THE INTERNATIONAL TRANSFER OF PERSONAL DATA: AN ANALYSIS OF THE ADEQUACY DECISION IN THE LEI GERAL DE PROTEÇÃO DE DADOS

Fabiano Menke* &Juliana Roman**

ABSTRACT: The objective of the paper is to analyze the international transfer of data under the LGPD and the role of the Brazilian National Data Protection Authority (Autoridade Nacional de Proteção de Dados - ANPD) in the decision of adequacy of equivalent level of protection of personal data by foreign country or international organization. Thus, the following question is raised: are the parameters established by the LGPD to guide the ANPD in recognizing an adequate level of protection for personal data by aforeign country or international organization sufficient? To answer this question, we will use the technique of micro-comparison addressing the discipline of data protection in the European context, considering the long European tradition in the culture of data protection.

The first part of the article, entitled "The Brazilian personal data protection panorama", will analyze data protection in the international context; the concepts and principles of the LGPD, and then deal with aspects of the ANPD. The second part, entitled "The international transfer of personal data and the adequate level of protection", will present the importance of the international transfer of personal data in the international context; the international data transfer in the LGPD, and then address the requirements of the adequacy decision before foreign countries or international organizations in the LGPD and GDPR.

KEY-WORDS: transfer of personal data — information technology — Lei Geral de Proteção de Dados — General Data Protection Regulation

I. Introduction

Given the growing dependence of individuals related to information technology and the "digitalization of everything" (EUROPEAN PARLIAMENT, 2016, p. 4), appropriate measures are needed that enable society and individuals to benefit from technological innovation. The processing of personal data, as stated by Danilo Doneda, does not constitute a problem in itself (2019, p. 23), since it is important to emphasize that the use of personal data enables the improvement of services, the creation of products and the improvement of public management, among other activities.

The development of a robust and prosperous digital economy requires instruments

* Associate Professor Faculty of Law Federal University of Rio Grande do Sul - UFRGS, Professor at the Postgraduate School Faculty of Law - UFRGS, Ph.D. University of Kassel, Germany (Scholarship CAPES/DAAD), Masters of Law Federal University of Rio Grande do Sul - UFRGS.

** Master's student in Law at the Post-Graduation Program of the Federal University of Rio Grande do Sul, linked to the Center for European and German Studies (2020).

that take into account the protection of the human person, the establishment of a series of procedures, principles and rights that limit the processing of personal data and, at the same time, empower citizens to control the flow of data related to them (MENDES, 2019, p. 78). Thus, it is necessary that it is made possible "to citizens an effective control in relation to their personal data, ensuring access, veracity, security, knowledge of the purpose for which they will be used, among many other guarantees that are necessary" (DONEDA, 2019, p. 24).

As pointed out (MENKE, 2020), among the main concerns of the data protection subject is that the individual is not manipulated by information that his interlocutors have about his person, without his knowledge. The holder of personal data has a legitimate expectation regarding the use of the personal information related to him, requiring that the processing corresponds to the informed purposes. Such trust constitutes alegal duty and must be maintained as to the use of personal data by the processing agents (COTS; OLIVEIRA, 2018).

The protection of personal data in the Brazilian legal system, previously treated sparsely in the national legal system, has recently been structured in a specific legislation. From Law No. 13,709, dated August 14, 2018, Lei Geral de Proteção de Dados (LGPD)[1] (BRAZIL, 2018), the country began to have specific rules on the treatment of personal data.

As an external and accelerating factor of the LGPD, one can invoke the entry into force, on May 25, 2018, of the *General Data Protection Regulation - GPDR* (EUROPEAN PARLIAMENT, 2016a). Regulation 2016/679 deals with rules on the protection of natural persons with regard to the processing of personal data and the free flow of such data; having repealed Directive 95/46/EC (EUROPEAN PARLIAMENT, 1995). Another factor that can be cited as accelerating the approval of the LGPD is the Brazil's interest in becoming a member of the Organization for Economic Co-operation and Development (OECD).[2]

In particular, within the broad scope of data protection, the international transfer of personal data has significant importance, which justifies the object of the present study. In the LGPD, the subject of international transfer of data is regulated by Articles 33 to 36. The international transfer of personal data is defined as the transfer of such data to a foreign country or international organization of which the country is a member (art. 5º, XV).

The objective of the paper is to analyze the international transfer of data under the LGPD and the role of the Brazilian National Data Protection Authority (Autoridade Nacional de Proteção de Dados - ANPD) in the decision of adequacy of equivalent level of protection of personal data by foreign country or international organization. Thus, the following question is raised: are the parameters established by the LGPD to guide the ANPD in recognizing an adequate level of protection for personal data by aforeign

[1] Could be translated as General Data Protection Act.

[2] The OECD is an international multilateral organization that currently has 34 member countries. It was created after World War II, in 1948, with the mission of promoting global economic and social welfare. It aims at acooperative relationship between its members to solve common problems that afflict them, establishing standards that trigger uniform responses.

country or international organization sufficient? To answer this question, we will use the technique of micro-comparison (VICENTE, 2011, p. 21), addressing the discipline of data protection in the European context, considering the long European tradition in the culture of data protection.

The document is divided into two main parts, subdivided into three items each. The first part, entitled "The Brazilian personal data protection panorama", will analyze data protection in the international context; the concepts and principles of the LGPD, and then deal with aspects of the ANPD. The second part, entitled "The international transfer of personal data and the adequate level of protection", will present the importance of the international transfer of personal data in the international context; the international data transfer in the LGPD, and then address the requirements of the adequacy decision before foreign countries or international organizations in the LGPD and GDPR. The article ends with brief reflections about the subject.

II. The Brazilian personal data protection panorama

According to Laura Schertel Mendes, the legal good of data protection is twofold, consisting of "the protection of the individual against the risks threatening his personality in face of the collection, processing, use, and circulation of personal data" (2019, p. 176) and "the assignment to the individual of the guarantee to control the flow of his data in society" (2019, p. 176).

Danilo Doneda, in turn, highlights that the protection of personal data derives from privacy, however, it is not limited to it (2018, p. 264). In this direction, the author argues that the interpretation of Clauses X and XII of Article 5º of the Federal Constitution must recognize the intimate connection that the rights related to privacy and data communication now bear (2018, p. 264):

> Art. 5 All are equal before the law, without distinction of any nature, guaranteeing Brazilians and foreigners residing in the country the inviolability of the right to life,liberty, equality, safety, and property, in the following terms:
> [...]
> X - privacy, private life, honor, and personal image are inviolable, and the right to compensation for material or moral damage resulting from their violation is assured; [...]
> XII - the secrecy of correspondence and telegraphic communications, data and telephone communications is inviolable, except, in the latter case, by judicial order, in the cases and in the manner that the law establishes for the purposes of criminal investigation or criminal procedure; (BRAZIL, 1988).

Before the LGPD, Brazil did not have a specific legislation on personal data protection. The theme was dealt within a decentralized approach. In the ordinary legislation, it is possible to find references to the theme in the Code of Consumer Protection (Código de Defesa do Consumidor - CDC, BRAZIL, 1990), in the Habeas Data Right (Direito de habeas data, BRAZIL, 1997), in the Positive Registration Law (Lei do Cadastro Positivo, BRAZIL, 2011a), in the Access to Information Law[3] (Lei de Acesso à Informação, BRAZIL, 2011b), and in the

[3] Art. 4º For the effects of this Law, the following are considered:
I - information: data, processed or not, that can be used for the production and transmission of knowledge, contained in any medium, support, or format;

Brazilian Civil Rights Framework for the Internet[4] (Marco Civil da Internet, BRAZIL, 2014).

A. Personal data protection in the international context

In 1980, the OECD issued two important documents: *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980)[5] and the *Declaration on Transborder Data Flows* (1985). Both influenced the development of personal data protection worldwide (BIONI, 2020, p. 113). In these instruments there were references to adequate guarantees for the international transfer of data, where the importance of guaranteeing the free flow of information was highlighted. The crucial link between economic and social development and information technology had been noted (OECD, 2011, p. 7). Thus, the extreme importance of reconciling economic development and the protection of personal data was highlighted.

At the same time, the Council of Europe began to address the issue of data protection, taking the first step toward an integrated European system of personal data protection (DONEDA, 2019, p. 193). In 1981, the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 108/1981*, came into force. Also known as Convention 108, the document defined personal data as "any information concerning an identified or identifiable individual"[6] (COUNCIL OF EUROPE, 1981, p. 1). According to Doneda, the organization oriented its discourse around Article 8º of the European Convention on Human Rights[7].

|In view of Convention 108 of the Council of Europe and the OECD *Guidelines, in* the early 1980s, a sort of "common core" was found related to the set of principles to be applied in the protection of personal data. The principle of publicity, accuracy, physical and logical security, finality, and open access have come to be identified in various laws, treaties, conventions, or agreements among private parties (DONEDA, 2019, p. 181).

In 1995, the document that effectively came to standardize the protection of personal data in the European Union appeared: the Directive 95/46/EC of the European Parliament andof the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (DONEDA, 2019, p. 195).

It should be noted that, prior to the GDPR, there was no uniformity of the matter in the European Union (DONEDA, 2019, p. 188). Directive 95/46/EC had its direct applicability only by way of exception, due to the need for transposition[8] of the matter by

[4] The Brazilian Civil Rights Framework (in Portuguese: Marco Civil da Internet) established principles and guarantees for the use of internet in Brazil, as well as minimum requirements for the treatment and protection of personal data. Decree No. 8,771 of 2016, which regulated the Brazilian Civil Rights Framework, defines personal data as all data "related to an identified or identifiable natural person, including identifying numbers, locational data, or electronic identifiers, when these are related to a person [...]".

[5] The document was updated in 2013, can be checked in its entirety on the OECD website: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[6] Translation from the original: "Personal data" means any information relating to an identified or identifiable individual ("data subject");

[7] Article 8 of the Convention deals with the right to respect for private and family life.

[8] The Directive is a typical normative instrument of the European Union. The approval of a directive implies that each member state adapts, within a certain period of time, its own legal system to the molds established by the directive, in a process known as transposition - and its effectiveness is all the greater if we take into account that the failure of a member state to transpose it in a timely manner entails a certain degree of direct effectiveness

each member state, so in specific cases, the national law of each country was applied (DONEDA, 2019, p. 188). The Directive, when transposed into each country's domestic law, gave rise to different practices for assessing the level of adequacy (ZINSER, 2004, p. 172).

The lack of standardization on the subject and the need to update the data protection discipline on several points were among the main reasons for updating European legislation in the form of a regulation, with direct applicability in all member countries (DONEDA, 2019, p. 188). Another relevant justification was the interest in the Strategy for the Digital Single Market in Europe (EUROPEAN COMMISSION, 2015), which assumes extensive use of data by various sectors of society.

B. General Data Protection Law: concepts and principles

The LGPD, in force since September 18, 2020, is a cross-cutting law that cuts across different economic agents in Brazil, both the private and public sector. The law came into force with the aim of protecting the fundamental rights of freedom and privacy, as well as the free development of the personality of individuals, bringing the premise of good faith to all types of processing of personal data.

The law provides for the processing of personal data, including in digital media, by natural persons or legal entities governed by public or private law (art. 1). The law applies to any processing operation performed by a natural person or public or private legal entity, regardless of the medium, the country of its headquarters, or the country where the data is located, provided that: (i) the processing operation is performed in the national territory; (ii) the purpose of the processing activity is to offer or provide goods or services or to process data of individuals located in the national territory; or (iii) the personal data object of the processing have been collected in the national territory (art. 3, *caput* and items I to III).

The law does not apply to data processing carried out by individuals, exclusively, for private and non-economic purposes or for exclusively journalistic, artistic, and academic purposes and by the government for national security and defense (art. 4). One of the evident characteristics of the LGPD is its principled and conceptual nature. The legislation presents,in addition to the rights of data subjects, concepts, principles, and terminologies that are fundamental to its understanding. The specification of the terms used, in the context of personal data, is particularly important and aims to solve the problems of categorization of theinformation collected.

To better understand this work, some of these concepts will be cited: personal data is defined as "information relating to an identified or identifiable natural person" (art. 5, I); sensitive personal data is defined as "personal data concerning racial or ethnic origin, religious conviction, political opinion, membership of a trade union or religious, philosophicalor political organization, data concerning health or sex life, genetic or biometric data, when linked to a natural person" (art. 5, II); data subject is defined as "a natural person to whom personal data are processed" (art. 5, V); international transfer

of the directive and also leads the country to answer for the delay before the European Court of Justice. The Regulation is directly applicable. Further information: https://ec.europa.eu/info/law/law-making-process/applying-eu-law_en.

of personal data is "the transfer of personal data to a country or region in which the data are processed" (art. 5, VI). International data transfer is the "transfer of personal data to a foreign country or international organization of which the country is a member" (art. 5, XV). The national authority is the "public administration body responsible for overseeing, implementing and supervising compliance with the Law throughout the national territory" (art. 5, XIX).

Guaranteeing the protection of the rights of personal data subjects is based on the indication of principles concerning data processing, the action of which must respect the limits of fundamental rights. According to Article 6, personal data processing activities must observe the principle of good faith, which operates as a guide to all others and serves as a reference to interpret open concepts (art. 6, *caput*). The law brings as principles the purpose (section 6, I); the adequacy (section 6, II); the necessity (section 6, III); the free access (section 6, IV); the quality of the data (section 6, V); the transparency (section 6, VI); the security (section 6, VII); the prevention (section 6, VIII); the non-discrimination (section 6, IX) and, finally, the responsibility and accountability (section 6, X).

Regarding the function of the principles in the legal system, Paulo de Barros Carvalho is assertive:

> Principles are guidelines that inform and illuminate the understanding of normative segments, giving them a character of relative unity and serving as an aggregation factor in a given bundle of normal. The principle exerts a centripetal reaction, attracting around its legal rules that fall under its radius of influence and manifest the force of its presence. (CARVALHO, 1991)

The principles represent a fundamental basis of the legal system and act as a model that guides the legal understanding. In this sense, there is the need to observe logical cohesion, interpretive harmony, and uniformity in applying these principles.

C. National data protection authority

The national authority is central to the effectiveness of the norms provided by the legislation in the country. In the original draft of the LGPD, the national authority was listed as a special autarchy, linked to the Ministry of Justice, and characterized by administrative independence, absence of hierarchical subordination, fixed term and stability of its leaders and financial autonomy. However, articles 55 to 59, which structured the ANPD, were vetoed by the President.

Provisional Measure (MP) No. 869, dated December 27, 2018, was essentially motivated with the intention of creating the ANPD. Transformed into law, through Law No. 13,583, of July 8, 2019, it conferred the nature of an agency of the direct federal administration, subordinated to the Presidency of the Republic (art. 55-A, *caput*), emphasizing its transitory legal nature. It may be transformed into an autarchy after 2 years, upon proposal by the Executive Branch (art. 55-A, § 1).

According to Law 13.583/19, the ANPD is formed by a Board of Directors, whose members are chosen by the head of the Executive Branch; a National Council, responsible for studies, analysis and suggestions to the Board of Directors, composed of authorities and members of civil society; an Inspector General's Office, and administrative units for law enforcement (art. 55-C). The organ has, among other

attributions, to elaborate directives for a National Policy of Protection of Personal Data and Privacy (art. 55-J, III); to inspect and apply sanctions (art. 55-J, IV); to promote among the population knowledge of the norms and public policies about protection of personal data and security measures (art. 55-J, VI); to promote and elaborate studies on national and international practices of protection of personal data and privacy (art. 55-J-VII), and to promote cooperation actions with personal data protection authorities of other countries, of an international or transnational nature (art. 55-J, IX).

In relation to international transfers of personal data, the activities of the ANPD are (i) to evaluate the level of adequacy of international entities and third countries (art. 33, I and art. 34); (ii) to authorize international transfers of personal data submitted to its approval (art. 33, V and art. 35, paragraph 2); (iii) determine the content of specific clauses and standard contractual clauses for international transfers of personal data (art. 35); (iv) designate bodies responsible for certifications in the context of the international transfer of data (art. 35, paragraph 3) and review their activities (art. 35, paragraph 4); (v) manage notifications regarding changes in mechanisms for safeguarding international data transfers (art. 36).

According to Ordinance No. 11 of January 27, 2021-01-30, which made public the ANPD's regulatory agenda for the biennium 2021-2022, it is expected that arts. 33, 34 and 35 of the LGPD will be regulated within 1 year and 6 months (BRAZIL, 2021). That is, the timeframe for the agency to publish a list of suitable countries or define the content of transfermechanisms will be, on average, 18 months.

III. International transfer of personal data and the adequate level of protection

There is great economic interest in the transnational flow of data, which is why the transfer of data is a matter of interest in several international treaties, whose feasibility is directly related to the proper adequacy between private autonomy and protection of the public interest (BURRI, 2017).

By considering that the international transfer of data presents a greater risk to the rights and freedoms of data subjects if adequate techniques and satisfactory measures are not employed, the chances of security incidents are increased (FUNDAÇÃO GETÚLIO VARGAS, 2020, p. 13). Thus, there is an obligation to ensure the security of personal data by the processing agents, to the extent of their responsibility in carrying out the processing (FUNDAÇÃO GETÚLIO VARGAS, 2020, p. 13).

International data transfers are a key component in the face of the activities of personal data processing (CIPL; CEDIS-IDP, 2020), and it is essential that efficient and appropriate mechanisms are applied to enable and encourage the flow of information.

A. The importance of the international transfer of personal datain the international context

Concern for the protection of personal data fosters the development of a healthy economic environment. (INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO, 2019). In a globalized context, it is clear that international transfers of personal data are essential for economic development and the provision of services. The social and economic importance of international transfer is recognized by the volume of data

circulating between different countries, worldwide (KUNER, 2010).
Aware of the importance of international data flow for economic strengthening, in 1978, the OECD established a group of *experts* on cross-border data traffic, with the task of drafting a model regulation for international data traffic (DONEDA, 2019, p. 193).

As a starting point for this work, were selected the principles designed to enhance the use of information technology without harming privacy: the *Fair Information Privacy Principles* (UNITED STATES OF AMERICA, 1973). These principles are: "(1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and

(5) Enforcement/Redress" (UNITED STATES OF AMERICA, 1973).

As already mentioned in the first chapter, the OECD work resulted in *the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, finalized in 1980 and revised in 2013. The document sets out a number of parameters for data protection regulation,stated through principles on which the activity should be based. These principles are: "(1) *collection limitation principle*; (2) *data limitation principle*; (3) *purpose specification principle*; (4) *use limitation principle; (*5) *security safeguard principle; (*6) *openness principle; (*7) *individual participation principle*" (OECD, 1981).

At that time, the central concern was with data traffic and not with the protection of theperson itself. That is, it aimed to ensure the development of the computer market and commercial transactions through the regulation of personal data (DONEDA, 2019, p. 193). This document became a reference in the area, even though it was not directly binding. At the time, OECD member countries were not required to legislate under the *Guidelines*, moreover, the Guidelines had no direct applicability on their domestic law (DONEDA, 2019, p. 193).

In this period, it can be said that the European Union adopted an intermediate position regarding the discipline of personal data, maintaining proximity with the OECD approach. However, over the years, its stance on the matter changed decisively, assuming a new determination that went beyond the formation of a free trade zone (DONEDA, 2019). From then on, the axis moved to a position closer to the respect and protection of citizens' fundamental rights, going through the construction of a European system of personal data protection (DONEDA, 2019).

It is also worth mentioning the Resolution (*The Madrid Resolution*) issued in 2013 with the aim of linking data protection and privacy to the normative provisions of international law, recommending the adoption of an additional protocol to article 17 of the United Nations International Covenant on Civil and Political Rights - which was internalized into Brazilian law by Decree 592/1992 (SPAIN, 2015). This update aimed to adapt the treaty's provisions to the international standard of data protection (SPAIN, 2015).

B. The international transfer of data in the LGPD

Following the parameters of the GDPR, the LGPD provides for the international transfer of personal data in Chapter V, entitled "International Data Transfer", addresses the aspects related to the transfer of personal data to countries and international

organizations and their respective rules. Countries interested in this type of transaction must offer personal data protection guarantees to the same degree as Brazilian legislation. Operations involving the transnational flow of information must respect the principles of data protection and safeguard the rights of the data subjects.

Among these principles, the principle of transparency stands out (CIPL; CEDIS-IDP, 2020). According to this principle, the data subject must have clear, precise and easily accessible information about the performance of the processing and the respective processing agents. Furthermore, additional information about the transfer must be provided to the data subjects, especially when sensitive data is involved (CIPL; CEDIS-IDP, 2020).

Art. 33 of the LGPD defines the hypotheses in which international transfer will be allowed[9]:

(a) the countries or international bodies provide a degree of protection of personal data adequate to that provided for in the LGPD (art. 33, I) - the equivalence must consider the personal data protection system of each country;

(b) the controller provides and proves guarantees of compliance with the principles, the data subject's rights, and the data protection regime foreseen in the LGPD (art. 33, II) - these mechanisms include: standard contractual clauses, contractual clauses that are specific to a given transfer, global corporate standards, seals, certificates and regularly issued codes of conduct;

(c) the transfer is necessary for international legal cooperation between public intelligence, investigative, and prosecutorial bodies in accordance with instruments of international law (Art. 33, III) - governs the international transfer of information for the purpose of investigations conducted in other states;

(d) the transfer is necessary for the protection of the life or physical safety of the data subject or of third parties (art. 33, IV) - authorizes the sending of data abroad in order to protect the life or physical safety of the data subject or of third parties, even if the level of data protection at the destination is lower than in Brazil;

(e) the national authority authorizes the transfer (art. 33, V);

(f) the transfer results from a commitment assumed in an international cooperation agreement (art. 33, VI);

(g) the transfer is necessary for the execution of a public policy or the legal attribution of the public service (art. 33, VII) - authorizes the international transfer of data in the scope of the activities and functions of the public authority, provided that due publicity is given to the transfer of the personal data in question;

(h) the holder has provided his specific and prominent consent to the transfer (art. 33, VIII), with prior information on the international character of the operation, clearlydistinguishing this and other purposes - the consent must be considered in a manner consistent with other provisions of the law; or

(i) is necessary to meet the hypotheses foreseen in clauses II, V and VI of art. 7 (art. 33, IX).

C. The adequacy decision in the LGPD and the GDPR

In the quest for an international standard of protection for personal data, the imposition of effective evaluation methods by the national authority in relation to foreign countries and international bodies becomes necessary.

As shown, the LGPD provides (art. 33, I) that international transfers of personal data

[9] Translation of the provisions made by the authors of this paper.

will be permitted to countries or international bodies that have a level of data protection that isequivalent to the protection offered by the LGPD. Public legal entities, within the scope of their legal powers, and those responsible for them, within the scope of their activities, may request the ANPD to evaluate the level of protection afforded to personal data by a country or international body (art. 33, sole paragraph).

Still in relation to art. 33, I: the fact of the legislative omission in relation to the detailsof the qualification of what would be "an adequate level of protection of personal data" in the parameters of the Brazilian legislation makes the task of defining the criteria challenging. This responsibility was delegated to the national authority, as provided in art. 34:

> Art. 34 - The level of data protection of the foreign country or international organization mentioned in subitem I of the head of art. 33 of this Law will be evaluated by the national authority, which will take into consideration:
> I. the general and sectorial norms of the legislation in force in the destination country or international organism;
> II. the nature of the data;
> III. the observance of the general principles of personal data protection and of the rights of data subjects provided for in this Law;
> IV. the adoption of security measures foreseen in the regulation;
> V. the existence of judicial and institutional guarantees for the respect of personal data protection rights; and
> VI. other specific circumstances regarding the transfer.
> (BRAZIL, 2018)

In this sense, it is interesting to compare the provisions of the chapter on international transfer in the LGPD with the chapters on the same subject in the European regulation. Recital 109[10] of the GPDR deals with the free movement of personal data. The theme is regulated in Chapter V, articles 44 to 50. The Regulation presents techniques that help to understand the parameters required for the adequacy decision to be granted to a foreign country or international organism.

According to the GDPR, all international data transfers must comply with the general principle of transfers, as regulated in art. 44:

> Art. 44 GDPR
> General Principle of Transfers
> Any transfer of personal data which are or will be processed after transfer to a third country or an international organization shall only take place if, without prejudice to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or international organization to another third country or international organization. All provisions in this Chapter shall be applied in a manner which ensures that the level of protection of natural persons guaranteed by this Regulation is not undermined. (EUROPEAN PARLIAMENT, 2016a)

[10] "The objectives and principles of Directive 95/46/EC remain valid, but they have not prevented the fragmentation of data protection enforcement at Union level, legal uncertainty or a widespread public perception that significant risks to the protection of natural persons remain, in particular with regard to electronic activities. Differences in the level of protection of the rights and of natural persons, in particular the right to the protectionof personal data in the context of the processing of such data in the Member States, may prevent the free flow of personal data within the Union. Such differences may therefore constitute an obstacle to the pursuit of economic activities at Union level, distort competition and impede authorities in the discharge of their obligations under Union law. These differences between the levels of protection are due to the existence of disparities in the implementation and application of Directive 95/46/EC." (Recital No. 9 of the GDPR)

Article 45, 1, states the principle that data transfers to a third country or international organization may only take place if the foreign country, territory, one or more specific sectorswithin that third country, or the international organization in question ensures an adequate level of protection. According to Article 45, 2, when analyzing whether a particular country has GDPR compliant level, the European Commission should assess the presence of the following elements:

> Art. 45 GDPR
>
> Transfers based on an adequacy decision [...]
>
> 2. When assessing the adequacy of the level of protection, the Commission shall, inparticular, take into account the following elements:
>
> a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation in force, both general and sectoral, including on public security, defence, national security and criminal law and concerning access to personal data by public authorities, as well as the application of such legislation and of data protection rules, professional rules and security measures, including the rules for onward transfer of personal data to another third country or international organisation, which are complied with in that country or by that international organisation, and case law, as well as the effective and enforceable rights of data subjects, and administrative and judicial remedies for data subjects whose personal data are subject to transfer;
>
> b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organization is subject, responsible for ensuring and enforcing compliance with data protection rules and endowed with adequate powers of coercion to assist and advise data subjects in exercising their rights, and cooperating with the supervisory authorities of the Member States; and
>
> c) the international commitments the third country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.(EUROPEAN PARLIAMENT, 2016a)

As Rücker and Kugler point out about international data transfer in the GDPR:

> the lawfulness of transferring personal data to a non-EU country or an international organization is measured by a two-step test. The first step is to check whether the general principles applicable to the processing of personal data are observed. The second step can be remedied when the European court makes a decision on the adequacy of the protection afforded by the country in question (RÜCKER; KUGLER, 2018. p. 195)

In addition, the European Commission should take into account the guidelines established by the Article 29 Working Party (Art. 29 WG)[11] with regard to the process of verifying the adequacy of the level of data protection of a third country or international body. According to the "Reference document on adequacy" adopted on February 6, 2018, prepared by the WG Art. 29:

> The four guarantees indicated must be met when it comes to access to data, whether for national security or law enforcement purposes, by all third countries for such access to be considered adequate:
>
> 1) The processing must be based on clear, precise and accessible rules (legal basis);
>
> 2) The necessity and proportionality in relation to the legitimate aims pursued must be demonstrated;

[11] The Article 29 Working Party (Art. 29 WG) is the independent European working group that dealt with issues related to personal data protection and privacy until May 25, 2018. After the GDPR came into force, it was replaced by the European Data Protection Board (EDPB), an independent European body that contributes to the consistent application of data protection rules in the European Union and promotes cooperation between EU data protection authorities.

> 3) Treatment must be subject to independent supervision;
> 4) Effective means of redress should be available to natural persons. (EUROPEAN PARLIAMENT, 2018)

These four guarantees can be considered as the main specific pillars on the matter, the main general values to be followed by the legislation concerning international data transfers.

IV. Concluding Remarks

The international transfer of personal data is a theme that deserves attention, especially in the context of globalization, where the international flow of data is unquestionably necessary. The subject must be treated with responsibility, not only because it involves relevant economic issues, but also because it is associated with fundamental rights.

One of the great challenges of Brazilian law, when it comes to data protection and the International transfer will consist of defining adequate and feasible parameters for the guarantee of the rights protected by the LGPD.

Regarding the international transfer of data, the Brazilian legislation presents vague concepts regarding the level of protection adequate for granting the adequacy decision, delegating to the ANPD the task of defining greater specifications about its requirements. In addition, according to Ordinance No. 11 of January 27, 2021, the agency may take upto 18 months to establish these parameters.

Thus, we conclude that the parameters established by the LGPD to guide the ANPD regarding the adequate level of data protection in foreign countries or international organizations are insufficient. It will be up to the National Data Protection Authority to establish specifications on the subject. The parameters established by the LGPD and the GPDR are quite different: while the European diploma is much more specific on the subject, the Brazilian legislation leaves room for possible subjectivism.

It can be seen that the European Union is articulated as a whole to ensure the soundness of the data protection regulation with regard to international data flows, although it is recognized that the task is complex and lengthy[12]. The GDPR provides adequate tools and techniques for effectively regulating the free flow of personal data without prejudice to the data subject. In addition, the European Union, due to its long tradition of personal data protection, has other documents related to the topic, such as the work of the former WG Art. 29 and the European Data Protection Board (EDPB).

The importance of allowing and preserving national differences with regard to privacy and the protection of personal data is stressed, however, it is important to emphasize that most data protection principles can and should be harmonized internationally.

In this vein, in relation to defining the content of international data transfer mechanisms and evaluations of adequacy decisions, the ANPD should engage with international bodies and examples that have already gone through this experience, such as the European Commission.

[12] SCHANTZ, Peter. Art. 45 DSGV. In: SIMITIS, S.; HORNUNG, G.;
SPIECKER, I. (Org.): Datenschutzrecht: DSGVO mit BDSG. Nomos: Baden-Baden, 2019, p. 972.

References

Bioni B.R. "Proteção de dados pessoais: a função e os limites do consentimento. " (2. ed.) Riode Janeiro: Forense, 2019.

BRAZIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília: Presidência da República, 2016. Available at: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 16 jul. 2020.

_____. Lei nº 8.078, de 11 de setembro de 1990. Available at: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Accessed on: 25 jan. 2021.

_____. Lei nº 9.507, de 12 de novembro de 1997. Available at: http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm. Accessed on: 25 jan. 2021.

_____. Lei nº 12.414, de 9 de junho de 2011. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Accessed on: 25 jan. 2021.

_____. Lei nº 12.527, de 18 de novembro de 2011. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Accessed on: 25 jan. 2021.

_____. Lei nº 12.965, de 23 de abril de 2014. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Accessed on: 25 jan. 2021.

_____. Lei nº 13.709, de 14 de agosto de 2018. Available at: http://www.planalto.gov.br/ccivil_03/_Ato20152018/2018/Lei/L13709.htm. Accessed on: 25 jan. 2021.

_____. Portaria Nº 11, de 27 de janeiro de 2021. Available at: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Accessed 30 jan. 2021.

Burri, M. "The governance of data and data flows in trade agreements: the pitfalls of legaladaptation". University of California, Davis, Vol. 51, p. 65-132, 2017.

Carvalho, P.B. Curso de Direito Constitucional Tributário. 4th ed. Saraiva: São Paulo, 1991.

Centre for Information Policy Leadership (CIPL); Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público

(CEDIS-IDP). "O papel da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) conforme a nova Lei Geral de Proteção de Dados Pessoais (LGPD)". 2020. Available at: https://www.idp.edu.br/o-papel-da-autoridade-nacional-de-protecao-de-dados-pessoais-anpd-conforme-a-nova-lgpd/. Accessed on: 25 jan. 2021.

Cots, M. & Oliveira, R. Lei Geral de Proteção de Dados Pessoais comentada. São Paulo:Thompson Reuters, 2018.

Council of Europe. Convention for the Protections of the individuals with regard to the Automatic Processing of Personal Data. Estrasburgo, 28 jan. 1981. Available at: https://rm.coe.int/1680078b37. Acesso em: 01 fev. 2021.

Doneda, D. Da privacidade à proteção de dados pessoais: elementos da formação da Leigeral de proteção de dados. 2. ed. São Paulo: Thompson Reuters Brasil, 2019.

European Commission. "Estratégia para o Mercado Único Digital na Europa". Bruxelas, 2015. Available at: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52015DC0192&from=EM. Accessed on: 25 jan. 2021.

European Parliament. Directorate-General for External Policies, Policy Departament. "Transatlantic Digital Economy and Data Protection: State-of-Play and Future Implications for the EU's and External Policies", 2016. Available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU%282016%29535006_EN.pdf. Accessed on: 25 jan. 2021.

_____. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de24 de outubro de 1995. Luxembourg, 1995. Available at: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT. Accessed on: 25 jan. 2021.

_____. General Data Protection Regulation. Bruxelas, 2016a. Available at: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Accessed on: 25 jan. 2021.

_____. Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. Documento de referência relativo à adequação. Adopted on 28 nov. 2017. Last version revised and adopted on 6 fev. 2018. 2018. Available at: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936. Acesso em:01 fev. 2021.

Fundação Getúlio Vargas. "Guia de Proteção De Dados Pessoais: Transferência Internacional, out. 2020. Available at: https://portal.fgv.br/sites/portal.fgv.br/files/transferencia_internacional.pdf. Acesso em: 01fev. 2021.

Instituto de Tecnologia e Sociedade do Rio. "Transferência de dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira", 2019. Available at: https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf. Accessed 30 jan. 2021.

Kuner, C. "Regulation of transborder data flows under data protection and privacy law: past,present, and future". TILT Law & Technology Working Paper, n. 016, p. 1-40, 2010.

Available at: http://www.kuner.com/my-publications-and-writing/untitled/kuner-oecd-tbdf-paper.pdf. Accessed on: 25 jan. 2021.

Mendes, L. S. "Privacidade, proteção de dados e defesa do consumidor: linhas gerais de umnovo direito fundamental". 2. ed. Saraiva: São Paulo, 2019.

Menke, Fabiano. "As origens alemãs e o significado da autodeterminação informativa". Migalhas, 30 out. 2020. Available at: https://migalhas.uol.com.br/coluna/migalhas-de-protecao-de-dados/335735/as-origens-alemas-e-o-significado-da-autodeterminacao- informativa. Accessed

on: 25 jan. 2021.

Organisation for Economic Co-Operation and Development - OECD. "Declaration on Transborder Data Flows". 11 abr. 1985. Available at: https://www.oecd.org/digital/ieconomy/declarationontransborderdataflows.htm#:~:text=Flows%20of%20computerised%20data%20and,known%20as%20Transborder%20Data%20Flows. Accessed on: 25 jan. 2021.

_____. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Elaboração André-Pascal. França: OECD Publications Service, 1980. Available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflo wsofpersonaldata.htm. Accessed on: 25 jan. 2021.

Rücker, D. & Kugler, T. "New European General Data Protection Regulation: APractitioner's Guide". Nomos: Baden-Baden, 2018.

Schantz, P. 45 DSGV. In: Simitis, S.; Hornung, G. & Spiecker, I. (Org.): Datenschutzrecht: DSGVO mit BDSG. Nomos: Baden-Baden, 2019.

Spain. International Standards on the Protection of Personal Data and Privacy. The Madrid Resolution, 2015. Available at: http://www.privacyconference2009.org/media/Publicaciones/common/estandares_resolucion_ madrid_en.pdf. Accessed on: 25 jan. 2021.

United States of America. Records Computers and the Rights of Citizens. U.S. Department of Health, Education and Welfare (HEW), 1973. Available at: https://www.justice.gov/opcl/docs/rec-com-rights.pdf. Accessed on: 25 jan. 2021.

Vicente, Dário Moura. "Direito Comparado". Vol. 1: Introdução e Parte Geral. Almedina:Coimbra, 2011.

Zinser, A. "European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers". Tulane Journal of Technology and IntellectualProperty, New Orleans, Vol. 6, p. 172, Spring 2004. Available at: https://journals.tulane.edu/TIP/article/view/2476. Accessed on: 25 jan. 2021.