. Accessed March 8, 2019.
[52] WOLTERS, P. T. J. The security of personal data under the GDPR: a harmonized duty or a shared responsibility? International Data Privacy Law, 2017, Vol. 7, Nº. 3, p. 165-178, 2017, p. 172.

> A German court might set different requirements for an 'appropriate' security than a Spanish court. […]. After all, the national courts and data protection authorities will still play an important role for the enforcement of the rules in specific situations.[53]

Considering the liability regime for the violation of the GDPR rules, there are also differences as to its scope, that is, whether it would be objective or subjective, and this would ultimately affect the data protection itself. The controversy arose because of the drafting of the Data Protection Directive (*Directive 95/46 / EC*) adopted in the European Union from 1998 onwards. It is based on the text of the Directive, "s*ome member states have adopted a system of strict liability. In other legal systems, the controller is not liable if he can prove an absence of fault.*"[54] As the text of Article 82, paragraph 3, of the GDPR[55] does not contain a totally clear content on the option of the liability regime, uncertainty may persist until there is jurisprudential understanding to pacify the issue in each Member State.

It is therefore clear that, despite the progress made by the GDPR in relation to the protection of personal data within the EU, there are still problems to be solved, especially those related to data protection effectiveness, regarding the uniformity of its application and those arising from the uncertainties surrounding the legal regime of accountability.

6. LAW 13,709/18

In Brazilian, the subject of data protection became regulated by Law 13,709/18, the so-called General Law on Data Protection (GLDP).

Previously, the protection of personal data was disciplined by other existing legal instruments. In this sense, SANTOS (2018):

> Notwithstanding the Federal Constitution (LGL \ 1988 \ 3), the Consumer Protection Code, the Civil Code (LGL \ 2002 \ 400), the Positive Registration Law and the Civil Registry of the Internet already protected, in some way, rights related to data and privacy, given the technological advances and as a way of granting greater legal certainty to relations so that Brazil would have a level of legislation and protection compatible with that of other countries, facilitating the investment and the flow of data, on August 15,2018, Law 13,709 / 18 (LGL \ 2018 \ 7222) was enacted and published, which provides for the protection of personal data and changes the Civil Registry of the Internet.[56]

Federal Law 13,709/18, a framework for the protection and processing of personal data in Brazil and which adhered to an overall trend of safeguarding these values, provides for the natural person's ownership of their personal data,[57] establishes the right

[53] WOLTERS, *idem*, p. 175.
[54] WOLTERS, *loc. cit.*
[55] Article 82, paragraph 3: The controller or subcontractor shall be exempt from liability in accordance with paragraph 2 if he proves that he is in no way responsible for the event giving rise to the damage.
[56] SANTOS, Fabíola Meira de Almeida. TALIBA, Rita. General Law on Data Protection in Brazil and the possible impacts. Revista dos Tribunais | vol. 998/2018 | p. 225 - 239 | Dec / 2018. P. 225.
[57] Art. 17 of Law 13,709/18: Every natural person is guaranteed the ownership of his personal data and guaranteed the fundamental rights of freedom, privacy and privacy, under the terms of this Law.

of access to their own data, correction of inaccuracies, as well as obtaining information about the sharing of data with public and private entities. In addition, it regulates the international transfer of data (articles 33 and subsequent articles of Law 13,709/18), restricting, even, the hypotheses where it is possible, which features a guarantor position. Besides, it expressly creates administrative sanctions for infringements to that provided by law.

Among the main aspects of the GLDP, it is worth mentioning:

> (a) its application to any activity that involves the use of personal data, including Internet treatment, of consumers and employees, among others;
>
> (b) the fact that data subjects will have broad rights: information, access, rectification, cancellation, opposition and portability;
>
> (c) application also to companies that do not have an establishment in Brazil;
>
> (d) provision of specific rules on sensitive data processing, international data transfer and data use of children and adolescents;
>
> (e) has discipline on data protection impact assessment (similar to DPIA), and
>
> (f) provides that any company responsible for data processing shall appoint a person in charge of the protection of personal data.[58]

In addition, it is worth to emphasize the wide extent of the law content. The law has wide scope, due to the concept of personal data treatment it adopted. As Laura Schertel Mendes and Danilo Moneda point out, "*all personal data processing is in principle subject to the GLDP, whether it is carried out by the public or private sector. The hypotheses of exception of application are restricted and are foreseen in its art. 4th*".[59]

Although most of the provisions of the GLDP only come into force twenty-four months after the date of their official publication, the ideal is that companies, of course, comply with the new law, as adequacy will require considerable technical, procedural and cultural activities.

It should also be noted that Law 13,709/18 is heavily influenced by General Data Protection Regulation in several respects. Both diplomas present similarities in the treatment conferred on aspects such as:

> consent of the holders of personal data, burden of proof of obtaining consent, right of information of the holders, portability of data, responsibility of the agents, indication of the person in charge of data processing and provision of safety parameters for their treatment, custody and handling.[60]

[58] REANI, Valéria. The impact of the Brazilian data protection law on labor relations. Available at: https://www.conjur.com.br/2018-set-21/valeria-reani-alei-protecao-dados-relacoes-trabalho. Accessed December 27, 2018.

[59] MENDES, Laura Schertel; DONEDA, Danilo. Commentary to the new data protection law (Law 13,709 / 18): the new paradigm of data protection in Brazil. Revista de Direito do Consumidor | vol. 120/2018 | p. 555 - 587 | Nov - Dec / 2018.

[60] MACHADO, José Mauro Decoussau; SANTOS, Matheus Chucri dos, PARANHOS, Mario Cosac Oliveira. GLDP and GDPR: a comparative analysis between legislations. Available at: http://www.pinheironeto.com.br/Pages/publicacoes-detalhes.aspx?nID=1362. Accessed March 5, 2019.

One of the important influences of the European law on the Law 13,709/18 appears in its art. 46, paragraph 2nd.[61] This paragraph provides that measures must be taken to protect personal data from the design stage of the product or service until its execution, which was inspired by art. 78[62] of the European regulation, whose application has the following effect:

> for any activity that involves the processing of personal data, it is necessary that the company responsible for the treatment observes, from the creation of the system for data collection, or for the provision of its services and products, the principles [...], adopting effective measures (such as data minimization, appropriateness for purpose, unambiguous consent, etc.). And such principles should be observed throughout the treatment, including, but not limited to, storage, access, transmission, archiving and destruction.[63]

Another example of GDPR's influence on Brazilian legislation concerns the similarity between the European Data Protection Committee (Article 68[64] and subsequent articles of the GDPR) and the National Data Protection Authority or NPDA (articles 55-A and subsequent articles of Law 13,709/18). Both are entities created to act with autonomy[65] and to supervise and promote the application of the respective law. Initially, GLDP devices dealing with the national authority were vetoed because of initiative flaws. However, with the edition of MP 869/18, there was change in the GLDP and the NPDA was created.

It is imperative that Brazilian law has as one of its main purposes to encourage the creation of an institutional custom of data protection, and especially through the National Data Protection Authority, the concern to ensure effectiveness in compliance with the norms on the subject. Among its main attributions, the National Data Protection Authority has exclusivity in the application of the penalties provided for in Law 13,709/18,[66] can determine to the controller the elaboration of an impact report

[61] Art. 46 §2º GLDP: The measures dealt with in the main section of this article should be observed from the design stage of the product or service until its execution.

[62] (78) - The protection of the rights and freedoms of natural persons in relation to the processing of their personal data requires the adoption of appropriate technical and organizational measures to ensure compliance with the requirements of this Regulation. In order to be able to demonstrate compliance with this Regulation, the controller shall adopt internal guidelines and apply measures in particular that respect the principles of data protection from design and data protection by default. Such measures may include the minimization of the processing of personal data, the pseudonymisation of personal data as early as possible, transparency as regards the functions and processing of personal data, the possibility for the data subject to control data processing and possibility for the controller to create and improve safety measures. In the context of the development, design, selection and use of applications, services and products that rely on the processing of personal data or use this processing to perform their functions, the manufacturers of products, services and applications should be encouraged to take into account the right to data protection when developing and designing it and, with due respect for the most advanced techniques, to ensure that controllers and subcontractors are in a position to fulfill their data protection obligations. The principles of data protection from design and by default should also be taken into account in the context of public procurement.

[63] SANTOS, Fabíola Meira de Almeida. TALIBA, Rita. General Law on Data Protection in Brazil and the possible impacts. Revista dos Tribunais | vol. 998/2018 | p. 225 - 239 | Dec / 2018. P. 225.

[64] Article 68 of the GDPR. European Committee for Data Protection. 1. The European Data Protection Committee ('the Committee') shall be established as a body of the Union and shall have legal personality.

[65] Art. 55-B of Law 13,709 / 18: Technical autonomy is guaranteed to the NPDA.

[66] Article 55-K of Law 13,709 / 18: The application of the sanctions provided for in this Law is the exclusive responsibility of the NPDA, whose other competences will prevail, as regards the protection of personal data, on the related competencies of other entities or bodies of public administration.

regarding the protection of personal data,[67] receives complaints from users,[68] in order to ensure efficiency in its activities,[69] publishes rules and procedures on the protection of personal data[70] and deliberates on the interpretation of Law 13,709/18, its powers and eventual omissions.[71]

Another point of note is the importance of Law 13,709/18 to the consumer relations, insofar as the protection of personal data in the scenario of expansion of new technologies, not only in Brazil, but on a world scale, is a topic which usually involves the legal sphere of consumers, and their hypo sufficiency that justifies the need for a greater legal protection. In this sense, KIMMELMAN:

> Some find it abusive that their privacy is the price to pay for access to socially or economically unavoidable Internet platforms. Others hate paying twice for their internet service, both with their money and with their personal information. And everyone is outraged by data breaches, hacks, revelations of corporate and state surveillance, and other social and political scandals. Consumers in the US, European Union (EU) and other countries want more control over their personal data and require privacy protection.[72]

Thus, the protection granted by Law 13,709/18 is crucial for the fruition of the most varied fundamental rights in Brazil, since, as Laura Schertel Mendes and Danilo Doneda point out, "*any data treatment, because it influences the representation of the person in society, can affect their personality and therefore has the potential to violate their fundamental rights*".[73]

7. CONCLUSION

The topic of personal data, in the context of new technologies evolution, deserves a particular approach, based on the analysis of specific cases, by regulatory models sufficiently capable of protecting this right in accordance with the degree of protection conferred not only by the 1988 Constitution, but also by institutes found in foreign norms.

---

[67] Article 38 of Law 13,709 / 18: The national authority may determine to the controller to prepare an impact report on the protection of personal data, including sensitive data, regarding its data processing operations, according to the regulation, observing the trade secrets and industrial.

[68] Art. 55-J. It is the responsibility of the NPDA: V - to implement simplified mechanisms, including by electronic means, to register complaints about the processing of personal data in violation of this Law.

[69] Article 55-J §2 of Law 13,709 / 18: The NPDA and the public bodies and entities responsible for the regulation of specific sectors of economic and governmental activity must coordinate their activities, in the corresponding spheres of action, with a view to ensuring compliance with its attributions with the greatest efficiency and promote the proper functioning of the regulated sectors, according to specific legislation, and the processing of personal data, in the form of this Law.

[70] Art. 55-J. It is incumbent upon the NPDA: II - to edit norms and procedures on the protection of personal data.

[71] Art. 55-J. It is incumbent upon the NPDA: III - to deliberate, in the administrative sphere, on the interpretation of this Law, its powers and the omitted cases.

[72] KIMMELMAN, Eugene. The limits of antitrust in privacy protection. International Data Privacy Law, Volume 8, Issue 3, 1 August 2018, Pages 270–276. P. 270: "Some find it abusive that their privacy is the price to pay for access to socially or economically unavoidable internet platforms. Others hate to be paying twice for their internet service, both with their money and with their personal information. And all are outraged by data breaches, hacks, revelations of corporate and state surveillance, and other social and political scandals. Consumers in the USA, the European Union (EU), and elsewhere want more control over their personal data, and they demand privacy protection".

[73] MENDES, Laura Schertel; DONEDA, Danilo. Commentary to the new data protection law (Law 13,709 / 18): the new paradigm of data protection in Brazil. Revista de Direito do Consumidor | vol. 120/2018 | p. 555 - 587 | Nov - Dec / 2018.

As seen, the examples offered by the *Carpenter v. United States 585 U.S.*, General Data Protection Regulation (GDPR) and Law 13,709/18 (GLDP) demonstrate a growing concern at the national and international level with data protection. In addition, they indicate constant changes in the courts' understandings, in the legal norms and changes of the new technology's users' rights.

The rapid change in this regulatory landscape does not dissociate itself from the constant evolution of the technological scenario and is indicative of the difficulty of adapting the legal plan to the factual plan Given the need for regulating new technologies, the responses offered by traditional legal mechanisms and case law have not been sufficient. The above experiences likewise tend to confer a high degree of protection to users and to extend controller and processor liability regimes, which reveals the high importance of safeguarding privacy in the contemporary world.

However, there is also the fact that there is no complete solution to the discrepancy between technological reality and legal protection. In this context, problems related to the uniformity of data protection between different systems are evident, which would be imperative, given the international nature of data circulation and processing, and the difficulty of implementing the various protection mechanisms of users, either because there is a wide discretion in the interpretation of the rules, as exists in the case of the GDPR, or because it was not possible to verify the degree of effectiveness of the legal rules, as in the case of the recent Law 13,709/18.

Thus, it is imperative to continue in the researches aimed at identifying a north for the regulation of disruptive innovations, which should be flexible, dynamic and sometimes detached from the traditional solutions. The effective preservation of privacy and personal data in the contemporary world depends, therefore, on the ability to adapt and to review traditional regulatory models to face the challenges posed by innovation.

8. REFERENCES

BAPTISTA, Patrícia F., KELLER, Clara. Why, when and how to regulate new technologies? The challenges brought by disruptive innovations. RDA – Revista de Direito Administrativo, Rio de Janeiro, v. 273

CASAGRANDE, Cássio. Is your cell phone an electronic anklet? No, says the US Supreme Court. American constitutional court restricts search of location data to telephone companies. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/o-mundo-fora-dos-autos/o-seu-celular-e-uma-tornozeleira-eletronica-nao-diz-a-suprema-corte-dos-eua-06072018. Accessed December 26, 2018.

CORTEZ, Nathan. Regulating disruptive innovation. Berkeley Technology Law Journal. Berkeley, n. 29, p. 175-228, 2014

DODE, Albi. The challenges of implementing General Data Protection Law (GDPR). 14th International Conference in "Standardization, protypes and quality: a means of balkan countries' collaboration", September 21 - 22, 2018, Tirana, Albania. Disponível em: https://www.researchgate.net/ publication/327829348 _The_challenges_of _implementing_General_ Data _Protection_Law_GDP R/download. Accessed March 8, 2019.

FERRAZ JÚNIOR, Tércio Sampaio. Secrecy of data: the right to privacy and limits to the state's oversight function. Cadernos de Direito Constitucional e Ciência Política, n. 1, São Paulo: Revista dos Tribunais, 1992.

FREIWALD, Susan. SMITH, Stephen. The Carpenter chronicle: a near-perfect surveillance. Harvard Law Review nº 205, 2018.

GDPR Key Changes. An overview of the main changes under GDPR and how they differ from the previous directive. Disponível em: < https://eugdpr.org/the-regulation/>. Accessed March 4, 2019.

GÖRÖG, Georgina. The Definitions of Sharing Economy: A Systematic Literature Review. Number 2. Volume 13. Summer 2018.

GRIFONI, Patrizia. D'ANDREA, Alessia. Sharing Economy: Business Models and Regulatory Landscape in the Mediterranean Are*as*. International Business Research; Vol. 11, No. 5; 2018.

HAWSKSWORTH, J. and VAUGHAN, R. The Sharing Economy—Sizing the Revenue Opportunity. PricewaterhouseCoopers, 2014.

HOOFNAGLE, Chris Jay, VAN DER SLOOT, Bart & BORGESIUS, Frederik Zuiderveen (2019) The European Union general data protection regulation: what it is and what it means. Information & Communications Technology Law, 28:1, 65-98

HU, H, 2014. Toward Scalable Systems for Big Data Analytics: A Technology Tutorial, 1, 658-659, 665.

LEMOS, Ronaldo *et al*. GDPR: the new personal data protection legislation in Europe. What will change in the international business environment? And what are the effects on Brazilian citizens and entities? Disponível em: <//www.jota.info/opiniao-e-analise/artigos/gdpr-dados-pessoais-europa-25052018>. Accessed March 4, 2019.

LEPANJUURI, Katriina; WISHART, Robert; CORNICK, Peter. The Characteristics of those in the Gig Economy. Final Report**.** Department for Business, Energy & Industrial Strategy. UK Government. Fev/2018. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment _data/file/687553/ The_characteristics_ of_those_in _the_gig_ economy.pdf . Accessed March 8, 2019.

KIMMELMAN, Eugene. The limits of antitrust in privacy protection. International Data Privacy Law, Volume 8, Issue 3, 1 August 2018, Pages 270–276.

KUNER, Christopher. JERKER, Dan. The GDPR as a chance to break down borders. International Data Privacy Law, Volume 7, Issue 4, 1 November 2017, p. 231–232.

MACHADO, José Mauro Decoussau; SANTOS, Matheus Chucri dos, PARANHOS, Mario Cosac Oliveira. GLDP and GDPR: a comparative analysis between legislations. Disponível em: http://www.pinheironeto.com.br/Pages/publicacoes-detalhes.aspx?nID=1362. Accessed March 5, 2019.

MAURO, Andrea de; GRECO, Marco; GRIMALDI, Michele. A Formal Definition of Big Data Based on its Essential Features. Library Review, vol. 65, nº 3, p. 122-135, 2016, https://doi.org/10.1108/LR-06-2015-0061.

MENDES, Laura Schertel; DONEDA, Danilo. Commentary to the new data protection law (Law 13,709 / 18): the new paradigm of data protection in Brazil. Revista de Direito do Consumidor | vol. 120/2018 | p. 555 - 587 | Nov - Dec / 2018.

MENDES, Gilmar Ferreira. BRANCO, Paulo Gustavo Gonet. Course of Constitutional Law. 13ª ed. rev. e atual. – São Paulo: Saraiva Educação, 2018

PRICE, Michael W. Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine. Journal of National Security. Law & Policy, vol. 8: p. 247-299, 2016.

REANI, Valéria. The impact of the Brazilian data protection law on labor relations. Disponível em: https://www.conjur.com.br/2018-set-21/valeria-reani-alei-protecao-dados-relacoes-trabalho. Accessed December 27, 2018.

SANTOS, Fabíola Meira de Almeida. TALIBA, Rita. General Law on Data Protection in Brazil and the possible impacts. Revista dos Tribunais | vol. 998/2018 | p. 225 - 239 | Dec / 2018. P. 225.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Course of Constitutional Law. 6ª ed – São Paulo: Saraiva, 2017.

STEMLER, Abbey. The Myth of the Sharing Economy and its Implications for Regulating Innovation. Emory Law Journal [Vol. 67:197].

TAYLOR-SAKYI, Kevin. Big Data: Understanding Big Data. 2016.

WALLENSTEIN, Judith; SHELAT, Urvesh. Hopping Aboard the Sharing Economy. Disponível em: https://www.bcg.com/publications/2017/strategy-accelerating-growth-consumer-products-hopping-aboard-sharing-economy.aspx. Accessed November 4, 2018.

WIENER, Jonathan B. The regulation of technology, and the technology of regulation. Technology in Society 26, 2004.

WOLTERS, P. T. J. The security of personal data under the GDPR: a harmonized duty or a shared responsibility? International Data Privacy Law, 2017, Vol. 7, Nº. 3, p. 165-178, 2017.

YARAGHI, Niam; RAVI, Shamika (2017). The Current and Future State of the Sharing Economy, Brookings India IMPACT Series No. 032017. March 2017.