Institute for Research on Internet and Society

GDPR and its effects on the Brazilian Law

First impressions and a comparative analysis

Institute for Research on Internet and Society

GDPR and its effects on the Brazilian Law

First impressions and a comparative analysis

Coordination
Fabrício Bertini Pasquot Polido
Lucas Costa dos Anjos

Authors
Diego Carvalho Machado
Davi Teofilo Nunes Oliveira
Lucas Costa dos Anjos
Luíza Couto Chaves Brandão

Graphic Project
André Oliveira, Felipe Duarte e Lucca Falbo

Cover
Freepik

Layout
Felipe Duarte

Editorial Production
Instituto de Referência em Internet e Sociedade

Revision
Lucas Costa dos Anjos

Finalization
Felipe Duarte

How to reference this paper
MACHADO, Diego Carvalho et al. **GDPR and its effects on the Brazilian Law:** First impressions and a comparative analysis. Institute for Research on Internet and Society: Belo Horizonte, 2018. Available at: http://bit.ly/2LH27Yc. Access: DD mmm. YYYY

SUMMARY

1. Introduction

Among so much expectation and uncertainty, the European Union General Data Protection Regulation (GDPR) entered into force on May 25, 2018 and, with it, a new personal data protection paradigm, not restricted only to the European continent. Its scope, legislative ambition and conceptual evolution corroborate the idea that this is an authentic blueprint regulation, in which several other national, regional and intra-community initiatives will also be mirrored in pursuit of data protection uniform normative standards. It would not be an exaggeration to say that the GDPR was born as a 'normative monster'[1], a Leviathan that induces compliance by agents in the public and private spheres in the data protection field, especially in the informational and digital environments.

Since its inception, Regulation n. 679/2016 seeks to adapt to a new scenario, involving the globalization of the technologies and services that use the internet as the basis for its operations. Governments, users and service providers will be directly affected by the Directive 95/46/EC of 1995[2] updated provisions on the processing of personal data in the European community. What already was a relatively advanced legislative standard of protection, compared to other jurisdictions, is about to adjust to terms and procedures that are more modern and compatible with the new technologies of computation, automation and artificial intelligence. In this sense, there are the concepts of data collection, processing, transmission and data breach, sensitive data, right to be forgotten, among others, besides the maintenance of the Data Protection Authorities and the creation of a Data Protection Officer in the bureaucratic context of the European Union's macro-structure.

Given the relevance of the European market in international commerce, not only as consumers of products and (digital) services, but also as providers of important online services nowadays, it is to be expected that several other relevant scenarios will be affected by the european regulation, like Brazil. In a legislative context that not only behaves, but also requires, the regulation of the processing of personal data by means of Brazil's Internet Bill of Rights (Law 12.965/2014), initiatives such as the Senate Bill Proposal 330/2013 are promoted by the entry into force of the new Regulation and gains greater relevance in the national Legislative Branch discussions' agenda.

The need for reflection about the European Union's General Data Protection Regulation consequences on national and international areas is what motivates the Institute of Reference for Internet & Society - IRIS research team to study this subject. From a comparative perspective, not only in relation to Brazil, but also to Argentina, due to the unequivocal interfaces between the free movement of people, goods and services in MERCOSUL and national laws, it is sought to make an effort to foresee the GDPR effects on Brazilian and Argentinian legal systems. In addition, the conflicts and modifications likely to happen to governments, users and service providers are examined.

Initially, the European Union's General Data Protection Regulation design will be contextualized from the legal and jurisprudential framework that preceded it, outlining its most innovative concepts and the guiding principles of the new legislation. Next,

1 Just to illustrate, the Regulation has 173 considerings and 90 articles, distributed among nine chapters. Article 4, specifically, has 26 definitions concerning the Regulation, its interpretation and application.

2 EUROPEAN UNION. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. **Official Journal**, Strasbourg, 23/11/1995. Available at: <https://eur-lex.europa.eu/eli/dir/1995/46/oj>. Access in: 15/05/2018.

we identify the extraterritorial elements of the new Regulation and its possible effects on Brazil. Finally, in a comparative analysis of the Argentinian legislation, this paper contextualizes current state of the art of data protection discussion in this important Latin American market, which is highly relevant to economic integration initiatives such as Mercosur. In final lines, recommendations are addressed regarding formation of a regional positioning about the course this subject will take in a global scope.

2. The new european data protection regulation and its general outlines

2.1. Context previous to Regulation n. 2016/679

The debate concerning third-party and state interference with the private life of individuals and their informational autonomy has been subject of discussions in European Community and European Union for many years. In 1950, European Convention on Human Rights presented primary notions on privacy in its article 8[3]. The Universal Declaration of Human Rights provided as well in article 12 ideas that initiated legislative framework that culminated in the conceptions that made possible the elaboration of an European data protection regulation in the present day[4].

These first declarations were elaborated in the post-Second World War period, with the objective of promoting the rule of law, democracy, human rights, and social development[5]. The European Court of Human Rights has decided a number of cases, elaborating on articles 12 and 8, involving personal information, mainly data related to private communications interceptions, surveillance, and data retention by public and investigative authorities. In these contentious scenarios, states were the main questioned in their conduct of violation of privacy-related fundamental rights.

The European Convention on Human Rights and the UN Universal Declaration of Human Rights were important in their respective contexts as they were the first international declarations subscribed by European countries mentioning privacy and the right to its protection. Still, as they dealt only vaguely and indirectly with the protection of personal data, in the early 1980s, the European Economic Community, seeking to create mechanisms specifically addressing the protection of personal information, adopted Convention 108 on the protection of individuals concerning automatic processing of personal data[6]. It aimed to establish more careful methods and provided for "guarantees regarding the collection and processing of personal data"[7]. In addition, the Convention prohibits, "in the absence of adequate legal safeguards, the processing of 'sensitive' data, such as data related to race, political opinion, health, religious beliefs, sex life

3 Article 8. 1. Everyone has the right to respect for his private and family life, his home and his correspondence. EUROPEAN COUNCIL. European Convention on Human Rights. 1950. Available at: <https://www.echr.coe.int/Documents/Convention_ENG.pdf> Access in: 05/05/2018.

4 Article 12. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. UN. *The Universal Declaration of Human Rights*. Paris, 1948. Available at: <http://www.un.org/en/universal-declaration-human-rights/>. Access in: 28/04/2018.

5 EUROPEAN COUNCIL. *Handbook on European data protection law,* 2014. Available at: <https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf>. Access in 10/05/2018.

6 EUROPEAN COUNCIL. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Strasbourg, 1981. Available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Access in: 02/05/2018; The Convention was altered in 18/05/2018 by European Council. The modifications can be accessed at: <https://www.coe.int/en/web/portal/-/enhancing-data-protection-globally-council-of-europe-updates-its-landmark-convention>.

7 EUROPEAN COUNCIL. *Handbook on European data protection law,* 2014. Available at: <https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf>. Access in 10/05/2018.

or someone's criminal records". In the context of data flows between national States, the Convention provides for the free flow of personal data among its signatory States, but imposes some restrictions on transfers to States whose regulation doesn't provide equivalent protection of the European Union's[8].

In 1995, in order to perfect and implement Convention 108, the European Union enacted Directive 95/46/EC, which aimed to provide, harmonize and promote equality in the processing of personal data by the Member States of the organization. This instrument presented principles for the processing of personal data and set down data subject's basic rights. With regard to international data transfer, the Directive defined criteria and standards for transmission of data between countries, but without providing for extraterritorial jurisdiction[9]. Another point established in the former Directive was the creation of a system of central authorities responsible for supervision, regulation and arbitration on matters involving data protection, known as data protection authorities[10].

The whole context and discussion of the legislative development in relation to data protection demonstrate how the European model was constructed from the recognition of the fundamental legal status of the right to privacy and the protection of personal data[11]. Since the processing of personal data poses risks and opportunities to the realization of fundamental rights and freedoms[12], European states have been guided by comprehensive and pervasive regulation of information processing activities related to natural persons.

In 2016, the European Union, by means of the Regulation nº 679/2016, which became known as General Data Protection Regulation - GDPR, replaced Directive 95/46/EC, seeking to unify the protection of personal data in the European Union. As it's a regulation, not a directive, it's directly applicable to the 28 Member States and no transposition is required for each national jurisdiction. Thus, it's considered an internal law, a practice that didn't occur with the Directive 95/46/EC, because it was necessary for States to adopt the community text in their domestic law, generating different levels of data protection in each of the european country[13].

The main arguments for GDPR's rationale support the relevance of a legislation capable of addressing the new issues raised by digital economy and the pervasiveness of information and communication technologies in an equal manner between the different countries of the European Union[14].

This initial chapter aims to point out key changes resulting from the new European regulation and its general outlines, fundamental conceptual changes, new rules and major issues that the legislation unveils. As the new communitarian data protection legislation

8 EUROPEAN COUNCIL. *Handbook on European data protection law,* Op. cit.

9 KAPLAN, Harvey. COWING, Mark. EGLI, Gabriel. A *Primer for Data-Protection Principles in the European Union*. Available at: <https://www.shb.com/~/media/files/professionals/cowingmark/aprimerfordataprotectionprinciples.pdf?la=en>. Access in: 04/05/2018

10 GUIDI, Guilherme. *Modelos regulatórios para proteção de dados pessoais.* Available at: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Access in: 30/04/2018.

11 BYGRAVE, Lee A. Data protection pursuant to the right to privacy in human rights treaties. *International Journal of Law and Information Technology*, v. 6, n. 3, p. 247-284, 1998.

12 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *EJJL-Espaço Jurídico: Journal of Law*, v. 12, n. 2, p. 91-108, 2011.

13 For more information, see GUIDI, Guilherme. *Modelos regulatórios para proteção de dados pessoais. cit.* : "Regulations are binding rules which apply directly to all countries, including its citizens and juridical persons, counting as domestic law. Directives are rules adopted by the Commission and by the European Parliament which establish a goal that all Member-States ought to achieve, each one being responsible for deciding the means for it, observing basic precepts of supranational norm." (author's translation from Portuguese) p.3.

14 CAMERON, Stephen. 'Light Reading '*The Digital Economy & GDPR*' 2017 Available at: <http://www.lightreading.com/oss-bss/subscriber-data-management/the-digital-economy-and-gdpr/a/d-id/730582> Access in: 04/05/2018.

is a very complex regulation, composed of 11 chapters and 99 articles, this study does not intend to exhaust the discussion, but rather to provide primary subsidies for studies and applications of the foremost changes arising from the European regulation and its impact on Brazil, as well as a comparison with Argentina's rules in this matter, one of the most important references in Latin America with regard to data protection.

Building legal guarantees that cover technology-related topics and innovations in informational and reticular environments (such as the internet and digital platforms) has been a challenge for legislators nowadays. In issues as sensitive as those that define the spectrum of legal protection of personal data, these questions become even more latent, as business models involving personal data are rapidly altered by the pace of innovation and business growth. It creates the risk that a law turns obsolete a few years after its publication[15].

2.2. Legislative technique and GDPR key legal provisions

In view of these challenges, the new data protection regulation in the European Union domain has been elaborated at several "levels". In the first stage, between Articles 1 and 11, broad fundamental guarantees and definitions were adopted which will be used throughout the Regulation text and its application. This multi-level structure and its principles allows for greater dynamization of the legislation, making it less susceptible to become outdated. This method establishes technologically neutral principles and safeguards - what ensures their future application, albeit with reasonable changes in the technological ground.[16]

In its first chapter, especially in Article 4, a number of critical concepts are defined which will be used throughout legislation - some previously defined in Directive 95/46/EC, but improved by the new regulation. In Article 4, it's possible to find more than twenty-five key concepts[17], such as personal data[18], profiling[19], consent[20], processing[21], controller[22], supervisory authority[23], among others. These initial definitions influence the entire legislation, as long as notions of consent and personal data define the scope and

15 Regarding the difficulty to legislate about the various subjects which comprehend internet and new technologies, see: KURBALIJA, Jovan. *An introduction to Internet governance*. 2010. Available at: <https://www.diplomacy.edu/resources/books/introduction-internet-governance> Access in: 04/05/2018.

16 GUIDI, Guilherme. *Modelos regulatórios para proteção de dados pessoais. cit.*

17 More information at: <https://gdpr-info.eu/art-4-gdpr/>.

18 Article 4 (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council, cit.

19 Article 4 (4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;. Idem.

20 Article 4 (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; Idem.

21 Article 4 (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; Idem.

22 Article 4 (7), 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; Idem.

23 Article, 4 (21), 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51. Idem.

application of the data protection rules.

In describing personal data, the GDPR adopted an expansionist concept[24]. This means that personal data can refer to any type of information that allows the identification of the data subject, even if the connection isn't established immediately, but indirectly or mediately. This is a legislative strategy that starts from the premise that "anonymous data is always reversible"[25]. In the repealed Directive, personal data were defined only as name, image, address, e-mail, telephone number and personal identification[26], therefore in a spectrum determined by practically exhaustive elements. It's the first generation of community rules on the regulation of issues related to new technologies and data protection, overcame by the upcoming of Internet and its developments.

In the new European Regulation, the concept of personal data includes any information that can be used to identify a person, such as user location data, mobile device IDs and even IP address in some cases.

The collection of **sensitive data** - those that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning one's sexual orientation - is expressly prohibited under article 9. The regulation provides for some exceptions, authorizing the collection of sensitive data for preventive and occupational medicine purposes, to evaluate the employee's work capacity, medical diagnosis, medical or social care and treatment or management of health systems and services, services on the basis of the Member State law or pursuant to contract with a health professional[27].

The new European legislation introduces significant changes compared to the Directive 95/46/EC: it strengthens the **notion of consent for personal data usage** and clarifies the scope of the relationship between consent and the collection and processing of personal data[28]. According to this formula, the GDPR establishes that the request for consent must be presented in a manner clearly distinguishable of other matters, in an intelligible form, easily accessible, and using plain language, rather than the obscure language generally adopted[29]. Another new element covered by the Regulation concerns the obligation to explain the data collection objectives or intentions. It must be preceded

24 BIONI, Bruno. *Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. Grupo de Estudos em Políticas Públicas em Acesso à Informação da USP – GPOPAI, São Paulo,* 2015. Available at: <http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf> Access in: 02/05/2018.

25 Idem, p.32. It is noticeable, nevertheless, that the possibility of data anonymization on european law is controverted. That's because in another perspective the anonymization isn't eliminated. Due to current computing capability and the numerous digital and network interconnected databanks, the data anonymization techniques could provide privacy assurance and be used for generating efficient anonymization procedures, but only if their use is adequately conceived - which means accomplishment of prerequisites. Besides, the goals of anonymization process must be defined clearly. The best technical solution would be adopted case by case, eventually by means of combining different methods. For more information, see: ARTICLE 29 WORKING PARTY. Opinion 2/2010 on online behavioural advertising. Brussels: [s. n.], 2010. Opinion 2/2010 on online behavioural advertising . p. 5-6. Available at: <https://iapp.org/media/pdf/resource_center/wp171_OBA_06-2010.pdf>. Access in: 21/05/2018.

26 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. of the European Union, Strasbourg, 23/11/1995. Available at: <https://eur-lex.europa.eu/eli/dir/1995/46/oj>. Access in: 15/05/2018.

27 Article 9 (1), GDPR: Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council. *cit.*

28 Regulation establishes that, on the case of children and teenagers, data treatment is licit from 16 years on. On cases in which the child is less than 16 years old, such treatment is only going to be licit when consent is given or authorized by the holder of parental responsibility, as long as the age is not below 13 years. Idem.

29 Article 7 (2), GDPR: If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. Idem.

by an explanation of its purpose, demonstrating how and who gave consent, and if the data collection is for various purposes, each one must be demonstrated to the user. Also important is the fact that the person who consented to the collection of his/her data has the right to withdraw the authorization at any time, and its withdrawal should be as simple as its concession[30].

Amid many rules established by the Regulation, is the **accountability principle**, central to relations involving data management by companies and public administration bodies. With the Regulation entry into force, all companies are held accountable for the storage and protection of all personal data they collect and store. Derives from the accountability principle the obligation to repair any damage caused to the data subject due to the violation or data breach[31].

With respect to the provisions concerning companies, safeguards and **data breach**[32], the Regulation sets out a series of duties and obligations. First, it is important to highlight the **obligation to notify**[33] the data protection authority within 72 hours for data breaches that result in risks to individuals' rights and freedoms. The Regulation states:

> Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

Another imposed obligation upon data controllers, either public or private, refers to the need for determination of a **data protection officer**. It has the role of bringing closer the regulatory bodies and the personal data subjects. This assignment will only be required, according to article 37, if the data controller or processor is a public body[34] or when the core activities of the private organization consist of:

- processing operations on a large scale which aims the regular and systematic monitoring of data subjects;

30 Article 7 (3), GDPR: The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. Idem.

31 With entering into force of the Regulation in 25 of may 2018, companies turn out to be directly responsible for ensuring all obtained information is safe, protected against any kind of risk of breach or violation.

32 **Data breach is defined, for regulation purposes, in article 4 as: "(12)'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;". Idem.**

33 **It establishes, on article 33: 1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay". Idem.**

34 WP29 considers that what constitutes an authority or public body must be established by national law and that those entities should name a data protection manager. Nevertheless, other juridical personalities, individual or collective, governed by public or private law (v. g., public transportation services, water and energy supply, public broadcasting infrastructure, public housing or disciplinary organizations) are not obliged to name a manager, even that it's highly recommended. For more, see: ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Data Protection Officers ('DPOs').* Available at: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>. Access in: 02/05/2018

- processing operations on a large scale of special categories of data, in other words, sensitive data, such as health, religious, racial, and sexual orientation information; and personal data relating to criminal convictions and offences.

Data protection officers (DPOs) perform diverse functions, which are basically listed in Art. 39 of the Regulation n. 679/2016. It's a person with some experience in the field of data security and data protection, designated by the companies that are considered controllers or processors for the personal data processing activity. Its immediate role is to supervise and advise the company on the obligations contained in the GDPR. Between these main functions, the following should be underlined: i) monitor and report on the organization's compliance with the GDPR policy; ii) to set up training with the parties involved in the processing of personal data; and iii) perform privacy impact assessments, its implementation, and results. They also act as proxies between stakeholders, such as supervisory authorities, data subjects and personal data-driven companies[35].

Article 24 of the Regulation makes clear that it's the controller's responsibility to "implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation"[36]. That is to say, the data protection officer will act as a communication channel between the parties involved in data protection and also as an inspector of all personal data processing practices in the organization, verifying if they comply with the GDPR, and raising awareness about the relevance of compliance in the processing of citizens' data[37]. The GDPR compliance monitoring is not a personal responsibility of the data protection officer, but of the company or institution responsible for the data collection[38].

2.3. New rights established and informational environments

Right to be forgotten

Two categories of rights enshrined in the European Regulation have raised discussions about their possible applications. The first, established in article 17, refers to the so-called "**right to erasure**" ("**right to be forgotten**"), allows the data subject to request the deletion of his/her data to whoever possesses it. It also provides for the possibility of the data subject to request the interruption of its personal data sharing and usage.

The conditions for a legal claim to removal are described in Art.17 and include, for example, data that is no longer relevant to its original purposes or which its consent has been revoked, providing that the "public interest in the data availability" shall be

35 Idem.

36 Article 24, GDPR: 1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council, cit.

37 BIONI, Bruno; MONTEIRO, Renato. *O papel do Data Protection Officer.* 2017. Available at: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-papel-do-data-protection-officer-04122017>. Access in: 28/04/2018.

38 ARTICLE 29 DATA PROTECTION WORKING PARTY. *The Role of the Data Protection Officer,* 2017. Available at: <https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/DPO%20Update%20Article%20Final.pdf>. Access in: 30/04/2018.

considered in such requests' acceptance. The right to be forgotten in the European Union Law has recently been highlighted by the case *Google Inc v Agencia Española de Protección de Datos, Mario Costeja González* (2014)[39]. The case genuinely officialized the CJEU's judicial precedent on the matter and promoted numerous discussions on its application, normative scope and balancing of rights[40].

According to Article 17 (1) (c), the GDPR ensures personal data erasure when requested by the data subject that exercises himself the right to object (Article 21) and there are no "overriding legitimate grounds for the processing". The notion of "legitimate interest" constitutes an indeterminate legal concept, therefore, demanding from the courts triggered the normative concretion in line with the judge's hermeneutical activity on the case. Thus, the courts must weigh whether there is an interest of the controller or third parties which is predominant in relation to the data subject's fundamental rights and freedoms protected by law. Some objective parameters are provided in respect of what may constitute "legitimate interest", both by GDPR[41] and by the jurisprudence of CJEU[42], in addition to other bodies of the European Union's data protection system[43].

Right to explanation and to object to automated decision-making

Another legal right category related to the information environment, established by the new european legislation, is associated with the **objection to automated decision-making**, in line with article 22 ("automated individual decision-making, including profiling") and articles 13 to 15 ("information and access to personal data") of the Regulation. Rules that restrict automated decisions and require "explanations" about how algorithms work have opened up several discussions among academics, experts and others interested in machine learning or artificial intelligence decision-making[44].

Decisions which are automated and have no human intervention seem to go against the concept of autonomy and personality in the European Regulation[45]. Therefore, the Regulation guidance in measuring the **right to explanation** seeks to provide some meaningful information about how personal data is used in automated decision-making. Countless controversies are raised regarding the possible applications of this legal right category and how it will effectively be put into practice. The already existing literature on the GDPR cautiously observes the implications of articles 13 to 15 and 22, considering its

39 EUROPEAN UNION. Court of Justice of European Union. Grand Chamber. Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Luxembourg, 13/05/2014. Available at: <http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=EN>. Access in: 15/05/2018

40 THE GUARDIAN, *Costeja González and a memorable fight for the 'right to be forgotten'*, 2014. Available at: <https://www.theguardian.com/world/blog/2014/may/14/mario-costeja-gonzalez-fight-right-forgotten>. Access in: 05/05/2018.

41 As in its Considerings no. 47 to 49.

42 As happened on case *Mario Costeja González.* According to the ruling, the Court considers that this obligation of suppression from results list comes from a right of the data holder that does not presuppose a damage for inclusion on the results list on the measure that "As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name (100/4)". EUROPEAN UNION. Court of Justice of European Union. Grand Chamber. Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Luxembourg, 13/05/2014. Available at: <http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=EN>. Access in: 15/05/2018

43 ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.* Bruxelas: [s. n.], 2014. Available at: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>. Access in: 23/05/2018.

44 SELBST, Andrew; POWLES, Julia. Meaningful information and the right to explanation. In: *International Data Privacy Law,* vol. 7, n. 4, 2017, p. 233 ss. Available at: <https://academic.oup.com/idpl/article/7/4/233/4762325> Access in: 05/05/2018.

45 JONES, Meg Leta. The right to a human in the loop: Political constructions of computer automation and personhood. *Social studies of science,* v. 47, n. 2, p. 216-239, 2017.

technical features and complexity[46].

2.4. Fines and penalties for non-compliance

Lastly, one of the essential points that raises discussion about scope and applications deals with fines and penalties, as specified in articles 83 and 84 of Regulation n. 679/2016. Failure to comply with European law requirements might result in administrative fines for companies in a number of circumstances. A written notification will be sent in case of initial non-compliance.

The pecuniary sanction degree depends on the examined infringement and includes fines up to € 10 million or 2% of the total worldwide annual turnover of the previous financial year, whichever is higher. In this case, several situations are stipulated in the GDPR, for instance, violation of principles such as privacy by design[47], failure to comply with obligations related to processing or not designating a data protection officer. The fines for these cases intend to remedy the actual or potential violation of the rights established in articles 8, 11, 25, 39, 42 and 43 of the Regulation.

There are other penalties like fines of up to € 20 million or 4% of the total worldwide annual turnover in the previous year for violations of the processing principles, data processing legal requirements, or either the data subject's rights. The imposition of these sanctions will require the supervisory authority a case-by-case assessment of the infringement circumstances, such as contravention severity and duration, intentional or negligent acts, mitigation measures that have been implemented, technical and organizational measures and, finally, how the supervisory authority became aware of allegedly illegal events[48]. These categories intend to protect the rights set out in articles 5, 6, 7, 9, 12 to 22 and the situations involved in international data transfer provided in articles 44 to 49 of the GDPR.

2.5. Partial analytical observations

Considering these aspects of the new Regulation on Data Protection in European Union, this chapter presented some of the general outlines as well as its most latent discussions. Due to the GDPR extension, in addition to the present section, a table of the GDPR systematized themes (annex) assists the debate that is established in Brazilian scientific production. The next chapters will deal with the extraterritorial elements of the Regulation and will investigate their possible impacts, taking into account the comparison between the data protection legal system in Brazil and Argentina.

46 For a broad discussion on that subject, see: WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the general data protection regulation. In: *International Data Privacy Law*, v. 7, n. 2, p. 76-99, 2017 e SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. In: *International Data Privacy Law*, v. 7, n. 4, p. 233-242, 2017.

47 This approach seeks to promote privacy and data protection since design and conceiving of an application.

48 According to article 83, fines should be effective, reasonable and dissuasive for each individual case. For decision whether if and which quantity of sanctions may be evaluated, the authorities have a legal catalogue of criteria that must be used on decision making. Among other things, intentional violation, disability to adopt measures for mitigation of damage occurred or the lack of collaboration with authorities may increase penalties. EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). **Official Journal of the European Union**, Strasbourg, 04/05/2016. Available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679>. Access in: 16/04/2018..

3. Extraterritorial interfaces of the Regulation (EU) n. 2016/679 and its impacts on Brazil

3.1. The GDPR scope of application and extraterritoriality

One of the main reasons for the statement that the GDPR "will change not only the European protection laws, but nothing less than the whole world as we know it"[49], is in the material and territorial scope of the Regulation.

Its rules cover all activities of "processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system" (article 2). The legal provision, in fact, isn't any different from the text inscribed in article 3(1) of the Directive 95/46/EC. The novelty, however, that resonates with and directly affects the major technology companies in Silicon Valley[50], is based on the GDPR spatial or territorial scope.

According to article 3(1), the Regulation applies to personal information processing carried out "in the context of the activities of an establishment" by a controller or by a processor **situated in the european territory**, even if the processing takes place **outside the territorial limits** of the European Union[51].

In order to understand the criteria chosen by the European legislator, it's important to point out that the concept of establishment was mostly drawn from the Court of Justice of the European Union's jurisprudence in its function of interpreting the Directive 95/46/EC, which was also founded on the enlargement of the territorial scope of application.

In the *Weltimmo* case, the Court clarified that the concept of establishment "extends to any real and effective activity — even a minimal one — exercised through stable arrangements"[52]. A flexible, non-formalist conception of the concept was then constructed, valid especially "for undertakings offering services exclusively over the Internet"[53]. According to the *Weltimmo* ruling:

> With regard, in the first place, to the concept of 'establishment', it should be noted that recital 19 in the preamble to Directive 95/46 states that establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements and that the legal form of such an establishment, whether simply a branch or a subsidiary with a legal personality, is not the determining factor (judgment in *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 48). Moreover, that recital states that, when a single controller is established on the territory of several

49 ALBRECHT, Jan. P. How the GDPR Will Change the World. In: *European Data Protection Law Review,* v. 2, n. 3, 2016, p. 287. Tradução livre do original: "[GDPR] will change not only the European data protection laws but nothing less than the whole world as we know it."

50 SOLON, Olivia. *How Europe's 'breakthrough' privacy law takes on Facebook and Google.* 2018. Available at: <https://www.theguardian.com/technology/2018/apr/19/gdpr-facebook-google-amazon-data-privacy-regulation>. Access in: 09 mai. 2018.

51 Article 3(1), GPDR: "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not".

52 EUROPEAN UNION. Court of Justice of European Union. Third Chamber. Case C-230/14, *Weltimmo s. r. o.* v. *Nemzeti Adatvédelmi és Információszabadság Hatóság*. Luxembourg, 01/10/2015. Available at: <http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN>. Access in: 10/05/2018. Tradução livre de: "[...] extends to any real and effective activity — even a minimal one — exercised through stable arrangements".

53 Idem. See also: DE HERT, P.; CZERNIAWSKI, M. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. In: *International Data Privacy Law*, v. 6, n. 3, 2016, p. 233.

> Member States, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities.
>
> As the Advocate General observed, in essence, in points 28 and 32 to 34 of his Opinion, this results in a flexible definition of the concept of 'establishment', which departs from a formalistic approach whereby undertakings are established solely in the place where they are registered. Accordingly, in order to establish whether a company, the data controller, has an establishment, within the meaning of Directive 95/46, in a Member State other than the Member State or third country where it is registered, both the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned. This is particularly true for undertakings offering services exclusively over the Internet.
>
> In that regard, it must, in particular, be held, in the light of the objective pursued by that directive, consisting in ensuring effective and complete protection of the right to privacy and in avoiding any circumvention of national rules, that the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question.

In the case described above, the activity performed by the Slovak business enterprise *Weltimmo* involved the exploration of websites that advertised properties located in Hungary. After a one month period providing free of charge advertising for real estate deals, the company would then bill the service and charge fees from the Hungarian advertisers, even after requesting, within the mentioned free of charge term, the advertise exclusion and the erasure of the personal information.

In addition to these circumstances, it was considered relevant in the CJEU examination that the company had constituted a representative in Hungary and that its website used the Hungarian language to operate its activities[54]. In the end, the CJEU ruled that the controller (and internet application provider) had engaged in a real and effective action in Hungarian territory.

For the Regulation, the place where processing of personal data happens is irrelevant if the controller's establishment is situated in the European Union. The new rules are clearly relevant in view of internet advances. It reaches, for example, companies and entities responsible for processing data using **cloud computing**, that is, they use "an arrangement whereby computing resources are provided on a flexible, location-independent basis that allows for rapid and seamless allocation of resources on demand"[55], in the different types of service that can be adopted.

In Art. 3 of the GDPR, an absent figure in the previous legislation was included: the **processor**. As provided in the Art. 4 (8) of the Regulation, the processor is the natural or legal person, public authority, agency or other body which processes personal data **on behalf of the controller**. In other words, an intermediary that performs the processing of personal information on behalf of a controller who decides to delegate, contractually, part or all of the data processing operations[56], such as in the provision of cloud computing

54 In the context of interpretation and application of GDPR, enterprise "means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;" (artigo 4(18)). EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council. cit.

55 MILLARD, Christopher (Ed.). *Cloud Computing Law.* Oxford: Oxford University Press, 2013. E-book. Tradução livre do orginal: "*an arrangement whereby computing resources are provided on a flexible, location-independent basis that allows for rapid and seamless allocation of resources on demand.*"

56 VOIGT, Paul; BUSSCHE, Axel von dem (Eds.). *The EU General Data Protection Regulation (GDPR):* A Practical Guide. [s.l]: Springer, 2017. p. 20.

service and other information technology - *e.g.*, transfer of processing capacity.

The acts and activities involving data processing, in turn, are defined fundamentally in article 4 (2) of the Regulation. Due to the scope of these acts and activities, besides the complex business networks and contracts concerning companies that operate in the computer and internet segments, GDPR article 3 (1) directly reaches subjects - operators - at any phase or stage of personal data processing, whether it occurs within or outside the Union's territorial domain.

There are two preconditions for the recognition of a natural or legal person as a processor: (i) be a separate entity and with legal autonomy in relation to the controller; and (ii) process information on controller's behalf[57].

Given the agent's nature as a processor, the factual framework of the **processor-controller** interactions can be subsumed into three distinct situations: (i) both the processor and the controller have an establishment in the European Union; (ii) the processor has an establishment outside the European Union and is hired by a controller with an establishment in an european bloc member country; and (iii) the processor's establishment is located in european territory, unlike the controller's, located in a country that is not part of the European Union.

To what extent does the GDPR apply in these situations?

In the first occurence, the european rules govern both agents. In the situation indicated in item **ii**, despite the obviousness of the Regulation employment to the controller, the question may arise as to the regulation of the processor activity whose establishment is located outside the European Union's territorial limits.

Then, the GDPR cannot be immediately applicable to the processor in light of the establishment's location criterion of article 3 (1) unless the processing carried out on behalf of the controller relates to personal information of EU residents for the offering of goods or services or the monitoring of the behavior of the data subjects, in the form of article 3 (2). However, even in the case of direct non-applicability of the Regulation, it will be indirectly binding to the processor due to the contract, or other legal act, which rules apply to its data processing activity, as established in article 28 (3)[58].

An example of indirect application is illustrated by Voigt and Bussche. X is a german company that provides temporary personnel allocation and hiring services to large automobile manufacturers throughout Europe. Due to the fact that its employees pool constantly change, X stores data on application processes through a cloud computing service provider located in the United States, Y. Although Y doesn't address its activities to the European Union (in the form of Article 3 (2) of the Regulation), it shall observe the GDPR data protection parameters expressly provided for in the contract with X[59].

In the third occurrence, having the processor an establishment in the European Union territory, the Regulation applies to it directly in relation to the processing of personal data activity. In that respect, given the novelty of the legal discipline concerning the

57 Ibidem.

58 "Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:[...]." EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council.*cit.*

59 VOIGT, Paul; BUSSCHE, Axel von dem (Eds.). *The EU General Data Protection Regulation (GDPR), cit.* . p. 25.

processor, EJ Kindt raises questions about application of the Regulation to the controller — which determines the purposes and means of processing personal data — with an establishment outside the European Union: is the GDPR fully applicable including to the controller from the moment that he contracts a processor located in an EU Member State? Or only the rules suitable to the processor apply — *e. g.*, Art. 32 on data security?[60]

The most appropriate solution seems to be to apply the Regulation within the limits of legal provisions addressed to the processor and not extend it in its entirety to reach even companies based in countries outside European Union (e.g., US and Latin American countries) whose activity is not included in the terms of article 3 (1) and article 3 (2) of the GDPR. Otherwise, there would be a binding effect of European regulations to any controller on the globe that might decide to optimize its data processing and information technology services by hiring a Europe-based processor[61].

This, in fact, it could put the European information technology sector at a considerable competitive disadvantage on international market. Problems regarding jurisdiction and effectiveness in application of the Regulation sanctions by the courts also appear[62] since it would be a unilateral extension of the extraterritorial application of the law with debatable legitimacy[63], at least from the point of view of the creation of a 'global jurisdiction' not negotiated with third States[64].

The unilateral extension of the European legislation seems inconsistent with the current structure of the international system, based yet on different sovereignties and on the respect for the non-interference principle[65]. Any approach modification around a "universal" application of data protection standards would only be legitimate and legal, from an international point of view, through normative instruments adopted between States and the use of globally agreed mechanisms of international legal cooperation.

3.2. Location of the data processing activity

The article 3 (2) is a legal provision that leads to significant change in the European Data Protection Law, "one of the more important 'achievements' of the reform"[66]. The regulation shall address the processing of personal data of European Union residents, even if performed by a controller or processor **not established in the European territory**, when the processing operations relates to (i) the offering of goods or services to such data subjects, irrespective of a payment requirement; and (ii) the monitoring their behavior, as long as such behavior occurs in the European Union.

From the legislative policy point of view, the GDPR was based on the moderate

60 KINDT, E. J. Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation. *Computer Law and Security Review,* v. 32, n. 5, p. 737, 2016.

61 Ibidem, p. 737.

62 Ibidem, p.737 .

63 See DE HERT, P.; CZERNIAWSKI, M. Expanding the European data protection scope beyond territory: article 3 of the General Data Protection Regulation in its wider context. In: *International Data Privacy Law*, v. 6, n. 3, p. 240, 2016.

64 BERMAN, Paul Schiff, The Globalization of Jurisdiction.In: *University of Pennsylvania Law Review*, v. 151, n. 2, p. 311-545, 2002.

65 Regarding the issue of international system, see reflections about past, present and future which surround sovereignty concept: KALMO, Hent; SKINNER, Quentin (Ed.). *Sovereignty in Fragments:* The Past, Present and Future of a Contested Concept. Cambridge University Press, 2010. No plano do Direito Internacional Público, c.f. MELLO, Celso, *Curso de direito internacional público.* Rio de Janeiro : Renovar, 2004.

66 DE HERT, P.; CZERNIAWSKI, M. Expanding the European data protection scope beyond territory. *cit.* , p. 239. See also: BU-PASHA, S. Cross-border issues under EU data protection law with regards to personal data protection. In: *Information & Communications Technology Law*, v. 26, n. 3, p. 218, 2017.

destination approach[67]. It takes into account a specific targeting of activity of subjects — notably internet application providers — located in a third country. In fact, moderate destination approach establishes a closer link between the personal information processing agents' activity and the European Union Member States, resulting in greater legitimacy in prescriptive jurisdiction exercise (regulatory-substantive approach, therefore) and in setting its limits by European legislator[68].

It is worth mentioning that, in this sense, the CJEU ruling in Google Spain[69] case was paradigmatic in determining the scope of the European Union's personal data protection rules beyond the territorial limits of the common market and the intra-community domain. Based on this Court's precedent, the Directive 95/46/EC was considered applicable to the case, due to the existence of an agency or subsidiary established in a European Union Member State, and the advertisement contracting with "inextricable link" to the personal data processing activity by means of a search engine, such as Google Search, although the company directly responsible for the operations is based in a third country[70].

The article 3(2)(a) establishes within the scope of the Regulation the activity of processing personal data of European Union residents, conducted in the context of **the offering of goods or services directed to them, irrespective of whether a payment is required**. For the interpretation of the legislative text, it's relevant to check GDPR's Recital n. 23 and the parameters therein:

> [...] In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

As regards article 3(2)(b), the provision has expressly established that the **behavioral monitoring** is sufficient to determine the European Union Law's guidance, which means that GDPR rules are applicable, as long as data subjects' conduct takes place within the European Union's territory. The rule has wide application for companies that provide internet services, such as social networking applications, email and search engines, in other words, services that somehow monitor online activity of its users, especially for advertising purposes. That's the case of **behavioral advertising**, in which

67 About that, Uta Kohl remarks: "[...] States have at times, in the private law context, sought to avoid the extreme positions of the outright country-of-origin approach and country-of-destination approach by opting for the middle ground. This middle ground is occupied by a moderate country-of-destination approach, according to which only the States which have been specifically targeted by online activity enjoy regulatory competence. Although this approach avoids some of the theoretical and practical flaws of the extreme positions, it is far from perfect. Ultimately, it is beset by the same enforceability problem as any country-of-destination approach, with the added drawback that some States clearly affected by certain online activity have to abstain from regulation". KOHL, Uta. *Jurisdiction and the Internet:* regulatory competence over online activity. 1ª ed. Cambridge: Cambridge University Press, 2007. p. 25-26.

68 DE HERT, P.; CZERNIAWSKI, M. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. In: *International Data Privacy Law*, v. 6, n. 3, p. 239-243, 2016.

69 EUROPEAN UNION. Court of Justice of European Union. Grand Chamber. Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Luxembourg, 13/05/2014. Available at: <http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=EN>. Access in: 15/05/2018

70 Cf. BU-PASHA, S. Cross-border issues under EU data protection law with regards to personal data protection.In: *Information & Communications Technology Law*, v. 26, n. 3, p. 218, 2017.

cookies are used mainly[71].

One must, however, pay attention to the interpretation of this extraterritoriality legal provision. The Regulation considers that the collection and processing of **behavioral information** on internet shopping habits, browsing history, devices' mode of usage, and the consequent interests and preferences identification, leads to sensitive issues regarding privacy and data protection.

Having access to this information, users' profiles are drawn whom, classified after applying the predictive knowledge obtained with automated **profiling techniques**, have their lives more and more affected. The level of intrusiveness on life, behavior and personality development of users has intensified with the advance of the Internet of Things (IoT) implementations and the improvement and diffusion of artificial intelligence and algorithmic decision-making technologies[72].

Therefore, if these technologies are used by controllers established outside the European Union, in order to monitor online and offline behavior, and to process personal information of data subjects located in the european block, it's very likely that GDPR rules will apply.

In this regard, based on the meaning of article 3, paragraphs 1 and 2, one can consider some of the sectors that will potentially be affected in Brazil by the material and territorial scope of the Regulation: (i) Brazilian companies in the area of information technology that function as processors, processing personal information on behalf of controllers with establishment in European Union; (ii) companies engaged in activities related to tourism or the movement of individuals residing in Europe to Brazil (e.g., airlines and their websites), who are responsible for the processing of personal data; (iii) companies engaged in e-commerce that offers personalized services or Brazilian applications that uses tracking software on its EU resident-users and individual or collective automated profiling techniques.

3.3. International data transfer

In spite of GDPR's extraterritoriality elements and the effects that European legislation can produce in Brazilian legal system or possible conflicts of laws, there's still the need to observe the possible repercussions in relation to the **international transfer of personal data**, normatively regulated in articles 44 to 50 of the European Regulation.

71 "Behavioural advertising is advertising that is based on the observation of the behaviour of individuals over time. Behavioural advertising seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests. Whereas contextual advertising and segmented advertising use 'snap shots' of what data subjects view or do on a particular web site or known characteristics of the users, behavioural advertising potentially gives advertisers a very detailed picture of a data subject's online life, with many of the websites and specific pages they have viewed, how long they viewed certain articles or items, in which order, etc. [...] Most tracking and advertising technologies used to deliver behavioural advertising use some form of client-side processing. It uses information from the user's browser and terminal equipment. In particular, the main tracking technology used to monitor users on the Internet is based on "tracking cookies". Cookies provide a means to track user browsing over an extensive period of time and theoretically over different domains." (ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 2/2010 on online behavioural advertising . p. 5-6. Available at: <https://iapp.org/media/pdf/resource_center/wp171_OBA_06-2010.pdf>. Access in: 02/05/2018).

72 With regard to article 3(2)(b), it is worth mentioning Consideration n. 24 of the GDPR: "The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes".

In analytical terms, a cross-border transmission of personal data[73] involves not less than three processing operations: (i) the one that made the personal information available to the controller or processor (transferor) – *e. g.*, data collection; (ii) the transmission by the transferor of such information to a recipient based or resident in a foreign State; and (iii) the processing that the personal data recipient performs in his or her establishment located in a third country (*e. g.*, storage in a database)[74].

In the international data transfer legal framework, at least the presence of the controller or processor-**transferor** and the controller or processor-**recipient** of the data is required[75]. In the light of GDPR, if the direct applicability of European legislation is unequivocal in the transferor's situation, some uncertainty may remain with regard to the law applicable to the recipient. For this reason, and in order to safeguard against risks to the European data subjects' fundamental rights and freedoms, since the Directive 95/46/EC came into force, it was adopted the model for transferring data to a third country that imposes prior verification and recognition of the destination country or international organization's **adequate level of protection**[76] (article 45).

In essence, the rule is anchored in a **geographical model** of data flows across national boundaries regulation, as it "aims to protect against risks posed by the country or location to which the data are to be transferred."[77] The European Commission is competent for analyzing the third country's level of protection and issuing an **adequacy decision** based on the criteria set out in article 45 (2) of the Regulation. With such decision - subject to a four-year review -, prior and specific authorization for the international data transfer is not required.

In addition to the adequacy decision, the cross-border transfer of personal data may also be grounded (i) whether the third country or the international organization presents **appropriate safeguards** (article 46), or (ii) the competent data protection authority manufacture **binding corporate rules** (article 47), which will be observed by groups of undertakings or multinational economic groups in the indispensable international flows of information within their organizational structure. One should notice, however, the derogations of the above rules for specific international data transfer situations expressly provided in article 49 of the Regulation. That's the case, for example, of the existence of a contract between a controller in the European Union and a processor established in a non-member country of the European Union, which does not have the European Commission's recognition of the adequate level of protection or guarantees (article 49 (1) (c)).

Besides the GDPR's discipline regarding the cross-border data transfers being based on the **geographical model**, rules inspired by the organizational regulation model were included as well. That is because it proposes to itself to manage risks generated

73 About this subject, see paper produced by IRIS with comments on Bill no. 5.276/2016: INSTITUTE FOR RESEARCH ON INTERNET & SOCIETY. Policy Paper - Transborder Data Flows and Bill n. 5.276/16: Some Remarks for the Brazilian legislative process. Belo Horizonte: IRIS, 2017. Available at: <http://irisbh.com.br/wp-content/uploads/2017/05/Policy-Papper-Ingles.pdf>. Access in: 20/05/2018.

74 GIMÉNEZ, Alfonso Ortega. *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*. Madrid: Agencia Española de Protección de Datos, 2015. p. 61; BU-PASHA, S. Cross-border issues under EU data protection law with regards to personal data protection.*cit*, p. 214.

75 BU-PASHA, S. Cross-border issues under EU data protection law with regards to personal data protection. *cit.*, p. 214.

76 Cf. PIRODDI, Paola. I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati. In: RESTA, Giorgio; ZENO-ZENCOVICH, Vincezo (Coord.). La protezione transazionale dei dati personali. Roma: Roma-Tre Press, 2016. p. 198-199.

77 KUNER, Christopher. *Regulation of transborder data flows under data protection and privacy law:* past, present and future. OECD Digital Economy Papers, n. 187, OECD Publishing, 2011. p. 20.

by the entity that will receive the transferred personal information. In this context, the European legislator sought to promote **organizational accountability**, to be achieved through the creation by personal data processing agents of comprehensive privacy management programs. These programs should, for instance, provide for the designation of a data protection officer (article 37), issue a data protection impact assessment (article 35), implement best practice rules, codes of conduct (article 40), corporate standards, etc, internal and/or external applicable guidelines, in accordance with the Regulation, throughout the processing information lifecycle, regardless of the place or jurisdiction in which it is.

The possible fields above mentioned are affected by the immediate implementation of the new European Regulation. There's still no decision that recognizes Brazil as a third country with a level of protection adequate to the European Union's standards of privacy and personal data protection. Then, a series of possibilities are opened for Brazilian public and private entities to be reached by measures related to the international personal data transfer in which the transferor is established in the European territory.

4. Comparative analysis of the impacts of the Regulation (EU) n. 2016/679 on the Brazilian and Argentinian laws

It's unquestionable that the most significant change in the European data privacy regulatory landscape stems from GDPR's expanded prescriptive jurisdiction. Its rules apply to all activities of companies involved in personal data processing of data subjects residents in the European Union Member States, irrespective of the company's headquarters location. Previously, the territorial scope of the Directive was ambiguous and referred to the data processing "in the context of an establishment".

The GDPR innovates by reinforcing and clarifying its scope in a very objective way: it will apply to personal data processing by controllers and processors in the European Union, regardless of whether the processing takes place in the European Union or not. The GDPR also applies to personal data processing of data subjects in the European Union by a controller or processor not established in the Union, where activities concern the offering of goods or services to European citizens and the monitoring of users' behavior in the European Union.

The scenario of uncertainty as to the compatibility between the application of the GDPR and national regulations on the subject transcends the European territory, as one can observe from the very principles of extraterritorial application of its legal provisions. The pursuit of market globalization of digital services in the 21st century corroborates the design of an international system increasingly interconnected by companies and users that operate in several markets, subject to different jurisdictions. In the context of GDPR's extraterritorial application, from one of the most important global markets for digital services provision and consumption, it is natural that other economies also seek to adapt itself to the current legal regime in order to maintain their competitiveness on international commerce.

Starting from this situation, the following lines present some parallels between

the GPDR and the Argentinian and Brazilian legislations, in order to contextualize the current state of the art of the discussion on personal data protection in the Mercosur domain and between Latin American countries as a whole.

4.1. Argentina

For nearly twenty years, since 2000, Argentina has had a Data Protection Law[78]. This legislation also derives from a specific constitutional provision on the subject, which determines, in its article 43, that:

> Any person shall file this action to obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data[79].

Although Argentina has been considered the first Latin American country with "adequate" levels of protection by the European Union through the recommendations of the Article 29 Working Party, several initiatives to update the Law were under discussion in the National Congress, among them a preliminary draft for a data protection regulation, presented by the National Data Protection Agency.

The preliminary draft was subject to public consultation by the equivalent of the Argentine Ministry of Justice, with participation of the public at large, academic institutions, companies, individuals and civil rights associations during the proposed period of reflection, as occurred with the Internet Bill of Rights and its regulatory decree in Brazil. The purpose of this consultation was to align the Argentine data protection law with the GDPR.

Current law has several areas that cover, in a conflicting or different way, the main points of the GDPR. One of such issues is data subject's information cross-border transfer to countries with inadequate levels of data protection. The Argentine law in force maintains excessive exceptions to the general rule that personal information could not be transferred to those countries.

According to Section 12 of the legislation in force, it's forbidden to transfer any type of personal information to countries or international entities that do not offer adequate levels of protection, except in cases of international legal assistance; in the exchange of medical information, whether for patients' individual treatment or in epidemiological research; in the trading of securities and in bank transfers; by means of the international treaties framework of which Argentina is a signatory; and when the transfer is carried out for international assistance purposes between intelligence agencies in the fight against crime, terrorism, and drug trafficking[80].

78 ARGENTINA. *Ley 25.326: Ley de Protección de los Datos Personales.* 30 de Outubro de 2000. Available at: <http://www.oas.org/juridico/pdfs/arg_ley25326.pdf>. Access in: 16/05/2018.

79 Translated from: "Artículo 43. Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos." ARGENTINA. *Constitución de la Nación Argentina.* Available at: <http://www.oas.org/juridico/mla/sp/arg/sp_arg-int-text-const.html>. Access in: 17/05/2018.

80 ARGENTINA. *Ley 25.326: Ley de Protección de los Datos Personales.* 30 de Outubro de 2000. Available at: <http://www.oas.org/juridico/pdfs/arg_ley25326.pdf>. Access in: 16/05/2018.

For the exceptions of article 23 of the Preliminary Draft on the Data Protection Law[81], data subject's consent for the international transfer would not be necessary: when the transfer is provided for by law or treaty; when such transfer is necessary for prevention or medical diagnosis, as well as for healthcare services management; when international transfer is made to **any company in the same economic group** as the controller's, provided that personal data are used for purposes that are not incompatible with those that originated their collection; when international transfer is necessary for performance of a contract concluded in the unambiguous interests of the data subject, the controller and a third party; when international transfer is necessary or legally required to safeguard a public interest, or to the public and justice administration; when the international transfer is necessary for recognition, exercise or defense of a right in judicial procedures; when international transfer is necessary to maintain or enforce a legal relationship between controller and data subject.

That is to say, despite Argentina's vanguard in the years 2000, regarding protection of personal data and adequacy of its legislative regime to the European guidelines that were in force at that time, the current system of consent exceptions for the international data transfer can lead to conflicts with the GDPR in the light of the location of establishment criterion of article 3 (1) of the Regulation. After all, in integrated digital economy environments around the globe, if there are online \ Argentinian service providers whose activities involve international data transfer of european citizens, or who are processors with establishment in Argentina but are hired by a controller with establishment in a country member of the European Union, for example, the GDPR rules also apply to such specific cases. This would mean, among other things, different exception regimes for the applicability of the European legislation, and not Argentinian, in cases such as these.

In this context, the Preliminary Draft also introduces new methods of determining whether an entity or certain data processing is subject to Argentine legislation, very similar to the criteria found in the GDPR. Argentina's current data protection regulation applies to all legal persons who perform the processing of personal data in the country, relevant to any action that is considered personal data processing within the Argentinian territory. If a single isolated act related to personal data (*e.g.*, data collection or transfer) occurs in Argentina, but the rest of the processing is performed abroad, Argentinian law applies as well to this isolated conduct[82].

In this regard, it is important to note that the focus of the 2000 legislation was, among other things, the introduction of basic concepts the personal data protection in the Argentinian legal system. The innovations proposed by the Preliminary Draft surpass this subject matter and, as a consequence, reflect more current concerns, such as the GDPR, as the extension of its scope:

> Article 4 - The rules of this law shall apply when:
>
> a) The controller is located in the national territory, even when data processing occurs outside the said territory;
>
> (b) the person responsible for the processing is not established in national territory but in a place

81 According to article 23 and following. ARGENTINA. *Ley 25.326: Ley de Protección de los Datos Personales.* 30 de Outubro de 2000. Available at: <http://www.oas.org/juridico/pdfs/arg_ley25326.pdf>. Access in: 16/05/2018.

82 D'AURO, Maximiliano; VARELA, Inés de Achaval. Data protection in Argentina: overview. *Association of Corporate Council's Multi-Jurisdictional Guide 2014/15.* P. 01. Available at: <http://www.ebv.com.ar/images/publicaciones/trdatap.pdf>. Access in: 16/05/2018.

where national law is applied under international law;

c) The data processing of owners residing in the Argentine Republic is carried out by a controller that is not established in the national territory and the activities of this processing are related to the offering of goods or services to the data subjects in the Argentine Republic, or with the monitoring of their acts, behavior or interests[83].

If approved in this fashion, the Preliminary Draft establishes mechanisms of verification of its applicability very similar to those of the GDPR, analyzed in the previous item of this study.

4.2. Brazil

The protection of personal data in Brazil is close to the European model, since it recognizes its status as a fundamental right, unfolded from the privacy protection[84]. However, Brazilian legal system still has a fragmentary and insufficient regulation. There is legislation - general or special - that regulates comprehensively the personal data processing activity performed by public and private entities, whether in an interconnected environment in digital networks or not.

Thus, one can notice that there is a significant difference in Brazil's protection of personal data in relation to the Argentinian law.

To some extent, the reason for the disparity between the systems of these two countries is found in the text of their respective Constitutions[85]. The content of article 43 of the Constitution of the Argentinian Nation, described in the previous item, deals with *habeas data* and giving to it multiple functions in order to protect the individual's informational self-determination[86].

On the other hand, in the 1988 Constitution of the Republic, although the right to privacy was enshrined in article 5, items X and XI, it was in item LXXII that the constitutional legislator directly approached personal information and its legal status, expressly legislating about the *habeas data* safeguard. It, however, has a very restricted legal function if confronted with the homonymous Argentinian legal mechanism.

The *habeas data* constitutional action in Brazilian legal system is intended to guarantee to citizens the power to access and rectify their personal data that may be stored in governmental records and public databases. As a constitutional remedy, in fact, it is not an instrument for achieving self-determination on your own information due to its very limited protection scope[87]. Considering that its genesis is associated with the

83 ARGENTINA. *Anteproyecto de Ley de Protección de los Datos Personales.* 2017. Available at: <https://www.justicia2020.gob.ar/wp-content/uploads/2017/02/Anteproyecto-de-ley-PDP.pdf>. Access in: 17/05/2018.

84 On that line, see: DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006. p. 323-326; LEONARDI, Marcel. *Tutela da privacidade na internet.* São Paulo: Saraiva, 2011. p. 67-90; MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 27-37; MORAES, Maria Celina Bodin de. Ampliando os direitos da personalidade. In: MORAES, Maria Celina Bodin de.(org.)*Na medida da pessoa humana: estudos de direito civil-constitucional.* Rio de Janeiro: Renovar, 2010. p. 140-145; SARLET, Ingo W.; MARINONI, Luiz G.; MITIDERO, Daniel. *Curso de Direito Constitucional.* São Paulo: Revista dos Tribunais, 2012. p. 418.

85 Cf. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais, cit.*p. 326 et seq.

86 Ibidem, p. 349. Regarding the *habeas data* in Argentina, cf. BÁZAN, Víctor. El Hábeas Data Como Medio de Tutela del Derecho Fundamental a la Autodeterminación Informativa. In: *Revista de Direito Público,* Porto Alegre-Brasília, n. 38, p. 205-208, mar./abr. 2011.

87 According to MENDES, Gilmar. *Curso de Direito Constitucional.* 12.ed. São Paulo: Saraiva, 2017, pp.459-60, "a free reflection on the subject must point out that the target of habeas data protection only in part transpose current preoccupation with self determination about personal data developed in many constitutional orders" (author's translation from Portuguese). The author has caveats, nevertheless,

context of the end of the Brazilian dictatorial regime, in which was adopted the "usage by public authorities of entirely false or error-containing data for political purposes and with serious damage to individual rights"[88], the *habeas data* has limited and peculiar role in the national legal system. These characteristics were observed in the regulation of the procedure by Law n. 9.507/1997. Likewise, the nature of the information accessed is very specific: as an instrument of protection of personality rights via constitutional remedy, *habeas data* reaches only data to be known or rectified, referring to the person of the petitioner, and devoid of a generic character[89]. In this sense of analysis, it presupposes a kind of 'contained' data self-determination.

In 1990, under the influence of the US Fair Credit Reporting Act, the **Consumer Protection Code (CDC)** sought to protect the vulnerable person in the consumer market from the databases created, in particular with credit protection scope, as can be seen in the Arts. 43 and 44[90]. In fact, the CDC was the first special law that, in infra-constitutional terms, disciplined the personal data processing activity. Nevertheless, the statutory approach of balancing the information collection on consumer's breach of contract for credit[91] purposes has reduced the application scope of its rules.

Still, a series of precepts provided in the CDC specify structuring norms of personal data protection, in order to avoid the widespread misunderstanding that there is no legal basis in Brazil for this field: (i) the possibility of access to stored consumer information in databases (access principle); (ii) the data must be objective, clear, true and in easy-to-understand language (data quality principle); (iii) the need to communicate the formation of consumer database(s) (transparency principle); (iv) 5 (five) years limit for the storage of negative information (necessity principle)[92].

With the Law nº 12.414/2011 enactment, the consumer databases regulation was supplemented with the processing of the compliance registration[93]. The legislation aims to regulate the formation of consumer **credit records**, in which the databases are regularly fed with "positive information"[94]. This is an important law for the data subject's protection before credit scoring companies, which process this amount of data to assess in a personalized way the risk degree in credit granting.

---

that the constitutional text does not leave space for doubt that the institute protects the person not only regarding public character data banks managed by government institutions directly; it also is addressed to safeguard the person in regard to private managed databanks of public character data.

88 DALLARI, Dalmo de Abreu. O *habeas data* no sistema jurídico brasileiro. In: *Revista da Faculdade de Direito da Universidade de São Paulo*, São Paulo, v. 97, p. 242, 2002.

89 Cf. Gilmar F. MENDES, *Curso de Direito Constitucional.* 12.ed. cit., p.460.

90 Article 43. Consumer, without prevention of dispositions of Article 86, will have access to informations which exist in registers, records and personal data and of consumption data stored about him, as well as about its respective sources; [...] Article 44. Public organs of consumer protection will keep updated registers of fundamented complaints against product and services suppliers, having the duty to publish it openly and annually. The disclosing will point if the complaint was attended or not by the supplier. BRASIL. Law no. 8.078, de 11 de setembro de 1990. *Código de Defesa do Consumidor.* Available at: <http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>. Access in: 21/05/2018.

91 DONEDA, Danilo. *A proteção dos dados pessoais nas relações de consumo:* para além da informação creditícia. Brasília: SDE/DPDC, 2010. p. 11.

92 Cf. MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 142-143.

93 BRASIL. *Law no. 12.414*, of 9 of june of 2011. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Access in: 21/05/2018.

94 To Leonardo Roscoe Bessa, "even though under the exclusively economic-financial optic it's possible to explain that not only the credit history of the history of credit of the loan's candidate but also other information are aids to better define the person's profile and consequently to make possible a more accurate risk analysis, avoiding defaults and, at the same time, the possibility of a lower interest tax, the juridical focus points in another way: the one of the need to delineate and restrict the number, quality and way of positive information by credit protection databanks. The raise of personal information may represent offense to human dignity, to personality rights (privacy and honor)" (author's translation from Portuguese). (BESSA, Leonardo Roscoe. *Cadastro positivo: comentários à Lei 12.414, de 09 de julho de 2011*. São Paulo: Revista dos Tribunais, 2011. p. 45),

The 2002 Civil Code, on the other hand, assigned only the article 21[95] to the discipline of the right to privacy, completely ignoring the notion of personal data protection, its restrictions against other rights and freedoms (*e. g.*, freedom of expression and communication) , and all the complexity that characterizes the contemporary information society, hyperconnected, with increasingly widespread access to information and communication technologies. In the words of Anderson Schreiber, "[the] mere observation of everyday life reveals that, contrary to the strong assertion of the art. 21, the human person's private life is systematically violated"[96].

As to the Law n. 12.527 of 2011, the **Access of Information Act (LAI)**[97], is applicable to organs and entities of direct and indirect public administration. Aiming the promotion of a transparent public administration and giving certain concreteness to Brazilians' right to information, LAI plays an important role on personal data protection field. In addition to designing of the concept of personal information in almost the same terms as the European law (article 4, IV)[98], it provides that the data subject will have access to the information that is relevant to him, and that privacy and protection of personal data confines access to information by third parties (articles 6, 31 and 32)[99].

In addition to this legal framework, the right to protection of personal data was also expressly included in the text of the Law n. 12.965 of 2014, the **Internet Bill of Rights**[100]. The Internet Bill of Rights' provisions are applicable to any operation related to the collection, storage, retention, processing and communication of personal data by internet access providers and internet application providers, when at least one of these actions occurs in Brazil. Recognized as a pioneering legislation in the world and a multistakeholderism example that characterizes internet governance, the Bill established in its article 3, III, the elaboration of a specific data protection law, therefore, a matter susceptible to the legislative activity.

In relation to the provisions that regulate the **international data transfer** in Brazil, the data protection offered by Brazil's Internet Bill of Rights is still limited when compared to the complex system provided by the GDPR[101]. Draft Bill n. 5.276, sent to the National Congress by the Presidency of the Republic on May 13, 2016, is one of the main draft bills of personal data protection currently under discussion in the National

95 "Art. 21, Civil Code: Private life of natural person is inviolable, and the judge, from request of the concerned party, will adopt necessary measures to stop or make cease action contrary to that norm" (author's translation from Portuguese). BRASIL. Law no. 10.406, de 10 de janeiro de 2002.

96 SCHREIBER, Anderson. *Direito da personalidade.* 2. ed. rev. e atual. São Paulo: Atlas, 2013, p. 142-143.

97 **BRASIL. Law no. 12.527, de 18 de novembro de 2011.** *Lei de Acesso à Informação.* Available at: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Access in: 21/05/2018.

98 Article 4, Access of Information Act: "For these law's applications, it's considered: [...] IV - personal information: that related to the identified or identifiable natural person" (author's translation from Portuguese).

99 Article 6, LAI: "It is up to the public power entities, complying with specific applicable norms and procedures, to ensure: [...] III - secret and personal information protection, ensuring its availability, authenticity, integrity and eventual restriction of access. [...] Art. 31. Treatment of personal information must be made in a transparent way, with respect to intimacy, private life, honor and image of people, as well as to the liberties and individual guarantees. Art. 32. Are illicit attitudes, which entice public or military agent liability: [...] V - to spread or allow the spreading or accessing or allow improper access to secret or personal information". (author's translation from Portuguese)

100 **Article 3, Brazil's Internet Bill of Rights:** The discipline of internet use in Brazil has the following principles: II - privacy protection; III - personal data protection, on the form of the law [...] Art. 8. The guarantee of right to privacy and freedom of expression in communications is a condition for full exercise of right to access the internet. [...]; Article 11. In any collect, storage, keeping and treatment of registers, of personal data or communications by internet connection and application providers in which at least one of those acts occur in national lands, must necessarily be respected Brazilian legislation and the rights to privacy, data protection and private communications and registers secrecy. (author's translation from Portuguese). BRASIL. Law no. 12.956, de 23 de abril de 2014. *Marco Civil da Internet.* Available at: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Access in: 21/05/2018.

101 This subject is approached in detail, especially on what comes to bills on National Congress, in study realized by IRIS: INSTITUTE FOR RESEARCH ON INTERNET & SOCIETY. Policy Paper - Transborder Data Flows and Bill n. 5.276/16:Some Remarks for the Brazilian legislative process. Belo Horizonte: IRIS, 2017. Available at: <http://irisbh.com.br/wp-content/uploads/2017/05/Policy-Papper-Ingles.pdf>. Access in: 20/05/2018.

Congress and has a complete chapter to regulate the international transfers.

Under the Executive Branch, the Preliminary Draft Bill on Data Protection at the time followed the public consultation model on which the Internet Bill of Rights was based. The text of the Ministry of Justice has been made available online and open to any internet user's comments. In this way, as in the process of elaborating the Internet Bill of Rights, the debate between multiple actors was made possible: members of civil society, academia, government, regulatory and industry sectors. In general, the Draft Bill deals addresses issues such as the users' rights and the personal data processing, collection and storage.

The analysis of Draft Bill n. 5.276/2016, especially with regard to the provisions related to international data transfer, reveals strong influence of the European model of data protection on future normative discipline in Brazil. The European model adopts an **essentially geographic criterion** to define situations in which international data transfer is permitted or not. In an increasingly globalized world, regulations based on territorial criteria prove to be problematic and obsolete, as geography becomes less and less important in technology and business.

The Institute of Research on Internet and Society has already positioned to recommend the adoption of an **organizational model** for these situations[102], not a geographic one, capable of transcending the States' borders, so that the level of data protection accompanies the informations to wherever it flows as diligence duties are assigned to the collecting entity and not to the State to which the data will be transferred. The organizational model would be fully compatible and consistent with article 11 of Brazil's Internet Bill of Rights, which demands the application of the brazilian law to the data collected in Brazil, and would not result in jurisdictional obstacles due to the fact that the data were transferred to other jurisdictions.

The organizational model, as recommended by IRIS, has the advantage of circumventing these problems by forcing the exporting entities to maintain continuous protection of personal data transferred to other organizations, regardless of their geographic location. The protection would take place through the binding contractual clauses between data exporter and importer, as well as the joint liability between them[103].

Article 33 of the Draft Bill n. 5.276/2016, if approved, will establish that an international transfer would only be permitted if provided to countries with equivalent levels of data protection, or when expressly consented by data subjects, after specific information on the operation's international nature, and the risks involved.

The Draft Bill n. 5.276/2016 is not the only one that currently addresses data protection issues in Brazil. Other legislative proposals are underway in the National Congress: Draft Bill n. 4.060/2012, authored by Deputy Milton Monti, and Draft Bill n. 181/2014, authored by Senator Vital do Rego. In July 2016, due to a proposal from

102 INSTITUTE FOR RESEARCH ON INTERNET & SOCIETY. Policy Paper - Transborder Data Flows and Bill n. 5.276/16:Some Remarks for the Brazilian legislative process. Belo Horizonte: IRIS, 2017. Available at: <http://irisbh.com.br/wp-content/uploads/2017/05/Policy-Papper-Ingles.pdf>. Access in: 20/05/2018.

103 In practice, the organizational model is more centered in strengthening the axes of liability shared among economic agents active on the markets of digital economy, computing, informatics and internet in general; in them, data protection authorities would have a much more important regulatory and adequacy role, remaining to the import and export companies the primary duty to preserve the integrity of data protected and processed in the transference chain. The geographic framework, on the other hand, may suffer from risks of degrading its own regulatory quality, considering that diligence duties are attributed primarily to the State to which the data will be transferred (destination country, receiving country), and not to the juridic or natural person that collects them. About variations and model applications: INSTITUTE FOR RESEARCH ON INTERNET & SOCIETY. Policy Paper - Transborder Data Flows and Bill n. 5.276/16, cit., p.33 ss.

the Deputy Alexandre Leite, the Draft Bill n. 5276/2016 was joined to the Draft Bill n. 4.060/2012, which helped to restore the uncertainty about the basic text's approval.

It is important to note that Draft Bill n. 5276/2016 is the one that approximates the most of the legislative design envisioned by the GDPR. In many ways, this proposal is the best reference to start the debate in the country. The PL 4060/2012, in turn, is aligned with the interests of digital marketing conglomerates, with the goal of facilitating access to consumer data for marketing purposes and leveraging business models and offering products and services in this area. Finally, PL 181/2014 is no longer as comprehensive as Draft Bill 5276/2016, nor as restrictive as PL 4060/2012.

5. Conclusions and recommendations

The GDPR is not only a law in force for the European Union; its reach is undoubtedly global[104]. Active economic agents in markets of countries that interact with the European Union or who wish to enter the contemporary digital economy new market segments should be concerned about possible alignments of their countries' data protection laws with the GDPR, binding since May 25, 2018.

In this scenario, compliance concerns with the new parameters being presented by GDPR lead actors from different areas of information economy to adopt legal and technical measures in personal data protection field. Among relevant actions, there may be included review of contracts and agreements, updating terms of use and privacy policies around the world, as well as adopting new corporate structures for effective data protection.

Accordance with the new regulatory provisions established by the new European Regulation should be the main focus of companies or international organizations recipients of personal information that comes from the European Union, controllers and processors to whom the Regulation applies, in the form of its article 3.

In the same way, based on the considerations regarding the GDPR extraterritorial repercussions, as a background for the comparative analysis of Argentinian and Brazilian laws, the Institute for Research on Internet and Society understands that the brazilian State, notably through its executive and legislative branches, must adopt measures and address domestic practices that align itself with a goal of maximizing the protection of personal data, among which:

(i) commit to the approval of a general law on the protection of personal data that comprehend the information processing activity of public and private entities and based on the risk generated to natural persons, with adequate guarantees for the protection of data subjects' fundamental rights and freedoms, as seen in the GPDR;

(ii) to accede to the Convention n. 108 of the Council of Europe, the most significant international treaty on privacy protection in the context of cross-border data flows[105], which has recently been updated to the new demands of data-driven technologies and

104 MADGE, Robert. *GDPR's global scope:* the long story. Available at: <https://medium.com/mydata/does-the-gdpr-apply-in-the-us-c670702faf7f>. Access in: 14/05/2018.

105 COUNCIL OF EUROPE. *Enhancing data protection globally:* Council of Europe updates its landmark convention, 2018. Available at: <https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=09000016808ac976>. Access in: 07/06/2018.

allows accessions by non-member States of the Council of Europe[106];

(iii) to develop and adopt public policies, governmental actions, as well as educational programs involving the executive, legislative, and judiciary branches, academia, industry sectors, civil society organizations, and citizens, to disseminate knowledge and practice around data protection and, hopefully, the future Law.

These recommendations are based on internal and external reasons. The creation of a law regulating the personal data processing activity in Brazil, in addition to meeting the 1988 Constitution of The Republic imperative and the Internet Bill of Rights' principles and guidelines regarding the right to privacy and data protection, will also maintain the country's strategic position in relation to the European Union Member States and within the Mercosur block. As seen, Argentina already discusses the reform of its legislation to adapt to the GDPR and to the digital economy new context, and Brazil should integrate itself in this debate and promote measures more in line with the position that it occupies between the great economies of the globe.

106 See procedure provided on Article 23 of the Convention - Accession by non-member States:After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee. 2 In respect of any acceding State, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

6. Bibliographic References

6.1. Books and book chapters

BESSA, Leonardo Roscoe. *Cadastro positivo***:** comentários à Lei 12.414, de 09 de julho de 2011. São Paulo: Revista dos Tribunais, 2011.

EUROPEAN COUNCIL. Handbook on European data protection law, 2014. Available at: <https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf>. Access in 10/05/2018.

DONEDA, Danilo. *A proteção dos dados pessoais nas relações de consumo:* para além da informação creditícia. Brasília: SDE/DPDC, 2010.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

GIMÉNEZ, Alfonso Ortega. *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita.* Madrid: Agencia Española de Protección de Datos, 2015.

KALMO, Hent; SKINNER, Quentin (Ed.). *Sovereignty in Fragments:* The Past, Present and Future of a Contested Concept. Cambridge University Press, 2010.

KAPLAN, Harvey. COWING, Mark. EGLI, Gabriel. *A Primer for Data-Protection Principles in the European Union.* Culture Clash! Data Protection, Freedom of Information and Discovery, 2009.

KOHL, Uta. *Jurisdiction and the Internet:* regulatory competence over online activity. 1ª ed. Cambridge: Cambridge University Press, 2007.

LEONARDI, Marcel. *Tutela da privacidade na internet.* São Paulo: Saraiva, 2011.

MELLO, Celso, *Curso de direito internacional público.* Rio de Janeiro : Renovar, 2004.

MENDES, Gilmar. Curso de Direito Constitucional. 12.ed. São Paulo: Saraiva, 2017

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MILLARD, Christopher (Ed.). *Cloud Computing Law*. Oxford: Oxford University Press, 2013. E-book.

MORAES, Maria Celina Bodin de. Ampliando os direitos da personalidade. In: _____. *Na medida da pessoa humana:* estudos de direito civil-constitucional. Rio de Janeiro: Renovar, 2010. p. 121-148.

PIRODDI, Paola. I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati. In: RESTA, Giorgio; ZENO-ZENCOVICH, Vincezo (Coord.). *La protezione transazionale dei dati personali.* Roma: Roma-Tre Press, 2016. p. 169-238.

SARLET, Ingo W.; MARINONI, Luiz G.; MITIDERO, Daniel. *Curso de Direito Constitucional.* São Paulo: Revista dos Tribunais, 2012.

SCHREIBER, Anderson. *Direito da personalidade.* 2. ed. rev. e atual. São Paulo: Atlas, 2013.

VOIGT, Paul; BUSSCHE, Axel von dem (Eds.). *The EU General Data Protection Regulation (GDPR):* A Practical Guide. [s.l]: Springer, 2017.

6.2. Scientific papers

ALBRECHT, Jan. P. How the GDPR Will Change the World. *European Data Protection Law Review*, v. 2, n. 3, p. 287–289, 2016.

BÁZAN, Víctor. El Hábeas Data Como Medio de Tutela del Derecho Fundamental a la Autodeterminación Informativa. *Revista de Direito Público*, Porto Alegre-Brasília, n. 38, p. 191-231, mar./abr. 2011.

BERMAN, Paul Schiff, The Globalization of Jurisdiction, *University of Pennsylvania Law Review*, v. 151, n. 2, p. 311-545, 2002.

BIONI, Bruno. *Xeque-Mate*: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. Grupo de Estudos em Políticas Públicas em Acesso à Informação da USP – GPOPAI, São Paulo, 2015.

BU-PASHA, S. Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law*, v. 26, n. 3, p. 213–228, 2017.

BYGRAVE, Lee. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology*, volume 6, pp. 247–284, 1998.

DALLARI, Dalmo de Abreu. O *habeas data* no sistema jurídico brasileiro. *Revista da Faculdade de Direito da Universidade de São Paulo*, São Paulo, v. 97, p. 239-253, 2002.

DE HERT, P.; CZERNIAWSKI, M. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law*, v. 6, n. 3, p. 230–243, 2016.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico,* Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

D'AURO, Maximiliano; VARELA, Inés de Achaval. Data protection in Argentina: overview. *Association of Corporate Council's Multi-Jurisdictional Guide 2014/15.* Available at: <http://www.ebv.com.ar/images/publicaciones/trdatap.pdf>. Access in: 16/05/2018.

GUIDI, Guilherme. *Modelos regulatórios para proteção de dados pessoais.* Available at: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Access in: 30/04/2018.

INSTITUTE FOR RESEARCH ON INTERNET & SOCIETY. *Policy Paper - Transborder Data Flows and Bill n. 5.276/16:Some Remarks for the Brazilian legislative process.* Belo Horizonte: IRIS, 2017. Available at: <http://irisbh.com.br/wp-content/uploads/2017/05/Policy-Papper-Ingles.pdf>. Access in: 20/05/2018.

JONES, Meg. The right to a human in the loop: Political constructions of computer automation and personhood. *Social Studies of Science***,** v. 47, n. 2, p. 216 - 239, 2017.

KINDT, E. J. Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation. *Computer Law and Security Review*, v. 32, n. 5, p. 729–748, 2016.

KUNER, Christopher. *Regulation of transborder data flows under data protection and privacy law*: past, present and future. OECD Digital Economy Papers, n. 187, OECD Publishing, 2011.

SELBST, Andrew; POWLES, Julia. Meaningful information and the right to explanation. *International Data Privacy Law*, v. 7, n. 4, p. 233–242, 2017.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, v. 7, n. 2, p. 76-99, 2017.

6.3. Legislation

ARGENTINA. *Anteproyecto de Ley de Protección de los Datos Personales.* 2017. Available at: <https://www.justicia2020.gob.ar/wp-content/uploads/2017/02/Anteproyecto-de-ley-PDP.pdf>. Access in: 17/05/2018.

ARGENTINA. *Constitución de la Nación Argentina.* Available at: <http://www.oas.org/juridico/mla/sp/arg/sp_arg-int-text-const.html>. Access in: 17/05/2018.

ARGENTINA. *Ley 25.326: Ley de Protección de los Datos Personales.* 30 de Outubro de 2000. Available at: <http://www.oas.org/juridico/pdfs/arg_ley25326.pdf>. Access in: 16/05/2018.

BRASIL. Lei 10.406, de 10 de janeiro de 2002. *Código Civil.* Available at: <http://www.planalto.gov.br/CCivil_03/Leis/2002/L10406.htm>. Access in: 21/05/2018.

BRASIL. *Law no. 12.414,* de 9 de junho de 2011. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Access in: 21/05/2018.

BRASIL. Law no. 12.527, de 18 de novembro de 2011. *Lei de Acesso à Informação.* Available at: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Access in: 21/05/2018.

BRASIL. Law no. 12.956, de 23 de abril de 2014. *Marco Civil da Internet.* Available at: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Access in: 21/05/2018.

BRASIL. Law no. 8.078, 11 de setembro de 1990. *Código de Defesa do Consumidor.* Available at: <http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>. Access in: 21/05/2018.

EUROPEAN COUNCIL. *European Convention on Human Rights.* 1950. Available at: <https://www.echr.coe.int/Documents/Convention_ENG.pdf> Access in: 05/05/2018.

EUROPEAN COUNCIL. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Strasbourg, 1981. Available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Access in: 02/05/2018;

EUROPEAN UNION. Directive 95/46/EC of the European Parliament and of the Council

of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *of the European Union*, Strasbourg, 23/11/1995. Available at: <https://eur-lex.europa.eu/eli/dir/1995/46/oj>. Access in: 15/05/2018.

EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, Strasbourg, 04/05/2016. Available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679>. Access in: 16/04/2018.

6.4. Court decisions

EUROPEAN UNION. European Court of Human Rights, *Case of Leander v. Sweden, of 26 of march 1987, Application no. 9248/81.* Available at: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57519%22]}>. Access in: 10/05/2018;

_____.European Court of Human Rights, *Case of Marper v. United Kingdom of 4 december 2008, Applications nos. 30562/04 and 30566/04.* Available at: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]}> Access in 11/05/2018.

_____. European Court of Human Rights. *Case of Klass and others v. Germany of 6 september 1978, Application no. 5029/71*. Available at:<https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}>. Access in: 05/05/2018;

_____. European Court of Human Rights. *Case of Uzun v. Germany of 2 september 2010. Application no. 35623/05*. Available at: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-100293%22]}>. Access in: 10/05/2018.

_____. European Court of Human Rights. *Case of Malone v. The United Kingdom* of 2 august 1984. Application no. 8691/79. Available at: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57533%22]}>. Access in: 12/05/2018;

_____. European Court of Human Rights. *Case of Copland v. The United Kingdom* of 3 of april 2007. Application no. 62617/00. Available at: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-79996%22]}> Access in: 15/05/2018.

_____. Court of Justice of European Union. Third Chamber. Case C-230/14, *Weltimmo s. r. o.* v. *Nemzeti Adatvédelmi és Információszabadság Hatóság*. Luxembourg, 01/10/2015. Available at: <http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN>. Access in: 10/05/2018.

_____. Court of Justice of European Union. Grand Chamber. Case C-131/12, *Google Spain SL, Google Inc.* v. *Agencia Española de Protección de Datos (AEPD), Mario Costeja González.* Luxembourg, 13/05/2014. Available at: <http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=EN>. Access in: 15/05/2018.

6.5. Other texts and documents

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Data Protection Officers ('DPOs').* Available at: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>. Access in: 02/05/2018.

_____. *Opinion 3/2010 on the principle of accountability*. Brussels: [s. n.], 2010. Available at: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf>. Access in: 15/05/2018.

_____. *Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.* Brussels: [s. n.], 2014. Available at: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>. Access in: 23/05/2018.

_____. *The Role of the Data Protection Officer,* 2017. Available at:<https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/DPO%20Update%20Article%20Final.pdf>. Access in: 30/04/2018.

_____. *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain.* Brussels: [s. n.], 2015. p. 4. Available at: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf>. Access in: 15/05/2018.

BIONI, Bruno; e MONTEIRO, Renato. *O papel do Data Protection Officer*. 2017. Available at: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-papel-do-data-protection-officer-04122017>. Access in: 28/04/2018.

BUERGER, Sarah. *How the GDPR changed the Argentina Personal Data Protection Act.* 2017. Available at: <https://www.michalsons.com/blog/argentina-personal-data-protection-act/25090>. Access in: 16/05/2018.

CAMERON, Stephen. *'Light Reading 'The Digital Economy & GDPR',* 2017 Available at: <http://www.lightreading.com/oss-bss/subscriber-data-management/the-digital-economy-and-gdpr/a/d-id/730582> Access in: 04/05/2018.

ARTICLE 29 WORKING PARTY. *Opinion 2/2010 on online behavioural advertising.* Brussels: [s. n.], 2010. Available at: <https://iapp.org/media/pdf/resource_center/wp171_OBA_06-2010.pdf>. 21/05/2018.

COUNCIL OF EUROPE. *Enhancing data protection globally:* Council of Europe updates its landmark convention**,** 2018. Available at: <https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=09000016808ac976>. Access in: 07/06/2018.

MADGE, Robert. *GDPR's global scope:* the long story. Available at: <https://medium.com/mydata/does-the-gdpr-apply-in-the-us-c670702faf7f>. Access in: 14/05/2018.

SOLON, Olivia. *How Europe's 'breakthrough' privacy law takes on Facebook and Google.* 2018. Available at: <https://www.theguardian.com/technology/2018/apr/19/gdpr-facebook-google-amazon-data-privacy-regulation>. Access in: 09/05/2018.

THE GUARDIAN, *Costeja González and a memorable fight for the 'right to be forgotten',*

2014. Available at: <https://www.theguardian.com/world/blog/2014/may/14/mario-costeja-gonzalez-fight-right-forgotten>. Access in: 05/05/2018.

EUROPEAN UNION. European Data Protection Supervisor. *Adequacy decision.* Available at: <https://edps.europa.eu/data-protection/data-protection/glossary/a_en>. Access in: 21/05/2018.