BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 2 • N° 5 • FEBRUARY 2016

THE RIGHT TO PRIVACY AND PERSONAL DATA PROTECTION IN BRAZIL: TIME FOR INTERNET PRIVACY RIGHTS?

by Vinícius Borges Fortes[1]

Abstract

The Brazilian Internet Bill of Rights, called 'Marco Civil da Internet', instituted various principles and parameters for Internet regulation in Brazil. There is however a persistent gap in the Brazilian legal system concerning laws and infrastructure for the effective guarantee of the right to data protection online, coupled with the absence of specific conceptual precision on the notion of privacy on the Internet. In this context, this paper examines the convenience of using the innovative concept of 'Internet privacy rights', composed of four rights. The study concludes that the express reception of such Internet privacy rights by the laws that govern it and related topics in Brazil, especially those that regulate or will regulate the protection of personal data in the country, allows the redefinition of the core of the fundamental right to privacy, where only the protection of private life, honour, intimacy and image are considered. Ultimately, it argues that Internet Privacy Rights shall be regarded as included in the core of the fundamental right to privacy in the Brazilian legal system.

Keywords: Fundamental rights. Internet. Internet privacy rights. Personal data protection. Privacy.

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html

ISSN N° 2565-9979. This version is for academic use only.

Disclaimer

INTRODUCTION

This research does not claim to completely resolve the gaps existing in the Brazilian normative construction in relation to the privacy, in the understanding the object that Law, as a science, does not have the capacity and control mechanisms for the neutralization of all the legal problems identified on the Internet. In this sense, Law is essentially one of the elements that, along with technological development, can contribute to the strengthening of the fundamental right to privacy.

It is also important to highlight at this stage the conceptual proposition for the normative construction in Brazil. Internet represents the transcendence of geographical boundaries and, because of this, there are specific situations involving the Internet in a transnational context. This research focuses on the incorporation of the concept of 'Internet privacy rights' in the normative production, with a regulatory bias towards privacy protection and the inviolability of personal data on Internet inside the Brazilian territory.

This research intends thus to establish a theoretical-conceptual link to answer the following main question: Should 'Internet privacy rights' be expressed and explicitly mentioned in the Brazilian legal system to ensure greater efficiency of the legal norms that protect the privacy of Brazilians in the context of the Internet?

Furthermore, beyond the debate about the need for regulation of Internet use in Brazil and the effectiveness of the Brazilian Internet Bill of Rights, also called 'Marco Civil da Internet', the general objective of this research is directly connected to the necessary reflection on how these rules will be applied and how they will regulate specific issues related to privacy and personal data protection.

If, in a particular way, 'Marco Civil da Internet' represents a breakthrough in the construction of norms related to the demands of the information society, bringing appropriate terminology to the Internet context. It also triggered the need for regulation of specific topics, such as the section dealing with privacy and personal data protection in the network. In addition, it is noteworthy that, in Brazil, there is also a debate on the creation of a Personal Data Protection Act to protect the use of personal data in a broad sense, covering even the data obtained, stored and handled from Internet applications. Thus, the results of this research connect directly with the imminent and necessary regulation of 'Marco Civil da Internet', as provided in article 10, paragraph 4[2] and article 11, paragraph 4,[3] and will contribute to the discussion around the regulation of personal data protection in Brazil.

The paper provides recent data about the context of the use of the Internet in Brazil to elucidate the vulnerabilities of rights in that space, thereby demonstrating the need for the establishment of a specific regulatory framework by introducing the concept of 'Internet privacy rights' and analysing the prospects of the theme of the protection of privacy and personal data in Brazil.

---

1 Lecturer and researcher at IMED Law School, Rio Grande do Sul, Brazil. Researcher in Law, Technology, Democracy and Development. Visiting Scholar at VUB's Law, Science, Technology and Society (LSTS) Research Group. E-mail: viniciusfortes@imed.edu.br.

2 Art. 10. The custody and the availability of connection records and access to Internet applications contemplated in this law, as well as personal data and private communications content must meet the preservation of intimacy, private life, honour and image of the parties directly or indirectly involved. […]
§ 4 the measures and procedures for security and confidentiality should be informed by the person responsible for service provision clearly and meet the standards set in regulation, respected their right to confidentiality as corporate secrets. (BRAZIL, 2015).

3 Art. 11. In any operation of collection, storage, custody and treatment of personal data records or communications connection and providers of Internet applications in which at least one of these acts from occurring in the national territory, shall be compulsorily complied with Brazilian legislation and the rights to privacy, to protection of personal data and confidentiality of private communications and records. […] § 4 Decree will regulate the procedure for verification of infractions of the provisions in this article. (BRAZIL, 2015).

1. LEGAL PROTECTION OF THE FUNDAMENTAL RIGHT TO PRIVACY AND PERSONAL DATA IN THE BRAZILIAN REGULATORY SCHEME IN THE PRESENT CONTEXT

The Brazilian Constitution[4] is clear in recognizing as fundamental rights the inviolability of intimacy, privacy, honour and image of persons and securing the right to compensation for property or moral damages. On this particular issue, article 5, subparagraph XII, includes, in the list of fundamental rights, the inviolability of the secrecy of correspondence and telegraphic communications, data and telephone communications, except for the situations related to the production of evidence in a criminal investigation or a criminal procedural statements.

It is thus worth examining the normative Brazilian panorama within two distinct contexts: the first, without the internalization of a legal understanding about the Internet as a social and technological phenomenon and, the second, based on a legal understanding of the Internet.

1.1 Privacy and personal data protection in a context devoid of a legal understanding about the Internet

Before the popularisation of the Internet as a means for the dissemination of information and communication, the Brazilian constitutional standard, unlike other constitutions,[5] did not expressly recognize privacy protection in relation to computer databases. According to Limberger,[6] the closest legal concept that provides for data protection is the habeas data provision referred to in the article 5, subchapter LXXII[7] of the Brazilian Constitution, regulated by Law No. 9.507/97.

As highlighted by this author, the scope of the right to habeas data is however highly restricted because it ensures that only the knowledge of information on the part of individuals in relation to databases of government agencies or public character getting impaired is protected in relation to private institutions or in consumer relations.[8]

Nevertheless, Law No. 8.070/90, which established the Consumer Defence Code (CDC), equated consumer data records with those of any kind of public character entities, as noted in article 43, paragraph 4. In addition, the CDC expressed the protection of consumer access to information and

4 Article 5 - All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property, on the following terms:
[…]
X – the privacy, private life, honour and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured;
[…]
XII – the secrecy of correspondence and of telegraphic, data and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts; BRAZIL, 'Constituição Da República Federativa Do Brasil' (*Website Oficial do Planalto*, 1988) <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> accessed 23 February 2014.

5 The example of this, the Spanish Constitution provides, in article 18.4: "[…] la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" David López Jiménez, 'Los Códigos Tipos Como Instrumento Para La Protección de La Privacidad En El Ambito Digital: Apreciaciones Desde El Derecho Español' (2013) 11 Estudios constitucionales 575 <http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-52002013000200015&lng=en&nrm=iso&tlng=en> accessed 24 September 2014. p. 575-614.

6 Limberger T, *O Direito à Intimidade Na Era Da Informática: A Necessidade de Proteção Dos Dados Pessoais* (Livraria do Advogado 2007). p. 116-119.

7 Article 5 [...]:
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 con dential process, either judicial or administrative; […] BRAZIL, 'Constituição Da República Federativa Do Brasil.'

8 Limberger.

existing data in registers, sheets, personal records and consumption, in the most diverse sources of record. Another relevant aspect presented by the consumer regulation concerned the obligation of communication to the consumer in writing or the opening of registration, schedule, registration and personal data without the consumer's request.

In the sphere of criminal procedure law, Brazilian law takes a timid approach with the protection of electronic and computer communications, however, not including specific limitations on the protection of personal data transmitted through such communications. Law No. 9.296/96, which regulates section XII of article 5 of the Brazilian Constitution, became popularly known as the 'wiretapping law'.

The 'wiretapping law' also refers to complementary Law No. 105/2001,[9] which provided the Brazilian legal system with articles that confer specific treatment for the secrecy of operations of financial institutions. According to the standard, banking information, such as deposits, payments, application values in investment funds, foreign currency transactions and credit card operations, are in the midst of operations that should be confidential; however, it maintained the exceptions provided for in this law.[10]

Within the legislative field of the Brazilian civil law, there is mention of the understanding of personality rights approved in Law No. 10.406/2002, which established the Brazilian Civil Code (BCC). According to this regulation, personality rights are indispensable, and no voluntary limitation on the exercise of these rights is allowed, except as provided in the law. Among the personality rights referred to by the BCC is the inviolability of the private life of the individual, including the possibilities of prevention and cessation of violations by judicial determination.

Thus, metadata, even if anonymous and protected by bank secrecy rules under Brazilian law, becomes vulnerable personal data that may allow identification of the person concerned, even if subject to legal protections, especially those relating to the protection of constitutional and civil law private life. In addition, there are also various possibilities of registering and processing data, including in an unlawful manner, by governments, businesses and individuals. Despite constitutional protection and the other regulations, there remains a need for better understanding of the Internet within the legal sphere to give more effectiveness to the protection of fundamental rights, as seen below.

1.2 Privacy and personal data protection in a context constituted from a legal understanding about the Internet

Different from the legal provisions mentioned above, Brazilian legal system has recently approved three laws that protect rights that consider the Internet as an environment worthy of legislative recognition: the Access to Information Act, in 2011; the Cybercrime Act, in 2012; and the Brazilian Internet Bill of Rights (Marco Civil da Internet), in 2014. In addition to the aforementioned legislation, it is relevant to consider, in the context of this research, a draft bill of rights on personal data protection, still being discussed in Brazil.

9 BRAZIL, 'Lei Complementar N.º 105, de 10 de Janeiro de 2001' (2001) <http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm> accessed 20 April 2015.

10 In the context presented, the mentioned Brazilian legal norms keep distancing situations linked to new phenomena provided by Internet in the information society. Just by way of example and to establish a relationship between the constitutional standards, consumer, banking and civil law, criminal procedure, respectively, cites a case observed in a recent study developed at the Massachusetts Institute of technology, published by De Montjoye et al. (2015) in the journal *Science*. The study entitled "*Unique in the shopping mall: On the reidentifiability of credit card metadata*" introduced the development of a mathematical algorithm that, installed inside the informational system of a financial institution, was able to collect anonymous, metadata stored under wraps, obtained from purchases made with credit cards at merchants. According to the results of the research, it was possible to identify a consumer by collecting data from, on average, four financial transactions by credit card.

The effect of Law No. 12.527/2011, generally known as the Access to Information Act, was to regulate access to information provided in articles 5, subparagraph XXXIII and 37, paragraph 3, subparagraph II, and 216, paragraph 2 of the Brazilian Constitution. The act applies to public agencies that are part of the direct administration of the Executive, Legislative and Judiciary, including the courts of Auditors and prosecutors, as well as local authorities, public foundations, public companies, joint stock companies and other institutions under the direct or indirect control of the Union, the States, the Federal District and the Municipalities, with extended application to private non-profit institutions that develop actions of public interest and receive public funds.[11]

It should be noted that the Access to Information Act is intended to ensure the fundamental right of access to information, observing basic principles of public administration, such as observance of advertising as a general precept, being an exception to the disclosure of confidential information of public interest, use of means of communication facilitated by information technology, among others.[12]

The right to access to information provided by the law in question is a mechanism for strengthening democracy and political participation. Thus, access to information is a prerequisite for full democracy because it is essential that citizens are informed or have sufficient knowledge about their participation in the democratic system.[13]

From a conceptual prism, the Access to Information Act represents a significant breakthrough for the Brazilian legal system, as it presents a list of definitions that are current and contemporary. This includes definitions of the terms 'information', 'personal information' and 'information processing'. This law understands 'information' as the "[...] data, processed or not, that can be used for production and transmission of knowledge, contained in any medium or format support". The definition for 'private information' corresponds to that "[...] related to identified or identifiable natural person". The concept of 'information processing' refers to the "[...] set of actions relating to the production, reception, classification, use, access, reproduction, transmission, distribution, archiving, storage, disposal, assessment, allocation or control of information".[14]

The Access to Information Act determines that the treatment of the personal information held by covered entities and institutions is carried out in a transparent manner, respecting the fundamental right to protection of the intimacy, private life, honour and image of persons, which, it is argued here, correspond to the protection of the fundamental right to privacy. The law imposes substantial restrictions of access to personal information, such as restricted access to information, the maximum period of one hundred years, the authorized public officials, as well as the possibility of access or disclosure to third parties upon prior consent of the holder of the information, except in the cases provided for in the regulation.

The second Brazilian contemporary legal standard relevant for the Internet context is Law No. 12.737/2012, also known as the Cybercrime Act, which amended the Brazilian Penal Code. This Act is relevant as an example of the terminology included in article 154-A, which defined the crime of computer hacking as "[...] Invading an alien computer device, connected or not to the computer

11 BRAZIL, 'Lei N.º 12.527, de 18 de Novembro de 2011' (2011) <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> accessed 20 April 2015.

12 ibid.

13 Fernando Galindo Ayuda, 'Democracia, Internet Y Gobernanza: Una Concreción. (Spanish)' (2012) 33 Revista Seqüência 33 <10.5007/2177-7055.2012v33n65>.from a legal perspective, about the reaching and the limits of the democratic usage of Internet, discussing: 1 p. 33-56.

14 BRAZIL, 'Lei N.º 12.527, de 18 de Novembro de 2011'.

network, through undue violation of safety and in order to obtain, alter or destroy data or information without the express or implied consent of the owner of the device or install vulnerabilities to gain an unlawful advantage".[15]

The third law from a normative scenario in contemporary Brazil is Law No. 12.965/2014, popularly called 'Marco Civil da Internet', adopted after broad collaborative debate in a global pioneering process and which established a Bill of Rights for the Internet in Brazil.

As noted, previously the access to data and the monitoring of the behaviour of Internet users were completely devoid of specific regulations, which had allowed the Internet to become a hostile environment where users could commit abuses or be the object of other violations of rights. An example of this is the deliberate collection of sensitive data, both in relation to information about the browsing history of Internet sites as well as the frequent request for time and content data by public authorities, without prior submission to judicial analysis.[16]

On this specific point, the Brazilian Internet Bill of Rights represents the largest normative civil advance directly linked to the use of the Internet in Brazilian civil life. It brought some of the legislative responses that have contributed to the strengthening of the Legal Democratic State and, in particular, the recognition of rights and their extension to the Internet.

The 'Marco Civil da Internet' did not only establish principles, guarantees, rights and obligations for the use of the internet in Brazil. It also established that the discipline of the use of the Internet in Brazil has its foundations in freedom of expression; a global recognition of the network; human rights, the development of personality and the exercise of citizenship in digital media; plurality and diversity, openness and collaboration; free enterprise, free competition and consumer protection; and the social purpose of the network.[17]

'Marco Civil da Internet' enshrined elementary principles for regulating the civil use of the Internet in Brazil. Thus, the discipline of its use in the country should follow the principles of the guarantee of freedom of expression, communication and manifestation of thought, in terms of the Brazilian Constitution; privacy protection; personal data protection, in the form of law; and preservation of net neutrality guarantees; the preservation of stability, security and functionality of the network, through means of technical measures compatible with international standards and by encouraging the use of good practices; accountability of agents according to its activities, in accordance with the law; the preservation of participatory nature of the network; the freedom of business models promoted on the Internet, provided that they do not conflict with other principles laid down by law.[18] Another important contribution of Law No. 12.965/2014 relates to the presentation of technical definitions that operate as facilitators of interpretative standards:

15 BRAZIL, 'Lei N.º 12.737, de 30 de Novembro de 2012' (2012) <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> accessed 20 April 2015.

16 Ronaldo Lemos, 'O Marco Civil Como Simbolo Do Desejo Por Inovação No Brasil' in George Leite and Ronaldo Lemos (eds), *Marco Civil da Internet* (Atlas 2014). p. 03-11.

17 BRAZIL, 'Lei N.º 12.965, de 23 de Abril de 2014.'

18 Full texts of these articles are in the footnotes 49, 50 and 51, where it can be understood in the specific context of this paper. ibid.

Term	Definition
Internet	the system made by the set of logical protocols worldwide, structured for public and unrestricted use, with the purpose of enabling communication of data between terminals through different networks
Terminal	the computer or any device that connects to the Internet
Internet Protocol address (IP address)	the code assigned to a terminal of a network to allow its identification, defined according to international parameters
Autonomous system administrator	the natural person or entity that administers specific IP address blocks and the respective routing system, duly registered in the national entity responsible for registering and distributing IP addresses geographically related to the country
Internet connection	enabling a terminal for sending and receiving data packets over the Internet, through the assignment of an IP address or authentication
Connection log	the set of information relating to the date and time of the beginning and end of an Internet connection, its duration and the IP address used by the terminal for sending and receiving data packets
Internet applications	the set of features that can be accessed through a terminal connected to the Internet
Records of access to Internet applications	the set of information relating to the date and time of use of the given Internet application, from the specific IP address

Source: Adapted from Brasil (2014).

The list of rights and guarantees for Internet users in Brazil is one of the strengths of the 'Marco Civil da Internet' because it gives greater effectiveness to the fundamental rights already enshrined in the Brazilian legal system before the advent of the Internet.

The Brazilian Internet Bill of Rights ensures users access to the Internet as an essential element of the exercise of citizenship, adopting the guarantee of the right to privacy and freedom of expression in communications as a condition for the full exercise of the right of access to the Internet. The rule of law also ensures the inviolability and protection of intimacy and privacy as well as indemnification for property or moral damage; the inviolability and secrecy of the flow of Internet communications, except when contrary to a court order; the inviolability and secrecy of stored private communications, unless contrary to a court order; the prohibition against providing personal data to third parties, including connection records and access to Internet applications, except through express and informed consent or as otherwise provided by law (Articles 3rd, 7 and 8)[19].
It is possible to observe, therefore, that the Brazilian Internet Bill of Rights relies on data protection on the Internet, requiring that information about the collection, use, storage, handling and protection of personal data be clear and complete; be limited to purposes that justify the collection; not be prohibited by legislation; and be specified in the service contracts or terms of use of Internet applications (Articles 10, 11, 13, 14, 15).[20]

Regarding the protection of personal data on the Internet, 'Marco Civil' welcomes the requirement of express consent on the collection, use, storage and processing of personal data, which should be noted more prominently than the other contractual clauses. 'Marco Civil' also provides for the possibility of permanent deletion of personal data that has been provided to a particular Internet application, at the request of the person concerned, at the end of the relationship between the parties, subject to the possibility of mandatory custody of records listed in the law (Article 22).[21]

Still, regarding the inviolability of personal data on the Internet as a guarantee of the fundamental right to privacy, 'Marco Civil' determines that the track and the availability of connection and

19 Full texts of these articles are in the footnotes 52, 53, 54, 55 and 56, where it can be understood in the specific context of this paper. ibid.
20 Full text of this article is in the footnote 57, where it can be understood in the specific context of this paper. ibid.
21 ibid.

access records to Internet applications as well as personal data and private communications content must preserve the intimacy, private life, honour and image of the parties directly or indirectly involved.[22]

In this sense, the provider responsible for guarding the data will only be obliged to make available the records autonomously or linked to personal data or other information that could contribute to the identification of the user or terminal by court order and proceed the same way with respect to the contents of private communications.[23]

There is another point that represents a normative evolution to the tutelage of rights on the Internet and responds, in part, to the frequent questions about the effectiveness of national regulation when it seeks to balance the sovereignty of States and the transnational character of the network. It concerns the determination that, in any operation of collection, storage, custody and treatment of personal data records, communication connections and providers of Internet applications, where at least one of these acts is occurring in the national territory, the parties must comply with Brazilian legislation and the rights to privacy, to protection of personal data and confidentiality of private communications and records considering that at least one of the terminals are located in Brazil, even if the activities are conducted by a legal person based abroad.[24]

There are however several articles of the Brazilian Internet Bill of Rights that should be submitted to regulation through a Presidential Decree. Among these are the measures and procedures of security and confidentiality that must be clearly informed by those responsible for the provision of services, in compliance with the standards set out in the regulation, respecting the right of confidentiality with regard to business secrets; the provision of information by providers and connectors of Internet applications, to allow verification regarding the fulfilment of the Brazilian legislation concerning the collection, guarding, storage or data processing as well as respecting the privacy and secrecy of communications; and the procedure for verification of infractions and the application of the penalties foreseen in the 'Marco Civil da Internet'.[25]

The discussion around the theme of the fundamental right to privacy protection and inviolability of personal data on the Internet does not end with 'Marco Civil da Internet', nor with the decrees that shall regulate the previously noted points. This is a discussion in progress from the call of contributions to the portal "Thinking the Law",[26] linked to the website of the Brazilian Ministry of Justice. Furthermore, as detailed below, in the same context, the process of receipt of contributions for a draft bill of rights on personal data protection was triggered.

Although explicit aspects related to privacy protection on the Internet are not present, the mentioned draft bill of rights on personal data protection in Brazil represents significant progress towards regulating the protection of data, in the same way as is happening with the regulation of aspects as laid down in the Brazilian Internet Bill of Rights.

As Doneda[27] notes, "[...]personal data protection is a guarantee of instrumental character, derived from the tutelage of privacy, but not limited to this, and that references a range of fundamental guarantees contained in the Brazilian legal system", especially with regard to legal norms formulated before the legal understanding of the Internet.

22 ibid.
23 ibid.
24 ibid.
25 ibid.
26 The debate on the regulation of the Marco Civil received contributions until April 30, 2015, on the Pensando o Direito platform (http://participacao.mj.gov.br/marcocivil/).
27 Doneda D, *Da Privacidade à Proteção de Dados Pessoais* (Renovar 2006) https://books.google.es/books?id=EHOkAAAACAAJ. p. 326.

In the way it was presented for consultation and public contribution, the draft bill of rights on personal data protection aims at the application of a standard to any processing operation performed through automated, wholly or partly by natural persons or legal persons governed by public or private law, regardless of the country of its headquarters and in the country where the database is located, provided that the processing operation is carried out within the national territory; or to personal data that has been collected in the national territory, except for the cases in which the processing of the data was performed by a natural person for personal purposes only; or held for journalistic purposes only.[28]

By comparative analysis of European policies, it turns out that the list of definitions of the draft bill of rights on personal data protection is significant and consistent enough to encompass several factual assumptions related to how the draft defines data processing. It should be noted that the draft welcomes the Brazilian concept of consent as an element of personal data protection.[29]

The principles related to purpose are directly linked to the data processing concept, which ensures that these should be processed with legitimate, specific purposes that are explicit and known by the data subject, going against the principle of transparency, which ensures clear and appropriate information about the completion of processing. In addition, the principle of adequacy suggests that processing should be compatible with those purposes and with the legitimate expectations of the data subject, according to the context of the processing.[30]

The principle of necessity notes that processing should be limited to the minimum necessary to carry out the desired purposes, including that data are relevant, proportionate and not excessive, in the same proportion in which the principle of security determines that technical measures must be used and constantly administratively updated, proportionate to the nature of information handled and able to protect personal data from situations of unauthorized access and accidental or illicit destruction, loss, alteration, communication or dissemination. In this sense, it is essential to apply the principle of prevention, which determines the need to adopt measures to prevent the occurrence of damage due to the processing of personal data, taking into consideration the existing risks.[31]

The principle of free access ensures the free and facilitated consultation by the data subjects on the modalities of processing and about the completeness of personal information. This allows application of the principle of data quality, which ensures the requirement of accuracy, clarity and updating of the data, in accordance with the frequency required for the fulfilment of the purpose of their processing, and the observance of the principle of non-discrimination, which ensures neutrality in the processing of the data, which cannot be carried out for discriminatory purposes, linking the concern expressed in the nucleus of the draft regarding sensitive personal data.

28 BRAZIL, 'Anteprojeto de Lei Para a Proteção de Dados Pessoais' (*Pensando o Direito*, 2015) <http://participacao.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/> accessed 28 April 2015.

29 According to Doneda (2006, p. 375), the "[...] reflection on the role of consent to the processing of personal data is required to remove him from a position in which, anchored in technicality, he could neutralize the action of fundamental rights". Like this "[…] The consent to the processing of personal data comes directly elements of own personality, however lacks these elements. It assumes more properly the robes of a unilateral act, the effect of which is to authorize a particular treatment for personal data" (DONEDA, 2006, p. 377-378). Doneda D, *Da Privacidade à Proteção de Dados Pessoais* (Renovar 2006) <https://books.google.es/books?id=EHOkAAAACAAJ>

30 BRAZIL, 'Anteprojeto de Lei Para a Proteção de Dados Pessoais.'

31 ibid.

2. PRIVACY AND PERSONAL DATA PROTECTION ON THE INTERNET IN THE CONCEPT OF 'INTERNET PRIVACY RIGHTS'

To begin this section, it is important to clarify that this research is linked to the category of rights developed by Bernal,[32] which consists of not only the recognition of the right to privacy on the Internet but also the definition of a set of 'Internet privacy rights'.

Currently, it has become incredibly difficult to separate data and information online and offline. As the Internet has become more integrated with the 'real world', data online and offline are easily mingled. A typical example of some data generated in the 'real world' being used in cyberspace can be observed in the case of the British Tesco supermarket network. From the Tesco Clubcard[33], a loyalty program created by the network, it is possible to collect data from purchases made in the 'real world' that are mapped and crossed with purchases made on the Internet.

In that sense, this paper supports the need to recognize rights for the effective legal protection of privacy and personal data on the Internet, particularly the incorporation of the concept of 'Internet privacy rights' as one of the pillars of the regulation of personal data protection in Brazil, thus seeking greater effectiveness of the fundamental right to privacy. However, for this purpose, it is relevant to note the rights identified by the doctrine for which contextual adjustments are performed under Brazilian law.

Thus, four rights are presented, which transcend the meaning of legal rights, as they represent real desires understood and considered by the people as their rights, especially from the perspective of protecting the autonomy of each individual. The following are considered the four rights that constitute Internet privacy rights: (i) the right to roam the Internet with privacy; (ii) the right to monitor those who monitor us; (iii) the right to delete personal data; and (iv) the right to an identity online.[34]

The first right binds to the possibility of navigation for web pages – whether in the search for information, the search for data, or the purchase of products on e-commerce platforms – with the reasonable expectation of doing so with privacy, not as an absolute standard, but as a general rule.[35]

Regarding this right, it should extend beyond search engines, also reaching any other navigation service, such as Internet Service Providers. The formal recognition of the right to roam the Internet with privacy could generate inevitable conflict with governmental practices, especially with regard to surveillance[36] and data retention.

The recognition of the right to roam the Internet with privacy does not represent a 'carte blanche' to operate without balance, without proper accountability or without consequences for each act

32 BERNAL, P. *Internet Privacy Rights: Rights to Protect Autonomy*. Cambridge (UK): Cambridge University Press, 2014. p. 15-19.

33 In this way, the network began to store details of every consumer in the United Kingdom, from the domicile to a range of demographic characteristics, socioeconomic and lifestyle. By means of an artificial intelligence system called *Zodiac*, it was possible to create intelligent profiles and segmentation of customer data. Thus, the client profile can be classified as his or her enthusiasm for promotions, fidelity to brands and other buying habits. On top of that, the company went on to sell access to the database named *Crucible* to companies from different segments, such as Sky (paid TV), Gillette (razors and cosmetics) and Orange (television and Internet services provider). Together, the *Crucible* and the *Zodiac* can generate a map of how an individual often thinks, works and shops. Furthermore, the map is able to classify consumers in 10 categories: (i) wealth; (ii) promotions; (iii) trips; (iv) charity; (v) 'green' consumption; (vi) financial difficulties; (vii) credit; (viii) lifestyle; (ix) habits; (x) adventures. BERNAL, P. *Internet Privacy Rights: Rights to Protect Autonomy*. p. 06.

34 BERNAL, P. *Internet Privacy Rights: Rights to Protect Autonomy*. p. 15-19

35 BERNAL, P. *Internet Privacy Rights: Rights to Protect Autonomy*. p. 140-142.

36 MORAIS, José Luis Bolzan; NETO, Elias Jacob. A insuficiência do Marco Civil da Internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da surveillance. In: LEITE, G; LEMOS, R (Org.). . *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 417–439.

committed on the network, which connects with the second right that makes up the core of the 'Internet privacy rights'.

The second right, which complements the previous one, concerns the right to know who monitors what, when and for what purposes. There are situations in which individuals want to be monitored, as it may be beneficial for some reason. From the perspective of privacy protection, data collection and constant monitoring might be absolutely negative acts, but under the prism of the symbiotic web there are acts that are absolutely beneficial to the usability of the network by the user.[37]

Given this conceptual and antagonistic impasse, users have a right to know what precisely is being tracked, logged, stored and analysed and when, by whom, and for what purpose. Monitoring the monitors means more than simple knowledge of what data are being collected. It is about the individual knowing if they are being monitored, possibly even without retention of data and information, and for what purpose such an act is intended. This is to establish a principle of collaborative consent, with the consent considered immediate, interactive, dynamic, and binary, within the processes of interaction on the Internet.[38]

The third right is about deleting personal data and deserves important differentiations. Some authors brought to light the expression the 'right to be let alone', employed by Cooley and reproduced by Warren and Brandeis (1890) providing the beginning of the recognition of the right to privacy[39].

However, such an expression is often understood as a synonym of a right already recognized, including under Brazilian law, namely, the right to be forgotten. However, according to the Brazilian conception of "forgotten" in Criminal Law,[40] the right to be let alone can not be confused with the right to be forgotten, as it is akin to the concept used by Bernal,[41] i.e., as it goes beyond the mere protection of private life, giving the possibility of deleting user data and personal information from the Internet.[42]

Complementary to the previous form, a fourth right is divided into three fronts: the right to create an online identity; the right to assert that online identity; and the right to protect that online identity. The relationship between privacy, identity and autonomy is complex, subtle and always evolving, particularly considering that the relations established on the Internet require, in one way or another, an identity, such as a username, to be used on social networks, to access online banking services, or to play online.[43]

What the identity reveals about the 'real person' behind the 'virtual' individual is a matter assigned exclusively to the law of that individual in determining such 'real' information. In some places and

37 BERNAL, P. *Internet Privacy Rights: Rights to Protect Autonomy*. p. 172-175.
38 BERNAL, P. *Internet Privacy Rights: Rights to Protect Autonomy*. p. 172-175.
39 BERNAL, P. *Internet Privacy Rights: Rights to Protect Autonomy*. p.200-206.
40 According to article 202 of Brazilian Penal Execution Act, the 'right to be forgotten' could be applied when fulfilled or extinguished worth, and in this context, should not be included in certificates or certificates provided by police authority or court officials any news or reference to condemnation. BRAZIL, Lei No. 7.210, de 11 de julho de 1984. Institui a Lei de Execuções Penais no Brasil 1984.
41 BERNAL, P. *Internet Privacy Rights: Rights to Protect Autonomy*. p.200-206
42 The question of the application of 'a' right to be forgotten was subjected to the analysis of the Court of Justice of the European Union, sued by the Spanish judiciary. This issue was raised in a lawsuit brought by the Spanish lawyer Mario Costeja *versus* Google, with the goal of deleting an article of the newspaper La Vanguardia, dating from 1998, which made reference to an auction of real estate and a garnishment for debts to the social security system. In that circumstance, the General Advocate of the European Union expressed his opinion of the failure to apply the right to be forgotten in cases of this nature. Due to this type of demand, Google has set up what he called 'Advisory Council to Google on the Right to be Forgotten' formed by *experts* in the subject. After a job schedule that included meetings and hearings with interested parties, the Advisory Council issued, on February 6, 2015, a 44-page report, with recommendations on what the company of information and communications technology can do in cases of requisition of right to be forgotten. GOOGLE. *Report of The Advisory Council to Google on the Right to be Forgotten Members of the Council*. San Francisco, EUA: [s.n.], 2015. Disponível em: <https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view>.
43 BERNAL, P. *Internet Privacy Rights: Rights to Protect Autonomy*. p. 250-262.

in some situations, the connection between the 'real' identities and 'virtual' identities needs to be shown clearly and explicitly, but these situations are less frequent than the systematic operation businesses generally suggest. In other words, the Internet, which adopts as standard rule a policy of 'real names', is the same in which the privacy and autonomy of people are needlessly compromised. Thus, a change of paradigm, relevant in the author's view, resides precisely in reversing the rule, the requirement of real identities being the exception.[44]

The amount of information that an Internet user needs to reveal to access a service or system should, in general, be minimized. The idea of minimized disclosure – and that includes the disclosure of online identity as a set of personal information – with the design data minimization configures a key aspect for a data protection regime and a crucial part for the privacy of the data on the Internet. Therefore, privacy on the Internet is primarily related to the protection of identities, whereas autonomy addresses the control of these identities by their holders.

3. THE CONCEPTUAL INCORPORATION OF 'INTERNET PRIVACY RIGHTS' IN REGULATING PRIVACY AND PERSONAL DATA PROTECTION IN BRAZIL

As stated earlier, this paper seeks to present as a proposal for the conceptual incorporation of Internet privacy rights as a way of contributing to the impending regulation of 'Marco Civil da Internet', specifically with regard to the protection of privacy and personal data protection through a special Bill of Rights in Brazil.

For analytical purposes, the research mapped and classified five categories of legal issues present in legal norms related to privacy and personal data protection on Internet in Brazil, Europe and the U.S.: (i) articles with interpretative criteria, definitions and recommendations of general principles; (ii) articles that feature the scope, limits and exceptions in the application of the standard under review; (iii) articles that list the holder's rights in the broad sense and/or rights to the data and personal information; (iv) articles that present the scope and limits of the processing of personal data; and (v) articles that establish the functioning of the competent autonomous authority, compliance with the standards of protection of personal data, the requisitions and processing of the penalties in the event norms are transgressed.

Based on this mapping, the research sought to elucidate that the impending regulation of privacy and protection of personal data on the Internet, whether through a Presidential Decree that will regulate the Brazilian Internet Bill of Rights or through a general Bill of Rights on personal data protection in Brazil, will have best and greatest opportunities to reach and ensure the fundamental right to privacy if it is built by the conceptual incorporation of 'Internet privacy rights', i.e., recognition and explicit insertion and expression of the Internet privacy rights amid legal norms of protection of rights in the legal relations established on the Internet and in spaces off the Internet, as a means of access to information and data.

Considering this fact, this research applied the standards mapped by implicit identification of the four rights, which constitute the concept of Internet privacy rights, which are inserted into each of the five categories of legal articles. This is the first chance to address the problem of research that suggests that Internet privacy rights may be implicit in the Internet-related legal rules in Brazil, to ensure greater magnitude in the effectiveness of the fundamental right to privacy.

44 BERNAL, P. *Internet Privacy Rights: Rights to Protect Autonomy*. p. 250-262.

It is worth emphasizing that the understanding of the fundamental right to privacy in this research considers the scope of the legal protection of private life, intimacy, honour and image and inviolability of personal data. In this sense, this research assumes that the amplitude in the effectiveness of the fundamental right to privacy, so understood, lacks the conceptual incorporation of Internet privacy rights.

Furthermore, as demonstrated throughout the research, the omission or even the implied presence of Internet privacy rights weakens the effective protection of the fundamental right to privacy, as noted in the case 'Xuxa vs. Google',[45] involving the right to be forgotten and Google's initiative to set their own parameters for requests to delete personal data stored in its database. Moreover, it is relevant to note the recent publication of an open letter to Google, signed by 80 researchers of cyberlaw, seeking more transparency from the company with regard to the processing of requests to apply the right to be forgotten.[46]

Despite the regulatory evidence providing a poorly representative number with regard to the right to delete the personal data, which joins the right to be forgotten, legal articles have had a significant impact on the legal protection of the right to privacy and the protection of personal data. One example is Regulation 45/2001/EC, which addresses the rights of the person concerned, i.e., the holder of the personal data, explicitly features the possibility of exclusion of the data (article 16).[47] However, such a possibility does not take into consideration data exclusions for intimate reasons and data that are not the result of a tort committed by another person, confirming the implied and partial presence of the right to delete personal data. In the same vein as the current European regulation is the draft bill of rights on personal data protection in Brazil.[48] In this document, it is possible to identify the implicit and partial right mentioned regarding the deletion of data and the limitations of its preservation, which would occur only after the processing of such data.

Most of the legal provisions related to the theme of privacy and data protection focus on topics that treat the autonomous authority as competent to manage the standards of protection of personal data as well as the procedural issues and penalties. Within these themes, which make up the fifth category, it is predominantly observed, although partial and implicitly, that the right to monitor those who monitor us serves as a kind of guardianship of the accountability of regulatory compliance vis-à-vis the subjects involved. Partiality referred to here is support based on the evidence of comparative legislation because the regulatory articles exclusively treat how the data are to be monitored and by whom are monitored, not extending this information to the right of the subject monitored to know further details of the registration of personal data, as the right in question is assumed.

45 The case involving Maria da Graça Xuxa Meneghel (Brazilian celebrity known by TV shows for children) *versus* Google Brazil Internet Ltda., in which the author of the lawsuit sought the removal of all search results involving a search using the terms "xuxa paedophile" or any others that have relation with her name. In the end, the site searches were victorious, the absence of recognition, in this case, the right to be forgotten, on account of the impossibility of the search engine perform the removal of the content intended by the author of the action (it should be noted that the decision of the Superior Court of Justice established itself in information technology and not on legal grounds themselves).

46 Ellen Goodman and Julia Powles, 'Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data — Medium' (2015) <https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd> accessed 15 May 2015.

47 Article 16. Erasure. The person concerned has the right to obtain from the controller the erasure of data if their processing is unlawful, in particular in case of violation of the provisions of sections I, II and III of chapter II Regulamento (CE) No. 45/2001, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e orgãos comunitários e à livre circulação desses dados 2001 22.

48 Article 15 – the personal data will be cancelled upon termination of their treatment, authorized the conservation for the following purposes:
I – compliance with legal obligation by the guardian;
II – historic, scientific or statistical research, guaranteed, whenever possible, the dissociation of personal data; or
III – transfer to third parties, in accordance with this Law.
Sole paragraph – the competent body may establish specific hypotheses of conservation of personal data guaranteed the rights holder, except for the provisions in specific legislation. BRAZIL, 'Anteprojeto de Lei Para a Proteção de Dados Pessoais.'.

These facts are evident in the regulations of the Head Office of Anglo-Saxon law, in parts IV (Exceptions), V (fulfilment) and VI (Miscellaneous and General Aspects) of the Data Protection Act 1998, in articles 30 (procedures for compensation for breach of the regulation) and 31 (compliance with part V of the Data Protection Act 1998) of the Privacy and Electronic Communications (EC Directive) Regulations 2003, both the United Kingdom, in the area of accountability of certain disclosures the Privacy Act 1974, in titles I (strengthening of national security against terrorism) and II (strengthening the surveillance procedures) of the USA Patriot Act, both of the United States.

Within the European Union, it is noted that the same bias above referred to in chapter II (general conditions of lawfulness of the processing of personal data), section IX (notification for control purposes of processing of personal data), in chapter III (judicial remedies, liability and sanctions), in chapter V (codes of conduct), in chapter VI (control authority) and in chapter VII (implementing Community measures) of the 95/46/EC Directive. In the same direction is the evidence found in chapters V (independent authority of control – European Data Protection) and VI (final provisions) of Regulation 45/2001/EC.

Aspects linked to the first category, which concerns the description of topics, definitions and interpretative criteria general principles are not legal norms in priority, although it is in that category that highlights the implicit presence of the right to roam the Internet with privacy and the right to an identity online.

Generally speaking, only within the legal chapters that address the rights of the person concerned, or the holder of the personal data, or even the user-specific Internet case of 'Marco Civil da Internet', are all four rights that make up the concept of Internet privacy rights partially and implicitly identified. Thus, it is useful to elucidate the way the Brazilian Internet Bill of Rights and the draft bill of rights on personal data protection consider Internet privacy rights.

Article 3 of 'Marco Civil da Internet'[49], presenting the guiding principles of the use of the Internet in Brazil and listing one of these as privacy and protection of personal data (these in the form of law, i.e., lacking specific regulation), implicitly assumes the first right, which is to roam the Internet with privacy. In addition to the above legal topics, articles 7[50] and 8[51]are the first right, noting that regarding access to the Internet, i.e., network browsing, the user must ensure the inviolability of intimacy and privacy as well as the inviolability and secrecy of communications stream over the Internet, in addition to the private communications stored. Also covered in this article re the prohibition of the supply of personal data to third parties.

In article 5 of the Marco Civil da Internet, where definitions that determine the interpretation of this rule of law are presented (see the table previously presented), it is possible to identify important elements to sustain, albeit implicitly, the right to monitor those who monitor us, identified in arti-

49 Art. 3rd discipline the use of Internet in Brazil has the following principles:
[…]
II-privacy protection;
III-protection of personal data, in the form of law; […] BRAZIL, 'Lei No. 12.965, de 23 de Abril de 2014.'.

50 Art. 7 Internet access is essential to the exercise of citizenship, and the user is granted the following rights:
I-inviolability of intimacy and privacy, your protection and compensation for material or moral damage resulting from your infringement;
II-inviolability and confidentiality of their communications over the Internet, except by court order, in accordance with the law;
III. inviolability and secrecy of their private communications stored, except by court order; […]

51 Art. 8. The guarantee of the right to privacy and freedom of expression in the communications is a condition for the full exercise of the right of access to the Internet. ibid.

cles 10[52], 11[53], 13[54], 14[55], 15[56] and 22[57]. The combination of article 5 with these shows how Internet users can potentially be identified (from the Internet protocol address) and connection records of Internet applications, properly defined and delimited in article 5. Under the normative assumption adopted by the European Union, which serves as a basis for the draft bill of rights on personal data protection in Brazil, the data that permit the identification of the subject in question receives the assignment of personal data. Thus, it is important that the connection records and Internet applications are also understood as personal data. Greater clarity in this particular aspect is evidenced in sections VIII and IX of article 7[58], which seeks to impose the requirement of access to information based on the limitations of guarding and personal data storage on the Internet.

Similar to European standards, the 'Marco Civil da Internet' presents a significantly restricted possibility of applying the right to delete the personal data on the Internet. This possibility is provided for in article 7, subparagraph X[59], which restricts the deletion of data to the hypothetical end of the contractual relationship between the user and the Internet application, at the request of personal data, except in the cases of mandatory custody of the records provided by law.

The fourth right, namely, the right to an online identity, unlike others, is identified with significant restrictions on its implicit character because there is a greater distance with the concept of the right in question. This right may be observed in two articles of the text of 'Marco Civil da Internet': in article 10, addressing the protection of private life, intimacy, honour and the image, which are

52 Art. 10. The custody and the availability of connection records and access to Internet applications contemplated in this law, as well as personal data and private communications content must meet the preservation of intimacy, private life, honour and image of the parties directly or indirectly involved.
§ 1 the provider responsible for guard will only be obliged to make available the records mentioned in the caput, autonomously or linked to personal data or other information that could contribute to the identification of the user or terminal, by court order, in the manner provided in section IV of this Chapter, comply with the provisions of art. 7.
§ 2 the contents of private communications may only be available upon court order, in the cases and in the manner established by law, respected the provisions laid down in sections II and III of art. 7.
§ 3 the provisions of the heading do not prevent access to registration data to inform personal qualifications, affiliation and address, in the form of law, administrative authorities having legal competence for your request.
§ 4 the measures and procedures for security and confidentiality should be informed by the person responsible for service provision clearly and meet the standards set in regulation, respected their right to confidentiality as the business secrets.

53 Art. 11. In any operation of collection, storage, custody and treatment of personal data records or communications connection and providers of Internet applications in which at least one of these acts from occurring in the national territory, shall be compulsorily complied with Brazilian legislation and the rights to privacy, to protection of personal data and confidentiality of private communications and records.
§1 the caput shall apply to data collected in the national territory and the content of communications, provided that at least one of the terminals are located in Brazil.
§ 2 the provisions of caput applies even if the activities are carried out by legal person based abroad, since the public service offer Brazilian or at least one member of the same group owns establishment in Brazil.
§ 3 The connection providers and Internet applications must provide, in the form of regulations, information allowing the verification regarding the fulfilment of the Brazilian legislation concerning the collection, to guard, to storage or processing of data, as well as regarding the respect to privacy and to secrecy of communications. ibid.
§ 4 Decree regulating the procedure for verification of infringements of the provisions of this article.

54 Art. 13. In the provision of Internet connection, it is the responsibility of the system administrator as its duty to maintain connection records, confidential, in a controlled environment and security for a period of 1 (one) year, pursuant to regulation.
§ 10 responsibility for maintenance of connection records cannot be transferred to third parties. ibid.

55 Art. 14. In the provision of connection, onerous or free, it is forbidden to keep the records of access to Internet applications. ibid.

56 Art. 15. The provider of Internet applications constituted in the form of legal entity and who performs this activity in an organized way, professionally and with economic purposes should keep their records of access to Internet applications, under wraps, in a controlled environment and security for a period of 6 (six) months, in accordance with regulation. ibid.

57 Art. 22. The interested party may, with the purpose of forming probative set in civil or criminal judicial proceedings, in incidental character or as request the judge to order the guard responsible for the provision of connection records, or records of access to Internet applications. ibid.

58 Art. 7 Internet access is essential to the exercise of citizenship, and the user is granted the following rights:
[…]
VIII-clear information and complete about collection, use, storage, handling and protection of personal data, which can only be used for purposes that: the) justify its collection; (b)) are not prohibited by the legislation; and c) are specified in the service contracts or in terms of use of Internet applications; IX-express consent regarding collection, use, storage and processing of personal data, which should occur prominently to the other contractual clauses; ibid.

59 Art. 7 Internet access is essential to the exercise of citizenship, and the user is granted the following rights:
[…]
X-final deletion of the personal data that you have provided to certain Internet application, at its request, at the end of the relationship between the parties, subject to the possibility of mandatory Guard records provided for in this law; ibid.

elements that make up the personality of the individual, and article 23[60], when judicial arrangements are expressed to the guarantee of the confidentiality and preservation of the intimacy, private life, honour and image of the Internet user.

Although in its early stages of construction and discussion, the draft bill of rights on protection of personal data was presented as an institutional agenda of the Brazilian Ministry of Justice, it is important to emphasize that, in the same manner as noted above-mentioned legislations, the presence of Internet privacy rights is also partial and implicit in the text of the draft.

In chapter II of the draft, which sets out the requirements for the processing of personal data, it is observed that, when presenting the conditions of consent to the processing of personal data[61], including underage holders[62]as well as the information on the treatment of personal data at the time

60 Art. 23. It is up to the judge to take the necessary measures to guarantee the confidentiality of information received and the preservation of intimacy, private life, honour and image of the user, and can determine under law, including the requests for registry guard. ibid.

61 Art. 7. The processing of personal data is allowed only after the free consent, express, specific and informed of the holder, except as provided in art. 11.
§1 the consent to the processing of personal data cannot be a condition for the supply of a product or service or for the exercise of law, except in cases in which the data is indispensable for its implementation.
§ 2 it is forbidden the processing of personal data whose consent has been obtained by mistake, fraud, State of necessity or duress.
§3 the consent must be provided in writing or by other means that ensure.
§ 4 the consent must be given prominently to the other contractual clauses.
§ 5 the consent should refer to certain purposes, being nil generic authorisations for the processing of personal data.
§ 6 the consent can be revoked at any time, at no charge to the holder.
§ 7 shall void the provisions establishing the holder obligations wicked, abusive, which put him at a disadvantage in exaggerated, or that are incompatible with good faith or fairness.
§ 8 the charge the burden of proof that the consent of the owner has been obtained in accordance with the provisions of this law. BRAZIL, 'Anteprojeto de Lei Para a Proteção de Dados Pessoais.'

62 Art. 8. The holder of personal data between the ages of twelve and eighteen years old may provide consent to treatment that respects their peculiar condition of developing person, subject to the possibility of withdrawal of consent by the parents or legal guardians, in your best interest. ibid.
Art. 9. In the case of the holder of personal data with age up to twelve years of age, the consent will be provided by the parents or legal guardians, and must respect their peculiar condition treatment of developing person. ibid.

of consent[63], circumstances that dispense with the consent[64],[65] treatment and security measures on sensitive data[66] the draft causes an interaction between rights to roam the Internet with privacy and the right to monitor those who monitor us.

Thus, as mentioned in relation to previous standards, the draft bill of rights on personal data protection in Brazil focuses on articles that address the fulfilment of standards of protection of personal data, procedural issues and penalties, as seen in chapters IV (communication and interconnection), V (international transfer of data), VI (liability of agents) and VII (administrative penalties). Therefore, there is the predominance, although partial and implicit, of the right to monitor those who monitor us, which plays a kind of guardianship of the accountability of regulatory compliance

63 Art. 10. At the time of the provision of consent, the holder will be informed in a clear, appropriate and ostentatious about the following elements:
I – specific purpose of treatment;
II – form and duration of treatment;
III – identification of the person responsible;
IV – contact information of the person responsible;
V – subjects or categories of subjects to whom the data may be communicated, as well as scope of dissemination;
Vi – responsibilities of the agents will perform the treatment; and
VII – the rights holder, with explicit mention to:
the) possibility of not providing consent, with explanation about the consequences of negative, subject to the provisions of §1 of art. 6;
b) possibility of accessing the data, rectify them or revoke the consent procedure free and facilitated; and
c) possibility to report to the competent body the violation of provisions of this law.
§1 it is considered null the consent if the information misleading content or have not been presented clearly, appropriately and ostentatious.
§ 2 in case of a change of information referred to in subparagraphs I, II, III or V of the caput, the person responsible must obtain new consent of the holder, after highlighting specifically the content of updates.
§ 3 in the event of amendment of information referred to in item IV of the caput, the responsible must inform the holder contact information updated.
§ 4 in the activities that matter in continuing personal data collection, the holder should be informed regularly about the continuity, as defined by the competent body. ibid.

64 Art. 11. The consent shall be discharged when the data is unrestricted public access or when processing is indispensable for:
I – compliance with a legal obligation by the guardian;
II – treatment and shared use of data relating to the exercise of rights or obligations provided for in laws or regulations by public administration;
III – implementation of pre-contractual procedures or obligations related to a contract which is part the holder, subject to the provisions of §1 of art. 6;
IV – historical, scientific research or statistics, guaranteed, whenever possible, the dissociation of personal data;
V – regular exercise of rights in judicial or administrative proceedings;
Vi – protection of life or physical safety of the holder or third party;
VII – protection of health, with procedure performed by health care professionals or by health authorities.
§1 in chance of waiver of consent, the data shall be processed exclusively for the purposes provided for and by the smallest amount of time possible, according to the General principles laid out in this law, guaranteed the rights of the holder.
§ 2 in the case of application of the provisions laid down in sections I and II, advertising will be given to these cases, in accordance with paragraph 1 of art. 6.
§ 3 in case of non-compliance with the provisions of § 2, the operator or the data controller may be held responsible. ibid.

65 Art. 12. It is forbidden the treatment of sensitive personal data, except:
I – with provision of special consent by the holder:
the) upon demonstration of its own, distinct from the manifestation of consent on the other personal data; and
b) with prior and specific information about the sensitive nature of the data to be treated, with alert about the risks involved in treating this kind of data; or
II – without providing the consent of the owner, when the data is unrestricted public access, or in cases in which is indispensable for:
the fulfilment of a legal obligation) by the guardian;
b) treatment and shared use of data relating to the regular exercise of rights or obligations provided for in laws or regulations by public administration;
c) historical, scientific research or statistics, guaranteed, whenever possible, the dissociation of personal data;
d) regular exercise of rights in judicial or administrative proceedings;
e) protection of life or physical safety of the holder or third party;
f) guardianship of health, with procedure performed by health care professionals or by health authorities.
(1) the provisions of this article shall apply to any treatment capable of revealing sensitive personal data.
§ 2 the treatment of sensitive personal data cannot be accomplished at the expense of the holder, subject to specific legislation.
§ 3 in case of application of the provisions in items ‹ a ‹ and ‹ b ‹ by public agencies and entities, will be publicised to the waiver of consent pursuant to § 1 of art. 6. ibid.

66 Art. 13. The competent body may establish additional safety measures and protection to sensitive personal data, which shall be adopted by the responsible or by other treatment agents.
§ 1 may be subject to the prior authorisation of the competent body, in accordance with regulation.
§ 2 The processing of personal data shall be disciplined by biometric competent organ, which will have about hypotheses in which biometric data are considered sensitive personal data. ibid.

vis-à-vis the subjects involved. Additionally, the bias also lies exclusively in the way data is monitored and by whom the data are monitored, not showing any prediction on the possibility that the holder will have greater knowledge about the registration of personal data considering the right in question.

CONCLUSIONS

The conceptual proposition of Internet privacy rights defended in this research cannot be limited to a mere recognition as conceptual category. We must seek the explicit inclusion and expression of Internet privacy rights in the process of construction of norms related to the theme as a means to improve the effectiveness of the fundamental right to privacy, in this case, in the context of the Internet. The four rights, individually, have great relevance to the full understanding of the theme of the Internet privacy rights. However, such rights associated with each other assume even greater importance, especially when combined in the context of the infringement of personal data.

The reception of the expressed Internet privacy rights, from rights jointly considered by legal rules that care, and yet will care related issues in Brazil, allows the recomposition of the core of the fundamental right to privacy that, according to the theories presented in this research, incorporating only the protection of privacy, honour, intimacy, image and personal data. In other words, the fundamental right to privacy should also integrate into its nuclear structure Internet privacy rights.

However, for this larger dimension of the fundamental right to privacy to be fully reached, it is relevant to consider Internet privacy rights, as captured in the four rights discussed above, when associated with each other, which assume significant importance, regarding the incorporation of these rights in the construction a normative concept linked to the theme of the protection of privacy and personal data on the Internet in Brazil.

The implementation of the right to roam the Internet with privacy, in the phase of data collection on the web, as seen in the Brazilian Internet Bill of Rights, when dealing with the care of and connection records of Internet applications, like the draft bill of rights on personal data protection, does not ensure full protection of the right to the Internet connection or the access to Internet applications with the fullness of the exercise of the right to privacy.

Thus, the way in which current legal provisions protect the navigation for web pages does not meet the reasonable expectation of privacy, as a general rule, especially by not allowing the full exercise of the autonomy of the Internet user to set, when Internet connection or when access to Internet applications what data can be collected, under what circumstances, for what purposes and with which treatment limitations and interconnection.

At this point, the first right associates itself with the right to monitor those who monitor us, which in turn must be applied in the phase of use of the data. Just as there are circumstances linked to the right to navigate the Internet with privacy, there are situations in which individuals want to be monitored, as they may be beneficial for some reason. In this respect, the consent of personal data collection is basic element for the understanding of these rights.

From the perspective of privacy protection, data collection and monitoring as a standard constant are acts which, a priori, violate rights. However, under the prism of symbiotic web, in which the provision of personal data can be beneficial to the usability of the network, the user's autonomy in issuing its consent is crucial.

Thus, 'monitoring the monitors' means more than simple knowledge of what data are being collected, as it is currently applied in the privacy policies of organizations that collect and process personal data, or as set forth in the 'Marco Civil da Internet', or even as proposed by the draft bill of rights on personal data protection in Brazil..

It can be also associated with the right to delete personal data on the Internet during the personal data retention phase, when it surpassed the phases of collection and use of data, from the application of two rights previously associated. Thus, the implementation of this right, especially when related to right to the 'right to be forgotten' must occur in the phase in which the personal data are already stored. At this point, it is necessary to emphasize the identification of a gap in all legal provisions examined, both the Brazilian as foreign regulation, which, when relating to the possibility of deleting personal data, restrict this possibility to the possible unlawfulness in the use of such data.

Thus, conceptually, the right to incorporate the deletion of personal data does not mean strengthening possible censure or attempts to rewrite history, but gives users more control over their personal information and stimulates companies and governments to exclusively own appropriate and useful data to meet particular purposes, thus avoiding risks of damages or overexposure of data and personal information.

Finally, the concept of an online identity protection means that the protection of the identity of the Internet user, as presented in the Brazilian Internet Bill of Rights and in the draft on personal data protection, should contemplate a right to create an online identity, a right to assert that online identity, and a right to protect that online identity. This right will strengthen the autonomy of the Internet user, in particular to define which data linked to his or her online identity will be collected, as well as by whom that data will be collected and for what purposes and limits they will be collected.

The flow described above is appropriated for the definitions set out in article 5 of the 'Marco Civil da Internet' to describe the steps that lead the user to Internet access and applications contained therein. Despite keeping a technical appearance and exclusively linked to ICTs, the steps that comprise the Internet connection and access to its applications maintain a significant closeness with the right, with the prospect of fundamental rights presented in this research, especially in regard to the fundamental right to privacy.

REFERENCES

Bernal P, Internet Privacy Rights: Rights to Protect Autonomy (Cambridge University Press 2014) <https://books.google.es/books?id=0TI4AwAAQBAJ>

BRAZIL, 'Constituição Da República Federativa Do Brasil' (Website Oficial do Planalto, 1988) <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> accessed 23 February 2014

———, 'Lei Complementar N.º 105, de 10 de Janeiro de 2001' (2001) <http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm> accessed 20 April 2015

———, 'Lei N.º 12.527, de 18 de Novembro de 2011' (2011) <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> accessed 20 April 2015

———, 'Lei N.º 12.737, de 30 de Novembro de 2012' (2012) <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> accessed 20 April 2015

———, 'Lei N.º 12.965, de 23 de Abril de 2014' (2014) <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> accessed 21 April 2015

———, 'Anteprojeto de Lei Para a Proteção de Dados Pessoais' (Pensando o Direito, 2015) <http://participacao.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/> accessed 28 April 2015

de Montjoye Y-A and others, 'Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata' (2015) 347 Science 536 <http://www.sciencemag.org/content/347/6221/536> accessed 30 January 2015

Doneda D, Da Privacidade à Proteção de Dados Pessoais (Renovar 2006) <https://books.google.es/books?id=EHOkAAAACAAJ>

Galindo Ayuda F, 'Democracia, Internet Y Gobernanza: Una Concreción. (Spanish)' (2012) 33 Revista Seqüência 33 <10.5007/2177-7055.2012v33n65>

Goodman E and Powles J, 'Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data — Medium' (2015) <https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd> accessed 15 May 2015

Google, 'Report of The Advisory Council to Google on the Right to Be Forgotten Members of the Council' (2015) <https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view>

Lemos R, 'O Marco Civil Como Simbolo Do Desejo Por Inovação No Brasil' in George Leite and Ronaldo Lemos (eds), Marco Civil da Internet (Atlas 2014)

Limberger T, O Direito à Intimidade Na Era Da Informática: A Necessidade de Proteção Dos Dados Pessoais (Livraria do Advogado 2007)

López Jiménez D, 'Los Códigos Tipos Como Instrumento Para La Protección de La Privacidad En El Ambito Digital: Apreciaciones Desde El Derecho Español' (2013) 11 Estudios constitucionales 575 <http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-52002013000200015&lng=en&nrm=iso&tlng=en> accessed 24 September 2014

Morais JLB and Neto EJ, 'A Insuficiência Do Marco Civil Da Internet Na Proteção Das Comunicações Privadas Armazenadas E Do Fluxo de Dados a Partir Do Paradigma Da Surveillance' in G Leite and R Lemos (eds), Marco Civil da Internet. (Atlas 2014)

Orwell G, 1984 (Houghton Mifflin Harcourt 1983) <https://books.google.es/books?id=kotPYEqx-7kMC>

Warren SD and Brandeis LD, 'The Right to Privacy' [1890] Harvard Law Review VO - 4 193 <http://roble.unizar.es:9090/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsjsr&AN=edsjsr.10.2307.1321160&lang=es&site=eds-live>

BRASIL, Lei No. 7.210, de 11 de julho de 1984. Institui a Lei de Execuções Penais no Brasil 1984

Regulamento (CE) n.º 45/2001, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e orgãos comunitários e à livre circulação desses dados 2001 22

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Contact: info@brusselsprivacyhub.org

N°1 **"The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area"** by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 **"The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection"** by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 **"Towards efficient cooperation between supervisory authorities in the area of data privacy law"** by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "**The data protection regime in China"** by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 **"The right to privacy and personal data protection in Brazil: time for internet privacy rights?"** by Vinícius Borges Fortes (23 pages)