Institute for Research on Internet & Society

Policy Paper

Transborder Data Flows and Bill n.5.276/16: Some Remarks for the Brazilian legislative process.

Institute for Research on Internet & Society

Policy Paper

Transborder Data Flows and Bill n.5.276/16: Some Remarks for the Brazilian legislative process.

SUMMARY

1. Executive summary

This *policy paper* is designed to submit the scientific contribution of the **Institute for Research on Internet and Society - IRIS** to a broader public discussion concerning the current text of Bill No. 5,276[1], which deals with data protection in Brazil. This research has been undertaken in collaboration with the International Study Group on Internet, Innovation and Intellectual Property - GNet, from Federal University of Minas Gerais (UFMG), under the coordination of Prof. Fabrício Bertini Pasquot Polido[2].

Under Brazilian law, "protection of personal data" is conceived as one of the underlying principles of Internet governance at domestic level, being ensured by Law n. 12.964 - the Brazilian Civil Rights Framework for the Internet ("Marco Civil da Internet"). Recognized as a pioneer legislation worldwide and an example of the multistakeholder approach typical of the internet governance related processes, Marco Civil establishes, in its Article 3.III, a specific regulatory provision for the further enactment of a statutory law dealing with data protection. Therefore, Bill n. 5,276 was sent to Congress by the President's Office, in May 13, 2016[3].

At the Executive Branch, the Bill draft followed the same public consultation model to which the Brazilian Internet Bill of Rights was submitted to. The Ministry of Justice made the text available online, open for comments from any user. According to the some specialists, this strategy made possible for all stakeholders - civil society, academia, government sectors, regulatory agencies and private entities - to actively engage in the legislative debate[4].

In short, the Bill seeks to target some important normative clusters such as internet users' rights and distinct aspects of data treatment, collection, processing and storing. This preliminary study, however, will focus on the analysis of specific material and procedural issues touching Chapter V of the Bill, namely the **international data flows and related international transactions**. The main goal of this policy paper is to collaborate, both from scientific and technical standpoints, to the current law-making process involving the Bill on Data Protection and its interfaces with extraterritorial application of Brazilian law, particularly how the provisions under discussion at the National Congress should affect the existing data protection legal regime(s).

This paper, conceived in an independent and nonpartisan fashion, aims to clarify,

1 Its legislative process can be followed at: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Accessed on January 9, 2017. The Bill was attached to the Bill n. 4.060/2012. Their process happen together, because their subjects are related. Available at: :<http://bit.ly/1TujEke>. Accessed on March 22, 2017.

2 Founder and Director of the Institute for Research on Internet & Society. Tenured Professor of Private International Law, International Intellectual Property Law, Internet Law and Comparative Law at the Federal University of Minas Gerais' School of Law. Prof. Polido holds a Doctor in Law degree in International Law, University of São Paulo School of Law (USP, 2010) and LL.M. in International Intellectual Property Law (University of Turin, 2007). He was Visiting Researcher at the Max-Planck Institute for Comparative and International Private Law in Hamburg. Member of the Private International Law and Intellectual Property Committee, International Law Association (ILA), of the International Economic Law Society and of the American Association for International Private Law. Head of the Study Group on Internet, Innovation and Intellectual Property of the Federal University of Minas Gerais (GNET). E-mails: fabricio@irisbh.com.br e fpolido@ufmg.br. Also contributed to this paper: Bruno Biazzatti, Bruno Tavares, Diego Machado, Lucas Anjos, Luíza Brandão, Matheus Rosa, Odélio Porto Junior, Pedro Vilela, Tatiana Resende, Túlio Campos and Victor Vieira.

3 It is Important to highlight that a great amount of this analysis is also related with, regarding content, to Bill n. 4,060/2012, from Congressman Milton Monti (PR/SP), about the "treatment of personal data". Bill 4,060/2012 is currently attached to Bill 5,276/2016 (according to the status of its legislative procedures in 2016).

4 SOUZA, Carlos Affonso Pereira; VIOLA, Mario; e LEMOS, Ronaldo. *Understanding Brazil's Internet Bill of Rights.* p.37.

for the general public and congress representatives, some of the legal and political matters emerging from from the cross-border transactions involving internet users and the management of their personal data at global level. At first blush, this may appear a small part of the upcoming legal regime to be established by Bill n. 5,276, of 2016 at domestic level. However, the converging subjects of international data flow and transfer of data are very sensitive from the standpoint of international and comparative legal patterns and are encompassed by discussions regarding jurisdiction and internet governance[5].

The social and economic importance of international data transfers is mainly based on the sheer volume of data circulating among different countries at cross-border level[6]. Multinational companies collect, treat and store data in different jurisdictions. In view of different corporate activities, they usually seek different jurisdictions and countries for their business practices that best fit their efficiency standards and that are less costly to their business models[7].

International data transfer also relates to users' rights, which, in connection with the internet context, are just under implementation according to Brazil's Internet Bill of Rights. Any law or regulation dealing with personal data and its international transfer ought to consider the great volume of information produced by, related with, or exchanged among individuals, organizations and companies. And even more significant are the effects of the international data transfer of internet users, over an inevitable mobility across borders, under the models and standards of their specific legal protection in each jurisdiction, particularly considering privacy and transparency of mechanisms used to "collect, store and treat data".

It appears to the authors of this paper that the current moment is an excellent occasion for the congresswoman and congressman to think about the various interests at stake: on the one hand, companies and governments in increasingly collecting and treating data; on the other hand, individuals, internet users and interested parties in the protection of personal data that circles among various territories, way beyond Brazilian borders.

Some questions are inevitably in place: i) To what extent the proposed regulation for international data transfer, from the Brazilian legal system standpoint, is compatible with the norms and safeguarding already established by Brazil's Internet Bill of Rights regarding users' rights and civil liberties? ii) What are the technical, material and procedural limits imposed to the Legislative Branch - according to the law-making powers assured by the Brazilian Constitution, by Brazilian law and applicable international instruments- to the regulation of this subject at the domestic level?

This policy paper attempts to critically comment on the state of the art of the pending Bill, approaching the debate to specialists' views and compared insights in order to submit recommendations for reshaping the existing models adopted by the draft legislation.

5 With this regard, presentations from the annals of the 1st Seminar on "Governança das Redes e o Marco Civil da Internet", held at Universidade Federal de Minas Gerais in May 2015, organized by POLIDO, Fabrício B.P. and ROSINA, Monica S.G, *Governança das Redes e o Marco Civil da Internet: Liberdades, Privacidade e Democracia*. Belo Horizonte: Faculdade de Direito da UFMG, 2015. Available at: <http://www.direito.ufmg.br/gnet/ebooks/grmcivil.pdf>. Accessed on July 15, 2016.

6 KUNER, Christopher. Regulation of transborder data flows under data protection and privacy law: past, present, and future. *TILT Law & Technology Working Paper*, n. 016, 2010.p. 34-35.

7 See, for instance, WEBER, Rolf H. Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law,* p. 117 - 130, 2013. p.118

2. Relevance of the discussion and methodology of analysis

The analysis proposed by this policy paper is not associated with any political or sectoral interests, and is based on two premises. The first one focuses on the attempt to clarify the importance, sensitivity and vanguard of the topic of internet users' data international transfer to Brazilian congresswoman and congressman. Secondly, there is a need to compare and contrast articles from Federal Law n. 12,965 (Brazil's Internet Bill of Rights) and Bill n. 5,276, which directly or indirectly undertake material and procedural aspects of international transfers of data.

a. Article 11 of the Brazil's Internet Bill of Rights

> *Art. 11. All transactions involving the collection, storage, retention or processing of records, personal data, or communications by internet service and applications providers must comply with Brazilian law and the rights to privacy, protection of personal data, and confidentiality of private communications and records, if any of those acts occurs in Brazilian territory.*
>
> *§1. The provisions of this article apply to all data collected in Brazilian territory and to the content of communications if at least one of the terminals is located in Brazil.*
>
> *§2. The provisions of this article apply to activities conducted by foreign-based legal entities, if they offer services to the Brazilian public or at least one of the members of the legal entities' economic group has an establishment in Brazil.*
>
> *§3. Internet connection and applications providers must provide, in the manner established by regulation, information needed to determine whether Brazilian law on collection, retention, storage and processing of data and on protection of privacy and confidentiality of communications has been complied with.*
>
> *§4. Regulations on the procedure for determining whether infractions of this article have occurred will be issued by decree*[1].

Since Bill 5,276 is still being scrutinized under a priority regime in Congress, Brazil's Internet Bill of Rights is the single statutory law in Brazil establishing mechanisms specifically addressing personal data online. For the purpose of this study, Article 11 of Marco Civil is related to four normative clusters regarding privacy and data protection in cases of international transfer:

1) A **compliance rule with Brazilian law** applicable to any action related to transborder data transfer, on situations in which at least one of them is effected or produces effects within national territory, therefore connected to Brazilian law ("*any operations of conduct, storage, safekeeping and treatment of records, personal data or communications by connection and application providers, in which at least one of these actions take place on national territory*"); here, we could talk about a "Brazilian law related compliance" test;

2) Enforcement of "*privacy rights, data protection and confidentiality of private communications and records*" by connection and application providers;

3) Statutory obligations for foreign legal persons (e.g. companies incorporated or based overseas) with regard to the respect of Brazilian laws when these foreign-based entities offer internet services in Brazil, even in case they do not own local offices or subsidiaries in the country; here we could talk about "domestic compliance rules" by foreign companies);

4) Legal and institutional expectations targeting companies, either incorporated and existing in Brazilian or in a third country, involved in activities concerning the collection of data and information by users/clients with to regard to access to their own data stored abroad.

Based on the structure and scope of application of Article 11 of Brazil's Internet Bill of Rights, it is important to analyse some components and functions of the legal regimes of personal data protection in digital environments, comparing them with international and domestic rules.

Data Protection on a Global Scale and International Data Transfer

In 1980, The Ministry Committee of the *OECD - Organization for Economic Co-operation and Development* - published the document named "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"[8], establishing basic principles underlying data protection frameworks and information exchange between countries with laws and regulations in compliance with these principles.

Although the 1980 Guidelines are not binding documents to OECD Member States (having a "soft law" character, as other similar instruments), they are susceptible to different kinds of implementation or domestication within state law. During the 1980s, however, countries do not seem to have received enough incentives for the adoption of laws and internal regulations dealing with data and privacy protection, in particular in view of the emerging communication systems[9].

One could contend that European Union Directive 95/46/EC of 1995[10] represented the first supranational piece of legislation regarding privacy and data protection. As set out in Article 1, EU Member States should ensure in their domestic legislation, following the parameters of the Directive, the protection of fundamental freedoms and rights, especially privacy, with regard to personal data. As a contextual matter, the Directive 94/49 resulted from an offensive by the European Communities in the 1990s to aggressively regulate the protection of personal data[11], differing from the legislative strategy

8 OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Available at: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part3>. Accessed on May 31, 2016.

9 Regarding the difficulties about reaching a consensus on the laws of data protection between the 1970s and 1980s, as well as multiple interests from the information and communication industries, during negotiations at the OECD and European Economic Communities, specifically, see COLE, Patrick E. "New Challenges to the US Multinational Corporation in the European Economic Community: Data Protection Laws", in *New York University Journal of Int'l Law & Policy*, vol. 17, 1984, p. 893.

10 *Directive 95/46/EC*, from October 24, 1995, regarding the protection of individuals on the treatment of personal data and the free circulation of such data. Available at: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX-:31995L0046&from=PT>. Accessed on May 30, 2016. For purpose of this policy paper, we are referring to the EU Directive to the extent that it clearly influenced the legislative patterns incorporated to the Brazilian Draft Bill. As further explored, the Directive was revoked by the European Union's Regulation n. 2,016/679, in April 27, 2016 (herein, the "EU General Data Protection Regulation 2016/679 (GDPR)), which wil come into force as of May 25 2018.

11 For critical comments on Directive 95/46, with different perspectives, see FROMHOLZ, Julia "The European Union data privacy

in the United States of America for a reputedly absenteeism in this sector. The European instrument was inspired by a liberal rationality about the legal framework for data treatment/processing by companies and associations, characterized by self-regulation, without governmental interference. Furthermore, the Directive envisaged a contractual safeguarding regime susceptible to bargaining between economic agents and users[12].

Article 4 of the Directive 94/46 already provided a solution to the "Applicable National Law", basically providing that those responsible for the processing of personal data within the limits of the European Union, even foreigners, ought to comply with the legislation of their State Members[13].

Brazil's Internet Bill of Rights, following this rationale and the contemporary ongoing debate in Europe, introduced a very similar rule in Brazilian law, maintaining certain parallelism with the formula adopted by the European Directive. According to the rule entailed by Article 11 of Brazil's Internet Bill of Rights, companies - Brazilian or foreign - or service suppliers carrying out activities involving data collection and processing in Brazil, must also comply with local law.

Between 2008 and 2015, the European Union was devoted to the modernization of its legislation, whereby Parliament and the Council enacted the **Regulation 2.016/679, of April 27, 2016**, on the protection of personal data ("European Union's Regulation on the Protection of Personal Data"), which will be directly applicable to Member state´s legal systems as of May 25, 2018[14]. In addition to provisions on user rights to their personal data, the newly enacted regulation provides for a set of rules regarding the transfer of data to "third countries" and international organizations, mandating the European Commission to monitor the "level of protection" granted or offered by a certain State, territory or processing sector abroad for personal data of users based in countries of the European Union. The assessment measure over this level of protection can be established, including objective criteria such as safeguards expressed by, *inter alia*, general contracting conditions, data protection clauses and binding business rules.

Amongst the recitals for adopting the Regulation, the EU institutions expressed their concerns and expectations regarding the data transfer regime, which are very significant for the Brazilian context:

> "(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new chal-

directive", in *Berkeley technology law journal* vol.15, 2000, p. 461-484; WESTIN, Alan F. "Social and political dimensions of privacy." *Journal of social issues* vol 59, n.2, 2003, p. 431-453 e BIRNHACK, Michael D. "The EU data protection directive: an engine of a global regime", in: *Computer Law & Security Review,* vol. 24, n.6, 2008, p.508-520.

12 With this regard, see Julia FROMHOLZ, Op.cit., p. 461-484, p.462: *"In the European Union , governments have moved aggressively to regulate the use of personal data. In the United States, on the other hand, the government has largely refrained from such regulation, instead allowing companies and associations to regulate themselves, save for a small number of narrowly drawn regulations targeting specific industries".*

13 It is important to highlight that, in the system of the European Union, the directives, unlike regulations that are directly applicable, are destined to straighten and harmonize national laws. From EU's Directive, there has been a movement of legal adjustment from Members. It has created new regimes of data protection, which varied in certain aspects. Only after the implementation of Regulation 649/2016, the movement of legal updating became complete.

14 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND COUNCIL on April 27 de abril 2016, regarding the proteção of individuals on the treatment of personal data and the free flow of this data, which also revokes Directive 95/46/CE (General Regulation about Data Protection). Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&-from=EN>. Accessed on December 19, 2016.

lenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision"[15].

Regarding the business practices of companies - either national and foreign - with activities related to the collection of customer data, Article 11.3 of Brazil's Internet Bill of Rights was strongly inspired by the repealed Directive 94/46, both of which complying with the principle of the right to information. Here, the principle appear to play a role to central to the relationship between companies and users/clients in relation to access to personal data.

Articles 10, 11 and 12 of the the Directive 94/46/EC established that those who held their personal data collected, regardless of the collection´s method or technique, should have been provided with mechanisms for accessing such data, as well as a basis for identifying the person responsible for the treatment and purpose of data collection. It should also be noted that Directive 94/46/EC did not establish how information would be processed, leaving that matter to the legal and administrative discretion of EU Member states.

Further on comparative legal trends, the emergence of national legislations to protect personal data is recent, although the concern raised by the theme goes back to the 1970s in the European Communities and OECD. At international level, specifically, there are no specific multilateral treaties and conventions on the subject.

The Organization of American States, to which Brazil is a Member, has been engaged in exploring normative issues regarding data protection since 1996, with a broad

15 Available at: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>. Accessed on March 24,2017.

mandate that provides for the drafting of a "comparative study on the different legal regimes, policies and enforcement mechanisms to protect personal data, including domestic legislation and self-regulation, in order to explore the possibility of a regional regulatory framework.[16]" Likewise, the OAS Department of International Law has prepared the "Preliminary Draft of Principles and Recommendations on the Protection of Personal Data", in which the Organization's concern to protect the flow of information and personal data in the Americas is evident[17].

Within the Latin American context, Argentina defined several statutory standards for the protection of personal data in Law 25,326, of 2000[18]. Art. 44 of the Law establishes that, in the case of personal data located in Argentine territory, the general principles regarding protection, the rights of data owners, users and responsible for files, records and databases, as well as the penalties applied, shall comply with national law exclusively. The original formula deployed by Brazil's Internet Bill of Rights is similar to the one entailed by Law 22.236/2000, since it is based on the immediate application of the national law for the protection of personal data that are stored or managed in their territory. From the standpoint of private international law technique, it appears that both solutions are based on a unilateral conflict rule, by which the only possible applicable law, in terms of **compliance rule to cross-border data transactions**, is the **law of the forum** (*lex fori*).

The difference, however, seems to lie in the extraterritorial application of domestic laws. Brazil's Internet Bill of Rights, in its Article 11, caput, expressly authorizes the application of Brazilian laws to reach acts of *"collection, storage, custody and treatment of records, personal data or communications by connection providers and internet applications"*, where at least one objective connecting factor linking the transaction to Brazilian legal system is identified. Among these connecting factors there is an objective contact with the "national territory".

Still with regard to Argentine law, the means by which foreign companies carry out international data transfer are regulated by Article 12 of Law 25,326, in a similar fashion to the repealed European Union Directive 95/46/EC. It prohibits the transfer of personal data of any kind with international countries or bodies that do not have adequate levels of protection. In addition, the existing legal regime in Argentina also provides for exceptions in cases of international legal cooperation (administrative and judicial), medical data exchange, banking transactions, transfers respecting treaties to which the country is a party, as well as transfers of data employed to assist courts and administrative bodies to fight against organized crime, terrorism and drug trafficking related practices.

This approach to international data transfer in Argentina appears to be consistent with the 2011 OAS Principles on Personal Data Protection, and it serves to elucidate how the Brazilian regulatory experience can be shaped into a specific law. Principle 8 of the OAS Principles provides **guidance** for the **development and interpretation of data protection standards** in the context of international transfer. For the purpose of ana-

16 See OAS General Assembly's Resolution n. 2661 (AG/RES. 2661, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES (Aprobada en la cuarta sesión plenaria , celebrada el 7 de junio de 2011), Available at: <http://www.oas.org/dil/esp/AG-RES_2661_XLI-O-11_esp.pdf>. Accessed on March 15, 2017.

17 CP/CAJP-2921/10, *Proyecto de Principios y Recomendaciones Preliminares sobre la Protección de Datos Personales*, 17 octobre de 2011. Avaliable at: <http://www.oas.org/dil/esp/CP-CAJP-2921-10_rev1_corr1_esp.pdf>. Accessed on March 15, 2017.

18 ARGENTINA. *Lei n. 25.326*, of October 30, 2000. Available at: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>. Accessed on March 15, 2017.

lyzing the Bill under discussion at Brazilian Congress, and its compatibility with the 1988 Constitution, existing treaties and conventions and the principles enshrined by Brazil's Internet Bill of Rights, it is important to understand the scope and reach of Principle 8 of OAS, as well as its guidelines to national legislators and courts:

a) **subsidiary nature of international data transfers**: according to the Principle, they should only be performed in the event that the data exporter assumes the subjective and objective responsibility for data protection, or when the State of the location or destination of the transferred data provides, at least the same pattern of protection of personal data as the OAS Principles;

b) **mandatory material and procedural protection of personal data**, according to the previous item, which must be met by the country of origin and the destination of the data: data transit countries (countries where data passes, travel) are not required to provide these standards of protection;

c) **"minimum protection" standard**: the degree of protection granted to data is assessed in accordance with the following factors: (i) the nature of the data; (ii) its country of origin; (iii) the country of destination of the data; (iv) purpose of processing the transferred data: (v) the existence and validity of security measures for the transfer and processing of personal data.

OAS Principle 8 provides for the international transfer of data even in cases where the country of reception or destination does not offer the same level of protection as that one guaranteed by the regulation of the country of origin. However, said transfer is subject to certain conditions of fair and legal processing as a matter of **safeguards**:

a) **accountability of data transferred and stored:** incidents in the event that local laws do not provide for protection of imported data and as an imposition to the exporter - the company responsible for the transfer - to ensure the protection of data regardless of its geographical location (residence, address of incorporation) and the possibility to provide sufficient evidence of protection when requested;

b) **the guarantee of a protection materialized by a contractual relationship between parties:** this condition suggests that personal data may be transferred to a receiving country which does not provide the same protection for personal data as that provided by the Principles, provided there is a contractual clause obligating the exporter to provide the same level of data protection;

c) **the existence of laws permitting international transfer:** a national law may allow the transfer of personal data to a third State which does not accord the same protection standard as that of the Principles if: i) the transfer of data is necessary and for the benefit of the person (data owner) in a contractual relationship; ii) the transfer is necessary for the protection of some vital interests, such as avoiding substantial damage or death of the person or of third parties; or (iv) the data exporter is responsible for the protection of the data[19];

d) **consent**: the transfer of personal data to a receiving country that does not grant the same protection standard may be allowed in the event that the af-

19 Principle 8 admits the alternative nature of the conditions for the case of laws permitting transfer to a country (destination) that does not grant the same protection standards as that of the OAS regulation.

fected person consents unequivocally to the transfer; and

e) **technological innovation**: rules governing data and information transfers between countries should reflect the reality of the use of the Internet, as well as the duty to take into account the fact that restrictions on data transfer may limit technological innovation and economic development.

There is some dissent among OAS Members regarding methods of regulating international transfers, specifically as to the determination of a concept as open as the one concerning the **equivalent protection in the beneficiary country**. At a first blush, it appears that technical and implementation difficulties exist in practice and they have also been subject to the previous work on modernization of European Data Protection legislation, which has resulted in the EU Regulation n. 679 of 2016 (replacing the old Directive 94/46/EC)[20]. On the other hand, the OAS Principles recognize that personal data must be protected within the context of international transfers, but Members might have some degree of flexibility as to the forms of protection to be granted[21]. This would be the case for the legislative choices to be made in connection with the current Draft Bill in Brazil.

Once the preliminary examination of the situation of international data transfer and the protection of personal data at the international and regional levels has been made, a **first conclusion** can be drawn:

Any option made by the Brazilian legislator must necessarily be tested in the light of a principle of compliance of Brazilian law with international norms and guidelines regulating the issue (as in the case of the OAS Principle 8 of 2011), as well as national comparative and regional experiences (as in the case of the European Union).

Why this conclusion is relevant to the context at stake? It appears to the authors that any solution designed to address a legal regime or regulation of data protection involved in international data transfer, from either a national or domestic perspective, could not disregard or collide with the major understanding of the currently adopted standards applying to the processing of personal data. Even though countries have yet to reach a consensus on specific statutory legal patterns, the methods of protection of personal data by means of treaties and conventions or the mechanisms to ensure legal and contractual minimum standards of security and privacy in the cross-border flow of data, the signatories of this policy paper understand that the minimum levels already outlined must be ensured and discussed, in favor of a principle endorsing a right of access by users to their personal data and a prohibition of less-favourable treatment in case of international transfers.

It is precisely in the favorable interpretation of this right of access, also reinstated by Brazil's Internet Bill of Rights, that the legislator should think around or design the reflexes or social impacts of the future objective law, for the sake of a harmonization that is projected globally.

20 This process culminated in the approval of the *General Data Protection Regulation 679/2016.*

21 See.Article 8 of the 2011 Principles.

Draft Bill n. 5,276 - Chapter V: "International Transfer of data"

Article 33. International transfer of personal data is only allowed in the following cases:
I - for countries that provide level of protection of personal data at least equal to that of this law;
II - where the transfer is necessary for international judicial cooperation between public intelligence and investigative bodies, in accordance with the instruments of international law;
III - when the transfer is necessary for the protection of the life or physical safety of the owner or third party;

IV - when the competent authority authorizes the transfer;
V - when the transfer results in a commitment made in an international cooperation agreement;
VI - when the transfer is necessary for the execution of public policy or legal attribution of the public service, being publicized in terms of art. 24.
VII - when the holder has given his consent to the transfer, with prior and specific information about the international character of the operation, with an alert regarding the risks involved.

Paragraph: The level of data protection in the country will be assessed by the competent body, which will take into account:
I - general and sectoral rules of the legislation in force in the country of destination;
II - nature of the data;
III - compliance with the general principles of protection of personal data provided for in this Law;
IV - adoption of security measures provided for by regulation; and
V - other specific circumstances relating to the transfer.

Article 33 of Draft Bill n. 5.276 defines the hypotheses in which international transfers shall be allowed in Brazil. The following boxes outlines the analysis of the legal provisions that, once approved, will inform the legal regime for international transfer of data involving parties related to Brazilian territory and further connecting factors:

I - for countries that provide level of protection of personal data at least equal to that of this law;

Subsection I of article 33 is based on the geographical criteria defined in the repealed European Directive 95/46 of 1995[22], for the authorization of international data transfer. In the old EU Directive, the legislative pattern took into account the potential risks of underprotection to which the data would be subject in third countries and, therefore, it set criteria based on the comparison between the domestic protection standards[23].

Any assimilation or comparison standard rule should be employed to scrutinize each country's data protection regime, according to the parameters outlined in the paragraph of proposed Article 33. Generally, a geographical model concentrates the equivalence and adequacy criteria that authorize the international transfer of data. It thus deal with the level of protection accorded by each country, as well as it defines personal data which are collected, processed and stored in this country´s territory, according to its domestic laws and international treaties.

The geographical model conceived in 1995 within EU law sought to promote the harmonization of national laws in order to guarantee equivalent standards of protec-

22 Article 25 (1) of the revoked European Directive 95/49 set out that: "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection." Available at: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX-:31995L0046&qid=1465326802683&from=en>. Accessed on June 7, 2016.

23 WEBER notes that the comparison established in the geographical model is expressed by the assessment of the recipient country's levels of protection as "adequate", "similar" or "equal". See WEBER, Op. Cit., p. 122. The Brazilian Bill uses the term "comparable", which also reveals the option for the geographic model.

tion and, as a consequence, to facilitate the transfer of data between EU Member states and to encourage it in a more preferential fashion than to third countries. This model is based on a regional levelling approach. The scope of application of the EU legislation is not realistic or suitable to Brazilian context. The rule of subsection I of the draft Article 33 should not be automatically implemented in domestic law, but adapted to an environment which does not correspond to EU law.

The 1995 European Directive, while pioneering the definition of the rules governing the transnational transfer of personal data, does not go without criticism. The geographical model - that is reproduced by Article 33.I of Brazilian Bill n. 5,276 - opens different levels of "protection adequacy" among countries over time, and, in spite of other hypotheses provided for by the system itself, has the effect of limiting international transfer processes of data[24]. This is because the comparison is static; it only takes into account the existing statutory laws or governmental standards for protection, without considering, for example, business practices related to the protection of data transferred at an international level.

The requirement of equivalent protection also raises some issues about its effectiveness, in particular because its inherent rigidity[25]. The difficulty of legislative harmonization between different countries that do not necessarily belong to the same community as the EU, and the bureaucracy that characterizes the procedure of authorization of transnational transfer, can generate illegal transfers, whose control, by volume, procedure and destination may not be monitored or inhibited by States adopting the geographical model. In the European Union, there are authorization to transfers in significantly lower numbers, which do not correspond to the economic and technological transactions that European countries establish with others around the world[26].

The legislator's option by the rule of article 33, I, based on article 25 (I) of the Directive, should also consider that the criterion is costly both for the state, which must maintain a structure of authorizations for the transfer and supervision of transnational operations to ensure their effectiveness, and for economic agents who must request permission to transfer the data. European experience thus reveals that a system based on equivalent protection and authorizations received, analyzed and delivered by State authority entails significant costs and the expenditure of time incompatible with the speed characterizing internet related transactions and interactions .

II - where the transfer is necessary for international judicial cooperation between public intelligence and investigative bodies, in accordance with international legal instruments;

Article 33, section II, deals with international data transfer for purposes of international legal cooperation, particularly with regard to the exchange of information in

24 The recommendation at an international level is that the transfer be as restricted as possible, even if data protection and security parameters are defined in each country. The OECD agrees with that according to the 1980 Recommendation on Protection of Privacy and the International Transfer of Personal Data. The text of the Recommendation is available at: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part3>. Accessed on May 31, 2016.

25 KUNER, Christopher. Regulation of transborder data flows under data protection and privacy law: past, present, and future. *TILT Law & Technology Working Paper*, n. 016, 2010. p.28.

26 According to KUNER, Op. cit., p. 28: "The fact that some of the largest economies in the world (such as China and Japan) have not been the subject of a formal EU adequacy decision means that there must be substantial non-compliance at least with regard to data flows from the EU to those countries."

the course of investigations conducted in other States. This topic is of utter relevance nowadays and has led to great discussion in a number of international fora. For example, during the XII United Nations Congress on Crime Prevention and Criminal Justice, held in Salvador in April 2010, parties adopted the *Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice and its Development in a Changing World*[27].

Paragraph 15 of the Declaration states that *"[UN] Member States are encouraged to strengthen international cooperation [in combating economic fraud and crimes of ideological deception], including through the exchange of relevant information and practices, as well as through technical and legal assistance"*.

Debates and progress on data transfer in the context of cross-border and collaborative criminal investigations have also taken place between the European Union (EU) and the United States. Both parties signed an *Umbrella Agreement*[28] in 2015 to establish a unified and comprehensive set of data protection rules to be applied to transatlantic information transfers within the framework of cooperation in criminal matters. Data security is such a key issue for European counterparts, so that the EU has conditioned the signature of the 2015 Agreement to the adoption of the *Judicial Redress Act*[29] by US Congress. This Act establishes equal treatment between citizens of the United States and the EU before the 1974 US Privacy Act. The Judicial Redress Act was promulgated by US Congress on February 10, 2016, and was sanctioned by President Barack Obama in February 24 of the same year[30].

In a report as of February 2016[31], the European Commission supported the view that the 2015 *Umbrella Agreement* is very important due to the fact that it sets standards for data processing, limitations on the use of information transferred and respect for individual rights. One of the rights ensured by 2015 EU-US Agreement is access to justice. It comprises the right of individuals to challenge, before domestic courts, decisions denying them access to data, or the right to rectify incorrect information. The right to judicial review will also enable them to seek damages for any unlawful disclosure of information[32].

In this context, Article 33, II, of the Brazilian Draft Bill is in line with the international trend to foster legal cooperation between different countries, ensuring authorization for the transfer of data associated to investigation procedures. In view of the potential clashes with existing provisions of Brazil's Internet Bill of Rights and the 2015 Code of Civil Procedure (in particular Art.26 on principles guiding requests of legal cooperation in international civil litigation[33]). It might be recommended to Brazilian legislators to in-

27 ONU, *Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice and its Development in a Changing World*. 2010. Available at: <http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/In-session/ACONF.213L6_Rev.2/V10529061A_CONF213_L6_REV2_S.pdf>. Accessed on June 1, 2016.

28 EUA-UE,*Umbrella Agreement.* 2015. Available at: <http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm>. Accessed on June 15, 2016.

29 EUA, *Judicial Redress Act,* 2015. Available at: <https://www.congress.gov/bill/114th-congress/house-bill/1428>. Accessed on June 15, 2016.

30 EUROPEAN COMISSION, *Transatlantic Data Flows: Restoring Trust through Strong Safeguards,* p.11, 117 final, Brussels, 29 February 2016, Available at: <http://europa.eu/rapid/press-release_IP-16-433_en.htm>. Accessed on June 15, 2016.

31 Idem.

32 Ibidem. p.12.

33 Art. 26. A cooperação jurídica internacional será regida por tratado de que o Brasil faz parte e observará: I - o respeito

clude a safeguard clause in the Draft Bill for procedural guarantees and due process in connection with international legal cooperation on data transfer.

> *III - when the transfer is necessary for the protection of the life or physical safety of the owner or third party;;*

Subsection III authorizes remittance of data abroad in order to protect the life or physical safety of the owner or third parties, even if the level of data protection at the place of destination is lower than the one accorded under Brazilian law. An example illustrating the importance of this subsection would be the transfer of medical records by a Brazilian health authority to a country where an individual suffered an accident or illness and his or her medical history becomes necessary to assist foreign authorities to decide on appropriate medical treatment. Without these data, the individual's life could be at serious risk. The purpose of the provision at stake is twofold: first, it addresses urgent situations demanding an exceptional treatment to personal data in transit; secondly, it refers to expedite and spontaneous cooperation proceedings involving the transfer of data, particularly where natural and legal persons are in intense mobility at international level.

The provision of Article 33, III, also mirrors a similar provision in the Directive of the European Union n. 2016/680, adopted on 27 April, 2016[34]. According to Article 38, paragraph 1, "a", it is possible to transfer personal data to a State which does not ensure an adequate level of protection when such a transfer is necessary "to protect the vital interests of the data subject or another person." The predecessor EU Directive n. 95/46/EC had a similar formula, as its Article 26(1)(e) authorizes the international transfer of data when "[...] necessary to protect the vital interests of the data subject".

European Union directives do not specify what would be the vital interests that justify the transfer of data. On the contrary, Brazilian legislature already determines, in the legal text itself, that transfers can only occur, with a focus in Article 33, item III, to protect the "life and physical integrity of the owner or third party". According to the Data Protection Unit of the General Directorate of the European Union for Justice, Freedom and Security, the term "vital interests" in the two EU directives above concerns serious medical emergencies. In this sense, there would be no considerable divergence between the European and Brazilian legal regimes with regard to the rule on data transfer for purpose of protection of life and physical integrity of the owner or third party.

Ireland, in turn, by means of the 2003 Data Protection Act[35], expressly authorizes the international transfer of data to protect not only life, but also property. This solution

---

às garantias do devido processo legal no Estado requerente; II - a igualdade de tratamento entre nacionais e estrangeiros, residentes ou não no Brasil, em relação ao acesso à justiça e à tramitação dos processos, assegurando-se assistência judiciária aos necessitados; III - a publicidade processual, exceto nas hipóteses de sigilo previstas na legislação brasileira ou na do Estado requerente; IV - a existência de autoridade central para recepção e transmissão dos pedidos de cooperação; V - a espontaneidade na transmissão de informações a autoridades estrangeiras".

34 EUROPEAN PARLIAMENT AND COUNCIL, *Directive 2016/680,* of April 27, 2016, on the protection of individuals with regard to the processing of personal data by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions and on the free movement of such data, and repealing Decision Framework 2008/977/JAI of the Council. Available at: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L0680&from=PT>. Accessed on June 15, 2016.

35 IRELAND. *Data Protection Act,* 2003. Available at: <https://dataprotection.ie/viewdoc.asp?DocID=1467&ad=1>. Accessed on June 15, 2016.

appears to be exorbitant in terms of the reach or coverage of the exceptional rule on data transfer to a less protective country. According to Article 11(4)(a), of the Irish Act, transfers of data to states without an appropriate level of protection may occur, as long as they are necessary "to prevent injury or other damage to the health of the data subject or serious loss or damage to property of the data subject or otherwise to protect his or her vital interests, and informing the data subject of, or seeking his or her consent to, the transfer is likely to damage his or her vital interests".

France, on the other hand, has a legal regime similar to that which Brazil intends to implement. Article 6(2)(e) of the Federal Data Protection Act (*Loi Fédérale sur la Protection des Données*)[36] indicates that data transfers may occur when "[...] necessary to protect life or the physical integrity of the person concerned[37]".

Article 33, item III, should be understood as entailing an important rule, which purpose is to protect the life and integrity of Brazilians who are at risk or in a urgent situation abroad. In addition, it is aligned with foreign and international regulatory instruments, in particular with EU directives.

IV - when the competent authority authorizes the transfer;

Cases of international transfer of data that will require prior authorization by the competent body are listed in Article 34 of Bill n. 5,276. The criteria for authorization by the competent authority are described in the same provision.

V - when the transfer results in a commitment made in an international cooperation agreement;

Art.33, V of the Draft Bill states that Brazil should transfer data to another State when an obligation to this effect is established through an international cooperation treaty. According to the Brazilian Supreme Court (STF), treaties and conventions have, as a general rule, the status of ordinary law within national legal system. Only human rights treaties may enjoy a specific constitutional level legal regime[38]. Thus, international cooperation treaties ratified by Brazil, in general, have the effect of ordinary laws.

Within Brazilian treaty legal practice, two relevant instruments impose the obligation for the domestic authorities to transfer data to other states. The first is the *United Nations Convention against Transnational Organized Crime*[39]. According to Its Article 18, which governs mutual legal assistance, "State Parties shall provide each other with all

36 FRANCE. *Loi Fédérale sur la Protection des Données.* 1992. Available at: <https://www.admin.ch/opc/fr/classified-compilation/19920153/201401010000/235.1.pdf>. Accessed on June 15, 2016.

37 The original text in french reads as follows "*la communication est, en l'espèce, nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée*".

38 Pursuant to Article 5, paragraph 3, of the Brazilian Federal Constitution of 1988, human rights treaties approved in each House of the National Congress in two rounds, for three fifths of the votes of the respective members, shall be equivalent to constitutional amendments. In addition, on December 3, 2008, in the judgment of SR 466,343-SP and HC 87,585-TO, the Brazilian Supreme Court, adopting the opinion given by Justice Gilmar Mendes, determined that human rights treaties that were not approved with a qualified quorum of Article 5, 3, of the Constitution will have supralegal status, that is, they will be hierarchically below constitutional norms and above the other infra constitutional norms.

39 UNITED NATIONS. *United Nations Convention against Transnational Organized Crime,* 2000. Available at: <https://www.unodc.org/lpo-brazil/pt/crime/marco-legal.html>. Accessed on MArch 15, 2017. The Convention was signed by Brazil on December 12, 2000, ratified on January 29, 2004 and incorporated into Brazilian law by Decree n. 5,015, of 2004, the year in which it came into force for the country. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm>. Accessed on June 15, 2016.

possible judicial assistance in the investigation, prosecution and other judicial acts relating to the offenses provided for in this Convention...". Article 18(3) expressly mentions that such reciprocal judicial cooperation may be requested to provide information, evidence and originals, or certified copies of documents, including administrative, banking, financial, commercial and business documents.

In addition, Article 18, paragraph 2, indicates that the transfer of data should also occur when the investigated or prosecuted is a legal entity. However, it provides that the transfer of information from legal persons shall only take place to the extent permitted by the "*relevant laws, treaties, agreements and protocols of the requested State Party*...". Hence, the Convention against Transnational Organized Crime expressly allows State Parties to limit the obligation to provide data of legal persons, either through another treaty or through the enactment of domestic laws.

Finally, Article 18, paragraph 4, of the Convention sets out the discretion (not an obligation) for State Parties to transfer unsolicited information when they believe that such data will assist in the conduct of criminal investigations and prosecutions in other countries. The competent authorities of a State Party may, without prior request, communicate information on criminal matters to a competent authority of another State Party, if it considers that such information would help to undertake or successfully conclude investigations and prosecutions, or lead the latter State Party to make a request under this Convention.

Another important treaty to analyse is the 2000 *United Nations Convention against Corruption*[40]. Pursuant to its Article 46, paragraph 1, "State Parties shall afford each other more extensive mutual legal assistance in respect of investigations, prosecutions and prosecutions relating to the offenses covered by this Convention."

Similar to the *Convention against Transnational Organized Crime*, the 2000 *Convention against Corruption* also provides an illustrative list of possible requests for legal aid. Among the topics on the list are the presentation of court documents, information and evidence and the delivery of original documents or certified copies, including public, banking and financial documentation, as well as the corporate or commercial documents of companies.

Another parallel with the *Convention against Transnational Organized Crime* is regarding the prerogative of Brazilian authorities to forward information not required by other States, when it is understood that these data is relevant to investigations of judicial procedures at another territory[41]. It also provides that the transfer of information from legal persons will occur "[...] "to the fullest extent possible under relevant laws, treaties, agreements and arrangements of the requested State Party with respect to investigations, prosecutions and judicial proceedings..."[42].

The existing treaties to which Brazil is a signatory party, be it at bilateral or multi-

40 UNITED NATIONS. *United Nations Convention Against Corruption*, 2000. Available at: <https://www.unodc.org/lpo-brazil/pt/corrupcao/convencao.html>. Accessed on June 16, 2016. The treaty was signed by Brazil December 9, 2003 and ratified in January 15, 2005. It came into force for Brazil in December 14, 2005, being incorporated in our legal order by Decreet n. 5,687, of January 31, 2006. Available at: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Decreto/D5687.htm>. Accessed on June 16, 2016.

41 *United Nations Convention Against Corruption*, Article 46(4): "Without prejudice to domestic law, the competent authorities of a State Party may, without prior request, transmit information relating to criminal matters to a competent authority in another State Party where they believe that such information could assist the authority in undertaking or successfully concluding inquiries and criminal proceedings or could result in a request formulated by the latter State Party pursuant to this Convention".

42 *United Nations Convention Against Corruption*, Article 46(2).

lateral level, will be equally of an utmost importance for the precise scope of application of the provision addressed by Art.33,V, of the Draft Bill. In sum, any interplay between data transfer, as it is understood by Internet Law in a narrow sense, and international legal cooperation under specific treaties and conventions may request a balanced approach for the interpretation and application of a such statutory provision by Brazilian courts.

VI - when the transfer is necessary for the implementation of public policy or fulfillment of legal duties in the public service, being publicized in terms of art. 24.

This provision seeks to authorize international data flow within the scope of certain public policies and legal duties of public service, as long as a due publicity is ensured in connection with the transfer at hand. At first blush, it refers to a rule also targeting discretionary powers of a public agent, who may decide upon the necessity of the data transfer, in line with the two determinants set forth by the rule - the context of implementation of public policy and fulfillment of legal duties.

In a comparative legal perspective, it may be noted that this authorization for international data transfers under the scope of public interest is taken in a narrow sense. In Switzerland, the transfer of data to countries that do not offer the same level of protections and guarantees may only occur when "indispensable to the safeguard of a preponderant public interest".[43]

The European Union Directive no. 2016/680, on its hand, provides that said transfers will be possible "for the prevention of an immediate and serious threat to public security of a Member State or a third country" [44]. Both of these instruments establish that data transfers to unsafe places, as means of protecting public interest, are exceptional measures.

Latin American States have also adopted restrictive legal instruments in this matter. Uruguayan law allows for transfer whenever "[...] necessary or legally required for the protection of an important public interest" [45]. Colombia las authorize transfers when "[...] legally required for the protection of public interest" .Argentina, by its turn, has no exception referring to the safeguard of public interest in its Data Protection legislation. [46] Colombia laws authorize transfers when "[...] legally required for the protection of public interest" . Argentina, by its turn, has no exception referring to the safeguard of public interest in its Data Protection legislation.

Article 33, VI, of Brazilian Draft Bill on the other hand, appears to turn data transfers to non-safe locations an integral part of public function or legal duties in connection with public service. Under said provision, such transfers may be carried out whenever

43 SWITZERLAND. *Loi fédérale sur la protection des données*, 1992. Available at: <https://www.admin.ch/opc/fr/classified-compilation/19920153/201401010000/235.1.pdf>. Accessed on June 16, 2016. Art.6(2)(f). Original text in French reads: "indispensable soit à la sauvegarde d'un intérêt public prépondérant".

44 *Directive no. 2016/680* art.38(1)(c).Original text in English reads: "*for the prevention of an immediate and serious threat to public security of a Member State or a third country*".

45 URUGUAY. *Ley 18.331 (Protección de datos personales y acción de 'habeas data'")*, 2008. Available at: <http://www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley-n%C2%B0-18331-de-11-de-agosto-de-2008.html>. Accessed on June 16, 2016. Art.23(5)(d). Original text in Spanish reads: "la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante"

46 ARGENTINA. *Lei n. 25.326*, Art.12, October 30, 2000. Available at: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>. Accessed on May 30 2016.

public service or the implementation of a specific public policy so demands, as long as they all comply with publicity norms.

In fact, said provision should foresee, in an express form, that its applicability would be limited to relevant public interests and ensure the right of individuals to oppose it before the Public Administration and domestic courts. On the contrary, public authorities could perform massive transfers of personal data to non-safe locations, threatening the effectiveness of the Article 33, I or Art. 33, VII. The intended provision under Art.33, VI, could not become an open letter or uneven harbour favouring Brazilian governmental bodies. It appears to represent one more obsession by public service empowerment in Brazil, with several concerns to personal data collection, management and transfer.

> *VII - whenever the right holder has granted its consent with the transfer, with previous and specific information about the international character of the operation, with alert as to any risks involved.*

Article 33, VII, deals with *consent*, which must be construed in a coherent and interactive fashion with other provisions of the Bill dealing with consent requirement for the collection and treatment of personal data. For instance, Article 7, I, of the Bill defines, amongst the conditions for data treatment the "free, informed and unequivocal" consent. Those three "steps" surrounding consent are reaffirmed in Article 9, according to which consent must be "made available in written form or through any other certifiable means". Finally, there is a consent requirement for treatment of sensitive personal data, which, according to Article 11, item I, is prohibited unless "free, unequivocal, informed, expressed and specified by its holder".

Adjectives such as "unequivocal" and "informed" appear to highlight the Bill's concern with the mandatory requirements for terms of use of services when dealing with personal data. The basic premise is that, as long as all the circumstances of use and treatment of the data are clear and well explained, users will have enough information to authorize or not the transfer of their personal data.

Based on the underlying legislative rationale, it might be possible to associate the provision at stake with the so called "*transparency and choice*" model (also known as *notice and consent,* or *informed consent* model). In such system, transparency by the part which seeks the data would offer conditions for a clear and valid choice by the other party which gives them. In that sense, it would be admitted that, as long as all information concerning the destination and use of the data are given to the user in a transparent form, he may make rational decisions regarding ceding his data. This informative process would confer greater control to the individual and therefore also guarantee his protection against improper use of his data. It is important to highlight that the model opts, most of the times, for a *take it or leave it* adhesion by the user - either he agrees with data transfers with all postulated reserves, or rejects the service entirely.[47]

Despite possessing adequacy features, the *transparency and choice* model in practice presents a few flaws. This is because information concerning treatment of data are handled to the user by means of documents such as "Terms and Conditions" and "Privacy Policy". These are extensive and complex texts, written in technical terminology

47 NISSENBAUM, Helen. A Contextual Approach to Privacy Online. *Daedalus, the Journal of the American Academy of Arts & Sciences*, v. 140, n. 4, p. 32, 2011. p. 34-35.

that circulate through most online services, such as social networks and communication platforms. For that reason, it cannot be expected that an user shall be fully informed about all the conditions under which his data will be submitted. Here, the requisite could not be satisfied by operational means due to the lack of or insufficiency of information regarding data treatment.

In practice, "terms of use", "terms of service" and "privacy policy" are ignored by users, creating what is called the "paradox of transparency". The user, despite having access to information, chooses to ignore the conditions under which its data is submitted to due to the complexity, extension and detailing of the terms[48]. This is likely to occur in such a manner that accepting the terms does not imply free, informed and unequivocal consent as presumably expected by the Draft Bill's provisions.

The transparency model proposed by the Brazilian legislator at this stage is replicated in connection with international data flows. Beyond the generic criteria for consent request, the cross-border nature of data flows must be made clear to stakeholders/agents, as well as its risks. The European Directive 95/46, in a similar vein, adopted the transparency and choice model as established by its Article 2(h), in which consent is understood as *"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"*[49]. Furthermore, Art. 26 of the Directive admits transfers between countries without an adequate level of protection as long as unequivocal consent is verified.[50]

Some concern has been raised as to a possible conflict between the consent model utilized by the Brazil's Internet Bill of Rights and that adopted by the Data Protection Bill. Brazilian law follows the principle in which specific legislation derogates broader legislation (*lex specialis derogat legi generali*). Under that hierarchy, norms from Brazil's Internet Bill of Rights would apply for all cases involving consent on the Internet, even though there are cases in which the model proposed by the Data Protection Bill would be better suited (i.e., matters involving data protection and consent on the Internet).

The parameter that serves as basis for the concept of consent on Articles 7 and 9, and that involves control of data by the user through information, seeks to reduce economic and informational asymmetries between consumers and entities collecting, processing and transferring data. The system established by Bill n. 5276 must also be applied to transborder data flows, especifically under item VII, which authorizes transfers when agreed upon by the user.

48 G EPI - Grupo de Ensino e Pesquisa em Inovação, FGV São Paulo. Contribuição ao Anteprojeto de Proteção de Dados Pessoais. São Paulo, p. 4-15, 2015. p. 5-6.

49 Recital 11 of the EU General Data Protection Regulation 2016/679 (GDPR), which will take effect in May 25 2018, reads: *'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.*

50 PARLIAMENT AND COUNCIL OF EUROPE, *Directive 95/46/CE*, from 24 of October 1995, relative to protection of single persons in what concerns personal data treatment and free flow of data. Available at: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Accessed on May 30, 2016.

Single paragraph. The degree of data protection will be evaluated by a competent authority, and shall take into account:

I - general and sectoral norms from active legislation in the destination country;

II - nature of data;

III - compliance with general data protection principles established by this Law;

IV - adoption of security measures foreseen in regulations; and

V - other specific circumstances related to the transfer.

The content of the single paragraph in Article 33 also resembles the criteria adopted by the 95/46 EU Directive for evaluation of protection degree in countries outside the European Economic Zone. The assessment or verification criteria for general and sectoral norms, concerning data nature and security measures, is expressed on the same terms on Article 25.2 of the Directive.[51]

The new GDP Regulation No. 2016/679 expands the list of criteria for certifying adequation. First, actors subject to verification of adequation might be third countries, its territories or specific regions and international organizations, according to Article 45, n. 1, of the GDPR. An analysis of Article 45, n. 2, GDPR[52] is expanded to a concept which appears to capture the actual objective connecting factor based on the place or country to which the data is transferred, as well as the degree of respect to human rights and fundamental freedoms within that country or location. Furthermore, the European Commission will seek to verify which is the effective application of protective norms, both through the analysis of judicial and administrative mechanisms available to the data rightsholder and through analysis of local case law.

Public security and national defense related rules, regarding the degree of access by public authorities to personal data, also stand as important assessment criteria. Such a recent concern was probably raised after Edward Snowden's leaks related to surveillance by several US State Authorities, mainly the National Security Agency (NSA) and by some European countries.[53] Another innovation was the concern with the third country's capabilities of having independent fiscalization authorities with proper means to achieve personal data protection and which are able to cooperate with European authorities.

Finally, international commitments by the country are also taken into consideration as well as its participation in multilateral and regional systems (such as Brazil's participation in the OAS, for instance), when related to privacy and data protection.

The expansion of evaluation criteria over data protection levels by the Europe-

51 Directive 95/46/EU, Article 25.2: "The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country." Available at: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&qid=1466131624407&from=EN>. Accessed on 20 of June, 2016.

52 General Data Protection Regulation 2016/679, Article 45. Available at: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN>. Accessed on 20 of June, 2016.

53 GREENWALD, Glenn. Sem Lugar para se Esconder: Edward Snowden, A Nsa e A Espionagem do Governo Americano. 1st Edition. Editora Sextante, 28/04/2014.

an Union shows how complex this analysis might be. The magnitude of change makes evident how insufficient the criteria on the Directive 95/46 are, from which Article 33 of Draft Bill n. 5276 heavily draws its inspiration.

> *Art. 34. The authorization referred to in item IV of Article 33 will be granted where a party responsible for the treatment presents sufficient guarantees of compliance with general protection principles and with rights of the holder, presented in contractual clauses approved by the competent authority for a specific transfer, in standard contractual clauses or in global corporate norms, according to terms of the regulation.*
>
> *§ 1º The competent authority may elaborate standard contractual clauses or enforce constant provisions in documents that serve as basis for transborder data flows, which shall comply with general data protection principles and with rights of the holder, being guaranteed the solidary liability of the transferor and of the transferee, regardless of fault.*
>
> *§ 2º Those responsible for treatment and which are part of the same economic group or multinational conglomerate might submit global corporate norms for approval of the competent authority, binding all enterprises integrating said group or conglomerate, in order to obtain permission for transborder data flows inside said group or conglomerate without the need for specific authorization, in compliance with general principles of data protection and with the rights of the holder.*
>
> *§ 3º During the analysis of contractual clauses, documents or global corporate norms submitted to approval by the competent authority, supplementary information or verification diligences may be required when dealing with operations of treatment.*
>
> *§ 4º Sufficient guarantees of compliance with general data protection principles and with the rights of the holder referred to on caput will also be analyzed according to technical and organizational measures adopted by the operator, in accordance to paragraphs 1 and 2 of Article 45.*

Article 34 of the Data Protection Bill starts defining the specific cases that require prior authorization to which the Article 33, IV refers to. Authorization for transborder data flows, in general, is granted in compliance with "general data protection principles and with rights of the holder", expressed both through (1) contractual clauses or (2) global corporate norms.

The model of previous authorization proposed by the Bill is similar to the exceptions to the "equivalent protection" criteria for transborder data flows outside of the European Economic Area, established by Article 26, paragraph 2 of the old Directive 95/46. In the European model, a Member State may authorize transfers of data to a country without equivalent protection levels when the "controller" guarantees "privacy, fundamental rights and individual freedoms" of citizens whose data are object of treatment, with special emphasis on contractual clauses as means of protection. [54]

During the 2000's, the European Commission adopted the standard contractual clauses[55] and the binding corporate rules[56] models, which were not originally existing in

54 Directive 95/46/EU, article 26, nº 2: " 2.Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.". Available at:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>. Accessed on 19 of December. 2016

55 Decision 2001/497/EC; Decision 2004/915/EC; e Decision 2010/87/EU.

56 Overview on Binding Corporate Rules. Available at: <http://ec.europa.eu/justice/data-protection/international-transfers/bind-

the Directive 95/46 text. In 2016, the General Data Protection Regulation (GDPR) 2016/67 was approved by the European Parliament, having an uniformizing character while keeping the same general model of "equivalent protection" of the Directive 95/46. That is to say, whenever a third country, specific territory or international organization does not meet European levels of data protection, or its adequation has not yet been assessed,[57] the transfer may still be made based on other parameters. According to the GDPR, parties still can rely on standard contractual clauses, specific clauses approved by competent authorities and corporate binding rules.[58]

The new European Regulation, on its Article 46, has expanded the list of exceptions that allow for transborder data flows in cases such as (1) existence of binding legal instruments between public authorities or organizations in Europe and the third party involved in the transfer; (2) the party responsible for data treatment or for subcontractors on a third country adopts a code of conduct of binding legal character, previously approved; and (3) the creation of certification procedures to be granted to parties responsible for data treatment or for subcontractors which adequate themselves to certain criteria. This legislative policy seems to resort to a model partially based on party autonomy but subject to some public constraints, whenever public authorities or organizations have the power to interfere with the content of contractual clauses or corporate codes (e.g. prior approval).

Article 34 of the Brazilian Data Protection Bill and its paragraphs refer to a **competent authority for data supervision**. However, **the Bill lacks any definition concerning the premises of its structure and operations, which may result in uncertainties and lower degrees of transparency for major stakeholders and - above all - internet users.** This contentious issue is not new. In *European Commission v Austria* case[59], the European Court of Justice has also discussed the establishment of an independent authority as a necessary component to a data protection systems. According to the Court, in order to operate in objective and impartial manner, said authorities require their own budget, even if bound to State structure.[60]

Despite the importance of the authority's independent operation, the goal is not to separate it completely from the State, but to grant it autonomy so it can serve its purpose of effectively protecting data to be transferred, complying with general data protection principles established on Article 6 of Bill n. 5276. **If the decision of the Brazilian legislator is to proceed with this model, an opportunity/feasibility assessment test has to be done in advance. This decision comprises, for instance, the option to create an independent governmental body or agency with clear and defined mandates.**

In practice, however, what has been seen in the European Union was that, in many

ing-corporate-rules/index_en.htm>. Accessed on June 17, 2016

57 GDPR 2016/679/EP, artigo 46, nº 1: "In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available." Available at: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN>. Accessed on June 17, 2016.

58 GDPR 2016/679/EP, articles 46 e 47.

59 European Court of Justice, Case C614/10, European Commission v. Republic of Austria, judgement on 16 October, 2012, available at: <https://tinyurl.com/kvt388s>.

60 BALTHASAR, Alexander. *'Complete Independence' of National Data Protection Supervisory Authorities – Second Try: Comments on the Judgment of the CJEU* of 16 October 2012, C-614/10 (European Commission v. Austria), with Due Regard to its Previous Judgment of 9 March 2010, C-518/07 (European Commission v. Germany).

cases, authorities are incapable of accomplishing their functions due to lack of human and financial resources.[61] This adds up to the increasing complexity of international governance regulations on data protection, resulting in a substantial concern as to the effectiveness of such a system. Furthermore, many international data transfers require the holders consent, and the lack of clarity and transparency might complicate an effective authorization.[62]

> *§ 1º The competent authority may elaborate standard contractual clauses or enforce constant provisions in documents which serve as basis for transborder data flows, which shall comply with general data protection principles and rights of the holder, guaranteed the solidary liability of the transferor and of the transferee, regardless of fault.*

Article 34 *in fine* highlights the influence of the European model over Brazilian Bill n. 5276. Paragraph 1 delegates to the competent authority the duty of elaborating standard contractual clauses as means of reducing bureaucratic costs for the private sector. On the same paragraph, it mandates the competent authority to previously approve contractual clauses specific to transborder data flows not dealt with by other provisions in the Bill.

The case of joint liability between transferor and transferee of the data, regardless of fault, indicates a safeguard against eventual attempts to avoid protections established in Brazilian legislation by handing over the data to a third party. The GDPR 2016/679 presents similar concern and goes beyond, establishing in its Article 44 that European protections are extended to any layer of transfer (*onward transfers)*. For instance, if company A transfers data to company B in another country X, and this one in its turn transfers it to company C located in country Y, European protections will hold A, B and C equally liable for the data transfer dealings.

> *§ 2º Those responsible for treatment and which are part of the same economic group of companies or multinational conglomerate might submit global corporate norms for approval of the competent authority, binding all enterprises integrating said group or conglomerate, in order to obtain authorization for transborder data flows inside said group or conglomerate without the need for specific authorization, in compliance with general principles of data protection and with the rights of the holder.*

Paragraph 2 of Art. 33 creates the possibility for groups of companies and multinationals to submit for approval their own **global corporate norms**, since approved transfers inside the same group may occur without the need for each specific transaction.

> *§ 3º During the analysis of contractual clauses, documents or global corporate norms submitted to approval by the competent authority, supplementary information or due diligences may be required when dealing with data treatment related transactions.*

61 European Union Agency for Fundamental Rights, 'Data Protection in the European Union: the Role of National Data Protection Authorities' (2010), Available at: <fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf>. Accessed on January 10, 2017. p. 46

62 KUNER, Christopher. Regulation of transborder data flows under data protection and privacy law: past, present, and future. *TILT Law & Technology Working Paper*, n. 016, 2010.

Paragraph 3 is expected to face resistance by certain economic sectors that fear the competent authority's fiscalization, which might require access to sensitive private data such as trade secrets. Article 10, paragraph 4 of the Brazilian Internet Bill of Rights might be pointed out as an example of balance, as it deals with the need for transparency on security measures adopted by ISPs while highlighting the necessary respect to rights of confidentiality as to trade secrets. Any decision at legislative process stage should take into account the needs of striking the balance between the goals of data protection and the transparency on security measures, in particular to avoid any undue data retention framework or disclosure of trade secrets not foreseen by existing statutory law.

> *§ 4º Sufficient guarantees of compliance with general data protection principles and with the rights of the holder referred to on caput will also be analyzed according to technical and organizational measures adopted by the operator, in accordance to paragraphs 1 and 2 of Article 45.*

Paragraph 4 states that, during analysis related to transborder data flows, technical and organizational measures adopted by the operator will be taken into account as relevant criteria. An example of possible technical measures to be considered is the use of any type of encryption for the data. An organizational measure, on the other hand, refers to which authorities or employees in a given business have access to said data.

> *Art. 35. The transferor and the transferee are held solidarily and objectively liable for treatment of the data, regardless of their location, in any case.*

Although the Data Protection Bill n. 5276/2016 has explicitly enshrined a general accountability principle, Article 35 of its texts appears to be - along with other provisions and instruments - an objective expression of *accountability* as a data protection principle. Said principle has been restated by the aforementioned European GDPR 2016/679.

A cautious reading of Article 35 might actually give room to a certain degree of confusion. The civil law tradition influencing Brazilian private laws takes different perspectives on contractual and non-contractual liability, ranging from distinct categories of joint liability, objective liability and torts (more specifically within the differences between Law of Obligations and Law of Extracontractual Obligations).

This provision comprises two approaches to transborder data flows: one lined with notions of accountability that rule the relations between personal data treatment agents and the holder of rights to that data; and one based on civil liability and the duty of paying damages for any harm suffered by a party.

C. Transborder data flows and the accountability principle

Geographic parameters are one of the main criteria determining transborder data flows on the Data Protection Bill n. 5276/2016 (Article 33, item I). Although such a model obviously promotes an improvement of legal protection levels for privacy on destination countries, it also contains serious limitations on its ability to guarantee effective protection of personal data through compliance to general rules and procedures. Such challenges have been already recognized by the Article 29 Working Group on the scope

of European law when those matters were addressed by Directive 95/46.[63]

By establishing that both the agent responsible for treating and sending personal data as well as the receiver may be held liable by the rights holder *"regardless of their location, in any case"*, the Bill also formulates, on its Article 35, a non-geographical criteria. Therefore, the location of data center in which personal information is stored or the territory where personal data treatment activities are carried out after transborder flows is of least importance, as well as the regulatory framework already in existence.

Due to the application of the *accountability principle*, transferor and transferee are held equally liable for operations with personal data. Therefore, they must adopt necessary management measure to give effectiveness and practical application to privacy protection rules, either internally on their organizational structure or externally in face of third parties.

Beyond those rules that impose an "equiparable" assessment of personal data protection levels, based on a geographical model for the regulation of transborder data flows, the Brazilian Data Protection Bill evokes what Christopher Kuner calls the "organizational model".[64] The model seeks to promote *organizational accountability* achieved through the creation of comprehensive privacy management-driven programs or policies by entities that handle an increasingly larger volume of data. These programs or policies must effectively implement best practices rules,[65] codes of conduct, corporate rules and external and/or internal guidelines along the entire lifecycle of data subject to treatment,[66] regardless of the place or jurisdiction where data is located.

Finally, resorting to joint liability between transferor and transferee in transborder data flows becomes unnecessary. The accountability principle which inspires Bill n. 5276 seeks to hold any personal data treatment agent accountable for the security and protection of collected data, whether located on Brazilian territory or not. Thus, the statutory provision of equal accountability for both seems to suffice.

D. Damages in the context of transborder data flows

Since the 1980's, notably with the *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* and Convention 108 of the Council of Europe, transborder data flows are inserted in a regulatory framework that seeks to achieve balance between protection of privacy and the free flow of personal data.

As further highlighted in this policy paper, transborder data flows are seen as essential, intermittent and ubiquitous in the digital economy. Therefore, data protection laws throughout the world, either of national or regional scope, are not intended to halt treatment of data - including transborder transfers - with regard to identified or identifiable group of individuals. The main goal of data protection laws is to accord rights

63 ARTICLE 29 DATA PROTECTION WORKING PARTY. *The future of privacy:* Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Bruxelas: [s. n.], 2009. p. 7-8.

64 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, passim.

65 See article 50 of Brazilian Data Protection Bill nº 5276/2016.

66 CENTRE FOR INFORMATION POLICY LEADERSHIP. *Protecting privacy in a world of Big Data*: the role of enhanced accountability in creating a sustainable data-driven economy and information society, 2015. p. 2.

holders with a proper level of effective control over their personal data, even if put under circulation, both in offline and online environments.

Bill n. 5276/2016 follows these guidelines, in a compliant fashion with a **procedural profile of the right to personal data protection**, expressed through the guarantee of progressive and exact forms of "*in itinere* control"[67], accorded to individuals and users, over the entire chain or flow of personal data. This approach can be seen, for instance, where the free and unequivocal consent is required for the legitimate treatment of personal data (Article 7, item I), especially if considered sensitive information (Article 11, item I). Such a consent requirement might also be considered as ground for authorization for transborder data flows (Article 33, VII).

This framework clearly reveals the primacy of a kind of preventive legal custody[68] which is sought to be granted for holders of any data disclosed, collected, stored, shared and transferred. That is to say, by designing a legal regime for personal data protection and transborder data flows, the Bill equally seeks to promote the enforcement of rights and freedoms of individuals (Article 1), reducing the potential risks of damages caused by treatment of such data.[69] One could contend that compensation-mechanism based custodies take a secondary role: civil liability will only take place when instruments made available for holders are insufficient in preventing damage caused by the treatment of personal data.

It is known that transborder data flows, whether online or offline, might create obstacles to the effective protection of personal data as well as risks involving wrongful uses.[70] For that reason, despite the preventive nature of the aforementioned provisions, civil liability framework may be considered an important tool for assuring a degree of minimal protection to victims of harmful use of data treatment operations.

According to the Bill, any damages that may fall on the data owner object to transfers by an exporting agent, located in the Brazilian territory, to the importing entity, located in another country, will be indemnified.[71] Furthermore, it is possible for the damage to be of patrimonial, extrapatrimonial, individual or collective nature, as prescribed by Article 42 of the Bill when it rules the civil liability of personal data treatment agents.

If transborder data flows are acts connected by causal links to damages suffered by the individual over his property, under Brazilian Law such damages will be subject

67 MESSINA, Mara. I diritti dell'interessato. In: CARDARELLI, Francesco; SICA, Salvatore; ZENO-ZENCOVICH, Vincenzo. *Il codice dei dati personali:* temi e problemi. Milão: Giuffrè, 2004. p. 75-76.

68 Idem ibidem. This scholarly comment was made in Italy after the enactment of the European General Data Protection Regulation. Both Law n. 675/1996 as well as the late Legislative Decree n. 196/2003 have transposed Directive 95/46/EC to Italian legal system. (DI MAJO, Adolfo. Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela. In: CUFFARO, Vincenzo; RICCIUTO, Vincenzo; ZENO-ZENCOVICH, Vincenzo (Coords.). *Trattamento dei dati e tutela della persona.* Milão: Giuffrè, 1998, p. 244-245; RESTA, Giorgio. Il diritto alla protezione dei dati personali. In: CARDARELLI, Francesco; SICA, Salvatore; ZENO-ZENCOVICH, Vincenzo. *Il codice dei dati personali:* temi e problemi. Milão: Giuffrè, 2004, p. 25-26).

69 Article 6,VIII, of Bill n. 5276/2016 deals with a category of *prevention principle*, "through which measures capable of preventing damages caused by treatment of personal data must be adopted."

70 GDPR 2016/679:"*When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information […]*".

71 Transborder data flows involve at least three treatment operations: i) the one making personal information available to the responsible agent (transferor) - *e.g.* data collection; ii) transmission of information to a foreign country by the transferor; and iii) treatment (*i.e.* storage or processing) executed by the transferee in facilities located in foreign location. (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).

to compensations of both actual damages as well as loss of future revenue.[72] The same applies when treatment given by transferor or transferee of personal data are basis for moral damages suffered by the data owner. In that sense, there will be an obligation to compensate when, from data transfers, the identified or identifiable person comes to suffer any kind of harmful acts in relation to his/her rights of personality (*e.g.* right of image, reputation, goodwill, rights to non-discrimination)[73].

It initially seems that damages for nonmonetary losses may have higher incidence rates as a consequence of poor or wrongful treatment of personal data, rather than damages of patrimonial nature. The reason for this would be based not only on the expansion of new damages to individuals,[74] but specially on the fact that the **right to personal data protection is of a complex nature**. This means that legal enforcement of privacy rights seeks to protect, in general, a myriad of legal interests and not only the right to be left alone (as it was conceived in a traditional in the past). Hence, more than safeguarding secrets - hiding certain information from common knowledge - privacy and data protection seek to grant individuals greater control of the data related to him/her - especially those regarding political, philosophical or religious beliefs, sexual life and orientation, health conditions and others as means of guaranteeing that freedoms are not hampered by promoting conformism or by social discrimination.[75] In sum, individuals have a role to play in deciding whether some specific data are still subject to both an autonomous decision and private discretion.

Due to these reasons, any inefficient data protection regime may lead to (i) violations of other fundamental rights and freedoms (Article 1) such as right to personal identity, freedom of speech and right to image; and (ii) damages for nonmonetary losses (moral damages) .

Likewise, Article 42 of the Data Protection Bill does not overlook the potential scenario where cases of collective damages arise from activities carried out by data treatment agents. As broadly understood, massive and continuous mobility of information of personal nature on the Internet and operations performed by public and private agents utilize advanced *Big Data* mechanisms. In this case, any act of data treatment conducted by transferor or transferee during transborder data flows eventually contravening homogeneous individual or meta individual interests may give rise to disputes within the context of collective claims, subject to the distinct regimes of the Consumer Protection Code (Law n. 8.078/1990) and Law n. 7.347/1985).[76] [77]

72 Regarding patrimonial or material damages, Article 402 of the Brazilian Civil Code: asserts that "*Except for the exceptions expressly provided by law, the losses and damages owed to the creditor include, in addition to what he effectively lost, what he or she reasonably failed to profit*" .

73 For a concept of moral damage in Brazilian Law, see MORAES, Maria Celina Bodin de. *Danos à pessoa humana:* uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2009. p. 182-192.

74 Cf. SCHREIBER, Anderson. *Novos paradigmas da responsabilidade civil.* 2. ed. São Paulo: Atlas, 2009. p. 87-89.

75 RODOTÀ, Stefano. *Tecnologie e diritti.* Bolonha: Il Mulino, 1995, p. 101-102; DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 141-147.

76 Article 22 of the Bill n; 5276/2016 so determines: *"The protection of interests and rights of data owners may be enforced in individually or collectively, as established by Law N. 9.507/1997, on Articles 81 and 82 of Law N. 8.078/1990 and on Law N. 7.347/1985, and on other instruments of individual and collective jurisdiction."*

77 Collective claims are currently under scrutiny of the 23rd and 9th Civil Courts of the Special Circuit of Brasília/DF, both filed by the Brazilian Institute for Policy and Information Law (IBDI) against Google, on which they request the condemning of the defendant to pay compensations in face of collective moral damages due to "indiscriminate" collection of data from Brazilian citizens, conducted by the corporation through the Google Street View and the extinct Google Buzz. See TJDF, Google/Instituto Brasileiro de Política e Direito da Informática - IBDI, Docket n. 2015.01.1.000575-6 - Ação Civil Coletiva, decision as of May, 02 2017, available at: <http://bit.ly/2qBGIT8>; and TJDF, Google/Instituto Brasileiro de Política e Direito da Informática - IBDI, Docket n. 2013.01.1.096604-4 - Ação Cautelar Prepa-

Another aspect of relevance concerning reparatory custody is the nature of the imputation criteria for liability on damages by agents importing and exporting information. The criteria may be *subjective* or *objective* and based on *fault* or *risk.*

Article 35 of the Bill, in line with its Article 42, opts for the *civil liability* model, meaning the damages caused by the data treatment agent is not determined by lack of diligence or lack of conformity to a certain standard when conducting operations with personal data. A similar choice has been made by the Spanish legislator in *Ley Orgánica 15/1999*. Its Article 19.1[78] prescribes liability regardless of fault by agents, who shall be held liable for any damages caused to the data owners.[79] Such a legislative choice made under Spanish Law does not directly reflect the provisions of EU Directive 95/46[80] , on its Article 23:

> 1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.
>
> 2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

By confirming this lack of unquestionable positioning during the transposition of the Directive to Italian Law - first by means of enactment of Law n. 675/1996,[81], subsequently by the Legislative Decree n. 196/2003[82] - the adopted regime was that of the *assumed liability*[83] or *semi-objective liability*,[84] which is similar to the idea of liability by presumed fault. This model puts the burden of proof to the data owner and admits the exclusion of liability in the event the agent demonstrates the adoption of legitimate measures in order to avoid damages.

The new European general data protection legislation (GDPR 2016/679), has not drifted away from the previous Directive, as the normative text has adopted nearly sim-

---

ratória, decision as of April 11, 2013, available at <http://bit.ly/2oV64iP>. In the United States, in the recent Mark Siegal v. Snapchat Inc., a class action was proposed against Snapchat because according to the claimant, the corporation has been illegally collecting biometric data from millions of users through facial recognition technology, not complying with the Biometric Information Privacy Act from the State of Illinois. (TASSIN, Paul. Snapchat Class Action Says Facial Recognition Technology Illegal. Available at em <https://goo.gl/O4JCG0>. Accessed on June 3rd, 2016.

78 SPAIN, *Ley Orgánica 15/1999,* 199. Available at: <https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>. Accessed on June 20, 2016. *"Artículo 19. Derecho a indemnización. 1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. [...]".*

79 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. 61-62.

80 Id., ibid., p. 62.

81 ITÁLIA. *Legge 675/1996,* 1996. Available at: <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/28335>. Accessed on June. 20, 2016.

82 ITÁLIA. Legislative Decree n. 196, 2003. Available at: <http://www.camera.it/parlam/leggi/deleghe/03196dl.htm>. Accessed on June 20, 2016. C

83 DI CIOMMO, Francesco. Il danno non patrimoniale da trattamento dei dati personali. In: PONZANELLI, Giulio (Coord.). *Il "nuovo" danno non patrimoniale*. Pádua: CEDAM, 2004. p. 261-263.

84 SICA, Salvatore. Le tutele civili. In: CARDARELLI, Francesco; SICA, Salvatore; ZENO-ZENCOVICH, Vincenzo. *Il codice dei dati personali:* temi e problemi. Milão: Giuffrè, 2004. p. 553.

ilar wording on its Article 82, which deals with the *Right to compensation and liability.* [85]

Should the choice for objective liability be confirmed by Brazilian legislator through Bill No. 5276/2016, liability for damages caused by transborder data flows shall be largely a matter of causality. In case the debate is left to the courts, it will be possible to require from the data treatment agent an unequivocal proof of exclusion of liability: only then will the compensations be removed, being admissible the dynamic distribution of compensations in order to avoid a situation in which the data owner is obliged to produce an impossible proof (Called *diabolical proof* in Brazilian Law). (Civil Procedure Code, art. 373, § 1º[86]; Bill n. 5276/2016, art. 42, unique paragraph).

Exclusions of liability may be alleged by the transferor or transferee and are namedly *facts exclusive to the victim or third party*, *cas fortuit* or *force majeure*. As to a fact by third party, said third party must be considered someone without any connections to the data treatment agent.[87] In that sense, should the data transfer be executed by a member of the organizational framework of a certain agent, this member will not be considered a third party, even if the act was not performed within the scope of powers or duties of the author of the wrongful act of transfer. Cases of *cas fortuir* or *force majeure* as disruptions of the causality links have distinct marks of *unpredictability* and *inevitability.* If the fact has none of these traits, the exclusion of liability won't apply.

If there happens to be any compensable amount of any kind imputed to transferor or transferee in transborder data flows, the compliance with the duty to compensate may be required from one and/or other data treatment agents due to solidary liability. In such cases, the solidary liability system established by Articles 275 to 285 of the Brazilian Civil Code will be applied. The wording of Article 44 of the Data Protection Bill is clear in that sense.[88]

85 "*Article 82. Right to compensation and liability.* 1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. 2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. 3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage. […]".

86 BRASIL. *Lei nº 13.105,* 2015. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>. Accessed June 20, 2016.

87 Cf. MARTINS, Guilherme Magalhães. *Responsabilidade civil por acidente de consumo na Internet*. 2. ed. rev., atual. e amp. São Paulo: Revista do Tribunais, 2014, p. 157.

88 *Brazilian Civil Code. Law n. 10.406*, 2002. Available at: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Accessed on June 20, 2016. "Art. 44. In cases involving transfer of personal data, the transferee will remain subject to the same legal obligations as the transferor, with whom it will have solidary liability for eventual damages."

3. Conclusions and Recommendations

The analysis of Chapter V of the Data Protection Bill n. 5276/2016 highlights the influence of the European Data Protection system on the transborder data flows regime proposed by the Brazilian legislator. Some criticism is commonly directed to this geography-based protection system, most of which can be overcome by the so-called ***organizational model***.

Unlike the European model, which follows geographical criteria centered on the State as a guarantor of data protection, the organizational model alternative places duty of diligence to data on the businesses that collect, transfer and treats it in a more equitable fashion. There are several reasons, listed below, for such a model to be favored in detriment to the geographic approach, or for a process of hybridization between the two, resulting in a *sui generis* model, in case the legislative scrutiny opts to follow a different approach.

The European model adopts essentially geographical criteria to define situations in which transborder data flows are allowed. In an increasingly globalized world, regulations based on territorial criteria are often revealed to be problematic or obsolete, as geography matter less each day. The organizational model is capable of transcending national State borders, making the data protection levels follow the data wherever it goes, as diligence duties are attributed to the agents that treat it and not to the State where data is transferred to. Basically, the organization model reflects a blend of liability models, balanced obligations and interests of both companies and individuals, while geographical model tend to concentrate obligations to the States and agents located at the final destination of data transfer flows.

The **organizational model** would be compatible with Article 11 of Brazil's Internet Bill of Rights, which demands enforcement of Brazilian law for data collected in Brazil, and wouldn't result in jurisdictional problems caused by the data being transferred to other jurisdictions.

One of the problems of attributing the duty of diligence in protecting transferred data to States in which the rules for protection are deemed of low efficiency. The European experience has shown that authorities responsible for data protection in every European country suffer with lack of resources. This results in slowness and inefficiency even when protecting data from their own national citizens, with several data treatment activities passing unnoticed to the fiscalization authorities.

European Data Protection Authorities (DPAs) are in general considered burdensome and inefficient. Their capacity of enforcing data protection rules is severely limited. Therefore, the idea that personal data from Brazilian users would be reasonably protected merely for having being transferred to countries with sufficient levels of protection on their legislation only is erroneous. Furthermore, the desired benefits seldom compensate for the economic costs derived from the bureaucracy involved.

The legislator must take into account that the structure of the Brazilian State is already significantly bureaucratic and inefficient, and its capacity of meeting up with the

demands related to the authorization of transborder data flows is limited.

The organizational model we recommend tries to overcome these problems by binding exporting entities to keep a continuous protection of personal data transferred to other organizations regardless of their geographical location. Such protection would be enforced by means of contractual clauses between transferor and transferee, as well as solidary liability between them. Currently, the Bill foresees this possibility on Articles 34 and 35. However, the main model still revolves around previous authorizations by a competent authority. We understand such a point is problematic and bureaucratic, and a hybrid model resulting in increased freedom and less barriers should be adopted in order to achieve balance between efficiency and protection.

For these reasons, we propose that transborder data flows to countries in which data protection levels have not been assessed or are not considered equivalent to Brazilian leves ought to be authorized *a priori*, if in compliance with the following conditions:

- Exporting entities are bound to adopt adequate protection measures both in their own international transfers as well as in those involving other foreign entities;
- Transborder data flow contracts with importers located in jurisdictions without adequate levels of protection must contain diligence and solidary liability clauses that meet requirements from Brazilian legislation;
- Transborder data flows contracts with importers located in jurisdictions without adequate levels of protection must contain clauses allowing the exporting entity to demand compensation from the importing entity for any expenses it might have had with damages and compensations required by Brazilian users.

From this arrangement, it would be an obligation of Brazilian data protection authorities to posteriorly and continuously inspect contracts and conducts from exporting entities as means of guaranteeing their compliance with Brazilian law. This model of *ex post* fiscalization is already used in Brazil in tax law. For example, a municipality must inspect provision of services in order to guarantee the ISS (Tax over Services) has been properly collected, even though it is not capable of inspecting all possible taxpayers. This limitation, however, does not become cause for barriers to business.

4. References

Books and Articles

ARTICLE 29 DATA PROTECTION WORKING PARTY. *The future of privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.* Bruxelas: [s. n.], 2009. Available at: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf>. Accessed on June 16, 2016.

_____. *Opinion 3/2010 on the principle of accountability.* Bruxelas: [s. n.], 2009, p. 7. Available at: < http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf>. Accessed on June 10, 2016.

BLAS, Frédéric. Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales. *Rev. Derecho del Estado*, v. 23, p. 37, 2009.

CARDARELLI, Francesco; SICA, Salvatore; ZENO-ZENCOVICH, Vincenzo. "*Il codice dei dati personali: temi e problemi*". Milão: Giuffrè, 2004.

CENTRE FOR INFORMATION POLICY LEADERSHIP. Protecting privacy in a world of Big Data: the role of enhanced accountability in creating a sustainable data-driven economy and information society, 2015. Available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_1_the_role_of_enhanced_accountability_21_october_2015.pdf>. Accessed on June 11, 2016.

CERDA SILVA, Alberto. "El 'nivel adecuado de protección' para las transferencias internacionales de datos personales desde la Unión Europea*." Revista de derecho (Valparaíso)*, n. 36, p. 327-356, 2011.

COMISSÃO EUROPEIA, *Transatlantic Data Flows: Restoring Trust through Strong Safeguards,*117 final, Brussels, 29 February 2016, Available at: <http://europa.eu/rapid/press-release_IP-16-433_en.htm>. Accessed on June 15, 2016.

CUFFARO, Vincenzo; RICCIUTO, Vincenzo; ZENO-ZENCOVICH, Vincenzo (Coords.). *Trattamento dei dati e tutela della persona.* Milão: Giuffrè, 1998.

DI CIOMMO, Francesco. "Il danno non patrimoniale da trattamento dei dati personali." In: PONZANELLI, Giulio (Coord.). *Il "nuovo" danno non patrimoniale*. Pádua: CEDAM, 2004. p. 255-281.

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

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Data Protection in the Europe-*

an Union: the Role of National Data Protection Authorities (2010), Available at <http://fra.europa.eu/fraWebsite/attachments/Dataprotection_en.pdf>. Accessed on June 20, 2016

GEPI - Grupo de Ensino e Pesquisa em Inovação, FGV São Paulo. *Contribuição ao Anteprojeto de Proteção de Dados Pessoais.* São Paulo, p. 4-15, 2015.

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

KUNER, Christopher. "Data protection law and international jurisdiction on the Internet (part 1)". *International Journal of Law and Information Technology*, vol. 18. n. 2, p. 176 - 193, 2010.

_____. "Data protection law and international jurisdiction on the Internet (part 2)". *International Journal of Law and Information Technology*, vol. 18. n. 3, p. 227 - 247, 2010.

_____. "Extraterritoriality and regulation of international data transfers in EU data protection law." *International Data Privacy Law,* v. 5, n. 4, p. 235-245, 2015.

_____. "Regulation of transborder data flows under data protection and privacy law: past, present and future." *OECD Digital Economy Papers*, n. 187, OECD Publishing, 2011. Available at <http://dx.doi.org/10.1787/5kg0s2fk315f-en>. Accessed on May 20, 2016.

_____. "The European Union and the Search for an International Data Protection Framework", in *Groningen Journal of International Law* vol. 2, n. 2, 2014, p. 55-71.

MARTINS, Guilherme Magalhães. *Responsabilidade civil por acidente de consumo na Internet*. 2. ed. rev., atual. e amp. São Paulo: Revista dos Tribunais, 2014.

MORAES, Maria Celina Bodin de. *Danos à pessoa humana:* uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2009.

MORGADO, Laerte Ferreira. *O cenário internacional de proteção de dados pessoais. Necessitamos de um Código Brasileiro?* Available at: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6336>. Accessed on May 30, 2016.

RODOTÀ, Stefano. *Tecnologie e diritti.* Bolonha: Il Mulino, 1995.

SCHREIBER, Anderson. *Novos paradigmas da responsabilidade civil.* 2. ed. São Paulo: Atlas, 2009.

SVANTESSON, Dan Jerker B. "The regulation of cross-border data flows." *International Data Privacy Law,* p. 180 - 198, 2011.

WEBER, Rolf H. "Transborder data transfers: concepts, regulatory approaches and new

legislative initiatives." *International Data Privacy Law,* p. 117 - 130, 2013.

NISSENBAUM, Helen. "A Contextual Approach to Privacy Online." *Daedalus, the Journal of the American Academy of Arts & Sciences*, v. 140, n. 4, p. 32 - 27, 2011.

REINALDO FILHO, Demócrito. *A Diretiva Europeia sobre Proteção de Dados Pessoais - uma Análise de seus Aspectos Gerais.* Available at: <http://www.lex.com.br/doutrina_24316822_A_DIRETIVA_EUROPEIA_SOBRE_PROTECAO_DE_DADOS_PESSOAIS__UMA_ANALISE_DE_SEUS_ ASPECTOS_GERAIS.aspx>. Accessed on May 30, 2016.

SOUZA, Carlos Affonso Pereira de Souza; VIOLA, Mario; LEMOS, Ronaldo. Understanding Brazil's Internet Bill of Rights, p. 17-18. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2015. Available at <http://itsrio.org/wp-content/uploads/2015/11/Understanding-Brazils-Internet-Bill-of-Rights.pdf>, Accessed on December 14, 2016.

Documents and Cases

GERMANY. Federal Data Protection Act, January 14, 2003. Available at: <http://www.gesetze-im-internet.de/englisch_bdsg/federal_data_protection_act.pdf>. Accessed on May 30, 2016.

ARGENTINA, *Decreto n. 1558/2001*, November 29, 2001. Available at: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70368/norma.htm>. Accessed on May 30, 2016.

_____. *Lei n. 25.326*, October 30, 2000. Available at: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>. Accessed on May 30, 2016.

BRAZIL, *Federal Constitution,* October 05, 1988. Available at: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Accessed on June 15, 2016.

_____, *Law n. 12965*, April 23, 2014. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Accessed on May 21, 2016.

_____. *Decree n. 5.015*, March 12, 2004. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm>. Accessed on June 15, 2016.

_____. *Decree n. 5.687*, de January 31, 2006. . Available at: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Decreto/D5687.htm>. Accessed on June 16, 2016.

_____. *Law n. 10.406*, January 10, 2002. Available at <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Accessed on June 20, 2016.

_____. *Law n. 13.105,* March 16, 2015. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>. Accessed on June 20, 2016.

CHILE, *Law n. 19.496*, January 28, 1997. Available at: <http://www.leychile.cl/Navegar?idNorma=61438>. Accessed on May 30, 2016.

COLOMBIA. *Statutory Law n. 1.581*, October 17, 2012. Available at: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>. Accessed on June 15, 2016.

DECISION OF THE COMMISSION, June 30, 2003, according with Directive 95/46/CE from the European Parliament and Council of Europe relative to the adequation of Argentina's personal data protection levels. Available at: < http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32003D0490&from=PT>. Accessed on June 30, 2016.

SPAIN, *Ley Orgánica 15/1999,* December 14, 1999. Available at: <https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>. Accessed on June 20, 2016.

USA, *Judicial Redress Act,* March 18, 2015. Available at: <https://www.congress.gov/bill/114th-congress/house-bill/1428>. Accessed on June 15, 2016.

USA-EU, *Umbrella Agreement,* December 08, 2015. Available at: <http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm>. Accessed on June 15, 2016.

FRANCE. *Loi Fédérale sur la Protection des Données,* June 19, 1992. Available at: <https://www.admin.ch/opc/fr/classified-compilation/19920153/201401010000/235.1.pdf>. Accessed on June 15, 2016.

IRELAND. *Data Protection Act,* 2003. Available at: <https://dataprotection.ie/viewdoc.asp?DocID=1467&ad=1>. Accessed on June 15, 2016.

ITALY. *Decreto Legislativo n. 196*, July 29, 2003. Available at <http://www.camera.it/parlam/leggi/deleghe/03196dl.htm>. Accessed on June 20, 2016.

_____. *Legge 675/1996,* December 31, 1996. Available at: <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/28335>. Accessed on June 20, 2016.

ONU, *Declaração de Salvador sobre as Estratégias Abrangentes para os Desafios Globais: Prevenção de Crime e Sistemas de Justiça Criminal e seu Desenvolvimento num Mundo em Mudança*. 2010. Available at: <http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/In-session/ACONF.213L6_Rev.2/V10529061A_CONF213_L6_REV2_S.pdf>. Accessed on June 01, 2016.

_____. *United Nations Convention Against Corruption*, 2000. Available at: <https://www.unodc.org/lpo-brazil/pt/corrupcao/convencao.html>. Accessed on June 16, 2016.

_____. *United Nations Convention Against Organized Transnational Crime,* 2000.Available at <https://www.unodc.org/lpo-brazil/pt/crime/marco-legal.html>. Accessed on June 15,

2016.

EUROPEAN PARLIAMENT AND COUNCIL, *Directive 2016/680,* April 27, 2016, regarding protection of individuals concerning treatment of personal data by competent authorities relative to prevention, investigation, detention or repression of criminal violations or enforcement of criminal sanctions, to the free flow of data, and which revokes Framework 2008/977/JAI of the Council. Available at: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L0680&from=PT>. Accessed on June 15, 2016.

_____, *Directive 95/46/CE*, October 24, 1995, relative to the protection of individuals concerning personal data protection and the free flow of this data. Available at: < http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Accessed on May 30, 2016.

SWITZERLAND. *Loi fédérale sur la protection des données*, June 19, 1992. Available at <https://www.admin.ch/opc/fr/classified-compilation/19920153/201401010000/235.1.pdf>. Accessed on June 16, 2016.

URUGUAY. *Ley 18.331 (Protección de datos personales y acción de 'habeas data'")*, de 11 de agosto de 2008. Available at: <http://www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley-n%C2%B0-18331-de-11-de-agosto-de-2008.html>. Accessed on June 16, 2016.