Quaestio Iuris

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

PERSONAL DATA PROTECTION IN BRAZIL: HOW FAR HAVE WE BEEN AND HOW FAR CAN WE GO?

Ricardo Sichel[1]

José Carlos Vaz e Dias[2]

Abstract

The headlines of the newspapers and attorneys' newsletters focused last August greatly on the enactment of Law nº. 13,709/2018 (the so-called Personal Data Protection Law). The greatest of this law has been the ability to empower the Brazilian citizens during their relationship with others and business transactions when involving the disposal and transfer of personal rights to third parties. This empowerment took place by means of establishing several novelties for a better control of their personal data and the adoption of a "package of rights" against the misappropriation and misuse of personal information. Moreover, enforcement instruments have been adopted to strengthen such rights, including the creation of a public authority that will monitor the system and the heavy fines. Nevertheless, the protection of personal data is not a novelty neither created from the scratch. Instead, it came from the legal development on the protection of human dignity, intimacy and security on personal relationship. This legal system has been under continuous development since the Federal Constitution in 1988. This article focus on the examination of the construction of the personal data protection system and the setting up of the principles that have guided the existing protection under Law nº. 13,709/2018. It addresses as a secondary objective the so-called "package rights" and the main novelties of the system. This article should be understood as a primary piece of academic nature to point out how the past influenced the legal scenario for personal data protection.

Keywords: Data Protection. Personal Data. Intellectual Property Rights. Privacy and Personality Rights.

[1] PhD Dresden – Germany. Professor on Civil Lw of the Federal state University UNIRIO and a Professor of the Academy Studies of the Brazilian Patent and Trademark Office (BPTO). E-mail: ricardo.sichel@unirio.br

[2] Professor adjunto em direito comercial e propriedade intelectual. E-mail: jose.dias@vdav.com.br

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

INTRODUCTION

It has been a unanimous voice in the last five (5) years among the public, legal scholars and businesspersons about the need to adopt a specific legislation to protect personal data in Brazil. The interest in a new law seems to justify from the fact that globalization and communication have influenced an increasing interaction between the persons with access to instant information and images. It further opened up the possibilities for third parties' unpleasant interference on private life thereby leading to misappropriation and information misuse.

Further to that, online sales and electronic and mobile marketing are business methods greatly explored in Brazil, since such businesses are viewed as opportunities to reach out consumers and increase commercial influence and profits. According to a research published in 2017[3], Brazil held nearly 140 million internet users in 2016. Also monthly internet usage in Brazil amounted to 25.7 hours per user in 2017 and 90% of Brazilian internet users accessed the internet every day for personal reasons.

Therefore, the internet worldwide web is a strong tool for producing and transferring personal data, especially in commerce. In a continental territory like Brazil, internet is an efficient way to connect people of different regions and costumes and increase trade penetration. Therefore, this way of doing business and exchanging electronically data must be promoted.

In addition to that, there is increasing information exchanged between existing communication channels that promotes the faster flow of data and image. If one piece of news about an individual is published in a daily newspaper, it is a question of seconds and minutes that the publication is propagated through the headlines of TV News. Even written personal data provided by a person when checking in a specific hotel has become a potential and valuable piece of information that may be used by companies eager for contacts and commercial connections.

Another useful information relates to clinical research or trials in Brazil. Although the Brazilian clinical research in the last eight years has not overcame the rate of 2% of clinical trial undertaken around the world, Brazil holds a reasonable infrastructure for such research with its regulatory authority certified at Level 4 by the World Health Organization (WHO).[4] Therefore, data privacy regulations concerning the limitations on the reveal and processing of the identity and information on patients is of importance.

[3] The statistics in Brazil evidences an increase internet penetration from 2002 to 2016. While 59.68% of the Brazilian population accessed the word web wide (internet), only 9.5% had access to online information back in 2002. Further to that, the expectation in Brazil is to increase the internet use to 135.91 million people to the year 2022. This information gives the conclusion that Brazil is regarded as one of the biggest online markets worldwide. Available at https://www.statista.com/topics/2045/internet-usage-in-brazil/. Viewed on August 3, 2018

[4] MAGALHÃES, Luis and CHIN, Le Vin. "Accelerating Clinical Research in Brazil". Journal for Clinical Studies. Vol.9. Issue 4. Page 14-16.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

If the information availability promotes nowadays culture and access to knowledge, online interaction raises concerns related to offline data collection (through cookies, for example) and to the increasing use of stored information and electronic transmission to third parties for trade purposes without the consent of the individual. It is a reality for internet users and consumers to receive advertisement and sales offers through mobiles from unknown traders and stores. It is further common for a person to be followed by different traders on each click in the mouse when acquiring products, services online or simply searching for them. It is not less relevant the fact that images and other personal data are used by third parties for blemishing, especially when related to famous personalities.

An additional matter has made urgent the adoption of a specific law on personal data protection in Brazil. On May 25, 2018, the General Data Protection Regulation 2016/679 (so-called GDPR)[5] was approved in the European Union. This Regulation repealed Directive 95/46/EC (so-called Data Protection Directive)[6] and increased the harmonization of data protection within the EU member states. To reinforce private data of the European Union citizens, the GDPR extended its enforcement to processing of information activities led by entities that although not domiciled in countries of the EU, such entities collected and held personal data from EU residents and/or offered goods and disposed services to consumers in the Union. The GDPR has brought further the relevance of adequate rules on international transfer of data and imposed requirements based on principles of transparency, prior approval and use for specific purpose for the effectiveness and legality of the international transfer of data. In view of the stringent GDPR's rules, diverse Brazilian attorneys have expressed their views on the applicable stringent GDPR's requirements to Brazil and other countries that do not hold adequate data protection.[7]

This means that the GDPR may influence greater countries that do not present a high level of personal data protection by determining the need of adopting specific compliance rules to match with the GDPR. Therefore, the adoption of high-level laws on personal data would reduce the transaction costs in a medium term as well as the risks for Brazilian companies to trade in EU and other countries, since data protection law in Brazil

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en. Viewed on August 5, 2018.

[6] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046.

[7] Newsletters have been published by law firms on the GDPR's impact on Brazil, such as Tozzini Freire Advogados on May 18, 2018 at http://www.mondaq.com/brazil/x/702702/data+protection/GDPR+overview+and+consequences+in+Brazil. Also, see the publication of Mayer Brown – Tauil Chequer in Lexology at https://www.lexology.com/library/detail.aspx?g=bf457bde-00f8-4bd0-9b4c-afe391d35459 and also at https://www.mayerbrown.com/brazil-the-gdpr-comes-into-force-this-year-now-what-03-08-2018. Those Newsletters address the enforceability of the GDPR and its influence in Brazil and companies that explore the European market.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

would establish high routine standards that would comply with such diverse regulations.

Following up the local needs and the international trend to data protection, the Brazilian President enacted Federal Law nº. 13,709 of August 14, 2018 (the so-called "Personal Data Protection Law).[8]

This law is looked upon as a landmark in the sense that it harmonizes applicable different laws that target the protection of private data, including the regulations of the financial sectors, the Consumer Rights Code and the Internet Law. Further to that, this law has used the GDPR as a source of inspiration. Therefore, it is framed as modern and high-level personal data protection. It further reinforces the principles sacred internationally concerning protection of personal data on the lawful processing and data minimisation.

Nevertheless, the 65 Articles and 10 Chapters that shape up Federal Law 13,709/2018 are far from being entirely new and revolutionary. If one looks closer at the legal framework prior to the law, it is possible to view that this law is a legal development or a step further for the personal data protection already existing in Brazil. The principles and foundations of the Brazilian Personal Data Protection seems to be already in the legal framework derived from the Inviolability of Private Life and the Right of Information promoted by the Brazilian Constitution of 1988. The existing sparse laws valued greatly the Transparency, Data Security and Minimisation.

This article aims therefore to address the concept of personal data and identify the rights that individuals hold in relation to acquiring and processing their personal data. This objective will be reached by exposing the legal foundations of the personal data protection and addressing the prevailing principles under which the new law is set. The basic question should be as follows: Were the foundations for the implementation of the new law on data protection already created, especially by the Federal Constitution?

By dealing with the legal framework before the enactment of Federal Law nº. 13,709/2018, it will be possible to identify how far the Brazilian legislation reached for the protection of private data up to the enactment of Federal Law nº 13,709/2018.

Another task of this article is to depict the main characteristics of Law nº 13,709/2018 that establish the new legal order related to the protection of private data and to point out the novelties and the key rights that apply to processing of personal data.

WHAT DOES PERSONAL DATA REALLY ENCOMPASS UNDER LAWS OF THE LAND?

[8] Available at http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Viewed on August 25, 2018. Notwithstanding such enactment, Law 13,709/2018 holds a *vacation legis* of one hundred and eighty (180) days, which means that this law will be effective as from January 15, 2018.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

Personal data is understood as a compiled information relating to an identified or capable to identify an individual, directly or indirectly, through the use and publication of personal and individual data. Such information may be the tax holder or identity number of a person, the identification of physical characteristics (silhouette), taste, preferences, the peculiarities of the individuals, name, residence address or location and other distinguishable characteristics (genetic information, mental, financial condition, cultural and social background, a specific commonly behavior among others).[9]

The valuable nature of the personal data that requires legal protection comes from the fact it compiles private information of a person that leads to the personality rights and the need to maintain the dignity of the human person. In this sense, it relates to the intimate life of an individual and reputation of the person as well as it evidences the peculiar manner the person relates to friends, family and/or does business in the market. By depicting the personal information, it is possible to determine how a person lives and interacts thereby evidencing its personality and desire.

Knowing the personality of the individual may be further an asset that generates profits to the individual or gives competitive edge to those third parties holding private information. Such private profiles guide decisions, determine commercial strategies and practices of those who control and process the information, including the elimination of a person due to the publication of a photo or a phrase in the internet that suggest an inappropriate behavior of the person.

Personal data encounters primarily protection under the Privacy Rights Principle set out by the Federal Constitution of 1988 in Item X of Article 5, as follows:

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: (...) Item X - *the privacy, private life, honor and image of persons are*

[9] Information relating to entities (companies and public organization) is also regarded as personal data in view of the fact that they comprise the manner the entities trade in a relevant market or organize themselves or whether they are into winding up and bankruptcy proceedings. This kind of information identifies an entity and is of personal nature. Nevertheless, framing entity information as personal data may suffer resistance in view of the existing treatment provided under the unfair competition rules. Accordingly, unfair competition is the prevailing protection to protect business information by preventing free riding misappropriation, opposing tarnishing with unsavory association or the blurring the distinctiveness of a business, product and mark with existing different products. Trade information can be further dealt with by confidentiality obligations a proprietary information. DIAS, José Carlos Vaz e, SANTANA, Leonardo and SANTOS, Bernardo. "The Legal Treatment of Know-How in Brazil: Peculiarities and Controversies of a New Intangible Form". Quaestio Juris. Vol. 09, nº. 04, Rio de Janeiro, 2016. pp. 2315-2318. REICHMAN, J. H. and SAMUELSON, Pamela. "Intellectual Property in Data". 50 Vand. L. Review 51 (1997) Pages. 139-145. See also BONE, Robert g. "Hunting Goodwill: A History of the Concept of Goodwill in Trademark Law." Boston University Law Review. Vol 86:547. Pages. 604-616.

Taking into account that specific information about an entity may serve to identify the entity among a group of individuals thereby imposing limitations by those who process and transfer the entity information, such data is treated in this paper as personal data. The treatment granted to personal data does not interfere with the protection of information under the unfair

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured;

By reading the above, one may clearly view that Privacy Rights have been placed as one of the most important Constitutional Principles and rights of a person, equaled to personal honor and image that are embedded into the very intimate nature of a person.

Nevertheless, the importance of privacy and personal data, as provided by Item X of Article 5 of the Federal Constitution have not been expressed or ruled adequately by the federal laws, at least up to the Personal Data Protection Law. Following up the contents of the Brazilian Civil Code[10], which set for the first time a specific Chapter to deal with Personality Rights (Articles 11 to 21 of Chapter II of Title I), the Privacy Rights and personal data were addressed broadly and in one specific Article, as hereinbelow provided:

"Article 21. The private life of a natural person is inviolable, and the judge, on application by the interested party, shall adopt such measures as may be necessary to prevent or cause to cease any act contrary to this provision."

This broad treatment was criticized in view of the importance of Privacy and due to the limited scope of protection.[11] Firstly, the violation of private life through electronic channels and the intensity of the exchanged personal data through the worldwide web (internet) were already a reality at the time of the Civil Code enactment. Therefore, personal data deserved a better treatment of the Civil Code. Secondly, the granted protection to private data was inadequate, since protecting personal data goes further than preventing third parties from intruding into someone's computer and life.[12]

competition rules, as personal data usually relates to known business trade, not necessarily of proprietary rights.

[10] Federal Law 10,406 of January 10, 2002. Available on http://www.planalto.gov.br/ccivil_03/Leis/2002/l10406.htm. Viewed on August 10, 2018.

[11] The scholar Anderson Schreiber criticizes the treatment given by the Civil Code to Personality Rights based essentially on the fact that it was a structured recognition of such right, but with rigid protection. The protection to the right of personal identity is not adequately protected, since the Civil Code focused essentially on the protection of fiver personality rights, as follows: right to control and use its own bod, right to the name, right to the honour, right to the image and privacy rights. See Schreiber, Anderson. "Direitos da Personalidade". 3rd. edition. Atlas. São Paulo. 2014. Pages 10-18 and 144-146.

[12] This practice derives from third parties accessing and disclosing private information from an individual, which is usually collected through hidden cameras or recording devices. This matter is dealt with by the Criminal Code (Decree-Law 2,848 of December 7, 1940), which provides in its Articles 150–154-B the offences for disclosing information regarding residence, private location, private correspondences and messages and information regarded as of confidential nature. A new offence was added to the Criminal Code in 2012 (by Law 12,737 of November 30, 2012) related to the private life of individuals. Accordingly, it is an offence for a person to invade or hack computers or devices with the purpose to obtain, collect, display or destroy data or information without the authorization of the holder. Available at http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Viewed on August 10, 2018.

"Leave me Alone" practice or the "Right to be Forgotten" is a development from third parties' intruding into someone's life. This is the right secured to individuals to demand the cease of publication about its private life, especially when information concerns their past life or untrue information about a person. This is a recent enforcement trend under examination of the Federal Supreme Court of Brazil (STF) by means of the Extraordinary Appeal RE 1010606 with Reporteur Minister Judge Dias Tofolli. This Extraordinary Appeal addresses the possibility of a crime victim or the member of its family to request the "Right to be Forgotten" taking into account the existing constitutional Principles of Freedom of Expression and the Right of Information on one side and the Intimacy

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

In reality, protecting personal private data needs to be understood as a dynamic mechanism of holding information that encompass diverse stages of protection from gathering, processing to transferring such information to third parties. Nowadays, holding personal data permits anyone to tailor a specific profile about a person or group of persons relating to the identity and the most important events of a private person. It is further valuable for commercial purposes to gather someone else's personal attributes and likeness, since it has become a tool for directing marketing and promotional activities.

The scholar Anderson Schreiber has pointed out clearly the different stages that comprehend the personal data protection, as follows: [13]

"Violates the privacy therefore not only a voyeur that uses a telescope to capture the intimate life of a neighbor, but also the company that holds access to the address and telephone numbers [of a person] supplied by a client who licenses such personal data to other company from a diverse relevant market without any contact or authorization from the individual, who start receiving marketing message. At the same time, suffers violation in its private rights who is included in certain register, without authorization or who has its financing request effused due to specific database that is denied from the individual person enlisted in it." (Free translation)

Therefore, personal data and the envisaged protection encompass the following stages, among others:

Collecting – Operation carried out with personal data that aims to gather and download information of personal nature that identifies directly or indirectly a person.

Processing – Retrieve, upload, store, eliminate and modify the collected personal data for specific purposes.

Classifying – Procedure to separate collected information based on diverse criteria, such as gender, age, height, religion, sexual preferences, beliefs and other systematic criteria of attributes of a person following up the interest of collector and third parties and the manner such information will be exploited.

Exploiting – Direct use of the private information processed by a third party for the specific purpose of use.

Transferring– Make available or license to third parties any information and connection logs and access to internet applications logs as well as the content of private communication, especially for commercial purposes. The access of information to third parties include the transfer grounded on court orders and legal compliances.

International transfer of data – Transfer of private data collected in a specific country and delivered it to

Principles on the other side. Available at http://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786. Viewed on August 10, 2018.

[13] SCHREIBER, op. cit. 11. Page 139.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

another person or international organization located in foreign country.

Each of the mentioned steps involves the adoption of "positive duties" or procedures to be fulfilled by the holder of the personal data, besides the abstention duty, which is the refusal to use the data that violates the intimate rights of persons. For example, the collection and modification of information from an individual requires always the prior and specific authorization from the individual. Likewise, the use of the private data by other purposes not encompassed by the authorization would demand the knowledge to the individual, since the person needs to maintain the control of the information.

For personal data to be of interest to legal protection and to be covered by Law 13,709/2018, the data on the person needs to be collected and exploited by a third party, directly or indirectly. This means that the legal system is interested in the movement of the information from one person to the other. Therefore, the access, compilation, modification and transfer of personal data is crucial to the level of protection.

Taking into account that the processing of personal data by a third party is a requirement for the legal protection, much discussion focuses recently on whether or not personal data would encompass data exclusivity in pharmaceuticals. To ensure safety, quality and efficacy of a developed pharma product, regulatory authorities determine the need to fulfil requirements and comply with clinical tests so that medicines may be released in the market for production, distribution and commercialization.[14] Therefore, clinical tests on humans happen by means of selecting a wider and diverse population duly chosen by specific criteria, such as age, physical structure, geography and peculiar situation (pregnancy or less hair) depending on the target and functions of the medicine.[15]

Data protection in pharmaceuticals is ruled by specific types of arrangements, as set by Article 39.3 of the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS Agreement),[16] as follows:

"3. Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public or

[14] In view of the population diversity, Brazil is recognized as one of the main countries where clinical tests take place to check the efficacy of the developed drug. The regulatory authorities for the approval of medicines in Brazil is the Brazilian Health Regulatory Agency (ANVISA), which is a public autarchy linked to the Ministry of Health and that coordinates the Brazilian Health Regulatory System (SNVS) throughout the Brazilian national territory. Available at http://portal.anvisa.gov.br/english. Viewed on August 14, 2018.

[15] SANTIAGO-RODRIGUEZ, Fernando. "Facing the Trial of Internationalizing Clinical Trials to Developing Countries: With Some Evidence from Mexico." United Nations University (UNU-MEIT). Working paper series #2008-023. Available on https://www.merit.unu.edu/publications/wppdf/2008/wp2008-023.pdf. Many reasons are leading the internationalization of clinical trials. Among them, there is the possibilities of pharma export and decrease of costs in comparison with the developing countries.

[16] Enactment of the TRIPs Agreement by means of Decree 1,355 of December 30, 1994 (Promulgation of the Final Act of the

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

unless steps are taken to ensure that the data are protected against unfair commercial use.

Item XIV of Article 195 of the Industrial Property Law[17] further implements data protection for clinical purposes and stipulates as unfair competition the disclosure and use of tests. However, it lacks further legal developments for keeping restrictive clinical tests for human purposes[18], as follows:

"Art.195. Commits crime of Unfair Competition who: (…)

XIV. divulges, exploits, or utilizes, without authorization, results of tests or other undisclosed data whose preparation involves considerable effort and that were submitted to government agencies as a condition for obtaining approval to commercialize products."

Although discussion on the property of data protection in clinical trials overcomes the proposed objectives of this work, it is worth mentioning that data exclusivity is still a raising issue in developing countries as some countries are flexible in permitting the use of collected data of individuals from a pharma company for the approvals of generic drugs.[19]

The doctrine on data exclusivity sets that legal protection takes place by regulations and legislations specifically related to clinical trials and under the rules of trade secrets. However, when undertaking the clinical tests, pharma companies gather and hold a great deal of private information on the selected person for the clinical trials that can be framed as private information.

As a result, data exclusivity also comprises issues related to the collection of personal data and the requirements for the pharma companies to use them. In fact, such data are framed as personal data and it should be therefore subject to the compliance of Law nº. 13,709/2018. In a very recent publication on the impact of the GDPR to patient's health the non-organization European Patient Forum published guidelines[20] for medical

Uruguay Round). Available at http://www.planalto.gov.br/ccivil_03/decreto/antigos/d1355.htm. Viewed on August 10, 2018.

[17] Federal Law 9,279 of May 14, 1996. Available at http://www.planalto.gov.br/ccivil_03/Leis/L9279.htm. Viewed on August 1, 2018.

[18] Federal Law 10,603 of December 17, 2002 rules the disclosure and use of animal clinical tests for veterinary products (fertilizers and related products). Accordingly, the approval authorities of veterinary products are not allowed to use such clinical tests for the approval of other generic products for a period of up ten (10) years as from the product registration or launching the product into the market. There are other specific ruling on disclosure of such information. The use of clinical tests related to human drugs and the authorities' rights to use such information for approving generic drugs are not specifically ruled by the laws of the land. Further discussion on the authorities' obligations to maintain secret clinical trial information see BARBOSA, Denis. "Exclusividade de dados sigilosos apresentados às agência regulatórias: agroquímicos". Available at http://denisbarbosa.addr.com/arquivos/200/propriedade/exclusividade_dados_sigilosos.pdf, Viewed on August 5, 2018.

[19] See discussion on the industrial property protection for data protection and data exclusivity. CLIFT, Charles. "Data Protection and Data Exclusivity in Pharmaceuticals and Agrochemicals" published in the book Intellectual Property Management in Health and Agricultural Innovation: A Handbook of Best `Practices." MIHR. PIPRA. Oswaldo Cruz Foundation and bio Developments-International Institute. 2nd. Edition. 2009. Pages 431 to 435. See also BARBOSA, Denis. "Do Sigilo dos Testes para Registro Sanitário". Available at www.nbb.com.br/pub/denis/sigilo_registro_sanitario.pdf. Viewed on August 10, 2018.

[20] "The new EU Regulation on the protection of personal data: what does it mean for patients?". European Patient Forum. Available at http://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf. Viewed

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

patients and patient's organizations and addressed interesting issues linked to the special data category so-called "sensitive personal data". Personal data gathered on clinical trials are regarded as "sensitive data". It is posed in the Guidelines several questions related to the extension of use of "sensitive data" and when such information leaves to be framed as "sensitive" and the conditions, under which it may be extensively disclosed, processed and used without the prior consent of the involved individuals.

The Brazilian personal data protection encompasses in this sense the protection of "sensitive data", as it provides in Item II of Article 5 that personal sensitive data encompasses those related to racial or ethnics nature, religious, political opinion and to the health and sexual directions. Paragraph 4 of Article 11 further provides a prohibition to communicate sensitive personal data related to health for commercial advantages unless prior consent by the individual.

An additional important point is to identify whose data will be protected by the personal data protection. According to Article 5 of Law 13,709/2018, personal data comprises those information that can identify or make identifiable a natural person, which means the capability to identify directly or indirectly a natural person, as follows:

Article – For the purposes of this Law, it should be understood:

I – personal data: information related to an identified personal data or identifiable (…)

V – Titleholder: natural person to whom the personal data are subject to treatment"

By defining personal data, Law 13,709/2018 has excluded information relating to identified or identifiable legal entities (i.e. companies, corporations, non-governmental organizations and other kind of legal associations). This is indeed an issue since extensive information on entities are also collected, modified, classified and transferred by third parties, which provide the manner under which such entities trade in a relevant market or organize themselves or identify whether they are under financial difficulties or hold a peculiar list of suppliers.[21] Therefore, such information is of personal nature in the sense that the entity is capable of being identified directly or indirectly.

This exclusion seems to be unreasonable and under a practical viewpoint as an anomaly. Legal entities hold personality under Brazilian law and assume rights and obligations as well as relate to other persons and do

on August 20, 2018.

[21] The inclusion of data about a company or entity as personal data is a recognition that such entities may be subject to inadequately collection, processing of exploitation by third parties that may affect their goodwill and reputation in the market. See BONE, Robert G. "Hunting Goodwill: A History of the Concept of Goodwill in Trademark Law". Boston University Law Review. Vol. 86.2006. Pages 554-572.The Brazilian scholar Sérgio Campinho detains a great part of its book on the definition and characteristics of legal entities (public and private), including business name. See CAMPINHO, Sérgio. "O Direito de Empresa à Luz do Código Civil". 13rd. Edition. Renovar Editor. 2014. Pages 35-70. Further to that, the federal tax holder number and the trademarks are also elements that identify directly a commercial entity. The inadequate use of these elements by unauthorized third parties may

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

business transactions with others. Therefore legal entities are exposed extensively to the misappropriation or unauthorized collection of information provided in business. Formation of a profile that can be commonly known by competitors and largely use in commerce by third parties and/or generate business to the titleholder of the information.

Such anomaly may be further justified by the fact that Article 52 of the Brazilian civil Code extends the personality rights to legal entities, as follows:

"Art. 52 Apply to the legal entities, to the extent applicable, the protection granted to personality rights."

Accordingly, it is guaranteed to legal entities protection related to peculiar identification, such as business name and the right to prevent unauthorized exploitation of their image and goodwill and obtain losses and damages from the violation.[22] In this sense, it is worth mentioning Precedent number 227 issued by the Superior Court of Justice, as follows:[23]

"Precedent 227, Legal entities may suffer moral damages"

In light of the above, it seems legally justified that personal data should further include collected, processed and transferred data of legal entities. However, this was not the legislators' view, as it restricted the concept of personal data to those applicable to physical persons.

The fact that information on legal entities is not expressly framed as personal data and therefore outside the scope of Law 13,709/2018, it does not mean that such information lacks protection under the laws of the land. The Internet Law – Federal Law 12,965 of April 23, 2014[24] - applies to any operation concerned with collecting, storing, treating and transferring personal data by connection providers and internet applications providers when at least one of these take place in Brazil.

Moreover, it should be reminded that the Federal Constitution and the Civil Code cover legal entities and grant them the right to seek the reestablishment of the *status quo* and indemnification in case private information (whether confidential or not) is exposed without consent. Such protection is extended to legal entities if one examines the contents of the Brazilian Consumer Code[25], the Bank Secrecy Act[26] and the access to

damage or interfere with the goodwill.

[22] See PEREIRA, Caio Mário da Silva. "Instituições de Direito Civil". Vol. I. 30ª ed. Ed. Forense. Page 286. SCHREIBER, op. cit. 10 at Pages 21-22.

[23] Available at http://www.stj.jus.br/docs_internet/VerbetesSTJ_asc.txt. Viewed on August 27, 2018.

[24] Available at http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12965.htm. Access on August 20, 2018.

[25] See Article 43 of Federal Law 8,078 of September 11, 1990. Available at http://www.planalto.gov.br/ccivil_03/LEIS/L8078.htm. Viewed on August 20, 2018.

[26] Complementary Law 105 of January 10, 2001 (Financial Transaction Confidentiality). Available at http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp105.htm. Viewed on August 20, 2018.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

Information Act,[27] among others.

Framing entity information as personal data does not interfere at all with the existing treatment and protection provided for confidential trade information under the unfair competition rules, as personal data usually relates to known business trade, not necessarily of proprietary rights or confidential nature. Accordingly, trade secret requires the fulfilment of three essential requirements to deserve legal consideration for protection that it is not necessarily encountered in the personal data or other type of intellectual property protection. Firstly, the information requires secrecy or not known or published to the public. Information in the public domain and that is already incorporated into the state of art cannot be secret. The second relates to the actual steps to maintain the secrecy in force[28].The third requirement is the evidence that the concerned information is of competitive edge or has direct or indirect applicability to trade and the competitiveness of the holder in a relevant market.[29]

As a final point, Law nº. 13,709/2018 enlists information that although regarded as personal data, it is not encompassed by the aforementioned legislation, as follows:

"Art. 3o. This law does not apply to treating the following personal data:

I – undertaken by a natural person strictly for personal purposes and not commercial;

II – undertaken for exclusive purpose of

news reporting purposes and artistic; or

academic, applying to this event arts. 7th and 11th of this law;

III – undertaken for the exclusive purposes of:

public security;

national defense;

security of the state or

investigation activities and repression of criminal penalties or

IV – deriving from outside the Brazilian territory and that are not subject to communication, share use of data with agents with Brazilian treatment or subject to international transfer of data with other country, except that

[27] Federal Law 12, 527 of November 18, 2011. Available at http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Viewed on August 20, 2018.

[28] The secrecy depends substantially on the manner its owner treats it in practical term. A document kept in a simple file and is commonly left unattended on top of an office desk is not eligible for trade secret protection although specific "Confidential" stickers are stuck on the document (TRT, 1a. Região – Ac. 3a. T. 550/70), as pointed out by Georges Charles Fischer. See FISCHER, Georges Charles. "Trade Secrets Protection in Brazil". Les Nouvelles, Washington. Dec. 1987. Page 69.

[29] Trade secret information can be further dealt with by confidentiality obligations a proprietary information. DIAS, José Carlos Vaz e, SANTANA, Leonardo and SANTOS, Bernardo. "The Legal Treatment of Know-How in Brazil: Peculiarities and Controversies of a New Intangible Form". Quaestio Juris. Vol. 09, nº. 04, Rio de Janeiro, 2016. pp. 2315-2318. REICHMAN, J. H. and SAMUELSON, Pamela. "Intellectual Property in Data". 50 Vand. L. Review 51 (1997) Pages. 139-145. See also BONE, Robert g. "Hunting Goodwill: A History of the Concept of Goodwill in Trademark Law." Boston University Law Review. Vol 86:547. Pages.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

of origin insofar as the country of origin grants a degree of adequate protection of personal data, as prescribed by law"

This means that not all personal data are protected by nº. 13,709/2018 although they comply with the basic and essential requirement of identifying a person, directly or indirectly,

THE FORMATION OF THE LEGAL FRAMEWORK TO PROTECT PERSONAL DATA IN BRAZIL

When the main newspapers published the enactment of the recent personal data protection[30], the impression was that Law nº. 13,709/2018 established a new legal order or era based on the prevailing of individual rights on personal relationship and business transactions.

Although Law nº. 13,709/2018 created a specific ruling on personal data protection and strengthened the rights by means of preventive and punitive measures, it is far wrong to say that the principles and elements of such protection came from the scratch and they were created by this law.

One of the important matters of Law nº. 13,709/2018 is consolidating the text in a sole piece of legislation and determining a higher security on storage and transfer of data. Nevertheless, the principles and elements of protection to individuals were set by the prior legislations.[31]

Before the enactment of the new law, the collection, storage, retention, treating and use of personal data were ruled by different laws and regulations scattered in diverse areas and applicable to different and specific group of people and activities. There was not a sole specific piece of legislation dealing with data protection.[32]

Three (3) pieces of prominent legislations set the foundation and the pace for the recognition of personal rights and data protection, which resulted in the creation of Law nº. 13,709/2018. The first one is the Federal Constitution 1988[33] that establishes as a fundamental right the dignity of the human person and

604-616.

[30] "Temer Sanciona Lei de Proteção de Dados" (Mr. Temer Enacts Data Protection Law" in OGLOBO Newspaper of August 15, 2018. Page 23.

[31] This understanding was briefly provided by the attorney Gabriel Rocha Furtado who informed that the Internet Law in 2014 represented an improvement to the legal background for future internet regulations in Brazil. A democratic country has to secure the rights to its citizens, impose the limits and identify the criminal events. FURTADO, Gabriel Rocha. "O Marco Civil da Internet: A Construção da Cidadania Virtual" in the book "Direito e Midia" coordinated by Anderson Schreiber. Ed. Atlas. 2013. Page 253.

[32] Applicable legislations and regulations that helped construct the legal backbone for protection of personal data were the following: Criminal Code (Decree-Law 2,848 of December 7, 1940 (Articles 150-154), Law 12,737 of November 30, 2012, Law 9.279 of May 15, 1996 (Industrial Property Law), Complementary Law 105 of January 10, 2001(Financial Transaction Confidentiality , among other scattered regulations.

[33] Federal Constitution of 1988. Available at http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Viewed on August 20, 2018.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

recognizes privacy, private life, honor and image of a person as essential to human existence and nature. In this sense, Item X of Article 5 of the Federal Constitution determines that private life and intimacy and image rights are inviolable and that cannot be never waived by its owner. These are the legal foundations to promote the protection of personal data.

As a result, any intimate or expression of the private and personality is legally secured to individuals, including those related to professional and commercial relationships not exposed to the public by any means. Privacy is an essential part of human being existence, as clearly expressed by Axel Nilsson: [34]

> Rights relating to personality refer to a set of rights belonging to all physical persons. The rights relating to personality, or personality rights, (Personlichkeitrechten) can be defined as "*subjective rights directly derived from human nature and from the inherent dignity of any person.*" Their aim is to protect the personal sphere of any human being in its physical and spiritual aspect. Examples of rights relating to personality are right to life and physical integrity and right to honor, privacy and image rights. The rights have been topic for discussion amongst legal scholars and almost everything about them have, at one point or another, been discussed as they are, in nature, political as well.

Related matters are the secrecy of correspondence and telephone communications as well as transmission of data classified as confidential and inviolable, except when the courts determine their disclosure or by means of legal obligation. This is expressly provided in Item XII of Article 5 of the Federal Constitution, as follows:

"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: (…)

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;

These principles are regarded as complementing to the Private Life Principle, since assure the adoption of measures to restrict communications to the private sphere and protect the human rights by securing its dignity to live in peace.[35]

It is also of concern the way information is controlled by third parties, as stated by Knapp van Bogaert D[36]:

[34] NILSSON, Axel. Personality Rights, Defamation and the Internet. Page 18. Faculty of Law. Lund University. Thesis: Master Studies. 2017. Available at http://lup.lub.lu.se/student-papers/record/8909002/file/8921940.pdf. Viewed on August 15, 2018.

[35] The Constitutional protection of communications further encompass situations related to business and commerce, such as trade secret, know-how disposal and data exclusivity of pharma ad veterinary products.

[36] SCHREIBER, Knapp van Bogaert D. "Confidentiality and Privacy: What is the Difference?", SA Fam Pract, Vol. 51, Issue 3. Page. 194.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

"Debated from various perspectives, the concepts of privacy and the right to privacy often remain elusive. Broadly, we can say that privacy means consensus involving two things: 1) Control over some information about us and 2) some control over who can experience us or observe us. Privacy is a term first used in tort law. Debuting from Warren and Brandeis' "The Right to Privacy" (1890), interest in the nature of privacy has included a vast number of publications, particularly in law and philosophy.

In South Africa, the right to privacy is a fundamental right as listed in the Constitution's Bill of Rights. The concept of privacy encompasses many perspectives. The most popular are: the right to make one's own decisions; the right to travel anonymously; the right to control the dissemination of information concerning oneself; and the right to control the dissemination of information about oneself. The right to privacy is the right of individuals, groups or institutions that have access to and information about others to ensure that it is limited in certain ways. Privacy is not in itself an intrinsic good but it is related to ethics in that it concerns (at least) the causal relationship between one's concept of 'being in control of their own lives' or their autonomy. In other words, unless a person is in the position to appreciate that they have the ability to determine their own course of action, to make their own choices, they cannot be considered as autonomous agents."

On the other hand, the Federal Constitution secures to any citizen through Item XIV of Article 5 the right to access information, facts, people and situations in daily life – so-called Right of Information - including checking the truth of facts, except those protected by confidentiality. [37]

Item XXXIII of Article 5 grants further to all persons the right to receive from public agencies information of private interest regarding such person or of collective or general interest store in any public agency, except information whose secrecy is essential to the national security to society. This Constitutional instrument is so-called Habeas Data and it is set, as follows: [38]

"LXXII – *habeas data* shall be granted:

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

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

[37] Both the inviolability of private life and the right of information are frequently examined in courts to assert individual rights and prevent censorship and violation of confidentiality obligations. Since they are in principle opposing principles, many discussions have been held on which principle should prevail to address data protection, especially regarding the internet, and how to establish checks and balances for the enforcement of the principles without jeopardizing privacy.

[38] Habeas Data is also an effective mechanism to secure to the titleholder of the personal data the right to know and rectify data in the hands of the public institutions and authorities. Habeas Data is resulted by Law 9,507 of November 12, 1997. Available at http://www.planalto.gov.br/CCIVIL_03/LEIS/L9507.htm. Viewed on August 20, 2018.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

The relevance of the Habeas Data may be explained by the fact that Brazil underwent into a political dictatorship between the periods of 1964 to 1985 that limited most political rights of citizens (including Presidential elections). It and secured to public authorities the access to private life, as a manner to maintain the political control of the population. Therefore, the Habeas Data derives from the Principle of Access to Information and may be the first effective instrument to promote the control of private information by an individual person (titleholder) and that led to the existing Personal Data Protection Law.[39]

Paragraph 3 of Article 37 of the Federal Constitution provides in this regard that the federal laws will rule, "the access of users to administrative records and to information about government initiatives, with due regard for article 5, items X and XXXIII". Then, Federal Law nº. 12.527 of November 18, 2011 (so-called Freedom of Information Act)[40] established procedures to be complied with by public agencies, the Federal government, the states of the Federation, the Federal District and municipalities to give access to all persons and citizens of private information stored at the public agencies. Such persons may update and rectify any incorrect information available in public database.

According to the scholar and judge of the Federal Supreme Court Mr. Luis Roberto Barroso, the Federal Constitution of 1988 may be recognized as the most successful local entrepreneurship led by society as it set the boundaries between the public and private arena and secured extensively the private rights against the state intervention, as follows:[41]

"The Federal Constitution of 1988 is the most successful institutional venture of the Brazilian history, as it demarcated clearly some private space that deserved special protection. It established therefore the inviolability of the residence, the secrecy of the correspondences and communications, the free initiative, the property guarantee, besides promising to protect the family. The most notable effort was however to seek safeguard the public arena from the private appropriation expressed in rules that demand exams to assume position as public servants or public employment, bidding for the execution of agreements with the public administration, accountability of those who administer public money … "

Therefore, the freedom of expression and the right to control its own information are looked upon as basic rights to sustain the democracy and assure the dignity of the person.[42]

[39] SILVA, José Afonso da. "Curso de Direito Constitucional Positivo". 40ª. edition. Malheiros Editores. 2017. Pages 456-460.

[40] Federal Law 12.527 of November 18, 2011. Available on http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Viewed on August 27, 2018.

[41] BARROSO, Luis Roberto. "Curso de Direito Constitucional Contemporâneo". 5th edition. Saraiva. 2015. Page 92.

[42] It is worth mentioning that the Brazilian political liberty was restricted twice in the 20th century. The first one took place between the period of 1937-1945 (so-called New State) and then between the period of 1964-1985 (Military Regime). Both regimes limited the civil and political rights of citizens in favour of the public interests set by the state. Bonavides, Paulo. "Teoria Geral do Estado". Malheiros Editores. 2015. Pages 564 to 577. Therefore, securing the individual rights, including the political and the private

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

The second relevant piece of legislation is the Brazilian Civil Code or the "Law of the Common Man" that revised concepts established by the Civil Code of 1916[43], adopted new principles and took into account the novelties in human and business relationship.

This law established for the first time a specific section - Chapter II of Title I of Book I – comprised of 11 articles ruling about privacy, private life, honour and image of a person (so-called personality rights). There is a clear objective to protect the moral integrity of a person against possible third parties' interference or unauthorized use. Therefore, legal measure may be granted to prevent violation of private life. The Brazilian Civil Code further recognizes that personal situations can be only exposed by the decision of individuals owing the rights and in some specific situations, such as court orders.

The third legislation relevant to data protection and that helped establish specific civil rights framework for data protection is the Federal Law 12,965 of April 23, 2014 (known as "Internet Law)[44] and its regulation (Decree 8,771 of May 11, 2016).[45]

The Internet Law establishes the principles, rights and obligations regarding the use of the internet in Brazil. It deals with the relationship between the provider and the internet user and grants the full access to the information collected and stored by internet providers and others involving the individual. This law addresses further the gathering, storing, using and making available to third parties of private data through the internet (connection logs to which these piece of laws relate). It ensures that the contents of private communications and transfer comply with the protection of privacy, private life, honour and the image of the involved parties.

Further to that, the Internet Law, by means of Decree 8,771/2016 sets the standards for security and confidentiality of records, personal data and private communications over the internet.[46] The standards aim to

ones, was of utmost importance for the construction of democracy and respect of the private rights.

[43] Law nº. 3,071 of January 1, 1916. Revoked by the present Civil Code. Available at http://www.planalto.gov.br/ccivil_03/LEIS/L3071.htm. Viewed on August 27, 2018.

[44] Available at http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Viewed on August 27, 2108

[45] Available at http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm. Viewed on August 27, 2018.

[46] According to the legal writer Jaqueline de Souza Abreu, Decree 8,771/2016 served to clarify pending questions on the extension of law enforcement access to account information and regulated better the stipulations of the Internet Law: ."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). That is, the authority 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. ABREU, Jacqueline de Souza. "Data Protection in Brazil". Page 11. Available at http://www.internetlab.org.br/wp-content/uploads/2017/03/Data-Protection-in-Brazil-InternetLab.pdf. Viewed on August 17, 2018.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

prevent undue transfer of private information and the flow of a user' communication over the internet to third parties and secure information for possible courts' and public authorities' use related to monitoring and infringement of rights.

Accordingly, the internet provider responsible for the retention of private record and/or data will only be obliged to provide the data, separately or in association with personal data or other information that permits the identification of the user or of the internet terminal, by court order and other provisions dealt with by this law. Further, the internet provider should observe standard security guidelines concerning the possession, storage and processing of personal data and private communications. Among them, we highlight the need to:

Establish strict control over access to data by creating responsibilities for those who have access and exclusive access privileges for certain users;

Create detailed access logs for connection and internet applications records.

Use management solutions for records of collected information that secures the inviolability of the collected data, such as encryption or related measures.

Delete private information after the purpose of collection, storage, retrieval and use has been achieved or after the deadline determined by the legal obligation has come due.

As for keeping connection records, Article 13 of the Internet Law sets out that the provider or entity responsible for the management of an autonomous data system must keep the connection records confidential and in a controlled and safe environment for a maximum period of one (1) year. Administrative and police authorities or the Public Prosecutor may require precautionary keeping of connection records for a longer period. The responsibility for the maintenance of such records cannot be transferred to third parties.

The Internet Steering Committee is responsible for the promotion of studies and recommendation of procedures, as well as for setting technical and operational standards for the better security and confidentiality of records, personal data and private communication.

In view of the confidentiality importance, Paragraph 2 of Article 14 of Decree 8,771/2016 establishes that internet providers must retain as little as possible personal data, private communications, connection, and internet applications records as possible. Article 16 further sets the events under which it is prohibited the storage of internet access, as follows: personal data that are in excess in relation to the objectives by which the consent was granted by the owner and the registration access to other internet application without the previous consent of the owner.

Other important legislation that help establish the basic backbone for the protection of the personal data

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

in Brazil is the Consumer Code Protection.[47] Such law addresses the gathering and using of consumer's data exploited in business and commerce. The most relevant item dealing with the personal data is Paragraph 2 of Article 43, which expressly determines that the creation of files and database, the registration of personal data and those related to commerce should be communicated prior to consumer. Consumer will have full access to the registered and gathered information about him/her. I will request rectification of collected data. This rule derives directly from Item X of Article 5 of the Federal Constitution.

By means of Decree no. 7,963 of March 15, 2013 new specific rules were set out for those consumers that buy products or hire services through the internet. Such rules deal essentially with three (3) aspects of consumer rights: (i) clear information about the products and services provided by the supplier through the internet; (ii) transparent rules to consumers and (iii) the right to regret and to cancel the transaction.

Further to that, Federal Law 13,543 of December 19, 2017[48] sets out the obligation for internet providers to disclose ostensive and clear information to consumers when offering services/products through the internet. In this regard, the law establishes that such disclosure should take place in characters that may be clearly viewed by consumers, with a font size not lower than 12.

According to the legal writer Jacqueline Abreu, when addressing the applicability of the Consumer Code Protection to internet business: [49]

"The Consumer Protection Code regulates the consumer privacy in the article 43. It aims to give the user/consumer a better control over his or her information, especially 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 cancelling 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."

The aforementioned legislations apply to Brazilian citizens and to Brazilians and foreigners living in Brazil

[47] Federal Law nº. 8.078 of September 11, 1990. Available at http://www.planalto.gov.br/ccivil_03/LEIS/L8078.htm. Viewed on August 27, 2018.

[48] Available at http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13543.ht. Viewed on August 10.

[49] ABREU, Jacqueline de Souza. « Data Protection in Brazil »» op.cit. 46.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

and companies and private organizations doing business or exercising their rights in the territory.

KEY PRINCIPLES TO PERSONAL DATA UNDER THE LEGAL FRAMEWORK: THE BASIS FOR A COMPREHENSIVE LAW

Following up the diverse legislation, applicable principles have been established to guide and justify the legal base and standards under which a great protection for personal data and business transactions are set.

By setting the principles, it is possible to identify the legislative option to favour the individuals/owners of the private data or those who access the information/controller, although it is recognized that the applicable principles conflict usually with one another in an attempt to balance rights and obligations in accessing private information.

The most relevant principles praised by the Federal Constitution and applicable laws are the following:

Transparency to Personal Data Protection = This Principle is derived from the Federal Constitution (Item X of Article 5) and expresses the manner personal data must be gathered, processed, stored and exploited by third parties holding access to the data.

Accordingly, the processing and use of personal information by others require the communication to the individuals about the purposes and limits of use. This may take place by providing a privacy policy in the form of guidelines, terms and conditions and express authorization for the handling of personal information.

This Principle also gives full access to the titleholder to possible update, modify and eliminate data.

The Transparency Principle is noticed further at the federal laws and regulations dealing with the data protection framework. For example, the Freedom of Information Act holds as a principle the "promotion of the development of a transparency culture within the Public Administration" and the free access to its information held in database of public agencies. In addition, Article 43 of the Consumer Rights Code grants to consumer the right to rectify and update any inaccurate information about himself in a file or register held by a company in a consumption relationship.

At this point, it is important to observe that[50]

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

[50] Abreu, Jaqueline, op cit, 46. Page 29.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

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.

The Transparency Principle is further guaranteed in the Internet Law and its regulation. Items VI and VII of Article 7 of the Federal Law determine the need to supply clear and full information entailed in internet service agreements, setting forth the details on the protection to connection records and records of access to internet applications, as well as on traffic management practices that may affect the quality of the service provided. Providers need to supply further clear and complete information on the collection, use, storage, processing and protection of personal data.

Lawful Basis for Processing = This Principle highlights the importance of obtaining the prior and express consent from the individual for the specific purpose for which the data will be used. This Principle encompasses further the requirement of any processing of personal data be lawful and fair, which means complying with the applicable legislations (Art. 7 (VIII) (b) of the Internet law).

Under Decree 8,771/2016 (regulates the Internet Law), it is determined the need for internet providers (and those responsible for the transmission, switching or routing) to adopt transparent measures to clarify to the user the reasons for network management. It further recommends providers to adopt guidelines setting security standards in personal data and private communication, including the processing, storing and disposal to the personal data. The set of guidelines in this particular principle aims to make the use legal, as the consent of use and the actual use by the consented third party will follow the terms and conditions of the guidelines.

The Freedom of Information Act also provides lawful basis for establishing rules for processing and using private data by public bodies and government agencies, including the specification of the events that consent is dispensed, as follows:

"Art. 31. Paragraph 3. The consent referred to in clause II of Paragraph 1 shall not be required when the information is necessary for:

I – medical prevention and diagnosis, when a person is physically or legally incapable, and solely and exclusively to guarantee due medical treatment;

II – the production of statistics and scientific research of public or general interest as established by the law; however, it is forbidden to disclose the identification of the person to whom the information refers;

III – the compliance of a court order;

IV – the protection of human rights; or

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

In the same matter, it is important to observe the comments provided on the information access in the financial sector, as provided by the author Pedro Ramos, as follows:[51]

"To reinforce the importance of this subject, the Securities Commission (CVM), authority responsible for regulating the securities market and its stakeholders in Brazil, issued Instruction 31 1984. This Instruction highlights the need to inform the whole market about information that can affect all investors of a company with shares on the stock market. In case the company prefers to keep some information in secrecy, such decision must be submitted to CVM and all managers and shareholders must respect such secrecy.

The secrecy obligations above presented can only be ruled out in the context of a judicial procedure, provided that the whistle blower's hearing is previously justified and authorized by a judge. In such cases, upon proof that the whistle blower is being coerced or threatened for his/her deposition, Brazilian law presents a series of provisions for the protection of the whistle blower and his/her family. Such provisions include financial help, protection of identity, security, among other protective measures to be adopted by public authorities."

Purpose Limitation = Personal Data gathering and processing need to follow strictly the legitimate purposes granted by the individual. Therefore, it cannot overcome the agreed purposes and limits. In case the holder of the information wants to use the personal data in a manner incompatible or that trespass the granted rights, the holder requires specific and prior authorization.

The Purpose Limitation Principle prevails in the existing data protection framework, as the upload, collecting and use of information about a person, including those related to communication data should be limited and directly related to the purpose for which it was retained, stored and used. In this matter, Article 12 of Decree 8,771/2016 clearly sets that "*connection and applications providers must retain as little personal data, private communications and connection and access to application records as possible*'. It establishes also that the retained information should be erased after the purpose of their use is achieved and the set legal deadline for storing data protection (as stipulated in the Internet Law) is complied with.

Further to that, collection, use, storage, processing and protection of user's personal data may take place when such acts are adequately justified, are not prohibited by the laws of the land and are specifically provided in the terms and conditions of the internet service agreement.

Accuracy of the Accessed Data = Personal data acquired by the third party needs to be accurate and represent adequately the characteristics and the identification of the individual. It needs to comply further with the information provided by the individual holder of the data. Therefore, the laws of the land recognizes the right to

[51] RAMOS, Pedro H., « Data Protection in the Financial Sector – Regulatories Perspectives ». Page 8. Available at , http://baptistaluz.com.br/wp-content/uploads/2017/06/Protecao-de-Dados-no-Setor-Financeiro.pdf,. Viewed on August 4, 2018.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

rectify and eliminate any information contained in the concerned registration.

Both the Freedom Information Act and the Consumer Rights (regarded as public order legislations) secure to the individual the right to rectify improper and inadequate personal information, as follows:

Consumer Code

"Art. 43. The consumer, without penalty from what is said on article 86, will have access to information that exists in registries, forms, and personal consumption data that has been reported about him, as well as their respective sources.

§ 1. Consumer registrations and data must be objective, clear, truthful, and in a language that is easy to understand. It may not contain negative information referring to a date over five years prior.

§ 3. If the consumer finds inaccurate information about himself in a file or record, he may demand its immediate correction. The party maintaining the file or record will have five weekdays to communicate the change of this incorrect information to any parties involved."

Such Principle should further encompass the right to request controller to destroy any personal data that the individual considers as incorrect, based on errors and imprecise facts or excessive in regard to processed information. Unlawful collection and processing of personal information grant to the individual the right to seek deletion.

Data Minimisation = Both specific laws on data protection – the Internet Law and the Freedom of Information Act – set rules dealing with the collection and storage of minimum personal data, specifically related to the purpose of their use. The Freedom of Information Act clearly establishes that the access, disclosure and processing of confidential information shall be limited to those who need to know it and who are properly certified following up the existing regulations without prejudice of the competencies of public agents authorized by law, as follows:

"Article 25. It is the duty of the State to control the access and disclosure of confidential information produced by its bodies and entities, ensuring its protection.

Paragraph 1. The access, disclosure and processing of confidential information shall be limited to those who need to know it, and who are properly certified in conformity with the regulations, without prejudice of the competencies of public agents authorized by law."

This is indeed a principle that limits substantially the unauthorized transfer of data, including the international transfer, as its exploitation should be compatible with the set objective for the access and processing operation.

Under this principle lies the Proportionality Principle, which sets the obligation to gather and process limited information on the individual in close relationship with the proposed purposes, including the commercial

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

sector of controller and others. This obligation serves as a limitation to any attempt to use personal data for other purposes not previously set.

As a manner to preserve the Proportionality Principle, the Internet Law grants to individuals the right to update and eliminate personal data provided to a certain internet application.

Retention Period = This Principle sets the obligation of controllers to maintain the personal information for a needed period required to fulfil the purposes for which it was gathered and processed. By examining the applicable laws on data protection, it is understood that Paragraphs 1 and 2 of Article 43 of the Consumer Rights Code (enacted in 1990) firstly adopted such Principle.

Accordingly, it is prohibited to maintain negative data about consumers at database for a period longer than five (5) years, independently of the fact that the consumer is still in debt against business.[52]

The Internet Law further adopted the Retention Principle. As for keeping connection records, it sets out that provider or the entity responsible for the management of an autonomous data system should keep the connection records confidential and in a controlled and safe environment for a maximum period of one (1) year. If required, administrative and police authorities or the Public Prosecutor may require precautionary keeping of connection records for a longer period. The responsibility for the maintenance of the data information and connection during the aforementioned period cannot be transferred to third parties. An administrative, police authority, or the Public Prosecutor Attorney may require precautionary keeping of connection records for a longer period of one (1) year. Such precautionary keeping request needs to be followed by a 60 day period (as of the date of the first request) to commence Court proceedings to request access to the records. As to application access logs, the internet provider needs to maintain the application access logs under confidentiality and in a controlled and safe environment for six (6) months.

It is important to state that the retention and the making available of connections logs and access to internet applications logs to which this law refers to, as well as, of personal data and of the content of private communications, must comply with the protection of privacy, honour and of the image of the parties that are directly or indirectly involved.

According to Article 15 of Decree 8,771/2016, private date should be kept in an interoperable and structured format, for easy access in case of court decision or in those events specified by law.

Another important piece of legislation is Law nº. 12,044 of June 9, 2011[53] that deals with data gathering

[52] Further discussions are held on the fact that the period of retention set by the Consumer Rights Code should be longer in view of existing legislations applicable to letters of credits and checks. See FRANK, João Fernando and JOBIM, Eduardo Schmidt. "O Artigo 4 do Código de Defesa do Consumidor e Suas Diversas Interpretações Quanto à Permanência de Inscrições Negativas" in Revista Eletrônica do Curso de Direito Da UFSM Março de 2008 – Vol. 3 N.1, p. 23-33.

[53] See Federal Law 12,044 of June 9, 2011. Available at http://www.planalto.gov.br/ccivil_03/_Ato2011-

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

and storing concerned with natural and legal person that adequately comply with their financial obligation, so called "Positive Data". The maximum period for storing "Positive Data" of a person is fifteen (15) as from the date of collection, as provided in Clause 14.

Confidentiality = Secrecy of personal data matches with the Data Minimisation Principle, which is set from the understanding that controller may use under the concept of the need to know it and use by who are properly certified. This means that security and confidentiality of recordal, personal data and private communication, especially over the internet are requirements under the personal data protection.

To set confidentiality standards, Decree 8,771/2016 establishes that the provider responsible for the retention of private records and/or data will only be obliged to provide them, separately or in association with personal data or other information that permits the identification of the user or of the internet terminal, by court order and other provisions deal with by the law.

In view of the importance of confidentiality, Paragraph 2 of Article 13 of Decree 8,771/2016 establishes that internet providers must retain as little personal data, private communications, connection, and internet application records as possible.

Consent and Prior Agreement = Prior consent on personal data was firstly adopted by Chapter II – Personality Right in the Civil Code. Article 19 addressed specifically the need for a third party to obtain the authorization to use a name of a person I commercial advertising and preserved a person intimacy.

Paragraph 2 of Article 43 of the Consumer Rights Code further addressed the need of a prior consent from the individual when a third party wishes to collect the information about the consumer and open a file and record on it. This right was regarded in practice as one of the most important ones, since it permitted consumes to have a better control on the data exploited commercially and for punitive purposes.

Since then the prior consent has been praised as a Principle, which is a policy followed by all legislators, judges and scholars. This has been seen in the Internet Law, as the prior Consent Principle is viewed as essential right to the internet access, as follows:

"Art. 7. The internet access is essential to the citizenship exercise and to the users are guaranteed the following rights: (…)

VII – no supply to third parties of their personal data, including connection log ana access to internet application, except by means of free, express consent and informed or in the events prescribed by law."

The individual consent does not need be in written, but it should follow the customs adopted in each field of use. For example, hotel accommodation is commonly followed by the need to fill in questionnaires with

2014/2011/Lei/L12414.htm. Viewed on August 25, 2018

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

private information on the guest and such information is required by for security reasons and placed in a specific data.

THE NEW PERSONAL DATA PROTECION LAW: OVERALL CHARACTERISTICS AND HOW FAR THE PROTECTION EXTENDS

When looking at the applicable legislation and principles that formed the legal framework for the protection of personal data, one may wonder if the new Data Protection Law (Law nº. 13.709/2018) was indeed required. This basic question arises when the existing laws seemed to cover a broader range of protection capable to encompass the personal data.

As an attempt to justify the adoption of the new law, there is indeed a general public perception that the Law nº. 13,709/2018 was an important step to strengthen personal rights in Brazil in view of the disrespect of acquired personal data by third parties.

Accordingly, diverse legislations addressed vaguely some aspects related to privacy linked to personal data. This is the case of the Consumer Rights Code, which has attempted to deal with database consumer protection in only one article by disposing vaguely that consumers should have access to information in registries and to data correction. The new law increases the need for transparent regulations and policies in the legal entities.

Although the diverse laws established the concept and the elements of protection, they seem not to be in entire compass with the technological scenario of intense online business transactional and personal relationship.[54] For example, it is a Brazilian reality the direct and insisting contact of companies to the locals (persons and companies) by phone call or mobiles offering products or services bearing in mind that the companies are not their clients and commercial contact. This is indeed an evidence that personal data is being transmitted from any database that hold the private information.

Law nº. 13,709/2018 empowers indeed the locals by providing better mechanisms for the control of personal information provided to a shopper and ensure that the collected data will be used for a specific end. The novelty is indeed the creation of the authority that monitors the compliance with the principles, secures the applicability of the Data Protection Law and imposes administrative penalties for the infringers, the so-called National Authority for the Protection of Data (ANPD).[55]

[54] As an example, the Internet Law provided the possibility for internet users to delete specific or the total set of information from a database, except in the events that the law makes compulsory the storage of information for a specific period of time. However, assurances on the deletion and cease of information use were vaguely provided due to the non-existing authority to monitor the personal data protection system.

[55] The provisions related to the creation of the ANPD (Articles 55 to 59) were vetoed by the President of Brazil when enacting the

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

The efficiency of the new personal data protection is shaped up by administrative penalties applied to infringers of the Law nº. 13,709/2018 that range from warning to a fine of two percent (2%) of the gross revenue of the entity. The amount of the fines will follow up specific criteria set up by Paragraph 1 of Art. 52, as herein provided:

"Paragraph 1. The sanctions will apply after administrative procedure that secures broad defense, in a gradual, isolated or cumulative way in accordance with the peculiarities of the concrete case, and bearing in mind the following parameters and criteria:

I – seriousness and nature of the infringements and of the personal rights affected;

II – The good faith of the infringer;

III – the advantage obtained and intended by the infringer;

IV – the economic condition of the infringe;

V – the recidivism;

VI – the damage degree

VII – the cooperation of the infringer

VIII – the repeated and evidenced adoption of internal mechanisms and procedures capable to reduce the damage related to the secure and adequate treatment of data, in observance to the stipulations in Item II of Paragraph 2 of Article 48 of this law;

IX – the adoption of good practice and governance;

X – the prompt adoption of corrective measures and

XI – the proportionality between the seriousness of the default and the intensity of the sanction."

As one may notice from the aforementioned enlisted criteria, the adoption of good practice and governance as a parameter for the application of a fine highlights the importance of legal entities adopting specific Personal Data Policy based on good practices and governance. This is the so called "database compliance" and involves stringent ruling on data security and confidentiality. One important matter that requires to be specifically provided in the Personal Data Policy is the safety measures to be adopted to protect the information against unauthorized access by third parties and accidental situations that leads to the destruction, loss and alteration of

law. The argument was based on the fact that the creation of this agency with detailed format would violate the Federal Constitution, since an agency of this nature will be financed by the Executive Power. Therefore, the agency needs to be created by the initiative of the Executive Power not by the Parliament. The President promised to send a Bill to the Parliament for the creation of the agency. Available at http://www2.camara.leg.br/camaranoticias/noticias/CONSUMIDOR/561337-MARCO-LEGAL-DA-PROTECAO-DE-DADOS-PESSOAIS-E-SANCIONADO-LEI-ENTRA-EM-VIGOR-EM-2020.html. Viewed on August 25, 2018.Notwithstanding the fact that the ANPD has not been created yet, which will prevent the application of the administrative penalties, the fines evidence the important of personal data protection and may push losses and damages further and higher by court actions.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

the provided data. This requirement determines the specification of technical measures (i.e. software or applicative to ensure safety) and administrative procedures, including emergency measures related to leakage information.

According to the new law, the national authority (the ANPD) may impose minimum technical procedures to be complied with by controllers to ensure security and safeguards against unauthorized or unlawful processing, accidental loss, damage or destruction of information. In addition, information leakage through cyber-attacks needs to be informed to the national authority in a reasonable timeframe and the specification of the technical measures undertaken by controller to cease the leakage and mitigate its effects, including applicable damages.

There is also specific treatment to the category of personal data so-called "sensitive personal data", which is a compiled information of a natural person specifically related to race, ethnic, origin, religious beliefs, political opinions, affiliation to trade unions or organizations of a religious kind, philosophic or political nature, health or sexual life or orientation data and genetic or biometric data. The use of such information will take in a more restrictive manner where no one may use them for discriminatory purposes.

The treatment of "consent" by the individual who grants the use of its personal information to the controller has been improved and matched with the personal data protection reality based on the protection of the different stages of data use. According to the law, consent should be express or by any other means that clearly evidence the manifested agreement by the individual. Although consent is already inserted into the diverse legislation on personal data (i.e. Internet Law and the Consumer Rights Code), the new law prevents the adoption of long, general and complex texts followed by a mouse click procedure for the agreement.[56] Consent is dealt with in a granular sense, which is specific for each type of use by controller and therefore further use requires specific consent by the individual.

About consent and the better control of the information by the individual, Law nº. 13.709/2018 addressed the institute of "portability", which is possibility of the individual/titleholder of the private information demand the transfer of its files from one collector to the other. It may further requests the share of the information between two collectors or the exclusion or anonymization of information in one collector. The portability involves the prior consent of the titleholder and clearly evidences the legal support to the better allocation of the personal data by the individual.

Last but not the least, Law nº. 13.709/2018 innovated in dealing with the transfer of international data. Besides determining the need of prior consent from the individual, the transfer of information to an international

[56] Articles 7 through 9 of Law. 13,709/2018 address the consent ruling and clearly stipulate that broad authorizations for the treatment of personal data are null. Moreover, consent may be revoked by any time. Also, the legal stipulation determines that the responsibility to evidence that consent was adequately provided by the individual lies on the controller.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

database or controller demand the fulfilment of specific requirements, such as the evidence that the data will be only transferred to countries or international entities that can secure similar adequate degree of protection to personal data.

This equivalence of rights will be examined by the public authority who will further check the specific involving circumstances to the transfer of international data,[57] but the controller is responsible for providing adequate assurances that the principles and rights of the titleholder will be duly respected.

Since Law nº. 13.709/2018 encompasses different issues applicable to personal data in its 65 articles, two matters are of interest to this paper that will assist the reader to understand the individual rights granted to the natural person. The first one relates to the beneficiary of the law or those parties that need to accomplish with the legal demands. The second one involves the specification of the rights granted to the titleholder (physical person). By dealing with those two matters, the reader will be able to comprehend better the individual rights secured to the natural persons.

Article 3 of the Law nº. 13.709/2018 specifies those who are affected by any means by the new provisions of the personal data protection. Accordingly, the beneficiaries of the law are natural persons or legal entities, public or private, regardless of the business activity and of the country where its headquarters are located and of the the country where the database is located (insofar as the treatment of personal information takes place in Brazil).

The immediate beneficiary of the legal protection is the titleholder of the information subject to legal protection. This item has already been addressed in Item I of this Article II – What Does Personal Data Really Encompass Under the Law of the Land? – and therefore personal data for the purpose of the law encompasses only those information capable to identify or that identifies, directly or indirectly natural or individual person. Therefore, the titleholder of the information is always a physical or natural person. The rules related to collecting, processing and transferring information are in benefit of the natural person.

Notwithstanding the aforementioned, those physical persons holding information not collected or treated in the Brazilian territory or disposed in trade to individuals located in the local territory are not protected by this law.

The effects of the law reaches further the Controller and the Operator of the personal data. The law of

[57] The equivalence of rights requirements and the ANPD's presence in examining the degree of protection in other countries are regarded by the representatives of specific sectors as an international trade hindrance due to the fact the importation/exportation of goods and services involves the use of personal information to validate quality data, among others. This concern overcomes the proposed objectives and contents of the present article, but it is herein highlighted as an intention to draw the attention of the reader. See "Comentários do Information Technology Industry Council em Resposta à solicitação feita pela Comissão Especial da Câmara de Deputados encarregada de discutir o projeto de lei sobre tratamento e proteção de dados". Available at http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/ITIInformationTechnologyIndustryCouncil.pdf. Viewed on August 28, 2108.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

the land distinguishes both persons by stating that the controller is the natural or legal entity (public or private) with whom lies the decisions relating to the processing of the gathered personal data. The Operator is the natural or legal person, in private or public law, who processes personal data on behalf of the data controller. The Controller and Operator may be the same person when the decision-making and the collection and processing of personal data of an individual are led by the same party.[58]

The identification of controller and operator is of utmost importance in view of the fact that the main objective of Law nº. 13,709/2018 is to set up a stringent control on the activities of those who process personal information. In this regard, the law has created a new "beneficiary" of the law so-called "officer" who is a natural person, appointed by the controller, to act as a communication channel before the data subjects and the competent public body. The activities of operator are of limited scope and encompass the following activities:

Paragraph 2 – The officer´s activities shall consist of:

I – receiving complaints and communications from the titleholders, provide clarifications and undertake appropriate measures;

II - receive communications from the competent public body and undertake appropriate measures;

III – instruct the entities` staff regarding the practices to be observed for the protection of personal data; and

IV – other duties established by additional rules or determined by the data controller.

Paragraph 3 - The competent public body will establish additional rules regarding the appointment and duties of the officer, including the possibility of exemption of the obligation to appoint an officer, considering criteria of nature or size of the entity, as well as the volume of data processing operations."

In view of that, the Operator's activities can be framed as a mandatary or representing person under the provisions of Articles 653 through 692 of the Civil Code. This means that the Operator is not co-responsible for the indemnification of individuals caused by the violation of the federal law or the infringement of the existing personal data policies. Nevertheless, the Operator is fully responsible for the acts that he was empowered of

Further to that, Law nº. 13,709/2018 has created a "package of rights" to personal data that permits the individual to have a better control of the provided information. Such rights derive from the Principles and guidance provided for by the legislations and regulations applicable to personal data prior to the new law. In addition, the "package of rights" that cannot be waived by the individual/titleholder of the personal information[59]

[58] According to item X of Article 5 Federal Law 14,709 of November 3, 2018, processing or treatment is classified as any operation undertaken to personal data, encompassing the collect, production, reception, classification, use, reproduction, transmission, distribution, processing, storing, eliminating, validation or control of the information, modification, communication, transfer, diffusion of extraction.

[59] A good discussion would involve whether the "package of rights" provided by Law nº. 13,709/2018 is set under the public order

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

brings obligations on the same level to the parties who collect, treat, and process and store information of personal nature.

Among the relevant rights to individuals on the processing of their personal data are the following:

Right to Express Consent– This is a basic right of individuals that want to participate in registers and database by granting access of private information to third parties. As informed before, the consent under Law nº. 13,709/2018 is granular and relates to specific acts undertaken by controller. Consent is expressly provided by Articles 7 through 9 and stipulate the manner the agreement should be provided. Controller has the burden to evidence that the individual provided on written by other means the requested consent.[60]

The law also deals with the events that consent are dispensed. The International Transfer of Data and the Right to Withdraw Consent can be framed as an extension to the Right to Consent. The Right to Withdraw Consent secures to the individual the possibility to withdraw the consent at any time and without any justifying reasons. Controller needs to create a free and easy mechanism to facilitate the withdrawal of the consent.[61]

Individuals may further exercise the right to withdraw the consent given to a controller or holder of files or database encompassing private data at any time in case of violation of private rights and intimacy. When a contract to exploit a database is fully complied with by the licensee, the withdraw consent will be accepted only in the cases provided in the contract, such as the "User Agreement and General Policy".

Right to Rectify Errors - The right to rectify errors and update information is guaranteed for an individual to access private information in files and specific databases and correct the data. Item III of Article 18 of the Personal Data Protection Law holds specific and direct ruling on the rectification of errors, outdated and inexact information on the individual. It allows consumers to correct immediately and eliminate imprecise and incorrect

law or whether the aforementioned law is a mandatory one. Public order laws and Mandatory laws holds the same characteristics, as they are cogent laws that cannot be dispensed by the holder. Public order laws are those aiming to protect essentially the best interest of the community or to preserve directly the values of the Brazilian society. Such laws are usually public administration laws, taxation, consumer rights and antitrust laws. Mandatory laws are cogent but do not aim to protect directly the community. Instead, they aim to balance business relationship or stipulate specific formalities for some acts and business. Further discussions and comments; please see FIGUEIREDO, Marcelo and BROLLO, Maria Alice Deucher. "Anotações a Respeito dos Planos Econômicos – Alteração e Política Salarial – Reajuste de Salários pela Lei antiga – Direito Adquirido, Mera Expectativa de Direito e Norma de Ordem Pública – Resenha Doutrinária e Jurisprudencial". Revista Trimestral de Direito Público 6. 1992. Pages 234-248. DIAS, José Carlos Vaz e. "Business Transaction of Intellectual Intangibles: The Evidence and the Peculiarities of a New Form of Property Rights". Quaestio Juris. Vol. 08, nº. 03, Rio de Janeiro, 2015. pp. 2050-2052.

[60] The applicable legislations do not address the use of cookies or other similar technologies. Therefore, cookies are permitted insofar as this mechanism of collecting private information complies with the following requirements: a) the prior and express consent of the person is adequately given and b) the storage and keeping of connection records, and the security and confidentiality measures are informed to the individual.

[61] Questions may arise on the legality of clauses stipulated in the Privacy Policy of the controller provides ruling on consent withdrawal, since it is recognized that consent and the withdrawal are mandatory. This question is of importance in view of Article 8 of the Internet Law that guarantees the right of privacy, private data and freedom of speech in the communications. Therefore, the withdrawal takes places with some restrictions when an applicable a specific consent that rules the withdrawal.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

information in the database, including those provided by internet providers. This right derived originally from the Freedom Information Act also entitles any individual to rectify errors and eliminate them from files and database in public agencies and entities. This grant comes from Item III of Article 3 and Article 6 of this law that states that protection of personal information shall observe its authenticity and integrity.

Right to Deletion – Item VI of Article18 secures the right to a definitive elimination of any personal data disposed to a controller, at any time. However, it is broadly stipulated and arises questions related to the event where the person (titleholder of the information) and controller holds a service agreement that permits the access of the private data (between the individual and the internet provider, for example).

Notwithstanding the aforementioned, the Right to Delete information at any time and the Right to be Forgotten are common matters of court action. A relevant decision on the matter was processed at the Superior Court of Justice (STJ) on the Special Appeal n.1.316.921-RJ (2011/0307909-6). [62]The decision issued on June 26, 2012 affirmed that Google Brasil Internet Ltda. had not the obligation to exclude from the search tools images and information that would be potentially illegal due to Freedom of Operation Principle secured by the Federal Constitution.

The Right to Deletion/Right to be Forgotten is yet an issue to be resolved, since this matter is under examination by the Federal Supreme Court (RE 1010606) and decision is expected to be issued next year.[63]

Right to Basic information and to Objet to Processing – Individuals hold the right to be informed on the existing information in the hands on controller. This right is regarded of utmost importance for the transparent processing of personal data and the good faith relationship. Moreover, it secures that the processing (collection, use, disclosure of any information about individuals) need to be previously and expressly informed to the involved person and consented. According to the new law, it is required the express consent of the individual for the collection, use, storage and processing of personal data. This consent needs to be addressed and obtained through a specific separate part of the document. Further to that, it is an obligation of controllers to supply clear and complete information on the collection, use, storage, processing and protection of user's personal data.

As mentioned before, there are discussions about the validity period of the express consent and therefore whether the express consent may be terminated at any time by the individual, which will permit to object the processing of information. The discussion lies on the fact that intimacy and the private life are regarded by Article

[62] See decision issued by the Superior Court of Justice (STJ). Available at https://stj.jusbrasil.com.br/jurisprudencia/22026857/recurso-especial-resp-1316921-rj-2011-0307909-6-stj/inteiro-teor-22026859?ref=juris-tab. Viewed on August 28, 2018.

[63] The Right to Deletion/Right to be Forgotten is yet an issue to be resolved, since this matter is under examination by the Federal Supreme Court (RE 1010606). See relevant information on the court developments at http://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=4623869&numeroProcesso=833248&classeProcesso=ARE&numeroTema=786. Viewed on August 28, 2018.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

11 of the Civil Code as personality rights. Therefore, they cannot be transmitted or renounced and their exercise cannot be voluntarily limited. On the other hand, both the Internet Law and the Consumer Rights Code value the Transparency Principle that understand that once the individual adhere to the "User Agreement and Privacy Policy", it needs to comply with its terms and conditions.

The common understanding is that individuals adhering to a specific "User Agreement and Privacy Policy" should comply with its terms and conditions, but provisions restricting the prior consent for deletion, transfer of information to third parties and others rights secured by the laws cannot be eliminated or disposed by the involving parties (the individual and the provider). Therefore, such violations would grant the user with the right to object processing.

Right to Restrict Processing – The new law secure to individuals the right to restrict processing, including the non-disclosure to third parties of personal data. The exception to this right would take place in case individuals expressly and freely consent on the transfer of files to third parties or in accordance with the cases provided by law, such as court order and the access by administrative authorities to access recorded data that informs personal qualification, affiliation and address.

Right to Data Portability – The Portability right is a novelty of the new law. It secures to the individual the right to transfer its personal data to a specific entity or person insofar as trade secret is duly protected. The transfer of data may take place by permitting the other entity to hold a copy of the personal data or demand the transfer of data and concomitantly request the deletion of the data from the first entity. According to Paragraph 7 of Article 18, the portability does not include data that are already anonymized by the controller.

Right to Complain to ANPD – The individual holds the right to lodge complaints before the public authorities that monitor the data protection system. This right is secured in addition to the ANPD's responsibility to monitor and enforce the rules of the system.

Moreover, the Federal Constitution grants to any individual access to court actions and to petition the government authorities in defence of rights or against illegal acts or abuse of power.

Right to Object to Marketing - The right to object to marketing is secured to individuals to prevent that personal data are exploited in the market without the individual's express and prior consent. As a result, the individual may grant access of its private information to providers, holders of files and database and establish restrictive use of the private data, excluding the use for specific purposes or maintaining the right to cancel the rights to marketing and other activities.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

CONCLUDING REMARKS

If a person takes a picture of the existing legal framework for personal data protection, one can notice that Law nº. 13.709/2018 represents indeed a step further to the strengthening of personal rights in Brazil. The fact that the law has created a "package of rights" to the individuals (independently of the business activity and characteristic of the individual) grounded on "granulated" already evidences the improvement of the personal data legal system.

The most relevant developments and novelties are those linked to the enforcement of rights, including the heavy fines and the assurance that consent, the right of deletion and others will be adequately recognized and observed. In this regard, [64] although the monitoring authority – through the ANPD - is looked upon as relevant for promoting the protection of the personal data system, one cannot disregard that the Data Protection Law secures great rights to individuals, which entitles them to enforce them greatly in court and seek losses and damages. Therefore, securing adequate instruments for individuals to assert their greater rights in courts is already a great legal development implemented by the law.

Another important issue addressed by this paper is the inadequate understanding that Law nº. 13,709/2018 has promoted a great development in the treatment to personal data and has come from the scratch. Before the enactment of the Personal Data Protection Law, there was already a comprehensive set of laws and regulations implemented throughout the several years as from the Federal Constitution in 1988. Based on the principles of democracy, human dignity and intimacy in 1988, the Consumer Rights Code in 1990, the Freedom of Information Act in 2011, the Civil Code in 2012 and the Internet Law in 2014 were enacted. They build up the legal grounds and prepared the adequate path for the adoption of the new and specific law on personal data protection.

Most significantly is therefore the recognition that the existing legal framework prior to the new law was well established thereby permitting the easy fit in of the new Data Protection Law (Law nº. 13,709/2018) into the Brazilian legal system.

This fact plays a relevant role on easing the public's acceptance to the new law, which is a regular and expected development of the system to strengthen the rights of the individuals against misappropriation or misuse of private rights. Furthermore, this fact puts aside the common understanding that Brazil was late on adopting a

[64] At the XXXVIII International Congress of Brazilian Association of Intellectual Property that took place in São Paulo from August 19 to 21, 2018, one of the discussed topic on the Data Protection Law was the veto of the President to the creation of the National Authority of Data Protection (ANPD). Accordingly, the ANPD will be the adequate agency to rule the data protection system and supervise the actors, such as the individual, controller and operator, among others.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

personal data protection law, as if there was no protection at all. This view is certainly wrong and most probably the diverse laws were not so effective to guarantee the private rights in view of the lack of mechanisms to enforce them and the broad concept of treating such right. As provided by the scholar Anderson Schreiber, personal data protection is encompassed of different stages that need to be addressed individually. Each step involves the adoption of "positive duties" or procedures to be complied with by the titleholder of the rights and by those who collect and process private information.

Therefore, the examination of the diverse applicable laws was relevant in this article and permitted to understand where Brazil was in regard to personal data protection and how far the personal data system can take, especially related to the novelties implemented by the Law nº. 13,709/2018.

PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: AONDE ESTAMOS E ATÉ ONDE PODEMOS ALCANÇAR?

Resumo

As manchetes dos jornais locais e dos boletins informativos dos advogados concentraram-se em agosto passado na adoção da Lei nº. 13.709/2018 (denominada Lei de Proteção de Dados Pessoais). A importância maior dessa lei relaciona-se à capacidade da lei em dar fortalecer os cidadãos brasileiros durante o relacionamento interpessoal e transações comerciais, quando envolver a disponibilização e transferência de dados pessoais a terceiros. Esse fortalecimento ocorreu por meio da implementação novidades para um melhor controle de seus dados pessoais e pela adoção de um "pacote de direitos" contra a apropriação indébita e o uso indevido de informações pessoais. Além disso, foram adotados instrumentos de execução para fortalecer esses direitos, incluindo a criação de uma autoridade pública que monitorará o sistema e a imposição de pesadas multas. No entanto, a proteção de dados pessoais não é uma novidade nem foi criada "do zero". Ela decorreu de um desenvolvimento legal baseado na proteção da dignidade humana, intimidade e segurança no relacionamento pessoal. Este sistema legal está em desenvolvimento desde a Constituição Federal em 1988. Este artigo foca no exame da construção do sistema de proteção de dados pessoais e na implantação dos princípios que nortearam a proteção existente sob a Lei nº. 13.709/2018. Aborda como objetivo secundário os chamados "direitos básicos" e as principais novidades do sistema. Este artigo deve ser entendido como uma abordagem inicial e natureza acadêmica, e objetiva apontar como o passado influenciou o cenário legal de proteção de dados pessoais.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

Palavras-chave: Proteção de Dados. Dados Pessoais. Direito da Propriedade Industrial. Direitos da Personalidade e Privacidade.

REFERENCE

ABREU, Jacqueline de Souza. "Data Protection in Brazil". Available at http://www.internetlab.org.br/wp-content/uploads/2017/03/Data-Protection-in-Brazil-InternetLab.pdf. Page 11.

BARBOSA, Denis. "Exclusividade de dados sigilosos apresentados às agência regulatórias: agroquímicos". Available at http://denisbarbosa.addr.com/arquivos/200/propriedade/exclusividade_dados_sigilosos.pdf.

_____"Do Sigilo dos Testes para Registro Sanitário". Available at www.nbb.com.br/pub/denis/sigilo_registro_sanitario.pdf

BARROSO, Luis Roberto. "Curso de Direito Constitucional Contemporâneo". 5th edition. Saraiva. 2015

BONAVIDES, Paulo. "Teoria Geral do Estado'. Malheiros Editores. 2015

BONE, Robert G. "Hunting Goodwill: A History of the Concept of Goodwill in Trademark Law." Boston University Law Review. Vol 86:547. Pages. 604-616.

CAMPINHO, Sérgio. "O Direito de Empresa à Luz do Código Civil". 13rd. Edition. Renovar Editor. 2014. Pages 35-70.

CLIFT, Charles. "Data Protection and data Exclusivity in Pharmaceuticals and agrochemicals" published in the book Intellectual Property Management in Health and Agricultural Innovation: A Handbook of Best ` Practices."
COSTA, Luiz. A brief analysis of data protection law in Brazil, pg. 7 http://www.crid.be/pdf/public/8003.pdf

DA SILVA, Ricardo Barreto. Data protection & privacy, https://gettingthedealthrough.com/area/52/jurisdiction/6/data-protection-privacy-brazil/

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

DIAS, José Carlos Vaz e. "Business Transaction of Intellectual Intangibles: The Evidence and the Peculiarities of a New Form of Property Rights". Quaestio Juris. Vol. 08, nº. 03, Rio de Janeiro, 2015

DIAS, José Carlos Vaz e, SANTANA, Leonardo and SANTOS, Bernardo. "The Legal Treatment of Know-How in Brazil: Peculiarities and Controversies of a New Intangible Form". Quaestio Juris. Vol. 09, nº. 04, Rio de Janeiro, 2016. pp. 2315-2318

FISCHER, Georges Charles. "Trade Secrets Protection in Brazil". Les Nouvelles, Washington. Dec. 1987

FRANK, João Fernando and JOBIM, Eduardo Schmidt. « O artigo 4 do Código de Defesa do Consumidor e Suas Diversas Interpretações Quanto à Permanência de Inscrições Negativas. » in Revista Eletrônica do Curso de Direito Da UFSM Março de 2008 – Vol. 3 N.1, p. 23-33.

FURTADO, Gabriel Rocha. "O Marco Civil da Internet: A Construção da Cidadania Virtual" in the book "Direito e Midia" coordinated by Anderson Schreiber

MAGALHÃES, Luis and CHIN, Le Vin. "Accelerating Clinical Research in Brazil". Journal for Clinical Studies. Vol.9. Issue 4.

MIHR. Pipra. Oswaldo Cruz Foundation and bio Developments-International Institute. 2nd. Edition. 2009.

NILSSON, Axel. Personality Rights, Defamation and the Internet. Page 18. Faculty of Law. Lund University. Thesis: Master Studies. 2017. Available at http://lup.lub.lu.se/student-papers/record/8909002/file/8921940.pdf.

PEREIRA, Caio Mário da Silva. "Instituições de Direito Civil". Vol. I. 30ª ed. Ed. Forense

RAMOS, Pedro H., Data protection in the financial sector – regulatories perspectives, pg. 8, http://baptistaluz.com.br/wp-content/uploads/2017/06/Protecao-de-Dados-no-Setor-Financeiro.pdf

REICHMAN, J. H. and SAMUELSON, Pamela. "Intellectual Property in Data". 50 Vand. L. Review 51 (1997) Pages. 139-145

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

SANTIAGO-RODRIGUEZ, Fernando. "Facing the Trial of Internationalizing Clinical Trials to Developing Countries: With Some Evidence from Mexico." United Nations University (UNU-MEIT). Working paper series #2008-023. Available on https://www.merit.unu.edu/publications/wppdf/2008/wp2008-023.pdf

SCHREIBER, Anderson. "Direitos da Personalidade". 3rd. edition. Atlas. São Paulo. 2014

SCHREIBER, Knapp van Bogaert D. "Confidentiality and privacy: what is the difference", SA Fam Pract, Vol. 51, Issue 3. Page. 194.

SILVA, José Afonso da. "Curso de Direito Constitucional Positivo". 40ª. edition. Malheiros Editores. 2017

Internet

https://www.statista.com/topics/ 45/internet-usage-in-brazil/.

https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046.

http://www.mondaq.com/brazil/x/702702/data+protection/GDPR+overview+and+consequences+in+Brazil.

https://www.lexology.com/library/detail.aspx?g=bf457bde-00f8-4bd0-9b4c-afe391d35459

https://www.mayerbrown.com/brazil-the-gdpr-comes-into-force-this-year-now-what-03-08-2018

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

http://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786. http://portal.anvisa.gov.br/english. Viewed on August 14, 2018.

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

European Patient Forum. Available at http://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf.

http://www.stj.jus.br/docs_internet/VerbetesSTJ_asc.txt.

http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12965.htm.

http://www.planalto.gov.br/ccivil_03/LEIS/L8078.htm.

http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp105.htm.

http://www.planalto.gov.br/CCIVIL_03/LEIS/L9507.htm.

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm.

Legislation

Federal Constitution 1988

Federal Law 14,709 of November 3, 2018

Federal Law 12.527 of November 18, 2011

Federal Law 12,044 of June 9, 2011

Federal law 10,603 of December 17, 2002

Federal law 10,406 of January 10, 2002

Federal Law 9,279 of May 14, 1996

vol. 11, nº. 04, Rio de Janeiro, 2018. pp. 2876-2915
DOI: 10.12957/rqi.2018.37426

Federal Law no. 8.078 of September 11, 1990

TRIPs Agreement by means of Decree 1,355 of December 30, 1994 (Promulgation of the Final Act of the Uruguay Round).

the Criminal Code (Decree-Law 2,848 of December 7, 1940)

Law no. 3,071 of January 1, 1916.

Trabalho enviado em 22 de setembro de 2018
Aceito em 29 de outubro de 2018