CONTRIBUTION FROM

PRIVACYBR COMMITTEE AND PECK LAW

WWW.PRIVACYBR.COM · WWW.PECK.LAW

Authors

Ana Rita Bibá Gomes de Almeida

Anamaria de Almeida Vicente

Carolina Henrique da Costa Braga

Daniela Motta Monte Serrat Cabella

Elizabeth Vian

Gisele Kauer

José Gomes Colhado Neto

Marcelo Crespo

Rafael Siqueira

Simone Henrique

PrivacyBR

PECK LAW

INTRODUCTION

The amount of information that individuals make available in the digital world nowadays reveal their private and intimate life. To prevent violation and exposure of such valuable data there is only one way: to adequate technology, regulation and awareness on human rights.

1. LAWS AND DECREES IN BRAZIL GOVERNING THE PROTECTION OF PRIVACY IN THE DIGITAL AGE

Although Brazil does not have a specific law regulating data protection, there are Laws and Decrees which already establish rights and obligations under the subject matter.[1]

Federal Constitution: States that **private life and intimacy are inviolable**, specially the interception of telephone calls or data communications. It also states that citizens can request the rectification of their own personal data using a legal instrument called *Habeas Data*.

Consumer Defense Code (CDC): Grants consumers **full access to information collected from them**. The CDC states that registrations and consumer data must be objective, clear, true and recorded in plain language. Negative information concerning them can only be stored for up to five years. The inclusion of any record must be communicated in writing to the consumer, who may demand the immediate correction of any inaccuracies.

Executive Decree No. 7,962/2013, which regulates the CDC applied to Electronic Commerce: Determines that every supplier must use safe mechanisms to process consumer data.

Brazilian Civil Rights Framework for the Internet (BCRFI), Law No. 12,965/2014: Establishes: a) the **inviolability** of users' stored private communications' content; b) the organizations' obligation to provide **clear information on the collection, storage, processing and protection of**

[1] PECK, Patrícia. **Direito Digital**. 6th edition. São Paulo: Saraiva. 2016, p. 484.

personal data, which may only be used for the specified purposes; and, c) the definitive exclusion of personal data, with a few exceptions to comply with legislation. It also sets forth that the Brazilian legislation must be applied to all data processes of collection, safekeeping and treatment of records, personal data or communications by connection providers and internet applications when with at least one of these actions take place within the Brazilian territory. Despite the variety of issues dealt within this Law, the BCRFI "is still subject to regulation of some of its points, especially regarding the application of penalties".[4]

Federal Decree No. 8,771/2016: Regulates certain provisions of the BCRFI and is intended to protect records, personal data and private communication. It establishes security standards to be observed by connection providers and applications in the custody, storage and processing of personal data and private communications, such as: authorization of exclusive access for certain users; the provision of authentication mechanisms to access records, using, for example, dual authentication systems, log access to records, and the use of record management solutions through techniques that ensure the inviolability of data, such as encryption or equivalent protection measures.

Brazilian Law No. 12,737/2012: Also known as "Carolina Dieckmann Law" (named after a Brazilian actress who had intimate photos published on the internet), defines the digital crime of "Device Invasion" as the act of hacking someone else's device through a breach of security, intending to obtain, change or destroy data without the owner's permission. Although this crime's legal provision is said to be the solution to some unlawful behaviors and also assumedly something that strengthens privacy and personal data protection, it is not as effective as it seems once it presents very confusing wording, which makes difficult to establish the responsible for this kind of hacking.

1.1. LEGISLATION TO BE ISSUED IN BRAZIL

With the General Data Protection Regulation (GDPR) entry into force on May 25, 2018 in the European Union, the eyes of the world turn to the technologies and processes that collect, treat, store, share and delete information and the new standard they must follow. And Brazil understands that, to recover its economic growth by creating opportunities for foreign businesses, it needs to comply with those standards. There are two main Bills on Data Protection which are being discussed in Brazil.

Bill No. 330/2013

Intended to **regulate natural persons' data processing that occurs totally or partially in Brazil or which can take effect in this country**, it considers "personal data" all the data that precisely identifies or has the potential to identify a single person. It established some categories of sensitive data, e.g. nationality, health and biometric information, defines the anonymization and data deletion processes, and adds the obligation to obtain consent from the data subject before processing any kind of personal data.

Bill No. 5,276/2016

It applies to data processing conducted by any legal or natural person from any country, if (a) the processing occurs in Brazil, (b) the goal is to offer goods or services or process data from persons located in Brazil, or (c) the data is collected in Brazil. It considers identification numbers, location data and all electronic identifiers as personal data, and adds union membership to the sensitive data category. The Bill defined "data deletion" as the final exclusion of data, and adds that the consent to data processing should be informed, unambiguous and freely given. The text addresses the international data sharing and establishes the responsibilities and activities for the person who should oversee the personal data processing. It also defines some good practices on confidentiality and information security, establishes administrative penalties to any breaches and creates a body with power to investigate and execute this regulation, the National Privacy and Personal Data Protection Council.

1.2. REFLECTION OF PRIVACY PROTECTION REGULATIONS IN THE BRAZILIAN COURT DECISIONS

Brazilian judicial decisions reflect the increasing importance of the right to privacy without, however, treating it as absolute. In that sense, it is common to find decisions that make such principle relative. The legislative development and a specific and suitable standardization will certainly mitigate the risk of subjective and conflicting decisions, and possibly keep away the chances of inappropriate relativization.

The Circuit Court, at **Civil Appeal No. 20140111840424 held in December 2015**, established that the breach of secrecy of IP address and personal data is an exceptional measure, suitable only to criminal investigation or procedural statement when there is proof of damage caused by the data subject. The

decision was based on the constitutional right for privacy, intimacy, inviolability, and confidentiality of data, as well as in the BCRFI.

The Rio Grande do Sul State Supreme Court's expressed, on the **Ordinary Appeal on Habeas Corpus No. 132062/RS, ruled in November 2016**, that data protection does not cover the protection of data contained in computers subject to investigation, justifying that "**it is not relevant to invoke the constitutional guarantee of data communication confidentiality when the access does not reach the exchange of data, being restricted only to information stored in electronic devices**. A binding decision from the Supreme Court points out that **'The protection referred to in article 5, XII, of the Constitution is related to 'data communication' and not to 'data itself', even when stored in computers'."**

In **Civil Appeal No. 70068063007, ruled in February 2016** by the Rio Grande do Sul State Supreme Court, the applicant alleged that the defendant disclosed her personal information, such as address and phone number, aiming to have profit. Despite the rapporteur understanding that "the court custody would be justified in the event there is concrete evidence related to the violation of privacy, with precise indication of facts, that may somehow result in harm to the individual in an objective way," the appeal did not succeed, maintaining the original decision of obliging the defendant to refrain from the alleged practice.

Finally, the Sao Paulo State Supreme Court, on a trial for **"Innominate Appeal" No. 1023161-81.2016.8.26.0577 in December 2017**, expressed its understanding that the data subjects' right to have their personal data deleted (provided in the BCRFI) is compulsory. However, it points out that the law requires the connection information (such as IP address), date, and time of access to be kept and not deleted.

2. LATIN AMERICA STATUS

Chile was the first Latin American country to issue a law on data protection, followed by Argentina, which stands out as the only country in the group whose legislation is recognized as adequate by the European Union standards.

Uruguay issued a law in 2004 and then replaced it with another law on data protection issued in 2008. It also issued the Act No. 18.331/18, which establishes data protection using "Habeas Data."

Colombia and Mexico also issued laws on Personal Data Protection to govern the legitimate, controlled, and informed handling of information, and establish a series of principles and rights for which the limits of observance and exercise are: national security protection, order, public security and safety, and the rights of third parties.

3. HOW CAN NEW TECHNOLOGIES HELP TO PROMOTE AND PROTECT THE RIGHT TO PRIVACY?

Although digital technology is constantly seen as the *cause* of privacy issues, it can also help to solve these problems both in the online and offline worlds. Personal information may have better protection with encryption (which has constant improvement), and it is possible to insert human values and principles within digital systems. Technology can be a strong ally after all.

3.1. DESIGN METHODS

Value Sensitive Design provides a set of rules and guidelines for designing a system with certain values in mind. One such value can be 'privacy', and value sensitive design can thus be used as a method to design privacy-friendly IT systems[2].

3.2. PRIVACY ENHANCING TECHNOLOGIES

Communication anonymizing tools like Tor (which allows the user to browse the web anonymously, with the possibility of making the activities untrackable with encrypted messages routed along numerous different computers) or Freenet (that allows the user to share anonymous content by storing it in encrypted form

2 Stanford Encyclopedia of Philosophy. *Privacy and Information Technology*, 2014. <https://plato.stanford.edu/entries/it-privacy/#HowInfTecItsSolPriCon>. Accessed on 23 Mar. 2018.

into different computers) are commonly known as privacy enhancing technologies[3].

3.3. CRYPTOGRAPHY

The wide development of Cryptography techniques and uses was only possible due to digital technology, once it demands advanced mathematic calculation capacity that extend way beyond human brain capacity.

A current example of this technology is *blockchain*, which basically describes a chain of linked blocks that are secured by cryptography. It could be used, for example, to create a decentralized personal data management system that provides data subjects control over their own data[4], avoiding the need to trust personal and sensitive data to third parties.

4. THE RIGHT TO PRIVACY IN THE DIGITAL AGE AND ITS EFFECTS FOR WOMEN, CHILDREN AND PERSONS IN VULNERABLE GROUPS

When we talk about anonymization in the perspective of human rights, it means that some groups like ethnic minorities, people under non-democratic governments, children and even women in some conservative and radical countries may have a voice, a chance of expressing themselves without suffering persecution. Technology becomes thus a very powerful tool to fight for democracy and human rights.

For people in vulnerable situations such as women, digital environments encourage them to share experiences and causes, and to unite around shared interests. Initiatives as the USA National Network to End Domestic Violence use the internet to assist women in situation of violence, protect their privacy and confidentiality, and find a safe place to overcome vulnerability[5]. “The internet is a way for women to raise their voices but also a way to keep their voices from being silenced”[6].

According to the United Nations Children’s Fund, addressing the issue of children’s privacy online is important to help the society and national states in building a more effective way to understand the risks based on age, maturity and

[3] DANEZIS & GÜRSES 2010, Other Internet Resources.

4 NATHAN, Oz; PENTLAND, Alex “Sandy”; ZYSKIND, Guy. *Descentralizing Privacy: Using Blockchain to Protect Personal Data*.

5 E.g. the manual that teaches women to protect their personal data in a digital network, available at <https://nnedv.org/mdocs-posts/being-web-wise/>. Retrieved on March 25th, 2018.

[6] “Mozilla’s contribution to UN High Commissioner report on ways to bridge the gender digital divide from a human rights perspective’”. Available at <http://www.ohchr.org/Documents/Issues/Women/WRGS/GenderDigital/MozillaFoundation.pdf>. Retrieved on March 25th, 2018.

vulnerability. It also helps to protect them from abuse and violence and to deal with the consequences of violations on children's rights to privacy, empowering them as active digital rights-holders[7].

The right to privacy, however, is limited by other human rights, such as freedom of expression, and by national security concerns, which comprises mass surveillance. It is widely reported that national state authorities "record phone calls and retain them for analysis[8]." This is especially sensitive since the digital society allows individuals to easily share information and provide businesses and States with their personal data, interests and profiles. Reports led by private enterprises and human rights entities show that States and businesses have an immeasurable capacity of interfering in individuals' private lives[9].

Mass surveillance shall be conducted strictly in accordance to the principles of lawfulness, necessity and proportionality. The legal framework must be "sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances"[10], or otherwise it will represent undue interference on the right to privacy.

For certain groups of minorities, such interference can be even more harmful: in countries where there is no freedom of expression or of sexual orientation, or even in countries where homosexuality is considered a crime, digital surveillance led by States can affect not only individuals' right to privacy, but also their freedom.

Another source of concern related to vulnerable minorities' right to privacy is the collection of data encouraged by new technologies, machine learning and tools that aggregate information (*metadata*), storing paths, profiles and behaviors, which may affect the individual's right to self-determination. Once the data is collected, it is difficult to keep it anonymous, which reinforces that the principles of lawfulness, necessity and proportionality must be preserved. In such cases, the technological tools for surveillance could pervade global markets and slip from Governments' control[11].

We must encourage and promote dialogue within society, involving associations and organized groups who work with vulnerable populations in the development of privacy policies and best practices manuals while providing education on

7 Privacy, protection of personal information and reputation rights. UNICEF. <https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf>. Retrieved on March 25th, 2018.

8 A/HCR, 27/37.

9 A/HRC/23/40, §33.

10 A/HRC/3/0, § 21.

11 A/HCR/27/37.

privacy rights, tools and knowledge to empower them for dealing with privacy matters in the digital age, creating a “healthy internet with equal opportunities for all online”[12].

5. CONCLUSION

There has been an increasing concern with privacy and data protection globally, and this demands new, safer technologies and regulations combined with education and dialogue with the society to ensure the proper fulfilment of the human right to privacy in the digital age.

[12] “Mozilla’s contribution to UN High Commissioner report on ways to bridge the gender digital divide from a human rights perspective’”. Available at <http://www.ohchr.org/Documents/Issues/Women/WRGS/GenderDigital/MozillaFoundation.pdf. Retrieved on March 25th, 2018.


PrivacyBR
PECK LAW