UiO : Faculty of Law
University of Oslo

International personal data flow:

Has Brazil reached an adequate level of protection according to the European Union standards?

Candidate number: 8015

Submission deadline: 01/12/2013

Number of words: 17.980

Table of Contents

1) INTRODUCTION

1.1) The importance of safeguards for cross-border transfer of personal data

The European Union (EU), Brazil, and the rest of the world face a constant challenge concerning the development of new types of relations in the digital era, as well as measures to line up internal legal systems with partner business nations.

Such issues are extremely pertinent for the protection of citizens' guarantees and rights established in one country when transferred to another. In light of this adequate system, individuals can benefit and create new opportunities to do lawful business.

In cyberspace, we might say, we are only a number, but this number has the same rights and obligations as a physical person, and behind this number is a citizen who belongs to a country. Within this nonphysical territory, we hold a precious economic asset for any type of business. This economic asset is called personal data.

Unfortunately, not all citizens are aware of the value of this economic asset, and for this reason, it is a fundamental duty of democratic nations to inform and protect their citizens properly against possible violations of their rights in the data-protection field.

In Europe, concerns about data privacy arose initially in Germany with the advent of the German State of Hesse, which enacted the first data-protection statute in 1970[1]. Since then, the motivations and principles across Europe that are related to the protection of individual privacy have become the golden standard. We can say that it is also one of the oldest human rights policies in the EU[2].

The EU has already taken several measures on this mentioned duty under internal legislation, and has signed international treaties and conventions. However, for the purposes of this thesis, we will solely analyze Directive 95/46/EC[3] (ED) and the proposed reform of this Directive in 2012, as the main issue specifically involves the international flow of personal data to third countries.

In South America in 1988, Brazil started to take effective measures on data privacy with the advent of the Constitution of the Federal Republic of Brazil, but the current Brazilian framework remains unfinished. The 1988 Constitution was drafted as a reaction to the period of authoritarian military dictatorship, which lasted from March 31, 1964 to March 15, 1985. However, the Brazilian government has not yet approved specific legislation on data protection (it is currently awaiting approval) but has a current framework for privacy in the mentioned Constitution, as well as through the judicial remedy called *Habeas Data*. The

[1]See: Swire, P.P. and Litan, R.E., None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive, Brookings Institution Press, Washington, D.C. p. 2, 1998.
[2] Bignami, Francesca, Privacy and Law Enforcement in the European Union: The Data Retention Directive; Chicago Journal of International Law, 2008, p. 233.
[3] On the protection of individuals with regard to the processing of personal data and on the free movement of such data.

framework for data protection is outlined in the Civil Code as well as in the Consumer Protection Code (CPC). Furthermore, a draft bill, which aims to guarantee civil rights in the use of the Internet in Brazil was introduced to Congress, and is also known as the *Marco Civil da Internet* in Portuguese. Additionally, it is worth mentioning that other aspects of privacy and data protection are present in other Brazilian instruments and that these will be discussed in section 2.3.7.

In fact, we cannot deny that the relationship between Brazil and the EU in terms of the export of goods and services has increased every year. Brazil is the largest economy in Latin America and its trade with the EU accounts for 37% of the EU's total trade with the Latin American region (2011)[4]. Obviously, the free movement of data is extremely interesting for both parties. However, to be able to receive personal data from the EU, Brazil's status as a third country[5] means that it has to ensure an adequate level of data protection according to the ED, as mentioned.

Nonetheless, it is possible for a country to fall within the scope of the exemptions[6], and we believe that complying with the rule under Article 25 of the ED might be an easier choice and less of a burden due the principle of legal certainty that surely attracts further investments in Brazil.

Article 25 is under Chapter IV of the ED and it handles the transfer of personal data to third countries. The motivation for this Chapter is of legitimate interest for the EU in making sure that third countries are not used as "data heavens" to deliberately circumvent the effect of European laws on European individuals[7].

On the other hand, since the requirements of adequacy are not formulated by the Council and the European Parliament in a narrow way, the mentioned Chapter challenges third countries to adequately develop their legal systems to comply with the Directive. Noncompliance with this Chapter might force competent authorities in EU Member States to exercise their existing powers, suspending data flows to a recipient in a third country in order to protect individuals with regard to the processing of their personal data.

On the basis of legitimate international transfer under the procedure provided under Article 25, we have to mention paragraphs 2 and 6 due to their importance in clarifying the EU requirements on this issue.

Paragraph 2 presents the appropriate circumstances for a lawful transfer of personal data to third countries. Fundamental analysis of the Working Party (WP)[8] guidance on this issue is indispensable. It is always important keep in mind that most of the European Commission's decisions explicitly consider the WP's advice.

In paragraph 6, the Commission was given the power to determine whether a third country has ensured the mentioned level of adequacy through its domestic law or through the international commitments it has entered into (we will analyze this further in section 2.3.6 on

[4] Available at http://ec.europa.eu/trade/policy/countries-and-regions/countries/brazil/
[5] Configured as a non-Member of the European Union and EEA.
[6] Derogations are under Article 26 of the Directive 94/45/EC, which emphasize the general principle that exemptions must be interpreted restrictively.
[7] See: Swire, P.P. and Litan, R.E., None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive, Brookings Institution Press, Washington, D.C. p. 9, 1998.
[8] Set up under Article 29 of the DPD, whereas opinion is elaborated on by the group of national data-protection commissioners. This body acts independently, yet it has considerable influence.

the international commitments that Brazil is part of relating to this paragraph). Bearing in mind that such a decision is vital to allow legal, personal data flow from the EU and European Economic Area (EEA) [9] Member Countries, and, consequently, to open the route for legitimate business.

Since there is no explicit answer to what is, in fact, an adequate level of protection under the mentioned Article 25, the European Member States shall provide that this international transfer—alongside the processing after the transfer has taken place on behalf of the legitimate flow—and that the third country receiving this data (for the purpose of this thesis, the Federal Republic of Brazil) have an adequate level of protection for this personal data in their internal system.

To date, the Commission has so far recognized an adequate level of protection[10] in Andorra, Argentina, Australia, Canada, Switzerland, the Faeroe Islands, Guernsey, the State of Israel, the Isle of Man, Jersey, the US Department of Commerce's Safe Harbor Privacy Principles, the transfer of Air Passenger Name Records to the United States' Bureau of Customs and Border Protection, and, recently, the Commission has recognized New Zealand, the Eastern Republic of Uruguay, and the Principality of Monaco as providing adequate protection.

Surprisingly, Brazil has no official evaluation by the Commission and we believe, for the purposes of encouraging and legitimizing even more business between the EU and Brazil that it is a matter of necessity to get official recognition that the standards of protection in Brazil ensure secure compliance in terms of the level of adequacy according to EU finding decisions.

Therefore, has the current legal system in Brazil reached this adequate level? Do the current framework and proposals on data protection in Brazil obey the objectives of the European standards? Would this framework be appropriate or breach the applicable standards?

Since the mentioned partnership between Brazil and the EU has developed, it is fundamental to reaffirm the legal guarantees of this relationship for both Member States and their citizens.

1.2) Scope of this work

The aim of this work is to answer the question regarding whether the current legal framework in Brazil (as well as the law proposals for the data-protection field) has provided an adequate level of protection according the EU standards in cases where one of the Member States intends to transfer the personal data of European citizens to Brazil, without additional guarantees being necessary.

Our analysis will consist of four chapters:

Chapter 1 is the present introduction.

[9] EEA Members (Norway, Liechtenstein and Iceland) are bound by the effects of these decisions, as they are party to the 1992 Agreement on the EEA.

[10] Official decisions issued to date by the European Commission can be found here: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

Chapter 2 presents the EU Directive on Data Protection and the new proposal for a General Data Protection Regulation concerning the international transfer of data. In addition, the historical context is examined on how Brazil has fared from its period under dictatorship to the present day. Further, we examine the current legal framework and also the proposals under the legal framework of privacy and personal data protection in Brazil. Additionally, further Brazilian legislation that we believe to be of note will be briefly mentioned under other considerations, as well as international commitments that Brazil is committed to regarding privacy.

In chapter 3, we will discuss the current EU requirements on finding an adequate level of data protection in an official decision. The decisions to date that present themselves as incorporating an adequate level of protection occur wherever the third country has a framework that we can divide into a minimum of a core of data-protection principles and into additional principles such as sensitive data, direct marketing, and automated individual decisions. Additionally, the legal system should identify three objectives of a data-protection procedural system, and on this basis, judge the variety of different judicial and non-judicial procedural mechanisms used.

In chapter 4, we present our conclusion and summarize the weakest and strongest points of the Brazilian framework.

1.3) Methodology used in this research

The research methodology was conducted through the analysis of legal dogmatic methods, Brazilian and European literature, as well as, historical methods regarding the background of Brazil before and after the military dictatorship.

2) THE LEGAL REGULATION OF DATA PROTECTION IN EUROPE AND THE LEGAL AND BACKGROUND DETAILS FOR BRAZIL

This chapter introduces the reader to the current EU Directive on Data Protection (95/46/EC) with an emphasis on the international flow of data (Chapter IV), as well as the legislative proposal for a General Data Protection Regulation released in 2012 by the European Commission.

In addition, in section 2.2 we will analyze the background of privacy and personal data protection in Brazil before and after the military dictatorship, due the importance of these periods for the outlook to date.

2.1) The European Union Directive on Data Protection and the new proposal for a General Data Protection Regulation concerning the international transfer of data

When the current Directive on Data Protection came into effect in October 1998, it was simply the next logical step in creating an internal market in a context of the development of the EU[11]. Preserving the EU Member citizens (as well as members of the EEA) against rights violations outside of the unified market in Europe still remains a goal. However, protection of this fundamental right and guaranteeing the free flow of personal data between Member States of the EU it is a challenge due to divergent interests.

The EU Directive on Data Protection, Chapter IV (Transfer of personal data to third countries), in an attempt to strengthen the personal data of European citizens, forbids the cross-border transfer of personal information out of Europe, unless the other country (termed as "third countries" by the Directive, in reference to non-European members) fits the requirements of an adequate level of protection of privacy, established in Article 25, or otherwise, fits into one of the derogations of Article 26.

The restriction on cross-border transfers of personal data is one of the greatest known features of the existing framework in Europe, because in practice, this requirement stipulates that data controllers set down adequate safeguards of some kind to comply with the Directive.

These safeguards do not involve the execution of model contractual clauses between exporters and importers, or developing binding corporate rules.

Under narrow circumstances, data controllers are allowed to rely on one of the construed derogations set up in Article 26, such as unambiguous consent given by the data subject, the necessity of the performance of a contract, or if the transfer is vital to protect the interests of the data subject and others.

However, the Article 29 WP issued an opinion concerning the derogations of Article 26(1) and highlighted that they must be applied only restrictively under two conditions: when the risks to the data subject are small or where other interests (public interests and those of the data subject himself) override the data subject's right to privacy.

We believe that to gain recognition regarding the adequacy of protection of Article 25 instead of attempting these derogations might be easier and less costly for a country such as Brazil, as well as for countries involved in business in this third country that has uses the personal data of European citizens, as the principle of legal certainty might serve as a form of investment attraction.

Another point to be explored on this topic is the new legislative proposal for a General Data Protection Regulation. Proposed on 25 January 2012, the proposal incorporated a package of major reforms relating to EU protection of personal data. Until 2014, all Member States must adopt the Regulation, and after 2 years, the Regulation will officially come into force after this transition period, as is usual with EDs. However, some topics still remain under discussion.

According to the Commission, the General Data Protection Regulation will strengthen individual rights and tackle the challenges of globalization and new technologies, as well as the free flow of personal data still remaining as a common goal.

[11] See: Swire, P.P. and Litan, R.E., None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive, Brookings Institution Press, Washington, D.C. p. 25, 1998.

We will discuss the main reforms concerning the international transfer of personal data, which, due the current complexity of the rules, are considered as constituting a substantial impediment to operations by economic stakeholders.

In the new proposal, the cross-border transfers are set out in Chapter V. The transfer to international organizations is explicit within this Chapter, as well as the recognition of the onward transfer of personal data from the third country or an international organization to another third country or to another international organization.

The harmonization of the rules is an aim, as the rules of the current Directive have been implemented differently within the 27 EU Member States and members of the EEA, and this practice has resulted in divergences in enforcement. With harmonization, it is expected that the burden on controllers undertaking this activity in several countries across the EEA might be substantially relieved. The reason is simple. Instead of dealing with the different approaches of the data-protection authorities in each country, thereby investing it time and expertise, the stakeholder under a harmonized environment can save a lot of time and money.

The structuring of the rules by means of mechanisms to allow for the transfer of data abroad remains much the same. Article 41 deals with "Transfers with an adequacy decision," Article 42 with "Transfers by way of appropriate safeguards," Article 43 with "Transfers by way of binding corporate rules," and Article 44 deals with the application of a derogation.

However, the process surrounding adequacy decision-making has changed. Article 41(2) (a) has reinforced the rights of the data subjects, establishing that: "to reach effective and enforceable rights, the third-country or the international organization shall include effective administrative and judicial redress for data subjects." Also, subparagraph (b) states the need for: "the existence and effective functioning of one or more independent supervisory authorities responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States." In addition, subparagraph (c) has included international commitments that the third country or the international organization has entered into.

We understand that the reforms for the process on adequacy decision-making are reasonable and pertinent. The aforementioned subparagraph (a) handles this with preventive measures via the inclusion of an option for effective administrative redress. Obviously, avoidance is better than dealing with the consequences. Under subparagraph (b), the awareness of the data subject is, in our opinion, one of the best mechanisms for transparency, as when the data subject is not aware of their rights and also does not know the value of or what it means to preserve their personal data, the protection of these aspects would remain innocuous. In addition, under subparagraph (c), it is vital to include the examination of the international commitments, as some of these commitments have the power of jurisdiction in certain countries that ratified. This means that even if the country does not fulfill a certain obligation internally, the individuals can fill out a complaint on the entity responsible and receive and forward it under the international commitment regime.

As we can see, the current ED, as well as the new Regulation, are in line regarding the maintenance of the international transfer of personal data and its principles and aims. However, the proposed new Regulation encompasses new issues of postmodern society, also

prioritizing the harmonization of the rules across the Member States, which will facilitate controllers in complying with the new Regulation.

2.2) Brazil before and after the military dictatorship

The presence of militarism in Brazil until the end of the dictatorship period in 1985 was meaningful since the Proclamation of the Republic in 1889. This historic fact came about due to a military coup d'état, which was led by a group of military officers of the Brazilian army in that period.

Visconde de Ouro Preto, a Brazilian politician and the last Prime Minister of the Empire of Brazil, has an interesting view on individual liberty during that time. He states that this guaranteed right is from the period of the monarchy. As we will discuss in what follows, this guaranteed right was suppressed during the dictatorship period.

Furthermore, according to Visconde de Ouro Preto, the Proclamation of the Republic was a mistake. He warns that the empire of Brazil actually "abolished the death penalty, slavery, gave Brazil undying glories, inner peace, order, security and most of all **the individual liberty** as there was never in any country"[12] (emphasis added).

The above-mentioned affirmation was used to refine the first Constitution in Brazil, which was elaborated on during the monarchy period in 1824. Article 179 included a list of individual rights and guarantees. Affirming these rights was the first step toward the legitimate right of privacy in Brazil.

Nevertheless, it was during the dictatorship, which started in 1964, when Brazilian society experienced one of its worst periods of the suppression of rights and of multiple violations.

At that time, it was believed that the President, João Goulart, was a defender of communism. On account of this, he was deposed by the military coup d'état in the name of National Security, resulting in a dictatorship. There are still various versions behind the motivation for this dictatorship.

The aforementioned ideological motivation was supported by the United States, which used these affirmations of a threat from communism to justify its own participation in the Cold War and its external political interventionism during that time.

One crucial issue was the creation of "institution acts" and laws, enacted by the heads of this regime. Clearly, these acts and laws were used to legally justify the atrocities during this period, which were characterized by massive violations against potential threats to the regime.

During these 21 years in Brazil, the regime exercised control and systematic censorship over the media, press, and education system, clearly suppressing the rights of the freedom of expression in terms of information. Furthermore, imprisonment, torture, murder, and the forced disappearance of opponents of the regime included citizens, artists, singers,

[12] Ouro Preto, Affonso Celso de Assis Figueiredo, Visconde de, Advento da Dictadura Militar no Brazil, Paris: Imprimerie F. Pichon, Paris, 1891, p. 91.

journalists, politicians, and even the current President of Brazil[13], and for those against the system there was arbitrary indefinite detention (a suspension of habeas corpus[14]).

Not remarkably, during this period of time, an agency called the National Information Service (*Serviço Nacional de Informações* in Portuguese), was created with the help of federal law 4.341. This public intelligence agency collected and stored personal data of individuals that was obtained by military control under different means, including physical and psychological coercion, according to reports from that time[15]. The collected data was related to, but not limited to the personal conduct and privacy of individuals, and data was stored regarding ideological convictions, political, and religious views, and was doubtless vital to affirm the new democratic order.

Another similar government agency was the Department of Political and Social Order (*Departamento de Ordem Política e Social* in Portuguese; the DOPS). This department was created in 1924 and lasted until 1983. It was broadly used to achieve the proposal regarding control and to repress the political and social movements against militarism. Defenders of liberty were arrested and then were faced with difficulties when putting themselves forward for any vacancy during those times; due the necessity to prove themselves under the "Attestation of Political and Social Background" order issued under the DOPS. Obviously, society was not prepared to hire someone that had been labelled as a "terrorist."

In the 1980s, after a long period of repression, the economy started to crash and chronic inflation followed. The pro-democracy movement gained momentum and had the Brazilian society, media, and sectors of the economy at their side in supporting the democracy.

Thus, under pressure, the regime had no choice but to pass an Amnesty Law for political crimes committed for and against the regime and it relaxed restrictions on civil liberties. In 1984, it held the first elections for president with civilian candidates, underlining the first phase of Brazil's democratic-transition process.

With the advent of the 1988 Brazilian Constitution, the period of repression remains in the past. As might be expected, concerns relating to privacy, intimacy, individual liberties, and data protection came sharply into focus after the dictatorship period. Measures regarding this field are constantly discussed in the Brazilian government but, unfortunately, due to the slow legislative process in Brazil, effective measures are still on paper, as we will discuss for the proposals regarding data protection.

On September 2011, the Chamber of Deputies approved "The National Truth Commission." This Commission has the power to investigate human rights violations during the military dictatorship and also to gain access to all government files from this period. It is expected that the Commission's work might also lead to revised laws that could improve the protection of human rights in Brazil.

---

[13] An article regarding the situation of the President of Brazil Dilma Rousseff during the dictatorship. Available at http://www.nytimes.com/2012/08/05/world/americas/president-rousseffs-decades-old-torture-detailed.html?_r=2&ref=global-home&.

[14] Legal instrument to safeguard individual freedom against arbitrary state action.

[15] See in Portuguese http://www.documentosrevelados.com.br/repressao/denuncias-de-tortura-de-preso-politico-frente-ao-tribunal-militar-da-ditadura/

Furthermore, the current president of Brazil, Dilma Rousseff, made an angry speech during the United Nations General Assembly earlier this autumn regarding the scandal surrounding the United States surveillance of personal data of (Brazilian) citizens and corporations. We transcribed it here[16]: "As did many other Latin Americans, I fought against authoritarianism and censorship and I cannot but defend, in an uncompromising fashion, the right to privacy of individuals and the sovereignty of my country."

Certainly after the period of military censorship, we might agree that the Brazilian government has improved in terms of reaching an even more adequate level of compliance in the data protection/privacy and human rights fields; however, progress has been relatively slow.

2.3) Current framework of data protection in Brazil

Currently, Brazil has dispersed privacy and intimacy rulings in various chapters, articles, paragraphs, and sections of different pieces of legislation. However, to date, a specific act on data protection is still under the status of a bill of law.

In this chapter, we will analyze all these different aspects contained within the 1988 Brazilian Constitution, including the constitutional remedy termed the "Habeas Data (HR) Right." Additionally, we will examine the Civil Code, the CPC, the law proposal on data protection, and the civil rights Internet framework proposal (*Marco Civil da Internet*). Additionally, under other considerations, we will briefly mention data protection aspects found in other Brazilian normative sources.

Furthermore, due the importance given by the ED under Article 25(6) to reach an adequate level in data protection, we will also mention international commitments that Brazil has entered into.

2.3.1) The Brazilian Constitution and the Habeas Data Right

In this chapter we will initially discuss the HD Right and subsequently the 1988 Brazilian Constitution and its articles concerning data privacy and intimacy, which are considered as a fundamental right.

The HD Right is a constitutional right that has been granted, and is set out in Article 5, LXXII/CRBF 1988 under information guardianship to guarantee, by means of an individual complaint presented to court concerning the protection of the individual's rights regarding the incorrect or excessive use of personal data that is stored by the state or by private entities that maintain public databases[17]. Nevertheless, even though it is not expressly stated in the

[16] Statement of the President of Brazil regarding USA illegal surveillance of Brazilians' data during the general assembly of the United Nations/2013. See in English http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

[17] According to Article 43.3 of the Argentina Constitution, the HD Right also applies to private entities.

Constitution, it is feasible to present a complaint requesting personal information held on private entities' databases[18].

Regarding the historical context of the HD Right, Brazil was the first country in South America[19], but not the only one after the 1980s, to adopt the HD Right into its Constitution at that time. Argentina, for instance, as mentioned under the European Commission decision[20], adopted the HD Right also. The adoption of the HD Right was a natural step in the process of democratization and political liberalization emerging from the authoritarian regime in South America.

In Brazil, it was during the period of the elaboration of the 1988 Constitution that the HD Right was idealized among the intelligentsia, including the remarkable Professor José Afonso da Silva[21], and it was inspired by the Portuguese, Chinese, and Spanish Constitutions.

Remarkably, with the advent of the 1988 Constitution in Brazil, the HD[22] Right was set out and the HD procedural law was enshrined in 1997.

Another point to be clarified is that the HD Right has a personal character; namely, the petitioner can only gain knowledge concerning the information that relates to himself. To access information that is of private interest or of collective or general interest, the appropriate constitutional remedy is the writ of mandamus (*Mandado de Seguranca*), as set out in Article 5, LXIX, CRFB/1988.

The modalities regarding the HD Right can be examined academically as falling into one of three types: habeas data cognitive understanding (to access the information), a modifier (in order to rectify), and integrative (to fill a gap).

The first and second types are specified explicitly under Article 5, LXXII, "a" and 5.LXXII,"b", respectively, of the 1988 Brazilian Constitution. However, the third modality was only enshrined by the legislative provision of the HD Right in 1997, due the necessity to complement and provide a novel way to inform third parties that certain personal data is under judicial contention. We transcribe it here:

"Habeas Data shall be granted:

a) To ensure the knowledge of information related to the person of the petitioner, contained in records or databanks of government agencies or of agencies of a public character;

b) For the correction of data, when the petitioner does not prefer to do so through a confidential process, either judicial or administrative."

Article 7, III of the 1997 legislative provision of the HD Right regarding the personal data under judicial contention, reads:

---

[18] Court decision nº 2.0000.00.310192-2/000(1) of the Tribunal of Justice of the State of Minas Gerais, August 2, 2000, the decision states : "The public character of the database is not in fact be part of the database or not be under the state apparatus, but the possibility of know whom stores specific information about individual."

[19] Colombia, 1991 (Article 15); Paraguay, 1992 (Article 135); Peru, 1993 (Article 200, 3); Argentina, 1994 (Article 43); Venezuela, 1999 (Article 28).

[20] Available at http://ec.europa.eu/justice/policies/privacy/docs/adequacy/decision-c2003-1731/decision-argentine_en.pdf, p. 3.

[21] SILVA, José Afonso. Curso de direito constitucional positivo, 28.ed.São Paulo: Malheiros, 2007, p. 454.

[22] Which is roughly translated as "[we command] you have the data."

"The settlements for the annotation of interested, presentation of the defense, or explanation on true data but justifiably and it is under pending litigation or friendly" (translated by the author).

What is to be noted on the positive side of the Habeas Data Right is the nature of special procedures in the tribunals. The petition shall be presented under a system of venues that change depending on the authority, government agencies, or for agencies of a public character. The reason for this distinction is reasonable, as the particularities of each tribunal can be judged, as well as taking into account any heavy political issues emanating from the decision. Thus, this special system of venues encourages and guarantees efficient judgments with adequate oversight.

The 1998 Brazilian Constitution that deals with these mentioned venues is to be found in Articles 102, II, "a," 108, I, "c," and 109, VIII, and, as well as in the 1997 legislative provision of the HD Right, and both stipulate what the court will be.

Nevertheless, in order to be applicable for court analysis, the petitioner must first prove that he has tried (administrative instance) to request/rectify or complement his personal information from the issuing authority, but that this was denied or not answered under the legal terms. This rule is in accordance with the principle of reasonableness and economy of justice, as well as providing a previous instance in which to resolve the conflict peacefully, which is one of the best features of the HD Right.

Another positive aspect is the guarantee of the free charge regardless of the economic situation of the petitioner. This privilege is due to the importance of the act as necessary for the exercising of citizenship.

In addition, the provisions under the procedure of the HD Right are beneficial. For instance, the public prosecutor is obligated by the law to issue an opinion in the concrete case. The judge has only five days under the legal term to issue a decision.

Regarding the 1988 Brazilian Constitution, the protection of the privacy/intimacy of the individual is mentioned in several articles. Under Article 5, X, the inviolability of privacy is ensured alongside appropriate redress to the injured party: "The privacy, private life, honor and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured."

Nevertheless, Article 5, items XI and XII, limit these mentioned rights, relativizing the guarantees in case of collective and general interest. We can mention a privacy case law that occurred in December 2003, when the Federal Supreme Court issued a decision mitigating the scope of privacy rights in this sense. According to the decision[23], the seizure of e-mails stored in computers, upon a court order, is an issue referring to privacy rights instead of the protection of electronic communications. The Supreme Court recognized that such privacy rights are not absolute, and may therefore be mitigated in view of the social and public interest, as well as in view of the interest of justice.

In addition, under Article 5, item XII, the protection of data is directly referred to. The secrecy of correspondence and of telegraphic, data, and telephone communications[24] has to be

[23] The Federal Supreme Court, regimental appeal, in extraordinary appeal n º. 373.058-4 – RS.
[24] Lei n º.9296/1996 regulates the conditions of interceptions for telephone calls in Brazil.

put in perspective, except, in the latter case, by court order, in cases concerning criminal investigation or criminal procedural fact-finding.

Another privacy ruling appears in Article 5, XI, where is possible to glimpse the home as an inviolate refuge of the individual, which can only be penetrated by a court order during the day, except in the event of flagrante delicto or a disaster, or to give help.

Another right recognized under the 1988 Brazilian Constitution is the right of petition under Article 5, XXXIII regarding information about private or public interests that shall be provided by public agencies, except in cases where secrecy is essential to the security of society. However, due the atrocity of the dictatorship, the Brazilian legal doctrine and precedent agrees that in accordance with the law, a family member of the deceased can petition requiring information regarding the deceased due the right of memory, which has protection under the Brazilian Civil Code.

As we have discussed, we can conclude that the HD Right and the 1998 Brazilian Constitution offer strong instruments that empower individuals in terms of the protection of their rights. Additionally, the different venues are an advantage of the Brazilian system for issues and proper decisions, according to the venue of the authority that has denied the possible right of information. Regarding the free access to justice, the Brazilian system offers, under these instruments, free charges, which encourage the individual to initially search for a solution under the administrative instance, which is positive in terms of the time spent on seeking a result.

2.3.2) The Civil Code

The 2002 Brazilian Civil Code[25] came into force in January 2003 and has brought considerable benefits for the protection of privacy under the Brazilian legislation. Since the 1988 Constitution introduced the principle of human dignity as an essential value that underlies Brazil (Article 1, III), it was expected that there would be a reformulation of the Civil Code toward consideration of the new context.

Due to the shifts in the paradigm, under Chapter II (Articles 11 to 21) of the 2002 Civil Code, the rights of personality were included. Influenced by the 1966 Portuguese Civil Code, (enshrined under Articles 70 and the following articles), the definition of these rights according to Carlos Alberto Bittar[26] are:

> Recognized in the human being taken in itself and in its projections in society, foreseen in the legal system, just for the defense of innate values to man as life, physical soundness, intimacy, honor, and other intellectuals.

Therefore, these rights are intended to protect the rights that are indispensable to the dignity and integrity of the person. Additionally, besides the natural person, the legal entity, under the Civil Code, also has a personality in terms of rights.

It is important to note that the list provided (under Chapter II) is not specific, implying that the legislator wisely predicted a broad and general view; thus, it allows access to all of

[25] Lei n º. 10.406/2002.

[26] ELESBÃO, Elsita Collor. Os direitos da personalidade no novo Código Civil brasileiro. In: Pessoa, gênero e família. Livraria do Advogado, Porto Alegre, Brazil, 2002, p. 17.

the hypothetical situations that have not yet happened but that may arise, and not just those provided for by the law, consequently conferring full protection in terms of personality rights. It is an essential view to further protect the individual due the speed of new technologies and relationships that are exercised through social media.

Regarding the characteristics, personality rights have absolute character, opposable *erga omnes*[27]; thus, everyone is obliged to respect them. This characteristic is closely linked to unavailability, yet covers their non-transferability (inalienability) and non-waiver character. Moreover, it is a right that the individual cannot change the ownership of, nor change by their own will because such a person is fully bound.

In cases of violation of the aforementioned rights, the 2002 Civil Code states under Title IX the civil liability and rules for the redress of the individual. It is important to mention that the sole paragraph of Article 927 establishes that due to the nature of the activity, if offers are not risky for the individual, the responsible person shall be liable for damages regardless of action or omission (this is called objective[28] civil liability) and the claimant has only to prove the damage and the causal link between the defendant's activity and the damage.

We will describe the articles under this chapter that are significant for the protection of privacy:

Article 11 provides the protection of the rights of personality, defining them as inalienable and non-transferable, and its exercise cannot suffer from voluntary restraint, except in cases provided for by the law.

Article 12 deals with the general protection of personal rights, protecting individuals from any threat or injury to their physical or moral integrity, as well as providing redress to the injured party due the loss and damages suffered.

Article 20 contemplates the protection of the intellect and image. It protects the image and the personal events from undue exposure, ensuring the individuality of the person. However, there are certain limitations to the right of the image, with a waiver of consent for disclosure when it is a notorious person or a holder of public office, and in all cases where there is public interest that prevails over individual rights.

The right to privacy and protection are guaranteed by Article 21, which provides that the private life of the person is inviolable; thus, it protects the person from the indiscretion of others and external interference in his private life.

In fact, under the current Brazilian Civil Code, the protection of privacy, as demonstrated, has been internalized in line with the 1988 Constitution, as well as providing for the proper and appropriate redress to the injured party in cases of violations.

2.3.3) The Consumer Protection Code

The defense of consumers is a guaranteed fundamental right under the 1988 Brazilian Constitution. Set out in Article 5, XXXII/CRFB/1988, the State shall provide, as set forth by

[27] This is a Latin term which literally means "towards all" or "towards everyone."
[28] The other type of civil liability in the Brazilian Civil Code is called subjective. In order to be constituted, it must prove the action or omission of the data controller to be liable.

law, the exercise of this individual right. Therefore, the state approved the Consumer Protection Code (CPC) in 1990 and it came into force in 1991.

In the CPC, the consumer has the right of access to information related to him in the databases and files, as well as knowledge of the source, according Article 43. The database and data must be objective, clear, genuine, and easily understood. In addition, the access to negative information on the consumer in the database is prohibited for a period not exceeding five years, as well as this negative information not being, after this period, provided to suppliers.

Furthermore, the consumer has the right to require the correction of his personal data and the deadline for fixing it is five days, and the entity responsible for the data must inform eventual recipients of the incorrect information in this period. Further, public consumer organizations must keep updated records of claims against suppliers and also disclose these to the public annually. This information is free to access for any person concerned.

The aforementioned provisions are in line with the data subject's right of access to data in the ED, and we consider the deadlines of the CPC effective in providing a quick and free-of-charge procedural mechanism.

In relation to the consent of the consumer, unfortunately, the CPC in our opinion failed, and it is not in line with the ED. The reason concerns the consent to open a database or file with the personal data of the consumer; this is solely to be communicated by writing to the consumer when it is not requested by him (Article 43, second paragraph). However, the Superior Tribunal of the Justice of Brazil understands that irregular annotation plus no communication to the consumer might result in moral damages[29].

Regarding the liability under the CPC, Article 43, paragraph 5 states: "Entities are considered public agencies (only when exercises this activity due the civil liability applied in this case), therefore, shall be liable for damages that any of their agents might commit. Additionally, it is ensured as a consumer's basic right, the redress for individual, collective or diffuse material or moral damages."[30]

In fact, the legislator was wise in establishing the provision on behalf of the private agencies that exercise the mentioned activity under the CPC is considered as public agencies; This condition shifts the civil liability of the management of data to being objective, instead of subjective. Civil objective liability means that the particular agent may also be compelled to provide compensation for damages, regardless of the existence of fraud or negligence, which means that neither blame nor negligence is relevant. The reason for this is due to the activity performed by the agent incurring risk (the theory of risk[31]).

Civil subjective liability is related to the existence of fraud or negligence on the part of the entity that caused the damage. When the victim demonstrates the existence of one of these elements, it is possible to claim compensation from the agent for damages. Adopting this liability would be inappropriate, by virtue of the difficulty of the consumer in demonstrating

[29] Precedent 385 of the Superior Tribunal of the Justice of Brazil.
[30] Article, 6, VI, CDC. See in English the Consumer Protection Code: http://procon.caxias.rs.gov.br/.
[31] According to the theory of risk under the Brazilian legislation, it is characterized when the activity developed normally entails, by its very nature, risk to the rights of others. There must be an obligation to repair the damage, regardless of fault.

the damage properly (inability of the consumer in access the technology system of the databases, per instance).

Another point that is worth mentioning concerns the recent Law 12.414/2011 (*Cadastro positivo* in Portuguese) that ruled on the formation and query of the database with information on the performance of natural or legal persons for the formation of a credit history. The main purposes of this cadaster are the reduction of interest rates on loans plus avoiding fraud by creditors. This is possible in view of the supplier being able to assess more accurately the risk of credit through the information presented by a positive cadaster with a list of compliant debtors. Therefore, there are benefits for both parties: banks in getting a favorable degree of safety in relation to certain legal business, and consumers, in being able to take advantage of special interest rates.

Obviously, the mentioned cadaster should be undertaken freely by the consumer in order to obtain benefits in the negotiation of financing. It is optional for the consumer to be part of this list, which respects the autonomy of the consumer in giving or not giving their consent. Thus, Article 4 states that registration is only held open through "prior consent by the potential registered by signing into a specific instrument." Further, the liability applied under this law is in line with the CPC, and is also the joint responsibility of the individuals involved in case of moral or material damages.

On the other hand, the adoption of this cadaster still has some concerns regarding the right to privacy in the history of the credits[32]. However, as we discussed in the HD Right, this right of privacy is not absolute and has to be put in perspective to account for collective and general interests.

We believe that to encourage the economy, the cadaster is an innovation in terms of maintaining secure private relations between consumers and suppliers. Further, can affect (as well as credit in general) compliant debtors, according to the interest rates, to establish such rates for the collective body of debtors. It also fights against fraud by creditors.

Worthy of note is the protection of consumer data administered by public agencies in contracts. Section II of the CPC set out in Article 51, item III, considers unfair clauses and lawfully void clauses, when the liability under the contract among consumers and suppliers is transferred to third parties. We understand that this provision may be more flexible and it allows for transfer with the consent of the consumer due to personal interests that might become relevant.

Furthermore, in August 2002, the Ministry of Justice issued Administrative Ruling No. 05/2002, enlarging the range of unfair clauses that injure the rights of the consumers and that can be deemed as abusive, pursuant to Article 1[33]:

(I) Authorizes the sending of the name of the consumer, and/or their guarantors, the databases and registries of consumers without attested prior notice;

(II) Requires a consumer, in standard contracts, the obligation to speak out against the transfer, if it is costly or not to third parties, of the registration data entrusted to the supplier;

[32] Accessible information about consumers consists of contract number, contract amount, number of installments, the amount of each installment, due date thereof, etc., although there is also information about income, profession, employer, payment history, payment habits, commitments, and regulations. In addition to these provisions, utility bills (water, gas, telephone, and light) can also be used as a reference.

[33] Translated by the author.

(III) Authorizes the supplier to investigate the consumer's private life.

To conclude, in general, the CPC has been carried out with sobriety by the Brazilian government; however, the CPC has not yet faced important issues regarding how the data of consumers must be stored and for what period. It also does not provide details about the processing of the data and the possibilities of personal data transfer to third parties. Furthermore, the absence of consent to open database files is not in line with the EU standards. Even though the answers will be given under the civil rights Internet proposal (section 2.3.5) and the law proposal on data protection in Brazil (section 2.3.4), the current situation is that the framework regarding the CPC in Brazil is incomplete, and in our opinion, amendments would be very welcome to update this framework.

2.3.4) The law proposal on data protection

Brazil is the only country in South America that does not yet have a data-protection act in force. The current situation might put feasible investments in Brazil at stake due to the lack of a principle on legal certainty. This is because it is particularly worrying as to how to deal with and enforce legislation with increasing technological challenges (for instance, cloud computing), with the use of the data of citizens for business, and cases of data breaches in postmodern society.

Thankfully, in 2012, after a period of public consultation[34], the preliminary draft on data protection in Brazil (PL 4060/2012) was proposed and issued through a cooperation process between the Ministry of Justice and the Getúlio Vargas Foundation[35]. Notably, the legal standards for the protection of personal data under this proposal are largely based on the standards set out in the ED.

The latest progress on the proposal was on August 22, 2013, and it resides with the Commission on Science and Technology, Communication and Information for assessment. We do not believe that the act will be enforced for several years; however, due to the recent spying scandals (mentioned at the end of section 2.2) and next year's elections for the Presidency, and the necessity of approving such a vital measure, it is undoubtedly a hot topic and this might influence its process.

Regarding the principles relating to the general data protection principles (Article 8), we consider these as being in line with the ED (Article 6). Both encompass the principles of finality, necessity, proportionality, data quality, and transparency. However, the Brazilian proposal goes further and covers principles of free access (meaning free of charge), physical and logical security (a higher level of demand, including cryptography), good faith, accountability[36], and prevention.

Regarding the definitions for the purposes of the proposal, we can point to a divergence. Differently from the ED, under the Brazilian proposal, the third party is defined

[34] Blog used as a public consultation for the preliminary draft of the law proposal on data protection in Brazil. Available at http://culturadigital.br/dadospessoais/.

[35] Is a Center for education dedicated to promoting Brazil's economic and social development. Available in English at http://portal.fgv.br/en.

[36] Related to feasible injury, including material and moral damages.

solely as a legal person. We understand this definition is incomplete as it does not include natural persons (whereby it diverges from the ED Article 2, (f), which, in turn, includes natural and legal persons). We can glimpse, in practice, conflicts arising due to the absence of the natural person aspect in the Brazilian proposal such as discrimination, violations of competition in law, and others.

We can mention another divergence regarding the absence of an express definition of the data subject's consent of Article 4 of the draft, which again diverges from the ED that defines this aspect thoroughly in Article 2(h). This absence weakens the draft and misses a perfect opportunity to establish efficient mechanisms (for instance: opting in) to ensure the best consent and awareness of the consent among the stakeholders.

Regarding the treatment of personal data, Article 6 of the draft, in our opinion, clearly establishes the treatment of personal data as a risky activity. The Article is in line with the Brazilian CPC that involves the same status for the management of databases. Additionally, as we have seen, this type of civil liability is undeniably positive for the individual, as the controller must assume liability for damage to consumers without intent, through reckless behavior, or by negligence. The ED does not mention differences in terms of liability, and we understand that this is due to the particularities of the Directive, and perhaps Member States would like to apply internally different mechanisms.

In relation to the treatment requirements of personal data, the draft sets out the data subject's explicit consent to the processing of those data in Article 9. We consider the draft is in line with (and we could say almost a copy of) the ED. However, the draft goes one step further and includes a condition in cases where the declaration of consent is given alongside with others; this shall be made in a separate document.

In relation to the requirement for information to be given to the data subject for their acceptance in cases of the collection and treatment of data by the controller, a criticism might be made. Article 11 solely defines the form to reach this agreement; however, it does not explain the mechanisms. We consider that this oversight might create a loophole for ill-intentioned stakeholders to take advantage of.

Concerning derogations and restrictions on the data subject's consent, Article 13 is in line with the ED. However, the ED and the draft did not analyze the behavioral analysis techniques[37] regarding the derogation for the treatment of data with the sole purpose of historical, scientific, or statistical research. We understand this derogation implicitly allows this practice and might violate the individual's rights.

In relation to the minimum period that data can be stored for lawfully, this remains in doubt, as Article 14, VI did not lay down this condition and left this responsibility to specific sectoral legislation and the supervisory authority (*Autoridade de Garantia*). We understand that as a general rule the more the controller is limited in terms of his freedom to choose the purposes, means, and conditions under which he processes the transferred data, the greater will be the legal security for the data subject. However, we presume that the supervisory authority will intervene when necessary.

[37] A methodology that uses disaggregated data and correlates this with the purpose of creating profiles of the consumers through particular forms of statistical analysis.

In line with the ED and also its proposal for a new Regulation, the proposal creates the supervisory authority (*Autoridade de Garantia* in Portuguese) under the National Council for the Protection of Personal Data (Title II, Chapter I). This body deals with inobservances of data subjects' rights, it is established as the controlling body, and is an independent body that has to approve its own internal bylaws, and it has administrative, management, and financial autonomy granted by law. Additionally, Article 40 grants concurrent authority to the Union, states, Federal District, and municipalities, who may create their own, personal data-protection authorities within their respective areas of administrative representation.

Further, the supervisory authority can apply sanctions and adopt preventive measures including imposing fines when it has noticed or has a well-founded fear that the entity responsible for the treatment might cause injury to the collective.

Regarding the processing of special categories of data (Chapter V), we consider it in line with the ED, the sole divergence being the inclusion of genetic data as sensitive data, which is a new topic that was not apparent at the time of creation of the ED; however, it is included under the newly proposed European Regulation.

Finally, Chapter XI is related to the international transfer of personal data and is remarkably in line with the ED. The supervisory authority may authorize a transfer to a third country that does not ensure an adequate level of protection when it is adduces adequate safeguards by the controller (Article 37).

To conclude, the Brazilian proposal has similarities with the current ED and also goes further by including genetic and biometric data as sensitive data, and other points, as we have seen. Some points might be reviewed as mentioned, such as nominating explicitly the mechanisms for data subjects' consent, the inclusion of geographic data[38], and an assessment of behavioral analyses. However, one major perspective is that the proposal was well drafted and had public participation during the period of consultation, which is very positive due the democratic system that Brazil lives by, and this demonstrates to the global community that the Brazilian government respects and considers the opinions of its people.

2.3.5) The civil rights Internet framework proposal (*Marco Civil da Internet*)

The civil rights Internet framework proposal (*Marco Civil da Internet* in Portuguese) came to fill the gap for an instrument that respects and preserves the diverse environment of the Internet and its regulation in Brazil. The proposal encompasses issues such as the rights and guarantees of users online, data records and storage of the connection logs, and the liability for damage caused by content generated by third parties. The latest progress for the proposal occurred on October 29, 2013, and it is under urgent status for senate voting; however, it might take at least another year to come into force due to the remarkably slow legislative process in Brazil.

In fact, a number of amendments were made to it, but the final draft finally became official under the bill of law 2126/2011. It has acceptance among civil society and

[38] Collection of information that can describe objects and things in relation to space. Divergences concern if this data might be used as personal data and if it can individualize an individual.

internationally. During the World Wide Web Conference of 2013 in Rio de Janeiro/Brazil, Tim Berners-Lee, also known as "the father of Internet" affirmed:

> With the ***Marco Civil da Internet***, you are on the brink of a remarkable achievement which would be a historic step not just for Brazil but for the world in securing an open and free Web for all. Passing without delay this legislation would cement Brazil's reputation as a world leader in democracy and social progress. (Emphasis added)

The *Marco Civil* bill is also recognized as pioneering in terms of the public consultation process, which contributes greatly to its legitimacy; the final content of the bill was discussed extensively through an open website[39]. The project is called the "Constitution for the Internet."[40]

Nevertheless, the bill contains a controversial issue concerning the liability of Internet connection providers, also as known as intermediaries, such as YouTube and Facebook, for example. Article 14, Section III of the *Marco Civil* bill states: "Internet connection providers shall not be responsible for damage arising from content generated by third parties." However, this rule is not absolute and the Internet application provider can be responsible **if, after** (emphasis added) receiving a specific judicial order, it does not take action, according to Article 15[41]. We consider this provision as fair, with the aim of not excessively burdening the Internet connection provider; however, this is not meant to remove the responsibility, but instead to bring balance to the system.

Although the European Directive on Electronic Commerce[42] adopts a different approach related to this issue, without spelling out the disregard of the specific judicial order to take action. However, we consider the bill reasonable, in part, concerning the liability of Internet connection providers. Further, we understand the natural essence of the Internet is the promotion of freedom, thus transfer to private agencies the obligation to remove alleged infringing content before an investigation is unreasonable, and it is the state's obligation to exercise the judgment on this conduct in legal terms. .

On the other hand, we disagree on the point that states that a specific judicial order is the sole instrument with which to cease the violation. Unfortunately, based on real life, to obtain this legal instrument quickly in Brazil due the flood of cases in the justice system is utopian as well as costly due to the legal fees involved.

In contrast, the bill contains a number of positive and essential elements for regulation of the Internet, in particular, concerning privacy. In line with the 1988 Brazilian Constitution, and established as one of fundamental principles is the Human Rights on Digital Means. Further, it is stated as a right of the user that there is protection against the inviolability of communication and secrecy online, except under judicial order (Article 7, I). In addition,

---

[39] Available at http://culturadigital.br/marcocivil/

[40] Statement of the Minister of Justice of Brazil in 2010 during the Seminar *Marco Civil da Internet no Brazil*. Available in Portuguese at http://g1.globo.com/brasil/noticia/2010/05/barreto-defende-criacao-de-constituicao-da-internet.html

[41] Article 15 states that: "Except otherwise established by law, Internet application providers can only be responsible for the damages caused by content generated by third parties if, after receiving a specific judicial order, they do not take action to, in the context of their services and under the established time frame, make unavailable the infringing content." *Marco Civil da Internet* in English is available at http://www.a2kbrasil.org.br/wordpress/wp-content/uploads/2011/09/Marco-Civil-Ingle%CC%82s-pm.pdf

[42] Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:En:HTML.

under data traffic, it is prohibited to monitor, filter, analyze, or supervise the content of data packages, except in the circumstances allowed by the law (Article 9, solo paragraph). On data records, concerning the storage and disclosure of data, it shall preserve intimacy, private life, and images of the individuals involved (Article 10).

As can be seen, the *Marco Civil* is a revolutionary tool and not merely a proposal that enables regulation, but also a model of a technology-empowered democracy exercise that might be followed by other countries looking to expand civil society participation on policy making and open government.

2.3.6) International commitments

Pursuant to Directive 95/46/EC, the Commission may find that a third country ensures an adequate level of protection within the meaning of paragraph 2 of Article 25 by way of its domestic commitments or of the international commitments that it has entered into for the protection of the private lives and basic freedoms and rights of individuals. Additionally, under the proposal for a General Data Protection Regulation[43], it is set up so that the Commission assessing the level of adequacy of the third countries shall give consideration on this subject.

First, it is must be mentioned that in order to demonstrate the seriousness of human rights in Brazil, it is vital to mention the status of this field under the 1988 Brazilian Constitution. From the enactment of Constitutional Amendment 45/2004, the treaties on human rights shall enter into force immediately[44], and are equal to Constitutional Rules. In addition, it is possible through the requirement of the Attorney General of the Republic to The Supreme Court of Justice (Article 109, V-A, CRFB/1988) that human rights violation cases be tried by the Federal Court rather than the State Court, due to the goal of promoting popular consciousness of the case.

Furthermore, it is established that the international relations of Brazil are governed by the principles of the prevalence of human rights, according to Article 4, II of the 1988 Brazilian Constitution.

In regard to international commitments, the first treaty is the Universal Declaration of Human Rights (UDHR), adopted by the United Nations General Assembly on December 10, 1948 after the atrocities committed during the Second World War. Brazil voted in favor of this treaty in 1948 and since that time has been an official member of the United Nations. Article 12 highlights the importance of preserving the privacy of the individual. We note this here: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

[43] Article 41(2) (c) states that: "When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements: (c) the international commitments the third country or international organization in question has entered into."

[44] Article 5, paragraph 3, CRFB/1988 states that: "International human rights treaties and conventions which are approved in each house of the national congress, in two rounds of voting, by three fifths of the votes of the respective members shall be equivalent to constitutional amendments."

The second is the American Convention of Human Rights (as known as the Pact of San José de Costa Rica), of November 22, 1969, and this came into force on July 18, 1978. It was ratified by Brazil in September 1992. This Convention aims to consolidate, among the American countries, a system of personal liberty and social justice based on respect for essential human rights, regardless of where the person resides or was born. The document consists of 81 articles (including transitional provisions). It lays down rules about fundamental human rights, such as the right to life, freedom, dignity, and personal integrity, among others. The Convention deals with judicial guarantees, freedom of conscience and religion, thought and expression, as well as freedom of association.

Furthermore, the aforementioned Convention has created the Inter-American Court of Human Rights with the purpose of judging cases of human rights violations occurring in countries belonging to the Organization of American States (OAS), which recognize its jurisdiction. Brazil recognized the jurisdiction in 1998 and has only been judged once since that time. We can also note that under the Uruguay Decision, participation in this treaty is mentioned, as well as the Uruguay recognition of the jurisdiction under the Inter-American Court.

In fact, we can state that violations of human rights in Brazil is not a common practice; however, if it happens, any individual has, under the Brazilian Constitution and international commitments, proper measures for redress. Further, the status of treaties on human rights and the special treatment in the Constitution, and possible assessment under the Federal Court, confirm the seriousness of this aspect under the Brazilian legislation.

2.3.7) Other considerations

In addition to the Brazilian framework mentioned in the previous chapter, it is worth briefly mentioning further legislation and regulation in different sectors regarding data protection/privacy.

The Child and Youth Statute[45] forbids the total or partial unauthorized divulgence of a child or youth's name, or their police, agency, or judicial documents. Additionally, this law was amended in 2003 due to the proliferation of pornography on the Internet involving children and teenagers, and expressly points out the online environment as a route for this crime. Furthermore, the penalty provided for such a violation is 2 to 6 years of imprisonment plus a fine. This inclusion was a very good initiative to combat pornography online, as well as incorporating a strict penalty in an attempt to inhibit such disgusting behavior online.

In October 1984, the Congress approved the Informatics Law[46], establishing the principles, objectives, and guidelines for the Brazilian Informatics Policy. Article 1, VIII, defines as a principle the establishment of mechanisms and legal and technical instruments for the protection of the confidentiality of the data stored, processed, and transmitted in the interests of the privacy and security of private entities, public, or private individuals, and legal entities.

[45] Lei n º 8.069 (1990).
[46] Lei n º 7.232 (1984).

The right of the user under the telecommunication service is established in Book 1, Article 3, V, of The Telecommunication Act[47], and states: "to the inviolability and to the secrecy of his/her communication, except under constitutional hypothesis and conditions legally provided for under such instances." This measure protects users of this service against illegal wiretaps and it is fundamental for the protection of the privacy of the individual under the contract.

Finally, Article 5, XII of the CRFB/1988, for the purposes of criminal investigation or criminal procedural fact-finding, enacted the law regarding wiretapping[48]. It is worth mentioning that the legal procedures on wiretapping are treated in secrecy by the judge and the parties involved in the case. The aforementioned Article defines the instruments for a successful and impartial investigation.

Furthermore, Article 313-A of the Brazilian Criminal Code[49] criminalizes certain activities exercised by civil servants, such as the insertion of false data into an information system, as well as unauthorized alteration of an information system. In both cases, it is considered as a punishable offence.

As we can see, the current framework of the Brazilian legislation encompasses the protection of data in diverse instruments. The violation of secrecy is treated as an important issue and properly safeguards the interests of the data subjects. Also, the Child and Youth Statute and the Criminal Code establish adequate punishments in regard to what these behaviors represent in Brazilian society.

3) ANALYZING BRAZILIAN LEGISLATION ACCORDING TO THE EUROPEAN UNION ADEQUACY ASSESSMENT

To date, we understand that there is no official procedure established by the European Commission; however, due the decisions issued, we can see that it is taken into account in the Article 29 WP opinion for the preparation of the adequacy assessment decisions, and, in turn, the WP taking into account its opinions under Working Document 12: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive[50].

Under this mentioned Working Document, we will analyze a supposed Brazilian assessment considering the valid arguments that constitute the compliance of the third country with minimums requirements for protection to be considered by the Commission on the basis of the judicial and non-judicial internal procedural mechanisms of Brazil.

The minimum requirements are a core of data-protection content principles (also additional ones such as sensitive data, direct marketing, and automated individual decisions) and a system of procedural and enforcement requirements that highlight the three objectives.

3.1) The core of data-protection principles

[47] Lei n º 9.472 (1997).
[48] Lei n º 9.296 (1996).
[49] Decreto lei n º 2.848 (1940).
[50] Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf.

The core of data-protection principles and the additional ones are part of the minimum requirements for the level of adequacy. It is worth mentioning that this can be downgraded or added to according to the particularities (for instance, the degree of risk) of the third country.

We will analyze the principles and initially compare them with the current framework of the Brazilian legislation and subsequently with the proposals:

> 1) The purpose-limitation principle: "data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the Directive."[51]

Current framework

This principle is not expressly covered in the CPC; however, regarding the law on formation and querying of the database with performance information for the formation of the credit history of consumers, Article 3, paragraph 3, II, forbids annotations with information not linked for the analysis of the credit risk of the consumer.

Regarding the procedure of wiretapping in Brazil[52], the law covers this principle in Article 1; a sole paragraph defines how the object of the investigation must be clear and points out the means for the wiretapping.

Proposed framework

Under the *Marco Civil da Internet,* one of the rights and guarantees of the user (Article 7, IV) is established as clear and complete information under the contract of services, as well as an express provision concerning the regime of protection of the user's personal data.

The Brazilian law proposal Article 8, I expressly contains the principle of finality:

> Non-use of the personal data that is object for different purposes or incompatible with those that supported their collection and informed to the data subject, as well as the limitation of this treatment to specified, explicit and legitimate purposes of the responsible.

Further, the derogations are set out in Article 13 and are similar to those of Article 13 of the ED. In addition, Article 33 of the proposal indicates further derogations such as public security, the protection of the rights of others, and legal or administrative investigation.

It is worth mentioning, under the decisions of Argentina and Uruguay made by the European Commission, that there is no evaluation of other legislative instruments, only the Data Protection Act in both countries. In addition, both decisions are in line with the Brazilian proposal, except that the Uruguayan Act regulates the procedure for authorizing data conservation for historical, statistical, or scientific purposes, and we understand that the Brazilian proposal may include a review of this point due to the reasons mentioned in section 2.3.4.

---

[51] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of data.

[52] See: item 2.3.7.

2) The data quality and proportionality principle: "data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed."[53]

Current framework

In relation to the CPC, Article 43, the sole paragraph does not refer directly to the obligation to maintain accurate data; however, keeping negative credit information on the consumer exceeding five years is mentioned as unlawful, and we understand due to the context of the CPC that this is an implicit rule to keep data updated.

Further, Article 44 declares that public consumer organizations must keep updated records of claims against suppliers. The Article misses the chance to include information alongside claims.

Proposed framework

This principle is expressly based on the law proposal under Article 8, V and is also defined as a data quality principle: "The accuracy of the personal data that are object of treatment, with updates performed at intervals necessary to fulfill the purpose of their treatment."

In addition, the principle of proportionality (Article 8, IV) declares: "the treatment of personal data solely in cases where there is relevance and adequacy in relation to the purpose for which the data was collected."[54]

3) The transparency principle: "individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) and 13 of the directive."[55]

Current framework

On the CPC, there is no obligation in provide information of identity of the data controller. Article 43, paragraph 2, defines that consumer must be communicated by written (when not requested by him) regarding sole the opening of cadaster/file or register of collection of his personal data. However, regarding the law on formation and query of the database of consumers it is established as an right be informed previously about the aims of the treatment , the identity of the manager of the data base and feasible recipients in case of sharing.

[53] The Working Party Document 12: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, p. 6. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf.

[54] Translated by the author.

[55] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of data.

Proposed framework

Article 8, VI of the law proposal states that: "Information to the data subject on the treatment of personal data, indicating the purpose, the categories of processed data, retention period of retention of the data and other relevant information."

Regarding the treatment of personal data, Article 9 specifies that this may only occur after free, express, and informed consent by the data subjects. The consent might be given in writing or by other means that it certifies.

Furthermore, according to Article 11, information shall be provided after prior notification to the data subjects, such as the purposes for the collection, the way that the data will be treated, the identity and address of the controller, the possible recipients, and the scope of dissemination. However, if misleading information is provided or information is not provided in a clear and explicit way, then the consent will be null and void. In respect of the information that must be provided for international transfer under this principle, the Brazilian law proposal provides for this under Article 35, I and states again the free, express, and informed consent required for the transfer of the information in Article 11.

Hence, the aforementioned provisions are in line with the EU standards concerning the consent of the data subject.

4) The security principle: "technical and organizational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller."[56]

Current framework

This principle is not covered in any current instrument under the Brazilian legislation, which we consider a serious issue due the lack of preventive measures.

Proposed framework

Article 8, VII of the law proposal develops this principle, stating the:

"Principle of physical and logical security. The use by data controllers of the personal data, such as technical and administrative measures proportional to the current status of the technology, the nature of the data and specific features of the treatment, constantly updated and able to protect personal data under their responsibility of the destruction, loss, modification and dissemination, accidental or unlawful or unauthorized access".

In relation to the procedure for the treatment of data made by those who are under the authority of the data controller, Article 25 establishes that the instructions must be given in written form by the data controller, and also, to become a more effective measure, the data controller shall carry out regular, periodic checks to verify if the instructions are being followed. In addition, this Article defined that the third party must have experience,

[56] The Working Party Document 12: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, p. 6. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf.

competence, and a good reputation to exercise the treatment of data. We do not agree on the experience aspect, since the Article does not define the meaning of the experience (number of years, contracts, etc.). This claim might affect small enterprises that wish to enter this market.

In relation to the supervisory authority (*Autoridade de Garantia*), it shall publish a policy with measures on preventive security (Article 24). We understand that this type of measure is positive because it provides harmonization among those who deal with personal data.

Another positive point is the right to information for data subjects in cases of security breaches regarding their data. Article 27 provides that the data subject shall be informed immediately. A criticism might be made relating to the moment of informing of a breach, since we understand that the Article missed the chance to fix a deadline, and that "immediately" might be interpreted in a variety of ways, perhaps causing conflicts of interest.

> 5) The rights of access, rectification, and opposition: "the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the directive."[57]

Current framework

In the 1988 Brazilian Constitution, as mentioned in section 2.3.1 regarding the information requested by the data subject, it is feasible through the HD Right to obtain/rectify and integrate personal information.

The CPC also establishes the right to rectification of personal data when they are shown to be inaccurate, and data must be corrected by the entity responsible for the databases/files in five days, and that they shall inform eventual recipients of the wrong information for this period.

Proposed framework

Under the law proposal, in relation to the right of access, Article 8, III states as a general principle of the data treatment: "the possibility of free consultation by the data subject on personal data, as well as their treatment modalities."[58]

Further, such information must be provided according to Chapter IV (rights of the data subjects) within five days of being requested. Furthermore, the information must be provided clearly, simply, and in a complete form by means of a statement, including information about the origin, as well as the logic, standards, and purpose of the treatment. The law proposal is in line with the CPC that requires under Article 43 the same information and deadline.

In relation to the right to rectification of the data where they are shown to be inaccurate, Article 16 provides the same deadline of five days for the entity responsible for the treatment of the data to resolve the request.

---

[57] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of data.

[58] Translated by the author.

To conclude, regarding the costs, all aforementioned requests for information are free of charge under the current system and proposals of the Brazilian framework, which enables the access of this right to be more effective.

The derogations of the Brazilian law proposal under the scope of the obligations and right of the data subjects are quite similar with the ones establishes under article 13 of the ED.

6) Restrictions on onward transfers: "further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive. (These exemptions are examined in Chapter Five.)"[59]

Current framework

The CPC did not provide, in its essence, the principle; however, it establishes joint responsibility among the individuals involved in the personal data treatment. We understand that in practice among the parties there is an awareness about providing an adequate level of protection, due the responsibilities applies in this regard.

Proposed framework

In relation to onward transfers, the proposed Brazilian law determines two different situations. The first (Article 31, I) includes the onward transfer when the treatment is over and is permitted whenever there is a need and relevance, solely with the free and express consent of the data subject in order to accomplish its objectives. The derogations are maintained for exclusively personal purposes and are not intended for communication or dissemination, as well as being preserved or transferred to a third party, solely for historical purposes, statistical, or scientific research.

The second situation involves the international transfer of data. Article 35 establishes as a general rule for transfer that transfer is only allowed in countries that provide a level of data protection comparable to the present law. The rules that establish a regulatory system for trans-border data are similar to those set out in Articles 25.1 and 26.2 of the ED, as well as the list of the exceptions under Article 26.1 of the Directive. Hence, we consider the proposal to be in line with the EU standards.

3.1.2) Additional principles

The additional sensitive principles are related to the application of special processing. The Commission follows the WP Document when issuing a decision. We will initially analyze the current framework in Brazil and, subsequently, the proposals.

[59] The Working Party Document 12: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, p. 6. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf.

1) Sensitive data: "where sensitive categories of data are involved (those listed in Article 8 of the directive), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing."[60]

Current framework

The law of the formation and querying of databases prohibits under Article 3, paragraph 3, II, any annotation regarding social and ethnic origin, health, genetics, sexual orientation, and political, philosophical, or religious convictions.

In relation to health data, under the current framework, there is no law that obligates service providers to ask data subjects for authorization to process data. The only guarantee is under the criminal code, which states that this type of information is a doctor–patient confidential record; hence, medical records shall not be transferred to third stakeholders.

Proposed framework

Article 4, IV of the Brazilian proposal defines sensitive data as:

> … personal data whose processing may give rise discrimination of the data subject, such as those revealing racial or ethnic origin, religious, philosophical or moral convictions, political opinions, trade union and politic affiliation, religious, political or philosophical organizations concerning health or sexual life, as well as genetic and biometric data.

The definition in this Article goes further regarding the ED and includes genetic and biometric data. However, the new European Regulation also includes this data.

Chapter V establishes general rules for the treatment of sensitive data. Article 20 defines as a general principle that: "no person can be compelled to provide sensitive data."

Article 21 is explicit in that it prohibits the formation of database content directly or indirectly regarding information that reveals sensitive data, and that this is exempt for reasons of general interest as authorized by law, respecting the rights of personality of the data subject, mainly the guarantee of non-discrimination. The first paragraph allows for the treatment of sensitive data, where the data subject has given free, informed, and written consent.

Derogations are allowed in cases involving statistical, historical, or scientific purposes, and also for the lawful finality uses of personal data of members without communication or dissemination to third parties, and guaranteeing the rights of the data subjects carried by nonprofit associations that have the nature of political, philosophical, and religious organizations or trade unions.

In relation to health data, Article 20, VI states that the treatment of sensitive data will be allowed when carried out by health professionals or sanitary entities that are indispensable in protecting the health of the stakeholder. Furthermore, subparagraph III in relation to the communication of health data states that the consent of the data subject may only be exempted in cases that are for the protection of his life, where he cannot exercise consent due to a physical impossibility or an inability in understanding.

[60] The Working Party Document 12: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, p. 7. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf

Further, the second paragraph of the aforementioned Chapter V considers the treatment of sensitive data manipulated for discriminatory purposes as illegal. Furthermore, the supervisory authority must indicate that it has secure measures and protection for the sensitive data of the data subjects, measures that must be taken by the responsible entity undertaking the treatment.

To conclude, we consider that this principle complies with the EU standards; we can also mention the Uruguay Decision, which provides the same standards as the Brazilian proposal under their Data Protection Act. However, regarding the Argentinian decision, there is one point that was included as an additional safeguard for the processing of sensitive data, which relates to cases of data on the records of criminals or for other offences that can only be processed by competent public authorities.

2) Direct marketing: "where data are transferred for the purposes of direct marketing, the data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage."

Current framework

In Brazil, there is a self-regulation code dealing with direct marketing, and even though it is not enforced as a law, it works as a rule for companies that work with e-mail marketing, and it is called CAPEM (a self-regulatory code of practice for e-mail marketing). It was issued by several regulation companies in 2009 and came into force in 2010.

The aforementioned code states the opt-in and opt-out functions as a general rule to send e-mails. In addition, to ensure proper measures in sending attached files, it is necessary to have gained previous and certified authorization from the recipient.

We understand the provisions of this private sector self-regulation to be adequate and in line with the EU standards. First, due the opt-in and opt-out measures that are included under the new EU Regulation, and second, in respect of the data-subject consent.

Proposed framework

The principle is covered by Article 17, II of the Brazilian proposal and establishes that the data subject might oppose either wholly or partially the personal data treatment for advertising purposes, even for data that was submitted for the procedure of decoupling.

The procedure of decoupling is not included under the ED, nor in the Argentina or Uruguay Acts; however, we understand that its inclusion under the Brazilian proposal is not a negative scenario, but a positive one.

3) Automated individual decision: "where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the directive, the individual should have the right to know the logic involved in this decision,

and other measures should be taken to safeguard the individual's legitimate interest."[61]

Current framework

There are no specific provisions under the current framework regarding this principle.

Proposed framework

This principle is recognized by Article 19 of the Brazilian proposal, which is based on the general rule that the data subject has the right in not to be targeted by decisions that affect them in a significant way and solely on the basis of an automatized treatment of personal data with the purposes of defining a profile or the data subject's personality.

In addition, Article 19 stipulates in the first paragraph that the affected data subject has the right to obtain information from the body responsible for the treatment, both regarding the assessment criteria and the procedure used for processing what was used to issue the decision that has been expressed. Furthermore, the second paragraph allows this automated decision in cases where the data subject expressly requested and provided the due legal process and legal defense.

To conclude, we consider the current framework insufficient; however, it is feasible in certain situations where the judges might consider, by analogy, the procedures used for a manual decision due the lack of the law.

3.2) Procedural and enforcement mechanisms: Three objectives for an adequate data-protection system

The WP's opinion on "Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive" as mentioned, indicates that the assessment of the adequacy of a third country's legal system should identify the underlying objectives of a data-protection procedural system, and on this basis, judge the variety of different judicial and non-judicial procedural mechanisms used in third countries. In that regard, the objectives of a data-protection system are essentially threefold:

1) To deliver a good level of compliance with the rules;
2) To provide support and help to individual data subjects in the exercise of their rights; and
3) To provide appropriate redress to the injured party where rules are not complied with.

Anticipating the conclusion, we consider that these three objectives are not completely fulfilled in the current Brazilian legislation; however, as soon as the law proposal on data

[61] The Working Party Document 12: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, p. 7. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf.

protection comes into force, these objectives will put in place a number of elements to serve these systems.

> 1) To deliver a good level of compliance with the rules: "A good system is generally characterized by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important role in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials."[62]

Related to effective sanctions against offences incurred by the controllers of the databases, we can identify Article 41 of the Brazilian law proposal that regulates administrative sanctions applied by the data-protection supervisory authority whereby it can also graduate the sanction according to the nature of the personal rights affecting the repetition of an offence, injury, and damage caused to stakeholders. The administrative sanctions may include different fines and in the case of an enterprise, between twenty percent of the gross annual earnings of the previous year, not including taxes, and in the case of other natural or legal persons, also encompassing any associations or entities (even temporary ones), between a minimum of two million reals (US$ 870,000) and a maximum of six million reals (US$ 2,600,000). Furthermore, in cases of the repetition of an offence, a double fine must be applied, and beyond the fines, blocking, dissociation, or cancellation of the personal data, prohibition in processing sensitive data, temporary suspension of activity, and prohibition of the use of the database take place.

The CPC also provides administrative sanctions against consumers' defense that may be imposed by administrative authorities. Article 56 states the administrative sanctions as:

> I - a fine; II. - Seizure of the product; III. - Destruction of the product; IV. - Cancellation of the product registration at the competent bodies; V. - Prohibition of the product manufacturing; VI. - Suspension of the product or service supply; VII. - Temporary suspension of the activity; VIII. - Cancellation of the concession or permission of use; IX. - Cancellation of the license permit for the establishment or activity; X. - Total or partial closing down of the establishment, work or activity; XI. - Administrative intervention; XII. - Determination as to counter-advertising.

> On the Brazilian Criminal Code, Article 313-A criminalizes the activities of the: Civil servers authorized in insert or facilitate false data, change or delete unduly correct data in computerized systems or databases of the Public Administration with the purpose of obtaining an undue advantage for himself or another or to cause harm: Penalty - imprisonment of two (2) twelve (12) years and a fine.

[62] Id.at.

In relation to specific regulations on investigation, inspection, preventive measures, promoting awareness of the matter, sanctions, and particularly authorizing international data transfers under the law proposal in Brazil, we can state that all of them are competences of the control authority for data protection, called the National Council for the Protection of Personal Data through the authority guarantee (*Autoridade de Garantia* in Portuguese), which, as mentioned in section 2.3.4, is an independent body that has administrative, management, and financial autonomy granted by law.

The aforementioned competencies, according to Article 39 of the law proposal by the mentioned Council are to plan, prepare, propose, coordinate, and implement the regulations. In addition, the Council receives, analyzes, and evaluates signpost queries, complaints, or suggestions submitted by data subjects, representative bodies, or legal persons of public or private law. For transparency purposes, the Council must create, maintain, and publish a record of the database including categories and sectors that the body deem relevant. Furthermore, regarding the awareness of the rights and obligations of the data controllers and data subjects, the body has competence to promote this awareness between them, as well as the safety measures related to personal data.

However, one of the points that is analyzed by the European Commission under the decisions on adequacy concerns the staff structure or members of the control body on data protection. Regarding the Brazilian law proposal, it was not stipulated, and instead, this issue was left for the Council when it enacts and establishes other provisions on matters within their competence. However, we believe, due to the context and principles of the law proposal, that we might expect a sufficiently rigid standard for hiring qualified individuals who have knowledge in the matter. Further, the ED stipulates an obligation under Article 28 (7) that is not complied with under the proposal regarding the subjection of the staff of the supervisory authority, even after their employment has ended, to a duty of professional secrecy.

On the scope of the CPC regarding regulations of investigation, inspection, preventive measures, and promotion of awareness, it is not as broad as the law proposal on data protection. However, it also establishes, under Article 44, the obligation of the public agencies in defense of the consumer to keep updated regarding claims against suppliers and services, and the obligation of publishing the results once a year, if the claim was attended to or not. The promotion of awareness is defined as a principle under Article 4, IV and includes education and information of the rights and obligations of the data controllers and data subjects.

We consider that the context of the current framework and the proposed framework are satisfactory in meeting this objective; however, it would be welcome if the proposal was reviewed, or subsequently, when establishing provisions regarding the staff members, if a provision regarding the professional secrecy of the confidential information to which they will have access is incorporated.

> 2) To provide support and help to individual data subjects in the exercise of their rights: "The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints."

As aforementioned in section 2.3.1, under Article 5, LXXII/CRBF1988 of the 1988 Brazilian Constitution, the HD Right is provided as a judicial remedy for the protection of personal data. It can be used by data subjects against any type of controller and is a quick remedy that is free of charge.

In relation to it being a quick remedy, we can consider a short period for the entire HD court proceeding. Starting with the special procedure, according to Article 19 of the 1997 legislative provision of the HD Right, it states:

> **The Habeas Data will take priority over all judicial acts**, except for the habeas corpus and the writ of security. Under the higher court, shall be brought to justice at first session following the date on which made the distribution are concluded and the send it to the rapporteur. Sole paragraph: the deadline for the conclusion cannot exceed 24 hours from the date of distribution. (Emphasis added by the author)

To present the HD Right, the data subject must directly request the body responsible for the treatment, and respect the following legal terms of ten days from the denial of the access of the information; fifteen days from the refusal of the rectification, and fifteen days from the denial of the settlements for the annotation of those interested.

After the HD Right has entered into the justice system due to a request from a judge or minister[63], it might takes more than ten days for further information, or if it is not the case, it can be sent directly to the public prosecutor, who is supposed to give an opinion in five days. After this legal term, the judge or minister has five days to deliver a judgment. This decision might result in imposing that the information be updated or rectified, to undertake settlements for the annotation of the interested parties, or to deny the request. If the request is denied, the data subject can appeal in fifteen days.

We can also mention that under the Argentina and Uruguay decisions, the HD action is considered as a proper mechanism to provide assistance and support to interested parties.

On Chapter IV of the Brazilian law proposal, the entity responsible for the treatment has five days to attend to the request of the data subject for an update/decoupling/cancellation or blocking of information and also to communicate to the recipient of the information the measures taken. Likewise in HD, the request for the mentioned information is free of charge as well.

On the CPC, regarding the deadlines for personal information in the databases of consumers, we can mention the efficient provisions of Law 12.414/2011[64]. Article 5 states that any update, rectify, cancel must to be communicate with other shared databases regarding the measures that were taken and the deadline it is seven days. In cases where the information shall be issued by the person that grants credit, the deadline is even better, at two days.

In relation to the point of an independent mechanism for the investigation of complaints, the Brazilian law proposal creates an administrative instance, according to Article 18: “in cases of violation of this law, the data subject may (referring to data subjects) claim their rights under the authority of guarantee, in the form of regulation.” Additionally, it

[63] Ministers might issue a decision, according the system of venues demonstrated on page 12.

[64] (This is called *Cadastro positivo* in Portuguese.) The law regulates the formation and rules of the consultation of databases with information on the performance of natural and juridical persons in terms of the formation of history credits that must be conceded.

establishes as one of the innumerous competences of the National Council for the Protection of Personal Data, through the authority of guarantee (the controller body), to receive, analyze, and forward a complaint presented by the data subject. The Council can apply through its own initiative or by request for sanctions, corrective measures, or preventive measures. In addition, it may veto wholly or in part the treatment of the data or blocking in cases that are unlawful or inappropriate. Finally, we can affirm that this body contains the elements necessary to provide support and help to data subjects in the exercise of their rights.

> 3) To provide appropriate redress to those affected when regulations are not observed: "the injured party where rules are not complied with. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate."

We understand that, in general, the Brazilian legislation contains the elements necessary to provide appropriate redress to the injured party where rules are not complied with, as will be analyzed.

The 2002 Brazilian Civil Code contains specific rules (Title IX) on civil liability that may apply for any person who has suffered damage by virtue of an unlawful act. Further, this type of civil liability (called objective) is configured regardless of the action or omission of the controller; the injured party has only to prove the damage and the causal link between the controller's activity and the damage, whereby the advantage is for the injured party.

Regarding civil liability and the CPC, we can affirm that the treatment of data is likewise configured as an objective civil liability. The consumer also has special protection against the controller, since consumers are entitled to have a more favorable interpretation of the law in cases of unfair or contradictory contractual clauses: In Brazil, the expression used to describe consumers when compared to economically powerful companies is "hypo-sufficient." Additionally, the CPC, in cases where more than one entity is responsible for the damage, holds all of them equally responsible (joint responsibility).

Meanwhile, the framework of the civil rights Internet proposal (*Marco Civil da Internet*) regarding the civil liability of Internet connection providers when damage it is caused by content generated by a third party might make it difficult to achieve this third objective. The Internet connection providers shall not be responsible for damage arising from content generated by third parties, except when, after receiving a specific judicial order, they do not take action to, in the context of their services and under the established time frame, make unavailable the infringing content. Even Article 16 specifies that the Internet connection provider must inform the user who is directly responsible for the content (of course, in cases where this can be identified) of the content of the judicial order. Therefore, we conclude that the injured party might face difficulties under this procedure in terms of redress (material as well as moral damages).

Regarding the liability under the proposed law on data protection, the activity of the treatment of data is considered as a risky activity and, as mentioned, in this case, the liability is characterized as objective.

Additionally, it is worth mentioning a concern issued by the WP under the Opinion[65] of the Argentina Act on Data Protection that allows for personal data to be processed without the data subject's consent when the data are obtained from sources subject to unrestricted public access. In this case, the WP mentioned that rules are needed that guarantee that the treatment of the personal data will not be likely to constitute a threat to the fundamental rights and freedom of the individuals, and in particular, to their right of privacy. Likewise, the Brazilian law proposal on data protection established the same rule as the Argentina Act, therefore, it would be adequate to review Article 13, II and, if it is the case, add guarantees for an eventual assessment by the European Commission.

4) CONCLUSION

To conclude, we will present below our consideration on the weakest and strongest points of the framework in Brazil.

Regarding the lack of a specific supervisory authority on data protection in Brazil, we consider that the current absence might create impediments regarding international cooperation between Brazil and the EU. Further, the proper application of the law under the treatment of personal data is undoubtedly more effective when exercised alongside staff members with expertise in this field. Hence, in the absence of a specific authority, the application of the law in this field in Brazil might be compromised.

Further, alongside the European supervisory authority, the proposed Brazilian supervisory authority would have effective powers of investigation for the redress of European citizens and vice versa. Nevertheless, it is important to bear in mind that this lack would be negated as soon as the proposal on data protection comes into force, which we consider is in line with the terms established in Article 28 of the ED.

The second weakness is the lack of consent for the opening of databases or files containing the personal data of consumers under the CPC. We consider the sole obligation of providing communication in writing to the consumer as a clear violation of the EU standards. However, under the law on the formation and querying of the database for the formation of a credit history regarding the consent of the consumer on the cadaster, this aspect should be carried out freely by the consumer as a pre-condition; therefore, we consider this consent adequate in relation to that of the EU standards.

Regarding the strongest point of the current framework, we consider the civil liability applied under the CPC. As we have seen, the management of databases in Brazil is considered a risky activity, and due to that, the burden of proof is laid upon the entity responsible for the treatment, which may also be compelled to provide compensation for damages regardless of the existence of fraud or negligence, which means that neither blame nor negligence is relevant. Further, the redress of individuals is more suitable under this liability, and we consider it effective in providing a first step for the appropriation of redress for those affected when regulations are not observed. In addition, as might be expected, the same liability will apply under the proposal on data protection.

[65] Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp63_en.pdf, p. 16.

However, the relativization of the liability of Internet providers for damage by content generated by third parties established under the *Marco Civil da Internet* we understand to be satisfactory and not a threat for the rights of users. Bearing in mind that the Internet provider is liable if they do not take action after receiving a specific judicial order.

The second strongest point concerns the administrative instances offered to individuals as a second channel of assistance for parties concerned about the protection of their rights. The provisions in the HD Right allow for the assessment of the rights of the individuals to be done quickly, efficiently, and free of charge. In addition, under the law proposal on data protection, assistance is given to those persons who need protection for the rights guaranteed by the law through the supervisory authority.

Lastly, we consider the international commitments that Brazil has entered into, and this is a strong feature concerning the level of adequacy of Brazil as a third country. It demonstrates the efforts of the country to be part of a global system, as it encourages building and equalizing systems in the best interests of their citizens as a common goal. In addition, Brazil recognizes other jurisdictions, and as we have seen, the Inter-American Court for the judgment of human rights violations is a great asset.

In fact, the current framework in Brazil highlights concerns about the assessment that might be made by the European Commission in the foreseeable future. However, as we have seen, the Brazilian system offers adequate measures in cases of violation and proper redress for individuals. Even though the absence of a specific supervisory authority might be a weakness in the communication between the EU and Brazil, however, in a system of checks and balances, we still consider the Brazilian system to be of value. Certainly, the amount of business might increase due the legal certainty following a decision of adequacy in Brazil, which surely would be an attractive proposition for both continents.

We also assume that the enforcement of the proposed Brazilian law on data protection might be feasible in a short time, due to the upcoming election for the President in Brazil and the scandal surrounding the United States surveillance this autumn, as mentioned. Therefore, the necessity of approving the law is undoubtedly a hot topic and this might influence the speed and path of the legislative procedure.

5) REFERENCES

5.1) Judgments

The Federal Supreme Court, regimental appeal in extraordinary appeal n º. 373.058-4 – RS.

Court decision nº 2.0000.00.310192-2/000 (1) of the Tribunal of Justice of the State of Minas Gerais, August 02, 2000

5.2) Directives/Decisions

Commission Decision 2003/1731/EC of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina.

Commission Decision 2012/5074/EC of 21 August 2013 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of data.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

5.3) Treaties/Statutes

Agreement on the European Economic Area of 1 January 1994.

Charter of Fundamental Rights of the European Union O.J. 3641/1, 18.12.2000.

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28.01.1981.

European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome 1950.

ECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data of 23.09.1980.

The American Convention on Human Rights (also known as the Pact of San José), Costa Rica of 22 November 1969.

The Universal Declaration of Human Rights, United States of 10 December 1948.

Còdigo de Defesa do Consumidor Brasileiro, Lei n º 8.078 (1990).

Constituicão da Repùblica Federativa do Brasil 1988.

Novo Còdigo Civil Brasileiro, Lei n º 10.406 (2002).

Còdigo Penal Brasileiro, Decreto-Lei nº 2.848 (1940).

Estatuto da Criança e do Adolescente , Lei nº 8.069 (1990).

Marco Civil da Internet no Brasil, Projeto de Lei nº 2.126 (2011).

Política Nacional de Informática , Lei nº 7.232, (1984).

Rito processual do Habeas Data , Lei nº 9.507 (1997).

Projeto de lei sobre o tratamento de dados no Brasil , Projeito de Lei nº 4060 (2012).

Lei Geral das Telecomunicações no Direito Brasileiro, Lei n º 9.472 (1997).

Còdigo de autorregulamentacão para a pràtica de Email Marketing of 14 January 2010.

5.4) Opinions

Article 29 Working Party, Opinion 01/2012 of 23.03.2012, on the Data Protection reform proposals.

Article 29 Working Party, Opinion 08/2012 of 05.10.2012, on providing further input on the data protection reform discussions.

Article 29 Working Party, Opinion 12/98 of 24.07.1998, Transfers of personal data to third countries. Applying Articles 25 and 26 of the EU Data Protection Directive.

Article 29 Working Party, Working document of 25 November 1995, on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995.

Article 29 Working Party, Working document of 3 June 2003, on transfers of personal data to third countries: Applying Article 26 (2) of the E Protection Directive to Binding Corporate Rules for International Data transfers.

Article 29 Working Party, Working document of 25 November 1995, on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 of 24 October 1995.

Article 29 Working Party, Opinion 04/2012 of 03.10.2002, on the level of protection of personal data in Argentina.

Article 29 Working Party, Opinion 06/2010 of 12.10.2010, on the level of protection of personal data in the Eastern Republic of Uruguay.

OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, 2007.

5.5) Statements/Comments/Guidelines/Proposals/Memos

Explanatory document on of the 29 Working Party in respect of: the Processor Binding Corporate Rules. Brussels, 19 April 2003.

Proposal for a Regulation of the European Parliament and of the Council in respect of: the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2013.

Transfers of Personal Data from the EU/EEA to third countries – frequently asked questions. Data Protection Unit of the Directorate General for Justice, Freedom and Security. Brussels, 2003.

5.6) Literature

Bygrave, Lee A. *Data Protection Law: Approaching Its Rationale, Logic and Limits*. Kluwer Law International (2002).

Bignami, Francesca, *Privacy and Law Enforcement in the European Union: The Data Retention Directive;* Chicago Journal of International Law, 2008.

Elesbão, Elsita Collor. Os direitos da personalidade no novo Código Civil brasileiro. In: Pessoa, gênero e família. Livraria do Advogado,Porto Alegre, Brazil, 2002.

Ouro Preto, Affonso Celso de Assis Figueiredo, Visconde de, *Advento da Dictadura Militar no Brazil*, Paris : Imprimerie F. Pichon, Paris, 1891.

Swire, P.P and Litan, R.E., None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive, Brookings Institution Press, Washington, D.C. 1998.

Silva, José Afonso. *Curso de direito constitucional positivo*, 28.ed.São Paulo: Malheiros, 2007.

5.7) Internet sources

Management Committee for the Internet in Brazil http://www.cgi.br

Digital Culture http://culturadigital.br

European Commission http://ec.europa.eu/index_en.htm

European Digital Rights http://www.edri.org

Annex 1

Abbreviations:

CPC – Consumer Protection Code

CRFB – Constitution of the Federal Republic of Brazil

CAPEM - Self-regulatory code of practice for e-mail marketing

DOPS – Department of Social and Public Order

EEA – European Economic Area

ED – European Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of data.

HD – Habeas Data

ICCPR – International Covenant on Civil and Political Rights

ICP – Internet Connection Providers

OAS – Organization of American States

SNI – National Intelligence Service

TSE – Superior Electoral Court

UDHR – Universal Declaration of Human Rights

WP – Working Party