A Brief Analysis of Data Protection Law in Brazil

Costa, Luiz

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

A Brief Analysis of Data Protection Law in Brazil

Report

Prepared by:

Luiz Costa
Researcher at the CRIDS
Federal Prosecutor in Brazil

Presented to the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD)
June 2012

TABLE OF CONTENTS

Introduction

This report was prepared upon request of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD). It presents the author's opinion and does not necessarily constitute the opinion of neither the T-PD nor the Brazilian Federal Prosecution.

The objective of this report is to provide information about the Brazilian legal framework on privacy and data protection and to compare it with the legal standards established by Convention 108, especially with regards to the scope of the Convention and possible status under Brazilian Law, data quality obligations and sensitive data, data security, rights of data subjects, trans-border data flows, supervisory authorities and enforcement.

I. The Context of Privacy and Data Protection in Brazil

Brazil is the largest country in South America and the world's fifth largest in area and population, which is estimated to be over 205 million by July 2012. Brazil is also characterized by its large agricultural, mining, manufacturing and service sector economy(CIA 2012), which became the world's sixth largest in 2011(Inman 2011).

Brazil is a federative republic composed by the Union – the federal entity, 26 member-states, 5561 municipalities, and the federal district, the country's capital. All of them are part of the federal structure and have their autonomy granted by the Brazilian Constitution. According to the Constitution, the Union has exclusive power to legislate on civil and criminal law, domains that include human rights and thus privacy protection (Article 22, I). Since consumer protection provisions might approach Privacy Protection, it must be added that the Union, the States and the Federal District have concurrent powers to legislate on consumption (Article 24). This concurrent legislative competence implies, for instance, that general law on consumer protection is edited by the Union; the legislative competence of the States in this domain must comply with the general rules established by the federal legislation(Câmara dos Deputados 2010).

At the federal level, the legislative power is exercised by the National Congress, which is composed by the Chamber of Deputies and the Senate (Article 44). The President of the Republic, assisted by the Ministers of State, exercise the Executive power (Article 76). Moreover, Federal courts and judges exercise the judiciary power. A similar model is adopted by State Members, whose legislative power is exercised by the State Assemblies, whose Governors are the chiefs of the executive power and are assisted by the Secretaries of State and whose state courts and judges exercise the judiciary power.

One point deserves special attention with regards to the organization of powers. It concerns the unusual status given by the Constitution to the Public Prosecution,

which is an independent Government Agency that exists at the federal and state levels and is neither a part of the Executive nor the Legislative or Judicial branches. According to the Brazilian Constitution, the Public Prosecution is a permanent institution, essential to jurisdiction, and it is its duty to defend the legal order, the democratic regime and the inalienable social and individual interests. (Article 129) The Public Prosecution promotes multiple interests, as various as the criminal prosecution, the protection of children and indigenous people as well as the promotion of public education, health, consumer and data protection. At the federal level the Federal Public Prosecution (MPF) is responsible for exercising the public prosecution functions. The chief of the MPF is the Attorney General of the Brazilian Republic, The Attorney General also has national responsibilities and actuates at the Supreme Federal Court.

The use of information and communication technologies is significantly increasing throughout the country in the last years, according to national indicators. To mention just a few, the proportion of households with computers in urban areas went from 17% in 2005 to 39% in 2010; the same year a great majority of the surveyed companies claimed to use computers (97%) and to have Internet access (95%) (Barbosa 2011, pp.321; 371–372). There are no comprehensive studies about the social attitudes of Brazilians with regards to privacy. However, privacy and data protection have been debated in Brazilian society, as older and recent celebrity photo leaks become apparent(G1 2012). We must also note that Brazil is quite mobilized with regards to child protection online, engaging in relevant initiatives as the SaferNet Internet Day (SaferNet 2012). A Government initiative in proposing a draft on data protection law is also to be considered. A growing concern about privacy and data protection issues must be brought to awareness.

II. Brazilian Law – Privacy & Data Protection

In this section we will glimpse at the Brazilian Law, especially with regards to existing privacy and data protection safeguards framework (II.1) and the proposed legislation in this domain (II.2).

II.1. *Lex lata*

The next paragraphs describe the main legal texts related to privacy and data protection and has added comments on procedural mechanisms and judicial developments.

International obligations

Brazil is a signatory to the International Covenant on Civil and Political Rights (ICCPR), which grants the right to privacy under Article 17, as well as to the American Convention on Human Rights (ACHR), which assures the right to privacy in Article 11, in the following terms:

"1. Everyone has the right to have his honor respected and his dignity recognized.
2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
3. Everyone has the right to the protection of the law against such interference or attacks" (Organization of American States 1969).

According to the Brazilian Constitution, "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" (Article 5°, §3°). However, this wording was adopted with the Constitutional Amendment n° 45 of 2004 and both mentioned treaties were signed and incorporated before that date, back when the enforceability of international treaties followed Article 5°, §2°, which states that "the rights and guarantees expressed in this constitution do not exclude others deriving from the regime and from the principles adopted by it, or from the international treaties in which the Federative Republic of Brazil is a party". What is then the *legal status* of these international treaties in the country? In 2008, while judging a case of detention for debt, the Supreme Court (STF for *Supremo Tribunal Federal*) decided that the ACHR, despite not having a constitutional status, had a "supra-legal" status, meaning that the national legislation must be in strict compliance with it. In the case, Article 7°, 7, of the Convention was the legal basis to invalidate preceding legislation authorizing the prison in the case of inability of fulfillment of contractual obligation(Mendes 2008).

It is worth noting that Brazil does accept the competences of both the Inter-American Court of Human Rights and the United Nation Human Rights Council, which means that the

privacy violations can be brought to the appreciation of these organizations. Furthermore, according to the Constitution, "Brazil shall strive for the creation of an international court of human rights".

Constitution

The Brazilian Constitution was adopted in October 5th 1988, three years after the end of a 21-year military dictatorship. Also known as "Constituição Cidadã" (the "Constitution of Citizenship"), the Constitution in extensive in assuring rights and liberties; only in Article 5° – the largest one concerning human rights – there are 78 entries, from which we highlight the following: the expression of thought is free, and anonymity is forbidden (IV); 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 (X); the home is the holy and inviolable refuge of the individual, and no one may enter therein without the consent of the dweller, except in the event of flagrant delict or disaster, or to give help, or, during the day, by court order; the secrecy of correspondence and of telegraphic, data and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts (XII) and, finally, *habeas data* shall be granted to ensure the access to the knowledge of information related to the person of the petitioner, contained in records or data banks of government agencies or of agencies of a public character or for the correction of data, when the petitioner does not prefer to do so through a confidential process, either judicial or administrative(LXXII).

The Civil Code

Privacy is protected by the 2002 Civil Code, under the Personality Rights chapter, particularly when it states that: "*Except as provided by law, personality rights are inalienable, can neither be renounced and nor undergo voluntary restraint*" (Article 11); "*One may be required to stop the threat or injury to the right of personality, and claim damages, without prejudice of other penalties provided by law*" (Article 12); "*Except as permitted or necessary to the administration of justice or the maintenance of public order, the disclosure of writings, transmission of the word, or the publication, display or use of the image of a person may be prohibited in response to his or her demand and without prejudice to compensation if a damage is caused to honor, good reputation or respectability, or if there was commercial use*"(Article 20) and the last provision "*the private life of the natural person is inviolable, and the judge, attending the applicant's request, may take the necessary measures to prevent or terminate action contrary to this standard* " (Article 21).

The Consumers' Protection Code

The Consumers' Protection Code (CDC for *Código de Defesa do* Consumidor) of 1990 regulates consumers' databases held by banks, credit agencies and other

companies like stores and files in a non-exhaustive manner. Nevertheless we stress the following points: A consumer's right to access is granted. Consumers' files must be objective, clear, truthful, easily understood and cannot contain the same negative information for more than five years. In the case of files not requested by the consumer, explicit information must be given to the consumer. Moreover, a right to rectification of inaccurate or incomplete data is granted (Article 43). Credit information protection is treated more extensively under the Credit Information Law hereafter.

Electronic surveillance, wiretapping and the Criminal Law

The Brazilian Wiretap Law of 1996 is a direct implementation of the Article 5°, XII of the Constitution. From this Law we emphasize that: 1. Wiretapping is possible only in criminal investigations and a judicial order is necessary (Article 1°); 2. Wiretapping must not be allowed if there is no reasonable evidence that the crime has been committed by the person pursued, if the aimed proof can be produced by other means (*rectius* less invasive) or, last instance, if the crime is punished with detention, which is a less rigorous kind of imprisonment (Article 2). 3. Furthermore, illegal wiretapping is punished with a two to five year penalty and fines (Article 10).

The Credit Information Law

On June 9th 2011 Brazil passed the Credit Information Law (CIL), which regulates "the creation and the access to databases related to credit information of citizens and companies". We highlight that this legal instrument enacts principles and rules related to data quality as objectivity, clearness, truthfulness and comprehensibleness of data. It forbids the processing of excessive information (data not necessary to credit granting or other banking services) and sensitive information (understood as related to social and ethnic origins, health, genetics, sexuality, and political, religious and philosophical convictions) (Article 3°). It covers the purpose principle and rights to the data subjects, so the right to access, the right of rectification and erasure of data, the right to know the criteria used by the banks in order to evaluate the credit's risk, the right to be informed previously about the existence of the data storage, the data base manager's identity and about the identity of the third parties that will have access to data, finally the right to be informed about the purpose of the processing and to have a second analysis of a decision based on automatic means (Articles 5° and 7°). Database managers are obliged to inform citizens about all the stored or obtained personal information as well as about the sources through which this information was obtained, to provide information about third parties that have access to personal data and to provide information about citizens rights (Article 6°). Last point, CIL also imposes data quality obligations to processors (Article 8°).

Right to Information Law 2012

The right of information is set in Article 5°, XXXIII of the Brazilian Constitution, which grants the right to obtain information from government agencies information according to their personal interest and justified by collective or public interest. The Constitution excludes from accessible information those whose secrecy is vital to the

security of the society and state. Right of information Law (RIL) of 2011 stipulates that that secret information must be classified according to different degrees of security and is setting up a commission to decide on the processing of classified information. The duration as regards to the obligation to secrecy might vary between 5 and 25 years for documents that are essential to the State or public security and 100 years for classified information on the grounds of the protection of intimacy, privacy, honor and a person's image. Despite this 100-year duration, which can seem that privacy is protected, there is no legal criterion to balance conflicts between the rights to privacy and the citizen's right to information, which can lead to the total absence of guidelines and ultimately to conflicts.

Procedural mechanisms and jurisprudence

Here are the main available ways by which citizens may obtain a remedy to privacy and data protection threats: a) if the violation involves a consumer relationship, one can lodge complaints with state non-independent supervisory authorities, which can impose fines and determine the interruption of activities for example (CDC, Article 56); b) still within a consumer relationship, NGOs, the Public Prosecution and some government agencies can claim judicial remedies (i.e., class actions) against every responsible for a consumer right's violation; c) in consumer law and other legal contexts, the right to start individual judicial procedures is granted by the Constitution (Article 5°, XXXV).

Despite the recognition that the right of privacy has and the existence of procedures, since there is no general data protection framework, and specially no clear definition of criteria to judge conflicts, jurisprudence tends to be erratic with regards to personal data protection. For example, despite the fact that financial information can only be disclosed by the data subject or in the context of a judicial procedure, complementary laws allow the Central Bank, the National Congress and its Commissions, the Internal Revenue Service, the Advocacy-General of the Union and the Prosecution Service to get access to this data without the data subject's consent. If the case-law of the STF is quite uniform concerning access by judges and courts and Congress Commissions, decisions are contradicting each other as regards to the limits imposed to the Central Bank, the Internal Revenue Service and the Prosecution Services when they request access to this type of financial information. Furthermore, the possibility of the Advocacy-General accessing financial information waits for a definitive judgment by the STF(Sampaio 2011, p.555). Other significant examples might be found in the fact that Federal and State Court decisions frequently refer to the "relative character" of the right to privacy in case of conflicts between the right to privacy and other values such as criminal investigation, public interest and the protection of honor. However, the establishment of balancing values criteria does not follow this general mention. Also, decisions on administrative authorities access to contact data detained by Internet Service Providers and privacy issues in workplaces fail to have substantial consistency[1].

[1] Regarding references concerning privacy jurisprudence see (Kaminski & Leonardi 2010).

Self-regulation

The E-mail Marketing Self Regulation Code (CAPEM for *Código de Autorregulamentação para a Prática do E-mail Marketing*) is an Internet Steering Committee project that put together private sector representatives involved with e-mail marketing. The Code establishes basic rules like those related to permission of recipients to receive communication, unsubscribe policy and oppose third parties content(CAPEM 2009).

II.2. *Lex ferenda*

Regarding future law, we are going to pinpoint two texts in particular.

The Executive power sponsors the *Brazilian Internet Bill of Rights*, which was sent to the National Congress in 2011. The Bill aims to establish principles and guarantee, rights and duties for the use of Internet in Brazil. We highlight the following provisions: 1. privacy protection principle is asserted (Article 3°); 2. The text recognizes the secrecy of Internet communications, which can only be excepted by court order in the context of criminal investigation or procedure (Article 7°, I); 3. The right to clear privacy policies is ensured (Article 7°, IV); 4. The right to privacy and to freedom of expression are considered together, even if they might be to a certain extent contradictory, as prerequisites for a free exercise of using the Internet (Article 8°) and judges must certify the secrecy concerning the personal data disclosed in a judicial procedure (Article 18)(Governo Brasileiro 2011).

Having been posed into public consultation from November 2010 up to April 2011, the *Brazilian Data Protection Draft* (DPD) is under governmental discussion since then. The text is clearly inspired by European legislation and aims to create a comprehensive data protection framework in Brazil. The draft establishes the enactment of data protection principles – finality, necessity, right to access, proportionality, data quality, transparency, security, good faith, responsibility and prevention (Article 8°), a consent framework, (Articles 9° to 13), rights of data subjects, as access, rectification and erasure (Articles 15 to 19), protection to sensitive data (Articles 20 to 22), security principles (Articles 23 to 27), processing rules in general, as well as related to governmental and private databases (Articles 28 to 34), trans-border data flow rules (Articles 35 to 37), supervisory authority and enforcement (Articles 38 to 44) and best practice codes (Article 45)(Ministério da Justiça 2011).

Up to now there is no official date about when the draft mentioned above will be presented as a Bill. Considering that Brazil will have municipal elections in the second semester of 2012, a period where parliamentarian activities tend to be less intense, a large number of observers speculate that the Bill could be presented before the end of the first semester. Once presented, unless the urgency regime is adopted (100 days maximum), the duration of the legislative process cannot be estimated. The outlines of the political debate about different data protection approaches are not completely clear in the moment. We point, however, that Brazil does have a strong civil law tradition and

a developing consumer protection culture. These elements define a certain tendency of this debate to be around the creation of a protective statutory law regime.

III. Brazilian Law and Convention 108

Having glimpsed at actual and possible future legal texts related to privacy and data protection in Brazil, we will now compare them to Convention 108. To assess Brazilian law we will use the following criteria, inspired from the structure of the Convention and its Additional Protocol of 2001: the scope of the Convention and possible status under Brazilian Law, data quality obligations and sensitive data, data security, rights of data subjects, trans-border data flows, supervisory authorities and enforcement.

III.1. Scope of the convention and possible status under Brazilian Law

International obligations (ICCPR and ACHR) and the Brazilian Constitution do not distinguish privacy protection provisions between private and public. We must, however emphasize that:

(i) some laws attribute exceptional powers to government agencies, whose interpretation is still unclear as in the example of financial information mentioned above (see item II.1),

(ii) the Data Protection Draft provides quite large exceptions in favor of governmental agencies such as the possibility to dismiss data subject consent when the processing is "necessary to exercise typical State functions" (Article 13, III), affords to the public authorities the right 1. To process sensitive data in favor of "state powers" (Article 20, VII) 2. to share data between different public organisms without the data subject's consent when these exchanges are "necessary to exercise their institutional competences" (Article 32, II) or 3. To impede the right of the opposition to protect public order (Article 33,I),

(iii) The country is now reflecting a specific social attitude that is the right to information, in which the Right to Information Law inserts itself. The openness of public data comes, nevertheless, without a strong data protection framework, a circumstance that can put citizens' privacy in danger.

Considering the Convention scope, especially its application to processing in both the public and private sectors (Article 3,1) and the exceptions and restrictions enacted by Article 9, we may consider that (a) Brazilian law is half-way to the standards of the Convention with regards to the necessity in a democratic society rights derogation criterion; no present Law foresees it explicitly, but we must recognize that the Data Protection Draft mentions the "indispensability" criterion (Article 33 of the DPD); (b) Actual law is far from the Convention's 108 requirements, including the absence of a clear reference to state security, public safety and rights of others exceptions; the DPD is however close to the Convention as it identifies clearly public safety, suppression of criminal offences and the rights of others as exceptions to the

general regime (Articles 3°, §2° and 33,I and II); (c) the DPD has large exceptions in favor of the public sector, which also raises serious concerns about Privacy .

With regards to the possible legal status under Brazilian law, because they concern human rights, the Convention and its Additional Protocol would be considered either as equivalent to constitutional amendments – if voted in two rounds by three fifths of the national congress – or as supra-legal texts if these conditions do not apply.

III.2. Data quality obligations and sensitive data

There is no law establishing general data quality obligations. However, it is worth noting that both the Consumers' Protection Code and the Credit Information Law impose that data must be objective, clear, truthful and easily understandable (Article 43 of CDC and Article 3°, §2° of CIL). Concerning the DPD, Article 14 insists that personal data shall be processed fairly and lawfully; collected and stored for determined, explicit and legitimate purposes; clear, truthful and easily comprehensible; they must also be pertinent, complete, proportional and not excessive in relation to the purposes for which they were collected and stored; preserved in a form which permits identification of the data subjects for no longer than is required for the purpose of which the data is stored and conserved for no longer than the established time within the specific laws or regulations.

Similarly, sensitive data processing does not have a legal framework. We must, however, point that the Credit Information Law prohibits processing related to sensitive data, understood as those related to social and ethnic origins, health, genetic information, sexuality, political, religious and philosophical beliefs (Article 3°, § 3°, II). Moreover, professional secrecy laws, as in the case of ministers and physicians, also protect some of these values. DPD mentions the establishment of specific rules for sensitive information, where sensitive data is any data whose processing can give rise to discrimination against the holder, such as those revealing social and ethnic origins; political, religious and philosophical beliefs; trade union, political party, religious, philosophical or political affiliations; health; sexuality and genetic and biometric data (Article 4°, IV). Under DPD the processing of sensitive data is interdicted unless (i) the processing is legally imposed and the data subject gives their free, informed, written consent; (ii) the processing is carried out in the course of the activities of political, philosophical, religious or trade union associations, subject to certain conditions, (iii) processing is necessary to protect life or physical safety of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; (iv) processing is performed only for historic, scientific or statistic research; (v) if it is related to data that data subject discloses; (vi) if, performed by health or sanitary authorities, its is indispensable to protect data subject's health; (vii) if it is necessary to the exercise of state functions, legally foreseen (Article 20).

Considering Convention 108 previsions on the quality of data (Article 5), we may consider that (a) Brazilian present legislation is halfway from the Convention since legal provisions on data quality are drafted in a restricted and restrictive manner according

to the Convention 108 requirements; (b) Brazilian law would however be very close to Convention 108 if DPD is approved; its Article 14 is nearly a reproduction of Article 5 of the Convention.

Considering Convention 108 previsions on sensitive data (Article 6), we may consider that (a) with regards to Credit Information Law, the interdiction to process sensitive data protection puts Brazilian law in a position more protective than the Convention; (b) DPD aims to establish a sensitive data regime which is similar to Directive 95/46; the conformity to Article 6 of the Convention 108 would, however, depend on a clearer statement of the exceptions regime in DPD. For example, it is not clear how the general "state powers" exception, as it is stated, could provide appropriate safeguard to data subjects.

III.3. Data Security

Since there is no comprehensive legislation concerning data security issues, current legislation can be applied in the context of general civil, consumer and criminal responsibilities and liabilities. With a look into the future legislation, we must add that the Brazilian Internet Bill establishes the network security principle (Article 3) and DPD sets up a security regime where: (i) data processing must minimize, through the adoption of appropriate measures to promote safety and to protect personal data against accidental or unlawful destruction or loss, unauthorized access or the use not allowed by the data subject or different of the purpose for which it was collected. These measures must be proportionate to the state of art, the nature of data and the specific characteristics of the processing, in particular when it involves sensitive data (Article 23); (ii) a set of minimum security measures must be established by the supervisory authority (Article 24); (iii) controllers and processors' responsibility and secrecy rules are established (Article 25 and 26); (iv) a data breach notification regime is created (Article 27).

With regards to Article 7 of Convention 108 we consider that (a) there is no obligation to controllers to take security measures for the protection of personal data in Brazil; legal protection is therefore restricted to general responsibilities and liabilities. Brazilian law is halfway from the Convention at this point; (b) projected data security regime in DPD is nevertheless close to the Convention.

III.4. Rights of Data Subjects

As seen above, data subjects rights are granted (under both CDC) rights to access, to be informed about the creation of personal data processing and to rectify inaccurate information – and CIL – which, in addition to the mentioned rights, also enables the data subjects' rights to erase data, access to the knowledge of the risk analysis criteria, to be informed about the database manager and third party identities, to be informed about the purpose of the processing and to have a second analysis of a decision based on automatic means. Regarding future law, DPD establishes a general

right to access and its procedure, the rights to rectify, cancel, dissociate and block data, to oppose to data processing and not to be submitted to a decision which significantly affects the data subject and which is based solely on automated processing of data.

Considering Convention 108 previsions on additional safeguards for the data subject (Article 8), we may consider that (a) Brazilian consumer protection and credit information laws are similar to Convention 108 since the rights to establish the existence of an automated personal data file, to access, to rectify and to erase as well as to have a remedy through supervisory authorities or courts are founded (b) DPD projected data subjects rights are also similar to Article 8.

III.5. Trans-border Data Flows

No Brazilian legislation, even sector-specific, regulates the trans-border data flows. With regard to future legislation, DPD translating the articles 25 and FF of the EU Directive, requires that (i) transfer of personal data to a third country has an adequate level of protection, complying with the Brazilian legislation's requirement; (ii) this regime is mandatory although excepted if the data subject has given their consent; if the transfer is necessary: for fulfilling obligations of a contract of which the data subject is a party; to assure a significant public interest; for international cooperation between intelligence and investigation agencies; to the establishment, exercise or defense of legal claims or to protect the life or physical safety of the data subject or a third party if the former cannot give their consent because of physical incapacity, or incapacity to act and understand (Article 34); (iii) the envisioned supervisory authority will evaluate the adequate level of protection (Article 37), and may authorize transfers if the third country provides adequate safeguards to privacy, security and the exercise of rights under Brazilian law (Article 38).

Regarding Convention 108 previsions on trans-border data flows (Article 12), we need to consider that (a) Brazilian legislation is far from the Convention given the absence of general and sector-specific rules and (b) DPD is similar to Article 12, especially with regards to equivalent protection; we note also that the projected law text is comparable to the Directive 95/46's.

III.6. Supervisory Authorities and enforcement

In Brazilian legislation, non-independent supervisory authorities must enforce data protection rules related to consumer protection (see item II.1). This means that consumers can file complaints with municipal and state authorities that have powers of investigation and intervention. These authorities are, nevertheless, in early stages of data protection practice[2]. DPD is setting up a Supervisory authority. Its structure and attributions will be fixed in specific legislation, and various competences in order to

[2] Despite some initiatives of the federal Government in professional qualification (for example (Doneda 2010)) there is still a long road ahead, since officials are not familiar with data protection's basic principles.

ensure enforcement of the legislative provisions, but also for assessing certain aspects of the national data protection policy or for investigating possible infringements including the enforcement of administrative sanctions, promoting data protection awareness, requiring privacy impact assessments from controllers (Articles 38 and 39). Furthermore, State and Municipalities will be able to create their own authorities (Article 40).

Comparing Article 1 of the Additional Protocol to the Convention we note that (a) regarding consumer protection, Brazilian law is half way to the Convention's standards since its existent supervisory authorities are non-independent (i.e., submitted to the Executive power); besides, the effectiveness with regards to data protection is restricted, most related to credit information (b) DPD is close to the Convention Additional Protocol with regards to authorities powers, lodging claims and decisions that may be appealed against through the courts. Independence is, however, a major issue and two points deserve special attention. The first one concerns the administrative, budgetary and financial autonomy model mentioned by DPD in Article 38. There is no mention to functional autonomy, which is a legal concept with significant impact in Brazil. An authority with functional independence is not submitted to the interference of any of the three powers while exercising its functions. This is the case for the Federal Audit Court, the Prosecution Service and the Public Legal Defense for instance. In its actual wording, Brazilian DPD will imply the setting-up of non-independent authorities strictly submitted to the Executive power, which is the same model adopted for consumer protection authorities[3]. The second point concerns the structure and assignments of the supervisory authority, to be established by "specific legislation". The absence of a clear reference to the authority who will choose and which criteria will guide the choice of the members of this supervisory authority leaves an open door to the risk of powers' concentration[4].

[3] This aspect was not ignored by a major Brazilian newspaper, who recently pointed to the giving of future control of the data protection authority exclusively in the hands of the Executive Power(Folha de São Paulo 2012).

[4] Common knowledge indicates that Brazilian laws that are made as open door "specific legislation", are frequently complemented by Provisional Measures, a President of the Republic's exclusive instrument that has the same status as a law even if it must be confirmed *a posteriori* by the National Congress.

Conclusions

As seen above, Brazilian Law does have a *privacy framework*, although it is not comprehensive. International obligations as ICCPR and ACHR, but also constitutional provisions and the Civil Code give the contour the right to privacy, private life, home, correspondence and reputation.

Concerning *data protection laws* some points must be stressed. We note that despite the *habeas data* constitutional provision adopted quite early by the Brazilian Republic was not operational. Moreover, other legal texts are sector-specific as the example of CDC's databases rules and CIL show. Because of this, conformity, closeness and distance with regards to Convention 108 are consequently partial. Brazilian courts provide some protection of privacy and personal data according to the legal texts mentioned above. Credit Information protection is possibly the most developed front in data protection in Brazil; CIL and RIL are recent laws whose effectiveness and impacts on privacy and data protection are still to be determined.

Concerning the self-regulation initiative, although restricted to e-mail marketing and its effectiveness is still to be established, it is a relevant example of private sector commitment in the data protection domain.

Looking at Brazilian Data Protection Law through Convention 108 standards, we found some areas of compliance with data protection principles, the data subjects' rights and data controllers' obligations, the creation of a supervisory authority and the means of enforcement, although restricted to consumers' protection domain. Looking forward, the Brazilian Data Protection draft legislation looks promising and transforming to Convention 108 standards, since most of the envisioned provisions about the principles, the D.S rights and D.C. obligations, the data security and trans-border data flows are theoretically and sometimes in their drafting, strictly conforming to Convention 108. However, enforcement in general and overindulgent rules towards public actors may raise concerns for which effectiveness of legislation, vulgarization of data protection rules and more plurality are possible antidotes; the real correspondence between the two legal systems is to be followed.

References

Barbosa, A.F., 2011. *ICT Households and Enterprises 2010. Survey on the Use of InformatIon and CommunicatIon Technologies in BrazIl*, São Paulo: Brazilian Internet Steering Committee. Available at: http://www.cetic.br/tic/2010/index.htm [Accessed May 15, 2012].

Câmara dos Deputados, 2010. Constitution of the Federative Republic of Brazil. Available at: http://www2.stf.jus.br/portalStfInternacional/cms/verConteudo.php?sigla=portalStfSobreCorte_en_us&idConteudo=120010 [Accessed May 15, 2012].

CAPEM, 2009. Código de autorregulamentação para a pratica do e-mail marketing. Available at: http://www.capem.org.br/ [Accessed May 22, 2012].

CIA, 2012. The World Factbook - Brazil. Available at: https://www.cia.gov/library/publications/the-world-factbook/geos/br.html [Accessed May 14, 2012].

Doneda, D., 2010. A proteção de dados pessoais nas relações de consumo: para além da informação credíticia. Available at: http://portal.mj.gov.br/main.asp?Team=%7BB5920EBA-9DBE-46E9-985E-033900EB51EB%7D [Accessed April 26, 2012].

Folha de São Paulo, 2012. Regular a Internet. *Folha de São Paulo*. Available at: http://www1.folha.uol.com.br/fsp/opiniao/44078-regular-a-internet.shtml.

G1, 2012. Carolina Dieckmann fala pela 1ª vez sobre fotos e diz que espera 'justiça'. *Pop & Arte*. Available at: http://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html [Accessed May 15, 2012].

Governo Brasileiro, 2011. *Projeto de lei - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*, Available at: http://www.planalto.gov.br/ccivil_03/Projetos/PL/2011/msg326-24ago2011.htm [Accessed May 18, 2012].

Inman, P., 2011. Brazil overtakes UK as sixth-largest economy. *The Guardian*. Available at: http://www.guardian.co.uk/business/2011/dec/26/brazil-overtakes-uk-economy [Accessed May 14, 2012].

Kaminski, O. & Leonardi, M., 2010. O direito à privacidade e proteção aos dados pessoais no Brasil. Available at: http://www.seminarioprivacidade.cgi.br/anteriores/i_seminario/programa.htm [Accessed May 21, 2012].

Mendes, G., 2008. *Banco Itaú S/A vs. Armando Luiz Segabinazzi*, Available at: http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%28RE%24%2ESCLA%2E+E+349703%2ENUME%2E%29+OU+%28RE%2EACMS%2E+ADJ2+349703%2EACMS%2E%29&base=baseAcordaos [Accessed May 16, 2012].

Ministério da Justiça, 2011. *Anteprojeto de lei sobre a proteção de dados e da privacidade*, Available at: http://culturadigital.br/dadospessoais/ [Accessed April 26, 2012].

Organization of American States, 1969. American Convention on Human Rights. Available at: http://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm [Accessed May 16, 2012].

SaferNet, 2012. Dia Internet Segura 2012. Available at: http://www.safernet.org.br/site/sid2012 [Accessed May 15, 2012].

Sampaio, J.A.L., 2011. A Suprema Inviolabilidade: a Intimidade Informática e o Sigilo Bancário. In *Direitos Fundamentais no Supremo Tribunal Federal Balanço e Crítica*. Lumen Juris, pp. 531–555.