DATA PROTECTION IN BRAZIL

DRAFT REPORT / REVIEW OF LEGAL BACKGROUND

Authors

Jacqueline de Souza Abreu
Fabiane Midori Sousa Nakagawa
Juliana Pacetta Ruiz

Collaborators

Francisco Carvalho de Brito Cruz

www.internetlab.org.br

DATA PROTECTION IN BRAZIL

DRAFT REPORT / REVIEW OF LEGAL BACKGROUND

***

INSTITUTIONAL TEAM **Executive Director** Dennys Antonialli **Director** Francisco Brito Cruz **Director** Mariana Giorgetti Valente / PROJECT TEAM **Project Leader** Jacqueline de Souza Abreu **Research Intern** Juliana Pacetta Ruiz **Research Intern** Fabiane Midori Sousa Nakagawa

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA, 2016.

INTERNETLAB / Rua Augusta, 2690, Galeria Ouro Fino, Loja 326 / www.internetlab.org.br

Table of contents

Team Members involved in this project

AUTHORS

JACQUELINE DE SOUZA ABREU / LL.M. Candidate at University of California, Berkeley, School of Law. She holds a Master of Laws from the Ludwig-Maximilians University of Munich (LMU) and a Bachelor's Degree in Law from the University of São Paulo (LL.B., 2014). During her graduate studies, Jacqueline received scholarships from Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) and Programa de Estímulo ao Ensino de Graduação (PEEG) to conduct research in the areas of Philosophy and Jurisprudence, and was a member of the Law, Internet and Society Nucleus of the University of São Paulo (NDIS-USP). Jacqueline participated in an academic exchange with LMU, at which time she received a scholarship from the German Academic Exchange Service (DAAD). She was also a junior researcher with FGV DIREITO SP.

FABIANE MIDORI SOUSA NAKAGAWA / Bachelor student of laws at the University of São Paulo Law School (FDUSP)., where she also attends courses of the double degree program in Law offered by the Jean Moulin University Lyon III. In 2015-2016, she was an exchange student at the Ludwig-Maximilians-Universität München (LMU), where she held a scholarship from the German Academic Exchange Service (DAAD) to attend the preparatory course for the LL.M. in German law. From 2013 to 2014 she was headmistress of the Centre of Studies in International Law of University of São Paulo Law School (NEI-FDUSP). Currently, she is a research intern at the InternetLab.

JULIANA PACETTA RUIZ / LL.M. Candidate at University of California, Berkeley, School of Law. She holds a Master of Laws from the Ludwig-Maximilians University of Munich (LMU) and a Bachelor's Degree in Law from the University of São Paulo (LL.B., 2014). During her graduate studies, Jacqueline received scholarships from Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) and Programa de Estímulo ao Ensino de Graduação (PEEG) to conduct research in the areas of Philosophy and Jurisprudence, and was a member of the Law, Internet and Society Nucleus of the University of São Paulo (NDIS-USP). Jacqueline participated in an academic exchange with LMU, at which time she received a scholarship from the German Academic Exchange Service (DAAD). She was also a junior researcher with FGV DIREITO SP.

COLLABORATORS

FRANCISCO CARVALHO DE BRITO CRUZ / Master in Philosophy and Jurisprudence by the School of Law of *Universidade de São Paulo* (FDUSP). Graduated in Law by School of Law of *Universidade de São Paulo* (FDUSP) and, in the course of that program, received a scholarship from *Programa de Educação Tutorial* (PET) –Sociology of Law. Visiting Researcher (2013) at the Center for Study of Law and Society of the University of California – Berkeley, through Rede de Pesquisa Empírica em Direito (REED) exchange program. Mr. Brito Cruz received the *Marco Civil da Internet e Desenvolvimento* Award of the School of Law of *Fundação Getúlio Vargas* (SP). Attorney-at-law, practices in areas such as CyberLaw, Intellectual Property, Consummer Law and Press. He was founder and

coordinator of FDUSP Group of Law, Internet and Society (NDIS) between 2012 and 2014 and is currently a director of InternetLab.

I. Introduction:

The following report presents the current legislative framework regarding data protection in Brazil. It was prepared by Internetlab in April and May of 2016 for the *Asociación por los Derechos Civiles*.

First, it goes through the constitutional provisions related to the matter **(Part I)**. Then it covers the sectoral privacy laws that, in absence of a general data protection law, constitute the legal landscape of data protection in Brazil. Next, bills of law are presented **(Part B)**. The last part presents the updates about the requested survey with the telecommunications companies, in order to learn some of their data protection practice **(Part C)**. Although we have assessed the companies with the questions (and are still awaiting their response) some answers could be provided to the questionnaire based on other research projects conducted by InternetLab during the last year.

II. Existing law

II. 1. Data protection in the constitution

Brazilian Constitution ensures protection of privacy and private life as a fundamental human right (art. 5, X) and guarantees to all persons residing in the country the secrecy of data (art. 5, XII); restrictions to that right can be made pursuant to the law, in principle through judicial decision.[1]

> *Article 5. All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property, on the following terms:*
> *X - the privacy, private life, honour and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured;*
> *XII - 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;*

There is an ongoing dispute as to the scope of protection of communications secrecy in subsection XII. There's no consent (i) as to whether the subject matter of protection of this fundamental right is information transmitted through the media so listed or the flow of such information while in transit and also (ii) about which categories, out of the four listed on that subsection, are included in the constitutional exception that allows for breach of secrecy ("*except, in the latter case*").

[1] As explained in section regarding financial data, there is one recent exception ruled constitutional by the Supreme Court.

Leading scholars are of the view, endorsed in a decision of the Federal Supreme Court[2], that the protection referred to in subsection XII of article 5 does not refer to information transmitted through correspondence, telegraph messages, data, and telephone calls in itself but rather to communication, to the flow thereof as it is taking place, and only the secrecy of telephone communication, while underway, could be breached for purposes of criminal investigation and prosecution; this possibility would not apply to the flow of data, telegraph, or letters.

When brought to the context of data protection, this very narrow interpretation of the scope of protection would implicate that only flows of data are protected under article 5, subsection XII. Literally, it would mean that data in transit is inviolable and its secrecy could not even be breached upon a court order. Although that position is advocated by some legal scholars, it is not mirrored in case law, which has already accepted the "breach" of secrecy of communications flow of all types as long as it is "proportionate," whenever it is based on a fundamental right or the public interest.

The right to privacy in subsection X, on the other hand, allows for protection of communications in a broader sense and has been used to cover data not protected by the secrecy of communications.[3]

The Constitution grants also the *habeas data* as a judicial measure that permits people to know and correct their personal data in governmental records.

> *LXXII - 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;*

II.2. Sectoral Privacy Laws

The following subsections present the relevant legislation applicable to telecommunications, financial, consumer, and health data.

II.2.1. Telecommunications data

[2] In the trial of *Recurso Extraordinário* 418.416-8/SC, of 10/May/2006, the case reported by the Justice Sepúlveda Pertence states that protection under subsection XII of article 5 does not refer to information transmitted in correspondence, telegraph messages, data and telephone calls in itself but rather to communications in transit, to the flow of communications as they occur. Implicitly, the decision excludes application of the exception set forth in subsection XII to article 5 to data flow.

[3] See, for instance Federal Supreme Court, *Mandado de Segurança* 24.817/DF, Case reported by Justice Celso de Mello, tried on 3 Feb. 2005, which associates breaches of the confidentiality of tax, banking and telephone records with restrictions on the rights provided for by article 5, X. Please visit http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605418. Accessed on: 17 June 2015.

- **General Telecommunications Law (Law no. 9,472 of 1997)**

The General Telecommunications Law guarantees the rights to secrecy of communications, privacy, and data protection in usage of telecommunications services (art. 3, V and IX and art. 72).

> *Art. 3 The telecommunications service user has the right to:*
> *V - inviolability and secrecy of their communication, except in the cases and constitutional conditions and legally established;*
> *IX - respect for their privacy in the collection documents and the use of personal data by the service provider;*
>
> *Art. 72. Only in the execution of its activity may the provider make use of information related to individual uses of the service by the user.*
> *§ 1. The disclosure of individual information will depend on the express and specific consent of the user.*
> *§ 2. The provider may disclose to third parties aggregate information about the use of their services provided that they do not permit the identification, direct or indirect, of the user, or the violation of their privacy.*

- **ANATEL's Resolutions**

Within its jurisdiction to pass regulatory provisions (article 19 of Law no. 9,472/97), and in discharging its duties as a telecommunications regulatory agency, the National Agency of Telecommunications (*Agência Nacional de Telecomunicações* - ANATEL) regulates and monitors the provision of services and enforces users' rights.

ANATEL's administrative resolutions repeat the protections pertaining to the secrecy of communications as contained in the General Telecommunications Law: the provider is responsible for guaranteeing secrecy of data and other personal information and must implement technical measures to that end. See article 23, *caput* and sole paragraph, of the *Resolução* no. 426/05 – Fixed Switched Telephone Service Regulation (*Regulamento do Serviço Telefônico Fixo Comutado*); article 89 of the Resolução no. 477/07 – Personal Mobile Service Regulation (*Regulamento sobre Serviço Móvel Pessoal*); and article 52 of the Resolução no. 614/13 – Multimedia Communication Service Regulation (*Regulamento do Serviço de Comunicação Multimídia*).

Additionally, ANATEL's resolutions also create data retention mandates: telephone records and personal data must be retained for 5 years, as prescribed by the *Resolução* no. 426/05, art. 22, and *Resolução* no. 477/07, article 10, XXII; and Internet connection logs must be retained for 1 year, as prescribed by *Resolução* no. 614/13 in article 53.

- **Marco Civil da Internet (Law no. 12,965 of 2014)**

Marco Civil is not a data protection law, but a substantial portion of it deals with privacy and data protection. The privacy provisions can be widely classified in three main groups: **(i)** principles and users' rights; **(ii)** specifications on log's retention; **(iii)** access to personal data.

(i) Privacy and data protection are – separately – mentioned as principles for the use of internet in the very beginning of the Bill.[4]

> *Art. 3. The discipline of the use of Internet use shall be grounded on the following principles:*
> *…*
> *II – privacy protection;*
> *III – protection of personal data, in the terms of the law*

Article 3, subsection III adds to the mentioning of the principle of protection of personal data the expression "in the terms of the law". This means that a general data protection regulation and its principles shall be found in another statute, which will regulate data protection in general terms, while the provisions in Marco Civil related to data protection consist of particular specifications that take into account the characteristics of internet. The related Data Protection Law Bills, especially Bill no. 5,276 of 2016, will be analysed in section B.

The Chapter II of the Law mentions the rights of internet users, several of which are related to privacy and data protection.

Art 7, I to III stresses that the general guarantees regarding privacy found in Brazilian Constitution, and partly replicated in the Brazilian Civil Code, are applicable to the internet.[5]

> *Art. 7. Access to the Internet is essential for the exercise of citizenship, and the following rights are secured to its users:*
> *I – the inviolability of intimacy and private life, assuring their protection and compensation for material or moral damages derived from their violation.*
> *II – the inviolability and secrecy of communications on the Internet, except under judicial order, in the hypotheses and form established by law;*

[4] The fact that privacy and data protection are mentioned separately evokes the concept of data protection as diverse from privacy and with a different scope – despite its similarities. This approach can be traced to the Charter of Fundamental Rights of the European Union, in which they are both mentioned but in different articles (7º and 8º).

[5] These provisions could be read as rather redundant, except for one very important point made clear by art 7, III. This particular provision concerns the interpretation Brazilian courts make of Brazilian Constitution, according to which the constitution only protects data when it is being communicated (i.e., in a telephone call) and not the data which is stored (i.e. in the memory of a computer or in a datacenter). The Law recognised this paradox and endowed stored data with the same level of protection as communications have, filling an old gap that wasn't reasonable anymore given today's feasibility of storing most of communications data.

III – the inviolability and secrecy of stored private communication, except under judicial order;

Art 7, VI, together with VIII, can be read as a mandate to make privacy policies or any terms of use applicable to personal data clear and understandable. This relates to the possible application of consumer law to personal data used on internet.

VI – the information provided in Internet service provider agreements must be clear and comprehensive, including detailed information on the protection of connection logs and access to Internet applications records, as well as network management practices that may affect quality;
VII – guarantee that personal data, including connection logs and access to Internet applications records will not be shared with third parties, except upon the user's express free and informed consent or as provided by law;

Regarding the disclosure of connection and application logs to third parties, free and informed consent is presented as the instrument of the individual to make this decision. This will not be required when there is specific law allowing the treatment of personal data even without consent.

In subsection VIII the Marco Civil states two main principles: transparency and purpose of the treatment.

VIII – there must be clear and comprehensive information on personal data collection, use, storage, care and protection, which can only be used for the purposes that
a) justify the collection;
b) are not prohibited by law; and
c) are specified in the Terms of Service or Use of Internet applications.

The consent requisite is mentioned again in subsection IX, but this time in general terms; the consent shall be obtained to any form of treatment of personal data, which is mentioned in its fundamental forms of 'collection, use, storage, processing'. A fundamental specification here is that consent cannot be obtained by a clause inserted in a contract with other provisions – it must be obtained separately

IX – clear consent of the collection, use, storage, processing of personal data, which shall occur separately from the other contractual terms;

Marco Civil included in subsection X a provision regarding data erasure:

X – upon a user's request, at the end of the term of the agreement between parties, personal data stored in connection with access to an application must be completely removed, except in case of mandatory record keeping established in this Law; and

Finally, for several data treatments conducted in internet are also subjected to consumer law endows, even when their use is free of charge, subsection XIII ensures that the internet can make use of consumer rules to assure that his personal data will be fairly used.

XIII – incidence of consumer protection and defence rules in all consumer relations conducted on Internet.

ii) Articles 13 and 15 impose a data retention obligation; connection providers that can be considered "autonomous system administrators[6]" must retain Internet connection logs for 1 year and application providers operated for for-profit purposes are to retain logs of access to applications for 6 months.

iii) Access to account information of subscribers of connection providers and users of Internet applications may take place whenever subpoenaed by authorities of appropriate jurisdiction (article 10, § 3). In the case of Internet connection and access to application logs, access requires a court order whenever there are grounded indicia of wrongdoing and logs may be useful to investigations or discovery; a specific time frame must be established (article 22). Access to content of communications can only occur pursuant a court order (article 7, II and III).

- **Marco Civil's Regulatory Decree (Decree no. 8,771 of 2016)**

The recently signed Decree clarified pending questions about the extension of law enforcement access to account information. First, it clearly states that "*the provider that does not collect registration data shall so inform the requesting authority, being under no obligation to provide such data.*" In this sense, there is no further data retention requirement for account information. Second, the decree established as a requirement to the delivery of the data the specification in the request of: i) the individuals whose information was required; ii) the legal basis and iii) the motivation (article 11[7]). That is, the authority

[6] See RFC 1930 of the Internet Engineering Task Force: https://tools.ietf.org/html/rfc1930

[7] *Art. 11. The administrative authorities referred to in art. 10, § 3, of Law 12,965 of 2014 shall indicate the legal basis of the explicit competence to access and the motivation for the request for accessing to registration data.*
§ 1 The provider that does not collect registration data shall so inform the requesting authority, being under no obligation to provide such data.
§ 2 are considered cadastral data:
I - membership;
II - address; and
III - the personal qualifications, understood as name, first name, civil status and user profession.
§ 3 Requests in terms of the first sentence of the article must specify the individuals whose data are required and the desired information, being forbidden collective applications that are generic or nonspecific.

must indicate explicitly which or what people are being investigated and why - another demand of civil society participants - being thus prohibited, collective generic requests of data.

One new feature regarding privacy and protection of personal data was the prescription of a collection limitation principle. According to article 13, providers must maintain "the smallest possible amount of personal data, private communications and records." With this, companies are now required to delete information from databases when achieved the purpose that justified their collection or when the custody term determined by the law is expired.

> *Art. 13. The connection and application providers should, in the custody, storage and processing of personal data and private communications, observe the following guidelines on safety standards:*
> *(...)*
> *§ 2. Considering the provisions of subsections VII to X of the caput of art. 7 of Law no. 12,965 of 2014, applications and connection providers should retain the smallest possible amount of personal data, private communications and connection records and access to applications, which shall be deleted:*
> *I - as soon reached the end of its use; or*
> *II - the deadline referred by a legal obligation expires.*

Additionally, the Decree also clarified the division of competence as to the enforcement of Marco Civil's provisions. ANATEL, Senacon (*Secretaria Nacional do Consumidor* - National Office of the Consumer), and SBDC (*Sistema Brasileiro de Defesa da Concorrência* - Brazilian Antitrust Service) share enforcement authority, according to their respective expertise areas. The Brazilian Internet Steering Committee (*Comitê Gestor da Internet no Brasil* - CGI.br) acts as a consulting agency.

- **Interception Law [Wiretap Act] (Law no. 9,296 of 1996)**

As foreseen in the Constitution, the secrecy of telecommunications data can be exceptioned by law. The Interception Law plays a key role in the regulation the wiretaps, which implicate the breach of the secrecy of *live* communications (telephone calls, telephone VOIP, emails, internet communications).

Interception can occur, pursuant to the provisions of the main clause of article 1 of Law no. 9,296 of 1996, for purposes of criminal investigation or discovery in a criminal proceeding, by court order, sua sponte ("ex officio") or upon request from a law enforcement officer or the Public Attorney's Office (article 3).

Article 2 limits even further the circumstance under which interceptions may occur: it shall not be allowed in case there is no reasonable evidence of criminal responsibility or conspiracy to commit a crime; in case evidence can be obtained by other means; or when the act under investigation is subject to no more than an imprisonment sentence of the type "detenção" (common for misdemeanors). The sole paragraph of article 2 and articles 4 and 5, in turn, ensure that interception shall only occur if duly justified: an interception request shall be supported by a clear description of what is being investigated,

including naming and identification of the subjects, unless this is clearly shown to be infeasible; the request shall specify the grounds for the investigation and the means to be employed; the ruling shall establish how it is to be carried out.

Article 5 provides that the period of interception shall not exceed 15 days, subject to renewal by court order: it shall be "renewed for an equal period of time when its necessity is required for evidentiary purposes." Although article 5 could admit the interpretation that the maximum period of time for interception is 30 days, prevailing court precedents are of the opinion that an interception order may be renewed for as long as it is required.

Article 7 grants police authorities powers to request "services and specialized personnel from public utilities" to perform interception procedures. Article 8 requires confidential treatment of records of interceptions, and article 9 requires their destruction if they are not useful, or cease to be useful, for evidentiary purposes.

Article 10 criminalizes illegal interception and breach of judicial secrecy and prescribes a penalty of incarceration from 2 to 4 years and fine.

- **Criminal Organizations Law (Law no. 12,850 of 2013)**

The Criminal Organizations Law (Law no. 12,850 of 2013) was created to regulate investigatory powers in the context of crimes authored by criminal organizations. Rather expansively, the law contains broad **(i)** data retention mandates and **(ii)** access to data powers.

Article 17 provides that "fixed or mobile telephone concessionaires shall keep, for five years, at the disposal of the authorities referred to in article 15 [chief of civil police and Public Attorney's Office], records for identification of incoming and outbound terminal numbers of international, long distance domestic and local calls."

Because this provision was not scrutinized for legality, necessity nor proportionality, and did not include detailed specifications of the data to be logged, the entities to which it applied, access limitations and usage conditions, nor data security rules, its constitutionality grounds were challenged under the case ADI 5063/DF, which is awaiting trial.

In its turn, article 15 establishes that "the chief of civil police and the Public Attorney's Office shall have access, irrespective of court order, only to such account information of the accused that indicates personal qualification, parents and address retained by Electoral Courts, telephone companies, financial institutions, Internet providers and credit card administrators (emphasis added)." This provision repeats language existing in article 17-B of the Money Laundering Crimes Law (Law no. 9,613 of 1999), which was recently added by Law no. 12,683 of 2012.

- **Penal Code**

Article 156-A of the Penal Code criminalizes breach of an information technology device with the intent to misappropriate data, with a penalty of imprisonment from 3 months to 1 year and fine. If the action results in access to content of private communication, the penalty is increased to incarceration, from 6 months to 2 years, and fine.

II.2.2. Consumer Data

- **Consumer Protection Code (Law 8,078 of 1990)**

The Consumer Protection code regulates the consumer privacy in the article 43[8]. It aims to give the user/consumer a better control over his or her information, specially concerning information stored in databases. It states that one will have access to existing information on any consumer database and will have the right of correcting it and canceling it at any given time. Also, all this information must be available in accessible formats, including for the disabled. The databases administrators are susceptible to liability claims in cases of misuse of personal information.

No one can open a registration on one's name if it was not requested by the user or if the user was not previously warned about it. The Superior Court of Justice (Superior Tribunal de Justiça) has ruled through its *Súmula* 359/STJ that if the customer is not previously notified before being registered in some Credit Protection System (it can occur when the customer fails to pay for some debt), the customer has the right to ask for moral damages (*danos morais*) in court.

Also, after the prescription period related to possibility of collection the consumer' debt, any information that could prevent or hinder access to new credit will not be provided by the Credit Protection Systems.

- **E-Commerce Decree (Decree Law 7962 of 2013)**

[8] *Art. 43. The consumer, without prejudice to art. 86, will have access to existing information on entries, registry, records and personal data and consumers' data about him/her, as well as their sources.*
§ 1. The registries and consumer data should be objective, clear, truthful and easy to understand and can not contain negative information for a period exceeding five years.
§ 2. The act of registering, opening a record or filing records with personal data should be communicated in writing to the consumer, if such act was not previously requested by him.
§ 3. The consumer, wherever you find inaccuracies in your data and entries, may require immediate correction, and the person responsible for the archive must report the change to the ones who received/had the wrong information within five working days.
§ 4 The databases and registries relating to consumers, credit protection services and similar entities are considered public character entities.
§ 5. After the prescription period related to possibility of collection the consumer' debt, any information that could prevent or hinder access to new credit will not be provided by the Credit Protection Systems.
§ 6. All the information referred in the heading of this article shall be made available in accessible formats, including for the disabled by request.

Decree 7962 of 2013 regulates some aspects of the e-commerce. However, it does not go into detail about the protection of consumers' data, it only states (article 4, subsection IV) that the websites must use "efficient security resources to process the payment and the data treatment of the consumer".

II.2.3. Financial Data

- **Constitution**

There is no express provision about financial data privacy protection. However, during the trial of the *Recurso Extraordinário* 219.780, of September 1999, the Federal Supreme Court has stated that "the privacy protection is granted by the incise X, article 5, according to the vote of the Justice Carlos Velloso, in the RR 219.780, in which he stated that 'by subsection X, article 5 of the Constitution, we can understand that the bank secrecy is also protected, since it is a kind of privacy right.'"

- **Complementary Law no. 105 of 2001**

The Complementary Law no. 105 of 2001 sets some rules about the secrecy of financial institutions' operations. The law states that the financial institutions will preserve the secrecy of its operations and services. It also includes some exceptions to this rule, such as:

> *I - the exchange of information between Financial Institutions for record / inscription purposes ,including the exchange made through risk centers, subject to the rules issued by the National Monetary Council (Conselho Monetário Nacional) and the Central Bank of Brazil (Banco Central do Brasil);*
> *II - the provision of information from the registry of check without sufficient funds issuers and of debtors to credit protection entities, subjected to the rules issued by the National Monetary Council (Conselho Monetário Nacional) and the Central Bank of Brazil (Banco Central do Brazil) ;*
> *III - the provision of the information in the referred § 2 of art. 11 of Law No. 9,311, of October 24, 1996[9];*
> *IV - the communication to the Competent Authorities about the practice of criminal or administrative Offenses, including the supply of information on transactions Involving resources from any criminal activity;*
> *V - the disclosure of confidential information with the express consent of the concerned people;*
> *VI - the provision of information on terms and conditions Sep Oct in Articles 2, 3, 4, 5, 6, 7 and 9 of this Supplementary Law.*
>
> *§ 4. A breach of confidentiality may be ordered if and when necessary to determine the investigation of any offense, in any stage of the investigation or the court proceedings, and especially concerning the following crimes:*
>
> *I - terrorism;*

[9] *§ 2. The Institutions Responsible for the retention and collection of the contribution / taxes will Provide the Federal Revenue the information Necessary for identification of taxpayers and the overall value of Their transactions, in Accordance with the conditions and terms que Shall be established by the Minister of State Treasury.*

II - illicit trafficking of narcotic drugs or similar;

III - smuggling or trafficking of weapons, munitions or materials used for Their production;

IV - extortion through kidnapping;

V - crimes against the national financial system;

VI - crimes against the Public Administration;

VII - crimes against the tax system and social security;

VIII - money laundering or concealment of assets, rights and values;

IX - by criminal organization offenses.

This law was brought to the Supreme Court. Some questioned whether article 6 was constitutional, since it allows banks to give their clients' data to the Federal Revenue Office without a court order in the case the client is involved in administrative investigations. In February 2016[10], the majority of the court declared that the article 6 was indeed constitutional, since, in this specific case, there would not be a violation of bank secrecy - the duty of secrecy would be merely "transferred" to the Federal Revenue Office, which would have to protect this data against third parties. However, one of the Justices alerted that this kind of operation still needs regulation before it is fully allowed and gave some conditions: **(i)** the data requested by the Federal Revenue Office must be pertinent to the investigation in course; **(ii)** the client must be previously notified about this "data transfer".

- **Financial Records Act (*Lei do Cadastro Positivo* - Law no. 12,414 of 2011)**

The Financial Records Act introduces some data protection principles and concepts in Brazilian legislation: it regulates the formation of financial records databases, including Credit Protection Systems (without prejudice of what is stated in the Consumer Protection Code) - those databases may be used to analyze the possibility of making funds available for some entity or person.

In article 3, 3rd paragraph, this Act forbids the collection and the use of excessive data (not linked to the credit analysis) and "sensitive data", which is information connected to the social and ethnical origins of the users, and any other information regarding health; sexual orientation; political, religious and philosophical convictions. It was the first law in Brazil that defined "sensitive" information.

Also, the owner of the data has to explicitly authorize its registry in financial databases (art. 4). The owner of the information has the right to (among others): (i) cancel the registry; (ii) free and unlimited access the information on the database in a safe platform; (iii) request corrections and the database has to either correct or delete the wrong information within 7 days; (iv) be previously informed about the collecting, who is administrating the database, and the way his/her personal data will be used; (v)

[10] *See STF garante ao Fisco acesso a dados bancários dos contribuintes sem necessidade de autorização judicial*, Notícias STF, Feb 24, 2016, available at http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=310670&caixaBusca=N

revision of decisions made by exclusively automated mechanisms; (vi) have the guarantee that the data will only be used for the purpose they were collected for.

Article 7 reinforces the principle of use limitation based on the specified purpose: it states that the information will only be used to the making of credit analysis and other related transactions.

The database and its related entities are responsible for eventual material and moral damages that they may inflict in the user.

- **Credit Score Case**

In 2014, the Superior Court of Justice (*Superior Tribunal de Justiça* - STJ) decided that "credit scores" are legal in Brazil if they observe what is stated in the Consumer Protection Code and in the Financial Records Act.[11]

The score system is used by some companies to decide if they will concede credits to a client or not - it's a way of evaluating risks. A software accesses the available data in public databases and calculates the score. However, a lot of people had sued score companies and asked for moral damages when they had a negative score or if they had a score at all, so the STJ had to settle this matter.

The decision stated that although legal, the consumer has the right to: (i) know where the data came from; (ii) request the removal data and exclude from his/her score data which have surpassed the prescription period, according to the Consumer Protection Code; (iii) request the removal of sensible or excessive data, according to the Financial Records Act.

II.2.4. Health Data

Except for some resolutions issued by Ministries and Regulatory Agencies, there is not much regulation regarding health data in Brazil. The Brazilian Constitution does not say anything about health data explicitly; the administrative regulations merely inform that the privacy will be protected, without offering further detail.

This lack of regulation (not only limited to health, but also the lack of regulation regarding data in general) is a concern[12], and the Ministry of Health has been trying to regulate it more properly since the early 2000s. Currently, there is the Executive Order no. 589 of 2015, which regulates the National Policy for Health Computerized Information (*Política Nacional de Informação e Informática em Saúde* - PNIIS), but it doesn't say much about data protection, only that: (i) all policies should preserve the

[11] REsp nºs 1.457.199 and 1.419.697, Superior Tribunal de Justiça, Notícias. More information available at: http://www.stj.jus.br/sites/STJ/default/pt_BR/Comunica%C3%A7%C3%A3o/Not%C3%ADcias/Not%C3%ADcias/Credit-scoring-%C3%A9-um-dos-novos-temas-do-%C3%ADndice-remissivo-de-recursos

[12] In some states, the public healthcare system is introducing a central database. For instance, since 2013, in the state of São Paulo, a healthcare authorized employee can access the data concerning any patient health record from anywhere in São Paulo. More information available at: http://www.saude.sp.gov.br/ses/noticias/2013/agosto/paciente-ganha-prontuario-unificado-na-rede-do-sus-paulista.

confidentiality and privacy of health information, it is a right of every individual; and (ii) that a policy controlling the authorized access to the information systems should be developed.

The Resolution no. 2073 of 2011 (Ministry of Health) regulates the patterns for dealing with health information within the public healthcare system (Unified Healthcare System - *Sistema Único de Saúde* - SUS), stating only that it will aim to protect the privacy (article 2, II).

The Normative Resolution no. 305 of 2012 of the Supplementary National Health Agency (*Agência Nacional de Saúde Suplementar* - ANS) defines patterns and rules so healthcare plan operators can exchange information, but it only states that it must protect the data privacy in general. It states that the health data protection is related to other data protection laws and professional secrecy rules - the Physicians Ethics Code says that the health professionals shall respect the professional secrecy, unless there is legal reasons that say otherwise or the patient consent to the sharing of information. Also, it states that it is forbidden for the health professionals to give access to the health records of any patient to people who are not bound by professional secrecy.

III. Proposed Law

As mentioned at the outset of this report, despite the aforementioned provisions, Brazil has no specific law on personal data protection. Sent to Congress on May 12, 2016 on an urgent basis, the Bill no. 5,276 of 2016 was an initiative of the Ministry of Justice to change this situation, by introducing standards for all collection and processing of personal data activities, in order to protect the privacy and personality rights of the data holders. In fact, there were already two other projects with proposals for the regulation of the matter under discussion in the Congress: Bill no. 330 of 2013, in the Senate, and Bill no. 4,060 of 2012 in the House. These two less comprehensive Bills are also going to be presented in this report.

- **Law Bill 5,276 of 2016 (version of the 12th May 2016)**

After a long process of discussion and public consultation conducted by the National Consumer Bureau (*Secretaria Nacional do Consumidor* - SENACON) in conjunction with the Office of Legislative Affairs (*Secretaria de Assuntos Jurídicos* - SAL) that took place on a governmental online platform, the Personal Data Protection Act was finally presented to the Congress as a bill on May 12, 2016.

The first public consultation about the subject was in 2010 and collected contributions from not only activists and academics, but also from representatives of the tech sector, acknowledging that they would also benefit from the standardization of rules and the supervision on the topic for investing safer in the data archiving area in Brazil and citizens, worried about the protection of their rights.

A preliminary text was submitted to public consultation in the same platform and after receiving critiques and suggestions, a new one was presented. Further discussion on the 52 articles of the proposed draft text took place. The various contributions from the public and private sectors, academia, citizens

and non-governmental organizations were used by the Ministry of Justice, who had returned to prioritize the issue after the Edward Snowden leak in 2013, for drafting the new version of the Draft, presented on 20 October 2015.

The text is complex and related to various activities that have access to personal data. It is inspired in the European model of an omnibus information privacy law. Next, this report presents the **(i)** definitions and principles applied to data protection, **(ii)** users rights; **(iii)** liabilities; **(iv)** data processing rules; **(v)** enforcement authorities; **(vi)** data transfer and cession rules; **(vii)** and remedies, as foreseen in the current draft.

(i) Definitions and principles applied to data protection law in Brazil

All definitions are made in article 5 of the Bill.

Subsection I defines *personal data* as "data related to identified or identifiable nature person, including identifying numbers, location data or electronic identifiers, when related to a person". Sensible data is defined in subsection III as personal data "about the racial or ethnic origin, religious convictions, political opinions, union membership or membership in religious, philosophical or political associations; data regarding health or sexual life; as well as genetic or biometric data".

Subsection II defines data treatment as "every operation made with personal data, such as operations related to collection, production, reception, classification, utilization, access, reproduction, transmission, distribution, processing, archiving, storing, elimination, evaluation or control of the information, modification, communication, transfer, diffusion or extraction".

Principles are found in several articles 1, 2 and 6.

Article 1 of the Bill sets the protection of liberty, privacy and freedom of personality development of the natural person as goals of the future Law. Article 2 provides the following principles to be applied to data protection: the respect to privacy; informational self-determination; freedom of expression, communication and opinion; inviolability of intimacy, private life, honor and image; economical and technological development; free initiative, free competition and consumer protection.

The Bill also establishes, in article 6, principles regarding data treatment. The treatment must be made in good faith; pursuant a legitimate, specific, explicit and informed aim; in adequacy with such aims and with the legitimate expectation of the holder; and comply with necessity. It should be guaranteed the free access of holders to the integrity of their personal data; and the quality of data, along with the right of holders to maintain the accuracy of data. Finally, data treatment must comply with transparency; security; prevention of damages; and non-discrimination.

> *Art. 6 The personal data processing activities shall observe good faith and the following principles:*
> *I - aim: for which the treatment must be carried out for legitimate, specific, explicit and informed purposes to the holder; and can not be further processed in a way incompatible with those purposes;*

II - adequacy: by which the treatment must be compatible with its goals and with the legitimate expectations of the holder, according to the context of treatment;

III - need: by which the treatment should be limited to the minimum necessary for the fulfillment of its purposes, including relevant , proportionate and not excessive data in relation to data processing purposes;

IV - free access: by which facilitated consultation and free on treatment modalities and the completeness of their personal data must be guaranteed to holders;

V - data quality: by which it must be ensured to holders the accuracy, clarity, relevance and updating of data, according to the frequency necessary for the fulfillment of the purpose of their treatment;

VI - transparency: by which clear adequate and easily accessible information must be guaranteed to holders on the completion of treatment and their treatment agents;

VII - safety: for which technical and administrative measures, which are constantly updated, proportionate to the nature of the information handled and able to protect personal data from unauthorized access and accidental or illegal situations of destruction, loss, alteration, communication or dissemination should be used;

VIII - prevention: for which measures to prevent the occurrence of damage due to the processing of personal data should be adopted; and

IX - non discrimination: whereby the treatment may not be performed for discrimination purposes.

(ii) Users' rights

The Bill mentions the rights of users, as data holders in different articles, including a whole Chapter entitled “Holder’s Rights”.

Article 8 speaks of the rights of holders to easy access to information on the treatment of his data and prescribes the form and depth in which such information should be provided, in clear relation to the principle of free access foreseen in art. 6 subsection IV.

Art. 8. The holder must have easy access to information on the treatment of his data, which shall be made available in a clear, proper and ostensive way on, among others:

I - specific purpose of treatment;

II - form and duration of treatment;

III - identification of the person responsible;

IV - contact information of the person responsible;

V - subjects or categories of subjects to which data can be communicated and diffusion area;

VI - responsibilities of agents who will carry out the treatment; and

VII - the rights of the holder, with explicit mention of:

a) the possibility of accessing the data, rectifying them or revoking consent through a free of charge and easy procedure;

b) the possibility of reporting to the competent body breaches of provisions of this Act; and

c) the possibility of not giving consent, in the event that consent is required, by providing information on the consequences of the negative.

Following, in Chapter III rights such as ownership of personal data and guarantee of freedom, intimacy and privacy are, in line with the principles explained in article 1 of the bill, made clear.

Art. 17. Every natural person is secured of the ownership of his personal data, guaranteed the fundamental rights of freedom, intimacy and privacy, under this Act.

The extent of the principle of transparency, provided in article 6 subsection VI is explained in article 18 as a right to have access to data in terms of art. 8, but also to receive confirmation of the existence of a treatment of his data; being able to maintain the "quality of data", also prescribed as a principle in article 6; having unnecessary, excessive data or not treated in compliance with the law anonymized, blocked or eliminated; revoking consent and being protected from consumer protection rules.

Art. 18. The holder of personal data is entitled to receive, in relation to his data:
I - confirmation of the existence of a treatment;
II - access to data;
III - correction of incomplete, inaccurate or outdated data;
IV - anonymization, blocking or elimination of unnecessary, excessive data or data treated not in accordance with the provisions of this Law;
V - portability, upon request, of his personal data to another service or product provider;
VI - disposal at any time, of personal data for which treatment the holder has consented; and
VII - enforcement of consumer protection rules, where appropriate, in the protection of personal data.

Article 20 considers eventual negative outcomes of the outlining of a profile solely on the basis of automated processing of personal data and guarantees a right to differ from these assumptions.

Art. 20. The holder of data has the right to request a review of decisions taken solely on the basis of automated processing of personal data affecting their interests, including decisions designed to define his profile or evaluate aspects of his personality.

Article 21 establishes a general protection rule of the interests of the holder.

Art. 21. Personal data related to regular exercise of rights by the holder may not be used to his detriment.

Finally, article 22 speaks of the enforcement mechanisms:

Art. 22. The defense of the interests and rights of data subjects may be exercised in Court individually or collectively, according to the provisions of Law no. 9,507 of November 12, 1997; of arts. 81 and 82 of Law no.

8,078 of September 11, 1990; Law no. 7,347 of July 24, 1985, and other instruments of individual and collective protection.

(iii) Data processors'/operators' legal duties/liabilities

The Act also establishes the duties of data processors and operators in the treatment of data.

Data Operators are obliged to a) keeping treatment records and b) adopting security measures to protect personal data; c) indicating a person in charge of the data treatment and, in case the competent authority orders, d) drawing up a Report on the Impact on Privacy of the user.

Art. 37. The person responsible and the operator shall keep records of the personal data processing operations they conduct.

Art. 45. The operator must adopt technical and administrative security measures, which are be able to protect personal data from unauthorized access and accidental or illegal situations of destruction, loss, alteration, communication or any form of inappropriate unlawful processing.

§ 1 The competent authority may provide for technical and organizational standards to make the provisions of first sentence of this article, taking into account the nature of the information handled, specific treatment characteristics and current state of technology, particularly in the case of sensitive data.

§ 2 safety measures should be observed from the product design stage service to its implementation.

Art. 41. The responsible person shall indicate a person in charge for processing personal data.

§ 1. The identity and contact information of the person in charge shall be disclosed in a clear and objective manner, preferably on the website of the responsible person on the Internet.

§ 2. The activities of the person in charge consist of:

I - receiving complaints and communications of the holders, providing information and adopting measures;

II - receiving communications from the competent body and adopting measures;

III - guiding employees and contractors of the entity regarding the practices to be taken for the protection of personal data;

IV - other duties determined by the responsible or established in supplementary rules.

Art. 39. The competent authority may determine the responsible to draw up impact report on privacy relating to their data processing operations under the Regulation.

Data processors are referred as treating agents in the Act and are obliged to a) secrecy and b) to communicating security incidents.

Art. 46. The treating agents or any other person involved in one of the stages of the treatment is obliged to secrecy with regard to personal data even after its termination.

Art. 47. The supervisor must notify the competent body the occurrence of any incident security that may cause risk or significant damage to the holders.

Single paragraph. The communication shall be made within a reasonable time, as defined by the competent body, and shall state at least:

I - description of the nature of the affected personal data;

II - information on holders concerned;

III - indication of the security measures used for data protection, including encryption procedures;

IV - risks related to the incident;

V - in case the communication had not been immediate, the reasons for the delay; and

VI - measures that have been or will be adopted to reverse or mitigate the effects of injury.

(iv) Data processing/treatment rules

The Bill establishes in article 7 the cases, in which data treatment is admissible. These hypotheses are: i) when holders provide their free, informed and unequivocal consent; ii) in order to comply with a legal obligation of the holder; iii) when processing and sharing data are made by the public administration, out of necessity in the implementation of public policies prescribed by the law; iv) for historical, scientific or statistical research; v) when necessary to a contract enforcement or preliminary proceedings related to a contract, of which the holder is party, at his request; vi) for the regular exercise of rights in judicial or administrative proceedings; vii) to protect holder's life or physical safety; viii) to protect the health, through medical procedures; ix) when necessary to meet legitimate aims of the the responsible or of a third party, except when interests or fundamental rights and liberties of the holder that demand data protection prevail, especially if the holder is a minor.

This article also determines an information duty of the responsible in paragraph 1 and his accountability in case of noncompliance.

§ 1. In case of application of the provisions of sections II and III, the responsible shall inform the holder of the cases in which it will be admitted the treatment of his data.

(...)

§ 3. In case of breach of the provisions of § 1, the operator or the responsible for the treatment of data might be held accountable.

The article also makes explicit the incidence of the principles of good faith and adequacy to the aims, already mentioned in article 6, and the necessity of considering the public interest of the treatment.

§ 4. The processing of personal data to which access is public should be carried out in accordance with this law, considering the purpose, good faith and the public interest that justified its availability.

(v) Enforcement authority

The Bill foresees the creation of a body competent for the enforcement of the Law.

Art. 53. The competent body appointed to oversee the implementation and enforcement of this Law shall have the following duties:

I - to care for the protection of personal data, under the law;

II - to drawn up guidelines for a National Policy Data Protection and Personal Privacy;

III - to audit the processing of personal data and processes involved with personal data aiming to ensure its conformity with the principles and rules of this Act;

IV - to promote among the population the knowledge of standards and public policies on protection of personal data and security measures;

V - to promote studies on national and international standards of personal data protection and privacy;

VI - to encourage the adoption of standards for products and services that facilitate the exercise of control by the holders of personal data;

VII - to promote actions of cooperation with personal data protection authorities of other countries, of international or transnational nature;

VIII - to provide for the forms through which to give publicity of processing operations;

IX - to request at any time, to the entities of the public authorities that carry out personal data processing operations, specific report on the scope, nature of the data and other details of the treatment performed, being able to issue additional technical advice to ensure the compliance with this Act;

X - to establish additional rules for the communication activities of personal data;

XI - to prepare annual reports on their activities;

XII - to edit rules on personal data and privacy protection; and

XIII - to perform other actions within its jurisdiction, including those provided for in this Act and in specific legislation.

vi) Data transfer and cession rules

International data transfers

The Bill authorises the international transfer of personal data in restricted cases provided by the Law and shows a concern for the existence of an equivalent level of protection in the country of destination.

Art. 33. The international transfer of personal data is permitted only in the following cases:

I - to countries that provide a personal data protection level, at least comparable to this Act;

II - when the transfer is necessary for international judicial cooperation between public intelligence agencies and research, according to the instruments of international law;

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

IV - when the competent body authorizes the transfer;

V - when the transfer results in commitment assumed in international cooperation agreement;

VI - when the transfer is necessary for public policy implementation or legal authority of public service, being made public pursuant to art. 24.

VII - when the holder has given his consent to the transfer, with prior and specific information about the international character of the operation, warning about the risks involved.

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

Transfer between responsible persons or private law operators

The Bill admits the communication - the transfer - of personal data between responsible persons or operators, when consent from the holder of data is given.

Art. 40. The communication of personal data between responsible persons or private law operators depend on the holder's consent, subject to the cases of exemption of consent under this Act.

Legal and regulatory obligations of the transferee

In case of non compliance, the Bill foresees a joint and objective accountability of both the transferor and the transferee.

Art. 35. The transferor and the transferee are jointly and objectively accountable by the processing of data, regardless of where they are located, in any case.

This can be explained by the provisions of article 44 that state an equal juridical regime for both.

Art. 44. In cases involving the transfer of personal data, the transferee will be subject to the same legal and regulatory obligations of the transferor with whom he will have joint liability for any damage caused.
Single paragraph. Joint and several liability does not apply to cases of treatment performed in the exercise of the duties mentioned in Law 12,527 of 18 November 2011 relating to the guarantee of access to public information.

(vii) Administrative and judicial remedies

Administrative remedies

The Bill grants the competence to the competent body to impose administrative sanctions as a consequence of eventual violations of its provisions.

Art. 52. The violations made by legal entities of private law to the standards laid down in this Law shall be subject to the following administrative penalties by the competent body:

I - simple daily fine;

II - publicity of the offense;

III - anonymisation of personal data;

IV - blocking of personal data;

V - suspension of the operations of processing of personal data;

VI - cancellation of personal data;

VII - database suspension of operations.

§ 1. The penalties shall be imposed on reasonable grounds, individually or cumulatively, according to the peculiarities of the case and the severity and nature of the offenses, the nature of affected personal rights, the existence of recidivism, the economic situation of the offender and the damages causes.

§ 2. The provisions of this article do not override the application of administrative, civil or criminal defined in specific legislation.

(...)

Judicial remedies

Independently of the said administrative penalties, violations that cause damage are also judiciable in order to obtain a reparation.

Art. 42. Whoever, due to the exercise of personal data processing activity, cause another person property, moral, individual or collective damages, is obliged to repair it.

Single paragraph. The judge in the civil proceedings, can reverse the burden of proof in favor of the data holder when, in his judgment, the allegation is probable or when the presentation of evidence by the holder is unreasonably burdensome.

Other Bills

While the discussion of the aforementioned Bill proceeds in the Ministry of Justice, ongoing initiatives are also being discussed in the the Legislative Branch.

- **Bill no. 4,060 of 2012 (authored by congressman Milton Monti, representative of the PR - SP)**

This Bill is a lot less comprehensive than the former. Besides, it also provides very differently on some matters.

(i) Scope of application of the Law

Different from the Ministry of Justice's bill, Bill no 4,060 defines more strictly the hypothesis of incidence of the law:

Art. 4. This Act applies to personal data processing carried out in national territory by individuals or legal

entities, public or private, even when the corresponding database, represented by files, records or other processing bases, is, permanently or temporarily stored in foreign territory.

It leaves out the processing activity that has the purpose of offering or supply of goods or services or the treatment of data of individuals situated in the national territory and the treatment that has persona data has been collected in the country as object.

It also establishes an exception of the scope of application of the law to "the data relating to individuals, when it refers exclusively to information relating to their professional and / or business activities" in subsection II of Article 6.

(ii) Data communication in an economical group

This Bill provides the possibility of a sharing of personal data between companies of the same economic group, including for commercial communication purposes. This possibility is not as wide in the other Bill.

Art. 14. Complying with the provisions of the preceding article, the responsible for the data processing can share them, even for commercial communication purposes, with member companies of the same economic group, business partners or third parties that directly or indirectly contribute to the achievement of the treatment of personal data.

(iii) Enforcement mechanisms

This Act provides sanctions provided by the Consumer Protection Code to data treatment:

Art. 21. Those responsible for the processing of personal data who incur in violation of the standards set by this law, shall be liable to the penalties provided for in the Consumer Protection Code, without prejudice to other penalties to civil and criminal penalties applicable.

(iv) Self-Regulating Body

This Bill provides that Self-Regulatory Councils may be created by entities who represent responsible persons to formulate ethical standards for data treatment:

Art. 23. The entities representing those responsible for processing personal data may institute Self-Regulatory Councils, which shall formulate codes that shall define ethical standards for data processing, commercial communications, as well as conditions for its organization, operation, control and sanctions.

- **Bill no. 181 of 2014 (authored by former senator Vital do Rego, representative of the PMSB - PB) and Bill no. 330 of 2013(authored by senator Antonio Carlos Valadares PSB - SE)**

On May 10th 2016, the senate Commission for the Environment, Consumer Protection and Control has issued an opinion on the three Bills that aimed to regulate personal data protection.[13] In this document, the Commission considers that Bill no. 181 of 2014 should not be presented to be voted, since Bill 330 covered the same subject and had been longer on the Senate; instead is of the opinion for the continuation and approbation of the Bill no. 330.

The main differences between Bill no. 330 of 2013 and Bill no. 5,276 of 2016 are:

(i) Specific consent

In contrast with the Bill no. 5,276 of 2016, Bill no. 330 provides that the consent of the holder must not only be unequivocal and informed, but also specific. That means, it has always to be explicit and, for that, it can be said that it has more weight.

> *Art. 12. The processing of personal data can only be done in the following cases:*
> *I - by consent, specific, unequivocal and informed by the data owner;*
> *Art. 13. The consent must be given separately from other statements and relate to legitimate, specific and delimited purpose.*
> *§ 1. The holder shall have access, before giving consent, to all relevant information on the processing of their data, as the for purpose, duration, who is the responsible for the database and their contact information and the information about third parties to whom may have access to the data.*
> *§ 2 The burden of proof on the consent and its adaptation to legal criteria is on the responsible for the data treatment.*
> *§ 3. Consent may, at any time and without charge, be revoked.*

(ii) Need of authorisation of legal guardian

The Bill provides that children younger as 16 years-old and absolutely unable persons (incapacitated/mentally handicapped) need an express authorization by their legal guardians in order to have their data treated.

> *Art. 14. The treatment of children's and absolutely unable personal data can only be done with the consent of their legal guardian and in their best interests.*

(iii) Hypothesis of admissibility of sensitive data treatment

[13] http://legis.senado.leg.br/mateweb/arquivos/mate-pdf/192563.pdf

This Bill foresees the possibility of treatment of personal data considered sensitive by non-profit organizations, which is not mentioned in the Bill 5276 of 2016; the conditions for treatment of sensitive data are much more elaborated in the other bill.

> *Art. 15. The processing of sensitive personal data is forbidden, unless:*
> *(...)*
> *III - when treatment is carried out in a legitimate way, with appropriate guarantees by a foundation, association or any other non-profit of political, philosophical, religious or trade union organization; when treatment is related to their members or people with regular contact or connection to the organization as long as it is related to its purposes, and the access by third parties without the consent of the holder is forbidden.*

IV. Telecommunication companies data protection practices

This part aims to map some of the data protection practices by the Telecommunication companies. In order to do that, ADC sent a questionnaire to InternetLab. Some of the answers were possible to answer based on previous research, as shown in the part 1. In part 2, there are the questions InternetLab sent to two telecom companies, since we did not have the answers or they were incomplete. The companies chosen to be part of this research are Vivo (*Telefonica*) and TIM (*Telecom Italia*).

IV.1. Questions answered

¿La empresa elabora informes de transparencia? En caso afirmativo, ¿qué información incluye en tales informes? ¿Son de acceso público? ¿Cómo se accede a ellos? ¿Con qué frecuencia los elabora? En caso que la respuesta fuera negativa, ¿Por qué no los elabora?

Most companies elaborate transparency reports (usually, they are referred as "Relatório de Sustentabilidade" in portuguese). However, these reports do not disclose any relevant information about data protection.

Those reports are released annually and they are available in their websites, addressing financial and infrastructure investments made during the year, social programs and corporate governance practices. Usually, they briefly mention their concern with their client's data security and state that they take the appropriate measures in order to ensure it. The only exception we could find is Oi's report, in which the company present the numbers of cases dealing with complaints about data leaks. However, they do not disclose any information about enquires from government.

¿El poder judicial o algún tribunal de su país le ha solicitado información de sus usuarios? En caso afirmativo, ¿qué tipo de información se le solicitó? ¿Cómo se formalizó la petición? ¿Tiene su empresa

protocolos de actuación o alguna política establecida para este tipo de solicitudes? En caso afirmativo, ¿puede entregar una copia del protocolo? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo? ¿Es de público acceso?

In Brazil, the judiciary may request the account information and connection logs, according to the Marco Civil da Internet (Brazil's Internet Bill of Rights), art. 10, second paragraph.

Most of the companies in Brazil have departments that deals with requests from the judiciary and the government in general. There is no information about the particularities of each company, but during the Parliamentary Inquiry Committee concerning cyber crimes and internet security, held in November 24th, 2015, in Brasilia, all the representatives of telecom companies (Vivo/Telefonica, Claro/Embratel, Oi and Tim) claimed that they have special teams whose task is to analyze these kinds of demands. In this matter, ANATEL said that they have a work group which aimed to elaborate a form to be used by all competent authorities when requesting this information.

Si no tiene protocolos de actuación o política interna para el caso mencionado en el punto anterior, ¿qué criterios sigue para la entrega de información? ¿Informa a sus usuarios en caso de solicitud de información? ¿Informa a sus usuarios en caso de entrega de información?

The companies follow legal guidelines to give the information. For instance, the request has to be specific: they have to inform the telephone number or IP address (when asking for account information) and also the determined period in which the information will be collected. They do not notify the users about those requests.

¿Cuenta la empresa con protocolos o políticas de procedimiento interno para cancelación y/o suspensión del servicio? En caso afirmativo ¿puede entregar una copia del protocolo o política? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo o política? ¿Es de público acceso?

Usually, the conditions that may lead to the suspension of the service are listed in the contract. The contracts are all available in the companies' websites. There is no information about the frequency of which this content is updated.

Examples of actions that if engaged by the client will end in the termination of the service and blockage of content are: lack of payment for the service, misuse of the service (according to the contract), dissemination of viruses, invasion of privacy, engagement (voluntarily or not) in any harmful activities to the the servers or to third parties. The dissemination of child pornography and racist content (in Vivo/Telefonica's case) may also engage the blockage of content.

En caso de no contar con un protocolo o política de procedimiento para la cancelación y/o suspensión del servicio, ¿cuál es la razón? ¿Qué criterios utiliza para la cancelación y/o suspensión del servicio? ¿Informa al usuario de la potencial cancelación y/o suspensión del servicio en forma previa a efectuarlo? ¿Informa al usuario de la cancelación y/o suspensión del servicio en forma posterior a efectuarlo? ¿Puede el usuario y/o titular del contenido manifestarse en forma previa y/o ejercer algún tipo de defensa en caso de no estar de acuerdo con la cancelación y/o suspensión del servicio? ¿Cuál es el procedimiento previsto? ¿Cómo conoce el usuario y/o titular del servicio acerca de este procedimiento?

The conditions and the proceedings are in service contracts. The user has to be notified and also has the right to defend himself/herself according to the Consumer Protection Code.

¿Existe en su país alguna normativa protectoria de datos personales? ¿Informa a sus clientes de los derechos que gozan de acuerdo a la ley de protección de datos personales? ¿Cómo?

Currently, there is no specific law about personal data - the bills are treated in the part B of this report.

As stated in part A, the Consumer Protection Act (act n.8078/90) regulates some aspects of the treatment personal data related to the manage of databases for credit analysis.

More specifically, this act, in the article 43, dictates that the consumers must be able to access their data and know about the source of each information. Moreover, the consumer must be informed about the creation of this kind of database and can ask for necessary corrections, which must be accomplished in a 5 day period.

Finally, databases may not contain negative information related to a period longer than five years.

IV.2. Pending questions

¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa, ¿está publicada dicha política de protección de datos? ¿Dónde? ¿Cómo se accede a su política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?

Pending

¿Algún organismo o repartición estatal le ha solicitado información de sus usuarios? En caso afirmativo, ¿qué tipo de información se le solicitó? ¿Cómo se formalizó la petición? ¿Tiene su empresa protocolos de actuación o alguna política establecida para este tipo de solicitudes? En caso afirmativo, ¿puede entregar una copia del protocolo? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo? ¿Es de público acceso?

The law no. 12.965/2014, article 10, 3rd paragraph, determines that competent authorities may request personal data without previous judiciary order. The law n. 12.850/2013 states that a chief

police officer (*delegado de polícia*, in Portuguese) and the public attorney's office, during investigations involving criminal organizations, may request personal data without a judicial order.

The personal data those authorities may request are: information regarding personal qualification exclusively, information concerned parentage and addresses kept by the electoral justice, telecom companies, financial institutions, internet providers (*provedores de internet*) and credit card companies.

Also, the regulatory agency of the telecom sector (*Agência Nacional de Telecomunicações* – ANATEL) may request personal data, according to the article 8o. of the law n. 9472/97. The Brazilian intelligence institution (*Sistema Brasileiro de Inteligência* - SISBIN) may have some partial access to these kind of information by forming collaboration with other public institutions, according to the decree n. 4376, article 6, V.

We have no information about specific protocols owned by each company. During the Parliamentary Inquiry Committee concerning cybercrimes and internet security, held in November 24th, 2015, in Brasilia, all the representatives of telecom companies (Vivo/Telefonica, Claro/Embratel, Oi and Tim) claimed that they have special teams whose task is to analyze these kinds of demands. In this matter, ANATEL said that they have a work group which aimed to elaborate a form to be used by all competent authorities when requesting this information. This form is already used by the Federal Public Attorney Office (*Ministério Público Federal*), Public Attorney Office of the states of Rio Grande do Sul and of Distrito Federal and by the Federal Police. We are waiting for the answer of the company to know more about this point.

Si no tiene protocolos de actuación o política interna para el caso mencionado en el punto anterior, ¿qué criterios sigue para la entrega de información? ¿Informa a sus usuarios en caso de solicitud de información? ¿Informa a sus usuarios en caso de entrega de información?

Pending

¿Cuenta la empresa con protocolos o políticas de procedimiento interno para el filtrado, retiro o bloqueo de contenido? En caso afirmativo ¿puede entregar una copia del protocolo o política? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo o política? ¿Es de público acceso?

As stated before, the contracts have some information (e.g child pornography), but we'd like to know more about this point.

En caso de no contar con un protocolo o política de procedimiento para el filtrado, retiro o bloqueo de contenido, ¿cuál es la razón? ¿Qué criterios utiliza para el filtrado, retiro o bloqueo de contenido? ¿Informa al usuario y/o titular del contenido del potencial filtrado, retiro o bloqueo del contenido, en forma previa a

efectuarlo? ¿Informa al usuario y/o titular del contenido del filtrado, retiro o bloqueo del contenido, en forma posterior a efectuarlo? ¿Puede el usuario y/o titular del contenido manifestarse en forma previa y/o ejercer algún tipo de defensa en caso de no estar de acuerdo con el filtrado, retiro o bloqueo del contenido? ¿Cuál es el procedimiento previsto? ¿Cómo conoce el usuario y/o titular del contenido acerca de este procedimiento?

Pending

¿Tiene su empresa bases de datos inscriptas en algún registro nacional o provincial o departamental? ¿Existe algún tipo de regulación normativa o legal?

Pending

¿La empresa comercializa o cede los datos personales de sus clientes a otras empresas? En caso afirmativo, ¿sigue algún procedimiento determinado para la comercialización o cesión? ¿Comunica esta situación a sus clientes en forma previa o posterior?

Pending

¿Cuáles son las medidas de seguridad adoptadas para proteger la seguridad y confidencialidad de los datos personales de sus clientes? ¿Estas medidas son de público conocimiento? ¿Son de conocimiento de sus clientes? ¿Con qué frecuencia son estas medidas revisadas o actualizadas? ¿Se notifica la revisión o actualización de medidas a sus clientes? ¿En forma previa o posterior?

Pending

¿Qué tipo de medidas toma para que el consentimiento necesario para el tratamiento de datos personales sea libre, expreso e informado?

Pending

¿Tienen un procedimiento para que los usuarios puedan ejercer los derechos de acceso, rectificación y supresión de sus datos?

Pending

¿Han habido de casos de usuarios/as que han solicitado sus registros de datos personales? ¿Cuál fue la respuesta de la empresa?

Pending

Teniendo en cuenta el uso de cookies que utilizan muchos sitios webs ¿Qué tipo de direcciones IP les asignan a sus usuarios? (las opciones son dinámicas o fijas)

In their website, the companies usually state that they use cookies and protect the data collected during the navigation. But we don't have further information.

Data Protection in Brazil: Critical Analysis of the Brazilian Legislation

Authors

Beatriz Kira
Clarice Nassar Tambelli

Collaborators

Francisco Carvalho de Brito Cruz

www.internetlab.org.br

DATA PROTECTION IN BRAZIL

CRITICAL ANALYSIS OF THE BRAZILIAN LEGISLATION

***

INSTITUTIONAL TEAM **Executive Director** Dennys Antonialli **Director** Francisco Brito Cruz **Director** Mariana Giorgetti Valente / PROJECT TEAM **Project Leader** Beatriz Kira **Research Intern** Clarice Nassar Tambelli

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA, 2016.

INTERNETLAB / Avenida Ipiranga, 344, Edifício Itália, Conjunto 11 / www.internetlab.org.br

Table of contents

Team Members involved in this project

AUTHORS

BEATRIZ KIRA / Bachelor of Laws from the University of São Paulo (LL.B., 2015). In 2013, Beatriz was an exchange student at the Ludwig-Maximilians-Universität München (LMU), on a scholarship from the German Academic Exchange Service (DAAD). In 2015, she participated in a training course in drawing up legislation and public policy development organized by the Brazilian Ministry of Justice. In 2016 she attended the Annenberg-Oxford Media Policy Summer Institute, held at the University of Oxford. She is a former scholarship holder from Programa de Educação Tutorial (PET), of the Brazilian Ministry of Education, and worked as junior researcher with the Brazilian Network of Empirical Legal Studies. Currently, Beatriz is a researcher fellow with the Law and Public Policy Research Group at the University of São Paulo and coordinator of the Policy Watch area of InternetLab, where she was also part of the project "Sharing economy and its regulatory challenges".

CLARICE NASSAR TAMBELLI / Bachelor student of International Relations at the University of São Paulo (IRI). In 2015-2016, Clarice was an exchange student at Katholieke Universiteit Leuven (KULeuven), in Belgium. In 2013, she received a scholarship from University of São Paulo to conduct a research at the CAENI (Center of International Negotiation) at the Faculty of Philosophy, Languages and Literature, and Human Sciences. Currently, she is a research assistant at the InternetLab.

COLLABORATORS

FRANCISCO CARVALHO DE BRITO CRUZ / Master and PhD candidate in Philosophy and Jurisprudence by the School of Law of *Universidade de São Paulo* (FDUSP). Graduated in Law by School of Law of *Universidade de São Paulo* (FDUSP) and, in the course of that program, received a scholarship from *Programa de Educação Tutorial* (PET) – Sociology of Law. Visiting Researcher (2013) at the Center for Study of Law and Society of the University of California – Berkeley, through Rede de Pesquisa Empírica em Direito (REED) exchange program. Mr. Brito Cruz received the *Marco Civil da Internet e Desenvolvimento* Award of the School of Law of *Fundação Getúlio Vargas* (SP). Attorney-at-law, practices in areas such as CyberLaw, Intellectual Property, Consummer Law and Press. He is founder and coordinator of FDUSP Group of Law, Internet and Society (NDIS) and director of InternetLab.

I. Introduction:

The objective of this analysis is to indicate the strengths and weaknesses of the Brazilian data protection legal framework in relation to international standards as well as to discuss contextual/national disputes regarding existing proposals to alter it. As the previous parts of the report have already mentioned, in the absence of a national legislation laying down specific rules for the protection of privacy in Brazil**,** the legal framework consists of sectoral privacy laws and general principles such as the right to privacy and intimacy, assured by the Federal Constitution.

In contrast, around the world, more than 100 countries already have special legislation in this regard, drawing inspiration from a regulatory model that started in Europe. Brazil's delay, however, does not mean that the agenda has been forgotten. Since 2007, the Brazilian Ministry of Justice is discussing proposals to regulate data protection in the country. These discussions intensified after Edward Snowden' allegations of mass surveillance, that also concerned Brazil, and which led the Federal Administration to boldly engage to approve the "*Marco Civil da Internet*" (Brazilian Internet Civil Rights Framework) and to promote two public consultations on the matter, gaining broad participation of key stakeholders involved.

From 28 January to 05 July 2015, the National Consumer Secretariat (SENACON) together with the Secretariat of Legislative Affairs (SAL) of the Ministry of Justice conducted the most recent round of public consultation process around a Data Protection Draft Bill, in an online platform. The aim was to receive contributions from different stakeholders to develop a general law for data protection in Brazil.

In May 2016, on the eve of President Dilma's removal from office, she decided to submit to Congress with urgency the draft text prepared by the Ministry of Justice, which is now being processed in the House of Representatives ("*Câmara dos Deputados"*) as Bill No. 5276/2016. The details of this project were already discussed in detail item III of the previous section of this report. Here, however, it is important to discuss the political context in which the project was received by the Brazilian Congress.

This bill, however, it is not the only that address data protection issues in Congress. While this data protection draft bill was being discussed within the Ministry of Justice, other proposals arose in the Brazilian Congress and sparked the debate among parliamentarians. Two of them are also worthy further discussion: Bill No. 4060/2012, authored by Representative Milton Monti, and Bill No. 181/2014, authored by Senator Vital do Rego.

In July 2016, due to a proposal of Representative Alexandre Leite, Bill 5276/2016 was attached to Bill 4060/2012, which contributed to restoring the uncertainty regarding the approval of the legislation. In October 26, 2016, a Data Protection Special Commission was established in the House of Representatives to especifically discuss these two projects. The debates of this Commission will be very

relevant, because even though the similarities and differences between the projects may often seem subtle, the interests behind them are quite distinct.

This legislative context is relevant here because Bill 5276/2016 is the closest we have to the EU General Data Protection Regulation and the most comprehensive text regarding the regulation of personal data. In this sense, in many aspects, Bill 5276/2016 is the best reference for benchmarking the Brazilian framework against international standards. Bill 4060/2012, in its turn, is aligned with the interests of big digital marketing companies, aiming at accessing consumers' data to marketing purposes. Finally, Bill 181/2014 meets the other two halfway, as it is neither as comprehensive as Bill 5276/2016 or as restrictive as Bill 4060/2012.

II. Critical analysis on key aspects of the Brazilian data protection framework

Regulating the use of personal data means to equate the interests of those who see unique opportunities to promote innovation and enjoy the benefits of big data in the collection and processing of data with the interests of those who advocate for limits to these capabilities as a condition for the protection of privacy. Different stakeholders competed - and continue competing - around multiple sensitive points in this debate as we will further discuss below.

II.1. Definition of personal data

One crucial discussion around the approval of a data protection law concerns the definition of ***personal data***. When it comes to establishing a law for the protection of such information, it is crucial to find a balanced description and to define exactly what it means. From that it will be possible to determine over which different types of data rules will apply or not.

The present definition of personal data established by the European General Data Protection Regulation (GDPR) is "*information relating to an identified or identifiable natural person", in which "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

In Brazil, however, in the absence of general data protection law, there was also no definition of ***personal data*** established by law, but only pieces of legislations making references to this concept until

very recently. *Marco Civil da Internet* refers to "personal data" and "treatment of data" in its article 7, without however defining those terms. For this reason, one of the issues addressed during the public consultation debate around the regulatory decree of the *Marco Civil* was precisely whether the text should establish definitions for these concepts or not. In this regard, many participants of the public consultation believed that this matter should be addressed by a future personal data protection law, which was also under debate, and not by the decree.

Nonetheless, as pointed out in item II.2.1 of this report, the approved text of *Marco Civil*'s Regulatory Decree (Decree No. 8771 of 2016) defined in its article 14, I, **personal data** as "*data related to an identified or identifiable natural person, including identifying numbers, location data or electronic identifiers, when these are related to a person*" and also **processing of personal data** as "*any operation carried out with personal data, such as: collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, disposal, evaluation or control of information, communication, modification, transfer, dissemination or extraction*". Identical definitions of both personal data and processing of personal data is in Bill 5276/2016, still subject to approval.

This definition of personal data was praised and criticized during the public debate around the data protection draft bill, both in the sense that the definitions were too broad or too narrow. On the one hand, experts interviewed by InternetLab argued that the concept of Bill 5276/201 is in accordance with international legislations, such as the European General Data Protection Regulation.

On the other hand, representatives of companies believe that this broad concept also encompasses data that not necessarily identify a natural person, but are merely "related" to an individual. According to them, the concept should leave out all data that is not effectively capable of reasonably identifying an individual, as well as all the data subjected to anonymization processes.

To some stakeholders, the definition in Bill 4060/2012 would be more adequate, as it defines personal data as "*any information that allows accurate and precise identification of a particular person*" (article 7, I) - which is a far less comprehensive definition. Bill 181/2014, in its turn, defines personal data as "*any information about identifiable or identified natural person*" (article 3, I), which encompasses data subject to anonymization but not does not mention data related to an individual.

II.2. Sensitive data

Another relevant discussion in the Brazilian scenario is about ***sensitive data***, understood as information that can be used in discriminatory ways and, therefore, need special protection. A mentioned in item II.2.3 of the report, the first law in Brazil that introduced the term "sensitive" regarding information was the Financial Records Act (*Lei do Cadastro Positivo* - Law No. 12414/2011),

which defined "sensitive data" as "*information connected to the social and ethnical origins of the users, and any other information regarding health; sexual orientation; political, religious and philosophical convictions*" (article 3, §3º, II).

Apart from that, Bill 5276/2016 also brings a definition of sensitive data in its art. 5º, III, as follows: "*personal data about racial or ethnic origin, political opinions, religious convictions, trade union membership or membership to religious, philosophical or political organizations, data about one's health or sexual life, and genetic or biometric data".* Such establishment of a special regime for sensitive data by the bill is in line with data protection legislation of most european countries and both the European Directive 95/46/CE and the new European General Data Protection Regulation (article 9).

In contrast, in both Bill 4060/2012 and 181/2014 there is no reference to sensitive data.

II.3. Enforcement authority

Internationally, many countries that have enacted general laws for personal data protection have also created a specific, independent and exclusive national entity, usually called "data protection authority" - or DPA. The importance of independent administrative entities to the implementation of data protection legislation is also recognized by the Charter of Fundamental Rights of the European Union, which prescribes the need for a supervisory authority to exercise control of data processing activities (article 8).

One central difference between the bills regarding the protection of personal data in Brazil is related to the enforcement of the future law. In Brazil, the bill submitted by the President is the only one able to create a competent authority to enforce the law, as according to the Brazilian Constitution the head of the Executive Branch has the exclusive initiative to propose laws about the establishment and structuring of government bodies (article 61, § 1, II, CF). Therefore, the creation of an enforcement authority is not foreseen in either Bill 4060/2012 or Bill 181/2014.

During the public consultation around what later became Bill 5276/2016 many different aspects of this competent authority were debated. Participants disagreed about whether it would involve an existing institution or it would be necessary to create a new authority to exclusively care for the implementation of the data protection law - and in that case which would be the characteristics of this body.

The final text of the Bill 5276/2016 established in its article 53 the competences of a body responsible for overseeing the implementation and enforcement of the law. This entity should be responsible for, among other things, developing the guidelines for a National Data and Privacy

Protection Policy and to promote studies on data protection and privacy. However, the bill does not indicate what would this organ be like and how it should work. Thus, even if the bill is approved, the question around which institutional design will be adopted to ensure compliance with the law by is still open. Currently, as the report mentioned, the enforcement is carried out by National Consumer Secretariat (SENACON) of the Ministry of Justice.

II.4. Data retention

As mentioned in item II.2.1 of the report, the MCI establishes mandatory data retention of user data and metadata, for both Internet Service Providers (ISPs) services and Internet Application Providers services, regardless of whether a user is part of an ongoing investigation or not (article 13 and 15). These obligations, however, required further regulation, and were broadly discussed during the public consultation debate around the *Marco Civil's* regulatory decree.

The decision of the Court of Justice of the European Union (CJEU) of April 2014, which invalidated the European Data Retention Directive under the argument that restrictions to basic rights imposed by the Directive were disproportionate, had repercussions also in Brazil and were reflected in the debate over the regulatory decree.

While law enforcement agencies in Brazil argued these predictions are necessary to ensure user's liability for offenses committed using telecommunications means and to assist prevention and punishment of other offenses, many participants raised concerns around the growth of State's surveillance over citizens. Questions were also raised regarding the constitutionality of such measures, as the information retained could offer portraits of user's personality, habits, interests, social contacts and location that are directly related to such user's privacy and affect secrecy of communications.

Regarding data retention, apart from the MCI and its Decree, two others existing laws refer to data retention in Brazil: Anatel's resolutions (426/05; 477/07 and 614/13) and Criminal Organizations Law (both analyzed in the item II.2.1). These laws also give rise to controversies, as they establish that telephone records and personal data must be retained for 5 years and Internet connection logs must be retained for 1 year.

The lack of a valid Data Retention Directive in Europe, however, makes it harder to draw a comparison with the Brazilian framework, as each Member States may provide for its own a data retention regulation. Even though, it's noteworthy that european data retention schemes must comply with the rules regarding the rights to privacy and personal data protection set out in Article 15 of the

ePrivacy Directive, the EU Charter of Fundamental Rights and also the CJEU ruling regarding Data Retention itself.

II.5. Legitimate interest

Another basic rule to be considered in the present analysis concerns what can authorize the processing of personal data. Bill 181/2014 establishes that "c*ollection, storage and processing in a lawful manner, in accordance with principle of good faith and assigned to certain purposes, prohibited the further use incompatible with those purposes*". In contrast, Bill 4060/2012 establishes that "*personal data will be treated fairly and in good faith in order to meet the legitimate interests of the owners*" (article 9). The most detailed definition is in Bill 5276/2016, which establishes that the treatment of personal data may occur *"upon freely given, informed and unequivocal consent of the data subject"* (article 7). This bill proposed by the President also establishes the ***legitimate interest*** of those responsible for processing the data (art. 7, IX) as one hypothesis to authorize the processing of personal data. The addition of this exception occurred in 2015, during the online public consultation.

This concept was included in the text to authorize certain situations in which the explicit consent would not be necessary, and is also present in the European laws for data protection. It is worth mentioning that in both the European Directive 95/46/CE and the new General Data Protection Regulation (GDPR) the unequivocal consent from the owner of the data is just one of the modalities that authorize the processing of personal data.

In Brazil, however, the provision of the legitimate interest was a source of concern from different stakeholders. Experts argue that it is relevant as it recognizes that other parties - apart from the owner themselves - may have legally protected interests in the processing, use or transfer of certain information. It also copes with circumstances in which the exercise of rights or the prevention of damage depend on the processing in situations when it is not possible to obtain the consent from the owner.

Nonetheless, some argue that the legitimate interest might be interpreted as an exception that could imply a general authorization for all types of processing, with many different purposes, without any control or knowledge from the owner of the data. Thus, for the provision to establish the necessary balance between protection of privacy and intimacy and the economic development and innovation, it should be accompanied by fundamental limits to its application, reducing the risks of abuse.

Moreover, as discussed in item II.2.1, apart from Bill 5276/2016, some existing laws in Brazil also bring the notion of *explicit* user consent: The General Telecommunication Law (Law No. 9472/1997), the Consumer Protection Code (Law No. 8078/1990) and the *Marco Civil da Internet* (Law

No. 12.965/2014). Both aim to give the user better control over his or her information, where the disclosure of individual information will depend on the specific consent of the user.

II.6. Big data

Finally, it is noteworthy to discuss the provisions of the Bill 5276/2016 regarding big data. Nowadays, many of features and services are available thanks to the ability to store, process and analyze massive amounts of data in innovative ways. The development of tools to perform these operations appears increasingly essential to much of the information technology sector and the automated processing of data performed by *algorithms* is a key piece in this puzzle. This issue was intensely debated in the public consultation about the approval of a data protection law.

To deal with this matter, Bill 5276/2016 sets forth in its article 20 that the data owners may request a review of automated decisions when these affect their interests. It also establishes an obligation to the controller of such data to provide, if requested, clear and relevant information on the criteria and procedures used for the automated decision. A similar rule can be found on the European Directive 95/46/CE of data protection, in its article 15, which states the "*right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.*".

In the Brazilian legal framework there is already a similar provision in force, in Financial Records Act (Lei do Cadastro Positivo - Law No. 12414/2011), which establishes in its article 5, IV, the right for the owner of the data to request "*the review of the decision made exclusively by automated means*". This norm is of core importance when applied to risk assessment system (credit scoring), as it allows the consumer to the review of an inappropriate "note" or a "value", which was assigned to them based on erroneous and outdated data, or data that could not have been stored.

III. Context-related remarks

It is important to analyze these regulations in light of the delicate political moment Brazil is going through. A new government is in place and president Michel Temer has already made significant changes in the Federal Administration structure, merging offices and appointing new ministers. Moreover, the current composition of the National Congress is the most conservative since Brazil's re-democratization (1988, with the current Federal Constitution), and the federal government has shown signs that it is committed with less progressive agenda.

Regardless of the disputes going on the Legislative and Executive branches the interpretation of the rules in force is also in dispute in the Judiciary. In this scenario, courts, prosecution offices, competition and consumer authorities might have surprising roles. At this point it is noteworthy that in the absence of a specific framework in Brazil to regulate personal data, local courts have few parameters to decide cases related to such issues. In this context, courts have been coming to conflicting decisions, that bring legal uncertainty to the Brazilian landscape.

For instance, in a recent decision regarding the website *Tudo sobre tudos*, that sold personal data online, the judge from the 1st Federal Court of Rio Grande do Norte decided that selling personal data such as social security number, address, date of birth, telephone etc without the *express* consent of the citizen **is unlawful**. In contrast, in a similar case judged by the Rio Grande do Sul Court of Appeals regarding the bureau *Procob*, the decision was in the opposite direction: **it is not against the law to sell such personal data**. Both decisions are an example of how the absence of a comprehensive framework to protect personal data can generate an environment of legal uncertainty.

IV. References

BIONI, B. R. (2016). Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasi. Available in: https://gpopai.usp.br/wordpress/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO2.pdf

INTERNETLAB. (2016). Data protection special. Available in: http://www.internetlab.org.br/en/data-protection-special/

INTERNETLAB. (2015a). *O que está em jogo na regulamentação de Dados Pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais*. Available in: http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf

INTERNETLAB. (2015b). *What is at stake in the regulation of the Marco Civil da Internet? Final report on the public debate sponsored by Ministry of Justice on Regulation of Law 12965/2015*. Available in: http://www.internetlab.org.br/wp-content/uploads/2015/08/Report-MCI-v2-eng.pdf

ROSSINI, C., BRITO CRUZ, F., & DONEDA, D. (2015). *The Strengths and Weaknesses of the Brazilian Internet Bill of Rights: Examining a Human Rights Framework for the Internet*. Available in: https://www.ourinternet.org/sites/default/files/publications/no19.pdf

DATA PROTECTION IN BRAZIL

DRAFT REPORT / UPDATE ON TELECOMMUNCATION COMPANIES' DATA PROTECTION PRACTICES

JUNE 13TH 2016

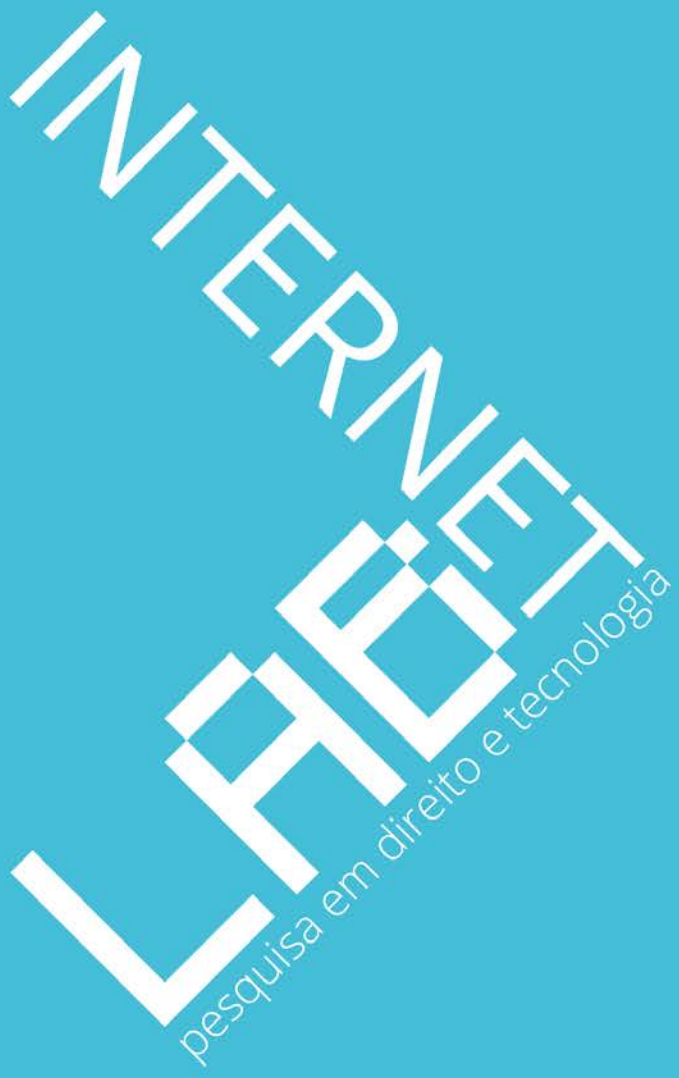
Authors

Fabiane Midori Sousa Nakagawa
Jacqueline de Souza Abreu
Juliana Pacetta Ruiz

Collaborators

Francisco Carvalho de Brito Cruz

www.internetlab.org.br



DATA PROTECTION IN BRAZIL

DRAFT REPORT / UPDATE ON TELECOMMUNCATION COMPANIES' DATA PROTECTION PRACTICES

JUNE 13TH 2016

***

INSTITUTIONAL TEAM **Executive Director** Dennys Antonialli **Director** Francisco Brito Cruz **Director** Mariana Giorgetti Valente / PROJECT TEAM **Project Leader** Jacqueline de Souza Abreu **Research Intern** Juliana Pacetta Ruiz **Research Intern** Fabiane Midori Sousa Nakagawa

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA, 2016.

Table of Contents

TEAM MEMBERS INVOLVED IN THIS PROJECT

AUTHORS

FABIANE MIDORI SOUSA NAKAGAWA / Bachelor student of laws at the University of São Paulo Law School (FDUSP)., where she also attends courses of the double degree program in Law offered by the Jean Moulin University Lyon III. In 2015-2016, she was an exchange student at the Ludwig-Maximilians-Universität München (LMU), where she held a scholarship from the German Academic Exchange Service (DAAD) to attend the preparatory course for the LL.M. in German law. From 2013 to 2014 she was headmistress of the Centre of Studies in International Law of University of São Paulo Law School (NEI-FDUSP). Currently, she is a research intern at the InternetLab.

JACQUELINE DE SOUZA ABREU / Jacqueline holds Master of Laws degrees from the University of California at Berkeley and the Ludwig-Maximilian University of Munich (LMU), and a Bachelor's degree in Law from the University of São Paulo (LL.B., 2014). During her graduate studies, Jacqueline received scholarships from Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) and Programa de Estímulo ao Ensino de Graduação (PEEG) to conduct research in the areas of Philosophy and Jurisprudence, and was a member of the Law, Internet and Society Nucleus of the University of São Paulo (NDIS-USP). Jacqueline participated in an academic exchange with LMU, at which time she received a scholarship from the German Academic Exchange Service (DAAD). She was also a junior researcher with FGV DIREITO SP.

JULIANA PACETTA RUIZ / Bachelor student of laws at the University of São Paulo Law School (FDUSP). She studied at the Brazilian Society of Public Law (SBDP, 2013) and was member of the Human Rights Law Clinic at FDUSP (2012-2013). In 2014-2015, she was an exchange student at Paris School of International Affairs (PSIA) of Sciences Po Paris, focusing on the International Public Management and International Development concentrations. She is currently a member of the Center for Analysis and Research in Legal Education at USP (CAPEJur).

COLLABORATORS

FRANCISCO CARVALHO DE BRITO CRUZ / PhD Candidate and Master in Philosophy and Jurisprudence by the School of Law of *Universidade de São Paulo* (FDUSP). Graduated in Law by School of Law of *Universidade de São Paulo* (FDUSP) and, in the course of that program, received a scholarship from *Programa de Educação Tutorial* (PET) –Sociology of Law. Visiting Researcher (2013) at the Center for Study of Law and Society of the University of California – Berkeley, through Rede de Pesquisa Empírica em Direito (REED) exchange program. Mr. Brito Cruz received the *Marco Civil da Internet e Desenvolvimento* Award of the School of Law of *Fundação Getúlio Vargas* (SP). Attorney-at-law, practices in areas such as CyberLaw, Intellectual Property, Consummer Law and Press. He was founder and coordinator of FDUSP Group of Law, Internet and Society (NDIS) between 2012 and 2014 and is currently a director of InternetLab.

I. INTRODUCTION

The following report addresses Brazilian telecommunications companies' data protection practices. It was prepared by Internetlab in May and June of 2016 for the *Asociación por los Derechos Civiles* (ADC) and and is structured according to the questionnaire provided by ADC. Answers in part II.1. were provided based on previous research conducted by InternetLab. In part II.2. were included answers to questions directed at telecom companies, which InternetLab sent to two telecom companies.

The companies chosen to be part of this research were **Vivo** (*Telefonica*) and **TIM** (*Telecom Italia*), which are two of the biggest telecom companies in Brazil. According to the Brazilian's Regulatory Telecommunication Agency (ANATEL), Vivo has 28,57% and TIM has 25,88% of the mobile broadband market share, for instance[1]. The other two comparable companies are Claro and Oi, with 25,28% and 18,6% of the market share, respectively.

InternetLab reached out to Vivo and Tim and sent the questionnaire on May 4th (Vivo was previously contacted at April 14th, with a noticed that the questionnaire would be sent). The project was briefly explained and the companies were asked about the possibility of engagement by answering the questionnaire. We explicitly informed that the answers did not need to go into detail and that they were free to adopt institutional positions. It is also important to stress that, since InternetLab had launched the project "Who Defends Your Data"[2] (Quem Defende Seus Dados? – QDSD) on the previous week, it was agreed that the questions would not be sent out before that date, so the companies would not think that ADC's project was related to the "Who Defends Your Data" research. When contacted, both companies expressed that they would prefer to answer the questionnaire in a written statement.

TIM was the only company that positively responded to the solicitation and sent the questionnaire on June 6th. InternetLab contacted once more on May 16th, but obtained no response.

The timid engagement and transparency were also hurdles experienced by InternetLab while conducting the "*Who Defends Your Data*" research. This project is the Brazilian version of the Electronic Frontier Foundation's "*Who Has Your Back*", published in the U.S since 2011, which has been expanded to countries in Latin America. It promotes transparency and best practices in the field of privacy and data protection by companies that provide Internet access, making Internet users aware of policies that affect the protection of their privacy and personal data, especially against government requests. TIM and Vivo differentiated themselves from other telecom companies as the only ones willing to engage with the project. Even so, they remained cautious and selective in their participation, what can be interpreted as a concern with taking any step that could potentially impair their reputation with clients and their

[1] Information available in: http://www.anatel.gov.br/dados/

[2] Quem Defende Seus Dados? – Lançamento. Available in: http://www.internetlab.org.br/pt/noticias/quem-defende-seus-dados/ .

relationship with the government and law enforcement agencies. Their engagement with the questionnaire must be considered against this backdrop.

As informed in the earlier version of this report, which described Brazil's legislative framework, there is no data protection law in force in Brazil. As a result, data protection practices remain mostly obscure. The information publicly disclosed concerning how all the four major companies deal with personal data and data requests by the government could be found in contracts[3], in websites, and in public statements delivered in processes of public consultation (such as public consultations for the regulation of the Marco Civil da Internet and a Public Hearing on 24th November 2015 concerning Cybercrimes, chaired by the Brazilian Congress).

No company in the sector publishes transparency reports disclosing relevant information about data protection – which is considered an "innovative" practice in Brazil. After the first edition of the QDSD project was finished, these companies (specially TIM) said that they would try to adopt more transparency practices, but these are still modest and uncommon in the sector.

II. TELECOMMUNICATION COMPANIES' DATA PROTECTION PRACTICES

1. QUESTIONS ANSWERED EXCLUSIVELY BY INTERNETLAB

In this section, InternetLab answers some of the questions in the survey based on previous research.

¿La empresa elabora informes de transparencia? En caso afirmativo, ¿qué información incluye en tales informes? ¿Son de acceso público? ¿Cómo se accede a ellos? ¿Con qué frecuencia los elabora? En caso que la respuesta fuera negativa, ¿Por qué no los elabora?

Most companies elaborate transparency reports (usually, they are referred as "Relatório de Sustentabilidade" in portuguese). However, these reports do not disclose any relevant information about data protection practices and policies.

Those reports are released annually and they are available in their websites, addressing financial and infrastructure investments made during the year, social programs and corporate governance practices. Usually, they briefly mention their concern with their client's data security and state that they take the appropriate measures in order to ensure it. The only exception we could find is Oi's report, in which the company present the numbers of cases dealing with complaints about data leaks. However, they do not disclose any information about demands from the government.

¿El poder judicial o algún tribunal de su país le ha solicitado información de sus usuarios? En caso afirmativo, ¿qué tipo de información se le solicitó? ¿Cómo se formalizó la petición? ¿Tiene su

[3] All the contracts analyzed in "Who Defends You Data" project are available in the webside: http://quemdefendeseusdados.org.br/pt/, under the item "Nossas Fontes".

empresa protocolos de actuación o alguna política establecida para este tipo de solicitudes? En caso afirmativo, ¿puede entregar una copia del protocolo? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo? ¿Es de público acceso?

In Brazil, the judiciary may request account information and connection logs, according to the Marco Civil da Internet (Brazil's Internet Bill of Rights), art. 10, second paragraph.

Most of the companies in Brazil have departments that deal with requests from the judiciary and the government in general. There is no information about the particularities of each company, but during the Parliamentary Inquiry Committee concerning cybercrimes and internet security, held in November 24th, 2015, in Brasilia, all the representatives of telecom companies (Vivo/Telefonica, Claro/Embratel, Oi and Tim) claimed that they have special teams whose task is to analyze this kind of demands. On this matter, ANATEL said that they have a work group which aimed to elaborate a form to be used by all competent authorities when requesting this information.

Si no tiene protocolos de actuación o política interna para el caso mencionado en el punto anterior, ¿qué criterios sigue para la entrega de información? ¿Informa a sus usuarios en caso de solicitud de información? ¿Informa a sus usuarios en caso de entrega de información?

Companies follow legal guidelines to give the information. For instance, the request has to be specific: they have to inform the telephone number or IP address (when asking for account information) and also the determined period in which the information will be collected. They do not notify the users about those requests.

¿Cuenta la empresa con protocolos o políticas de procedimiento interno para cancelación y/o suspensión del servicio? En caso afirmativo ¿puede entregar una copia del protocolo o política? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo o política? ¿Es de público acceso?

Usually, the conditions that may lead to the suspension of the service are listed in the companies' contracts with customers. The contracts are all available in the companies' websites. There is no information about how frequently this content is updated.

Examples of actions that if engaged by the client will end in the termination of the service and blockage of content are: lack of payment for the service, misuse of the service (according to the contract), dissemination of viruses, invasion of privacy, engagement (voluntarily or not) in any harmful activities to the the servers or to third parties. The dissemination of child pornography and racist content (in Vivo/Telefonica's case) may also engage the blockage of content.

En caso de no contar con un protocolo o política de procedimiento para la cancelación y/o suspensión del servicio, ¿cuál es la razón? ¿Qué criterios utiliza para la cancelación y/o suspensión del servicio? ¿Informa al usuario de la potencial cancelación y/o suspensión del

servicio en forma previa a efectuarlo? ¿Informa al usuario de la cancelación y/o suspensión del servicio en forma posterior a efectuarlo? ¿Puede el usuario y/o titular del contenido manifestarse en forma previa y/o ejercer algún tipo de defensa en caso de no estar de acuerdo con la cancelación y/o suspensión del servicio? ¿Cuál es el procedimiento previsto? ¿Cómo conoce el usuario y/o titular del servicio acerca de este procedimiento?

The conditions and the proceedings are in service contracts. The user has to be notified and also has the right to defend himself/herself according to the Consumer Protection Code.

¿Existe en su país alguna normativa protectoria de datos personales? ¿Informa a sus clientes de los derechos que gozan de acuerdo a la ley de protección de datos personales? ¿Cómo?

Currently, there is no specific law about personal data. As stated in the previous version of this report, the Consumer Protection Act (Act n. 078/90) regulates some aspects of the treatment personal data related to the manage of databases for credit analysis.

More specifically, this act, in the article 43, dictates that the consumers must be able to access their data and know about the source of each information. Moreover, the consumer must be informed about the creation of this kind of database and can ask for necessary corrections, which must be accomplished within a 5-day period.

Finally, databases may not contain negative information related to a period longer than five years.

2. PENDING QUESTIONS: COMPANIES' ANSWERS

In this section, we will compile the questions sent to the companies and add our commentary when necessary in order to clarify some answers.

¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa, ¿está publicada dicha política de protección de datos? ¿Dónde? ¿Cómo se accede a su política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?

TIM: We respect customers' personal data and do not authorize undue access and use of it. Our 'Customers' Data Privacy Policy' guarantees that the acquisition of users' records and communication data will be allowed only to the collaborators that need to access this information for professional activities. Besides, we guide our actions based on the best market practices, in compliance with the ISO 27001, international norm for information security.

Quite the contrary, in the absence of a specific discipline on personal data privacy and protection, TIM adopts as beacon the most compliant practices to the body of norms in force, directing its conduct not only by the Constitution and current law of telecommunications services but also in Law no. 12,965 of 2014 ("Marco Civil da Internet"), Law no. 10,406 of 2002 ("Civil Code") 8078/1990 ("Consumer

Protection Code), Law no. 12,850 of 2014 ("Criminal Organizations Act") and Law no. 9,613 of 1998 ("Money Laundering Act").

InternetLab Commentary: *TIM did not say whether they publish their 'customer's data privacy policy' and how can we access it, nor has it provided us with a copy of its terms. The only privacy policy InternetLab has been able to find was that relating to the use of TIM's website, in the following link: http://www.tim.com.br/sp/sobre-a-tim/institucional/seguranca/politica-de-privacidade/coletas-de-dados-do-usuario .*

¿Algún organismo o repartición estatal le ha solicitado información de sus usuarios? En caso afirmativo, ¿qué tipo de información se le solicitó? ¿Cómo se formalizó la petición? ¿Tiene su empresa protocolos de actuación o alguna política establecida para este tipo de solicitudes? En caso afirmativo, ¿puede entregar una copia del protocolo? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo? ¿Es de público acceso?

TIM: All requests for customer information coming from public agencies, are attended only if required under the law or court order. Despite not having a Privacy Chief Officer, any data request made by public agencies to TIM is necessarily subject to the assessment of the internal area responsible for processing such requests, in addition to legal and regulatory sectors of the provider, which act to ensure that the formalities related to such requests are met, including in terms of the legitimacy.

Notwithstanding TIM has chosen transparency as one of the values, including the strengthening of internal and external relations grounded on the principles of loyalty and exchange of information, the provider considers - in the absence of legal protection - the publication of statistics not to be recommended, for security reasons, except in case information sharing with oversight committees of the judiciary or law enforcement, when so specifically requested. In fact, whenever so requested in a motivated form by the competent authorities, TIM provides statistics and depersonalized information. Example of TIM's performance in this regard was the collaboration in the parliamentary committee of inquiry of Illegal Wiretapping, in the House of Representatives.

IntenetLab Commentary: *TIM preffered not to disclose details about user data requests made by government authorities. Although we acknowledge that TIM is not legally obliged to do so, we consider the transparency about data demands is a best practice to be adopted.*

Law no. 12.965/2014, article 10, 3rd paragraph, allows competent authorities to request personal data without previous judicial order. The law n. 12.850/2013 states that a chief police officer (delegado de polícia, in Portuguese) and the public attorney's office, during investigations involving criminal organizations, may request personal data without a judicial order.

The personal data those authorities may request are: information regarding personal qualification exclusively, parental information, and addresses kept by the electoral justice, telecom companies, financial institutions, internet providers and credit card companies.

Also, the regulatory agency of the telecom sector (Agência Nacional de Telecomunicações – ANATEL) may request personal data, according to the article 8o. of the law n. 9472/97. The Brazilian intelligence institution (Sistema Brasileiro de Inteligência - SISBIN) may have some partial access to these kind of information by forming collaboration with other public institutions, according to the decree n. 4376, article 6, V.

*We have no information about specific protocols used by each company and it was not provided by them. During the Parliamentary Inquiry Committee concerning cybercrimes and internet security, held on November 24th, 2015, in Brasilia, representatives of the major telecom companies (Vivo/Telefonica, NET/Claro/Embratel, Oi and Tim) claimed that they have special teams whose task is to analyze these kinds of demands. On this matter, ANATEL said that they have a work group which aimed to elaborate a form to be used by all competent authorities when requesting this information. This form is already used by the Federal Prosecution Office (*Ministério Público Federal*), State Prosecution Offices of the states of Rio Grande do Sul and of Distrito Federal and by the Federal Police.*

One of the companies stated that the members of those teams have their identities protected inside the company – the other departments do not know who the people who evaluate data requests are as a measure of security.

Si no tiene protocolos de actuación o política interna para el caso mencionado en el punto anterior, ¿qué criterios sigue para la entrega de información? ¿Informa a sus usuarios en caso de solicitud de información? ¿Informa a sus usuarios en caso de entrega de información?

InternetLab Commentary: *As mentioned in the previous answer, companies follow legal guidelines to give information. During the "Who Defends Your Data" project, InternetLab found out that companies do not notify their users about data demands. It is not mandatory to the companies to do so, but it was mentioned during the meeting with the companies that there was the possibility that most of the requests might be made with a gag order (even if the subject might not require such confidentiality), making it impossible to inform its users in those cases.*

InternetLab believes that there are plenty of situations in which confidentiality is not a requirement and that user notification is possible. For instance, in cases in which the Federal Reserve (Receita Federal) might request data: the law does not say those requests are confidential.

¿Cuenta la empresa con protocolos o políticas de procedimiento interno para el filtrado, retiro o bloqueo de contenido? En caso afirmativo ¿puede entregar una copia del protocolo o política? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo o política? ¿Es de público acceso?

InternetLab Commentary: *As stated in the first part, the contracts have some information (e.g child pornography) about this point, but companies did not supply additional information.*

En caso de no contar con un protocolo o política de procedimiento para el filtrado, retiro o bloqueo de contenido, ¿cuál es la razón? ¿Qué criterios utiliza para el filtrado, retiro o bloqueo de contenido? ¿Informa al usuario y/o titular del contenido del potencial filtrado, retiro o bloqueo del contenido, en forma previa a efectuarlo? ¿Informa al usuario y/o titular del contenido del filtrado, retiro o bloqueo del contenido, en forma posterior a efectuarlo? ¿Puede el usuario y/o titular del contenido manifestarse en forma previa y/o ejercer algún tipo de defensa en caso de no estar de acuerdo con el filtrado, retiro o bloqueo del contenido? ¿Cuál es el procedimiento *previsto? ¿Cómo conoce el usuario y/o titular del contenido acerca de este procedimiento?*

InternetLab Commentary: *As stated in the first part, the contracts have some information (e.g child pornography) about this point, but companies did not supply additional information.*

¿Tiene su empresa bases de datos inscriptas en algún registro nacional o provincial o departamental? ¿Existe algún tipo de regulación normativa o legal?

InternetLab Commentary: *The companies did not inform about this point.*

¿La empresa comercializa o cede los datos personales de sus clientes a otras empresas? En caso afirmativo, ¿sigue algún procedimiento determinado para la comercialización o cesión? ¿Comunica esta situación a sus clientes en forma previa o posterior?

TIM: We respect customers' personal data and do not authorize undue access and use of it. Our Customers' Dada Privacy Policy guarantees that the acquisition of registrations and communication dada of users will be allowed only to the collaborators that need to access this information for professional activities. Besides, we guide our actions based on the best market practices, in compliance with the ISO 27001, international norm for information security.

¿Cuáles son las medidas de seguridad adoptadas para proteger la seguridad y confidencialidad de los datos personales de sus clientes? ¿Estas medidas son de público conocimiento? ¿Son de

conocimiento de sus clientes? ¿Con qué frecuencia son estas medidas revisadas o actualizadas? ¿Se notifica la revisión o actualización de medidas a sus clientes? ¿En forma previa o posterior?

TIM: Particularly regarding the safety standards adopted in collection routines, use, data processing and storage of its users, TIM follows in its practices rather strict and rigid standards, as can be seen from the provider's internal policy of customer data privacy. Still on security standards regarding operations involving personal data, TIM, committed to the protection of its user information, submitted comments to the Public Consultation on the regulation of the "Marco Civil da Internet" promoted by CGI.br by the National Telecommunications Agency ("ANATEL") and the Ministry of Justice, arguing, among other things, the need for detailing in the regulation of Law - in the name of legal certainty - of the minimum standards of information security to be observed by connecting providers and application providers, as well as the obligations relating to transparency and publicity for such measures. For no other reason, TIM is quite enthusiastic about the current draft of the regulatory decree of the "Marco Civil da Internet".

In the case of an eventual claim by the customer of any situation of violation of privacy, we analyze the situation and provide for the necessary clarifications for the solution of the eventual problem. Data privacy practices are communicated to customers through the terms of use of the service plans at the time of signature of the contract. In 2015, no complaints about loss of privacy were recorded. TIM's contracts and website provide users with a link to the website of ANATEL and the direct contact with the Agency, allowing consumers broad access to the current law to be observed by the provider. In addition to being easily accessible on the TIM website, contracts and service provider plans are available to users in the interaction page. By providing in the service contract that [TIM] "shall respect the inviolability of privacy and secrecy of its users communications," TIM extends the reach of the agreement, enabling the aforementioned clause to be filled out with all the regulations established on the protection of rights of telecommunications users, in the best spirit of an irradiation of fundamental rights on private relations. In fact, either for a historical position of TIM or because of its own regulations, the provider does not restrict the protection of its users' data to provisions in the contract.

InternetLab Commentary: *The company did not inform how often those measures are updated and are unlikely to do so in the future for security reasons.*

¿Qué tipo de medidas toma para que el consentimiento necesario para el tratamiento de datos personales sea libre, expreso e informado?

InternetLab Commentary: *The company did not comment about this point, but all the companies agreed during the public debates regarding the Data Protection Law Bill that it should be considered that the user consented to have his/her data treated in the moment it signed the contract – the consent is implicit, not explicit. InternetLab considers that the consent debate is complex and multilayered. It might be too costly*

for companies to adopt "explicit" consent policies, but if consent could be "implicitly" given, it would be indispensable to provide throughout information about data treatment (which is not a current practice).

¿Tienen un procedimiento para que los usuarios puedan ejercer los derechos de acceso, rectificación y supresión de sus datos?

InternetLab Commentary: *The company did not provide more information on this point. However, as stated in the report regarding the review of the Brazilian law background on data protection, the Consumer's Law, in its article 43, states that one will have access to existing information on any consumer database and will have the right of correcting it and canceling it at any given time – the company did not inform how or if there is a specific protocol in this situation.*

¿Han habido de casos de usuarios/as que han solicitado sus registros de datos personales? ¿Cuál fue la respuesta de la empresa?

InternetLab Commentary: *TIM stated that in case of a breach of confidentiality regarding users' data, the users have ways to contact the company*.

Teniendo en cuenta el uso de cookies que utilizan muchos sitios webs ¿Qué tipo de direcciones IP les asignan a sus usuarios? (las opciones son dinámicas o fijas)

InternetLab Commentary: *TIM did not reply our questions on the implications of the use of cookies in the IP assignment. All it says about cookies in the Terms of Use[4] of its website is what information is collected (number of accesses to the website; technical information about the browser, IP, operating system, and addresses of reference websites; and eventual solicited personal data, such as name, e-mail, telephone number and mobile device type), how it will not share this data with third parties, unless TIM in good faith understands that "disclosing this information is necessary to respond to claims that the content that you submit to this Site infringes the rights of others or is necessary to protect the rights, property and/or safety of TIM, the users of the TIM website and/or the general public" and how it has the right, but not the obligation to keep this data for a period that do not exceed the term provided by the law.*

[4] Available in: *http://www.tim.com.br/sp/sobre-a-tim/institucional/seguranca/politica-de-privacidade/coletas-de-dados-do-usuario* . Last access on June 10th 2016.

Vivo also informs[5] that by accessing its website, some information and data will be obtained by cookies and online research. This data will only be used (with the user consent) to: send information about the company by mail; send email with news; inform about awards and special deals; do e-marketing research and actions.

[5] Available in: http://www.vivo.com.br/portalweb/appmanager/env/web?_nfpb=true&_nfls=false&_pageLabel=vivoVivoInstPrivacidadePage# Last access on June 10th 2016.