FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

SWP

Privacy and Surveillance in the Digital Age: a comparative study of the Brazilian and German legal frameworks

An input to the workshop "Privacy under mass surveillance: a multi-stakeholder international challenge" to be held in the Internet Governance Forum, in João Pessoa, Brazil

Privacy and Surveillance in the Digital Age: a comparative study of the Brazilian and German legal frameworks

An input to the workshop "Privacy under mass surveillance: a multi-stakeholder international challenge" to be held in the Internet Governance Forum, in João Pessoa, Brazil

Center for Technology and Society of the Rio de Janeiro Law School of the Getulio Vargas Foundation (CTS/FGV)

German Institute for International and Security Affairs (SWP)

Anja Dahlmann
Jamila Venturini
Marcel Dickow
Marilia Maciel

November, 2015

INDEX

ABOUT THE BRIEFING

This briefing is an input to the discussions that will take place in the session "Privacy under mass surveillance: a multi-stakeholder international challenge" to be held on November 9th in João Pessoa, Brazil, during the "Day Zero" of the Internet Governance Forum. This document is one of the outputs of the first phase of the project "Privacy in the digital age: fostering the implementation of the bilateral German-Brazilian strategy in response to massive data collection**",** jointly developed by the Center for Technology and Society of the Rio de Janeiro Law School of the Getulio Vargas Foundation and the German Institute for International and Security Affairs (SWP), with the support of FGV.

The project Privacy in the Digital Age seeks to identify legal, political, technical, and economic incentives for the implementation of resolution 168/67 on Privacy in the Digital Age, proposed by Germany and Brazil, and approved by the United Nations General Assembly and to identify other potential areas of collaboration between Germany and Brazil in the field of Internet Governance.

The first phase of the project maps out the Brazilian and German legal frameworks related to privacy and confidentiality of communications, data protection and intelligence activities. As such, it seeks to identify how both countries are dealing with the challenges brought about by massive data collection and processing by (i) mapping the regulations on data protection and privacy and trying to understand how they shape the ways in which data can be accessed and (ii) understanding the general framework and exceptions that apply to intelligence activities.

The present report mainly focused on the analysis of domestic legislation. The analysis of case law was included only when necessary to clarify the rules governing the collection, processing and access to personal data by law enforcement authorities or intelligence services. Issues related to implementation will be addressed in the second phase of the project.

BRAZIL

Recent developments in the domestic legal framework - which include the approval of the Civil Rights Framework for the Internet in Brazil (Marco Civil da Internet) and, in 2011, of the Freedom of Information Act - provide an initial approach to a regulatory framework that reconciles the needs to foster openness with regards to information and to protect privacy. The Chamber of Deputies, the Senate and the Executive, through the Ministry of Justice, are also increasingly promoting discussions over the need to adopt a data protection law.

Civil society engagement in pressuring for both State obligations to disclose governmental information (including as open data) and protections for the Internet users on the processing their personal data by public and private entities were important to push forward these initiatives.Despite these efforts, Brazil still lacks a coherent legal framework to deal with the rights to privacy and data protection.

With regards to intelligence, law No. 9.883/1999 created the Agency of Intelligence (ABIN) to be responsible for planning, executing, coordinating, supervising and controlling the intelligence activities in the country. Nevertheless, Brazil lacks a specif national policy on intelligence and there are shortcomings in the Brazilian Intelligence System related to the need to develop frameworks for day-to-day operations and the need to modernize the mechanisms of oversight, which is carried out by the Parliament.

Although intelligence activities cannot be held on the sidelines of the Constitution or of individual human rights – this means, for example, that ABIN is not allowed to carry out telephone interceptions – there are new areas that still lack clear guidelines of operation, such as the possibility to monitor online activities, strengthened after the 2013 street protests in Brazil.

This section maps out the applicable norms that seek to protect the rights to privacy and data protection in Brazil, including relevant case law, and maps the most relevant laws concerning intelligence activities.

1. The protection of privacy

In Brazil, the principle of the presumption of innocence, the right to privacy, the inviolability of the home and the confidentiality of communications enjoy constitutional protection. An important exception to the confidentiality of communications is the confidentiality of telephone communications, which may be waived by court order and solely for the purposes of criminal prosecution.[1] The rationale for this is that: a) only the judicial branch may guarantee independence and objectivity, thereby preventing abuses of power; b) criminal cases are considered more serious and would therefore justify the suspension of a fundamental right. The Constitution further enshrines the right to *habeas data* (regulated by Law 9.507/1997), that is, the right to access and rectify one's own personal data.

The right to privacy in Brazil is considered to be included in the broader category of personality rights, such as the right to the protection of one's own image, honor and intimacy (Doneda,

[1] Brasil. Constitution of the Federative Republic of Brazil: constitutional text of October 5, 1988, with the alterations introduced by Constitutional Amendments no. 1/1992 through 64/2010 and by Revision Constitutional Amendments no. 1/1994 through 6/1994. – 3. ed. – Brasília: Chamber of Deputies, Documentation and Information Center, 2010. Art. 5º, X, XI, XII.

2006). They are all facets of the right of the individual to exclude from public knowledge facts that are exclusively related to her private life.[2]

With respect to international laws and principles that have been incorporated to the domestic sphere, Brazil signed and ratified a number of human rights treaties that enshrine the right to privacy, including the Universal Declaration of Human Rights (UDHR)[3], the International Covenant on Civil and Political Rights[4], and the American Convention on Human Rights[5].

For many decades, the Brazilian Supreme Court held the position that all international treaties, regardless of their subject matter, should be approved with the status of an ordinary federal law. This meant that, in spite of the international responsibility this would engender, any treaty - including human rights treaties - could be rendered internally inapplicable by a supervenient law of the same hierarchy.

Since 2004, however, the status of Human Rights treaties in the Brazilian legal system depends on the procedure followed for their internalization. Article 5, paragraph 3rd of the Constitution (introduced by amendment 45/2004) determines that international treaties and conventions on human rights that are internalized following the procedure to approve constitutional amendments - which means, human rights treaties that are approved in each house of Congress, in two rounds, by three fifths of the votes of its members - shall be equivalent to constitutional amendments.

The practical consequence of amendment 45/2004 was that, once a human rights treaty is internalized with constitutional status, the prevailing legal doctrine affirms that this treaty cannot be denounced by the Brazilian State, because fundamental rights are immutable clauses (cláusulas pétreas) of the Brazilian Constitution, according to art. 60 paragraph 4, IV.

In the case of treaties approved before the amendment, or if the internalization of the treaty does not follow the procedure enshrined in article 5 paragraph 3, human rights treaties present "supra-legal" character.[6] This means that these norms would have infra-constitutional status (and are subject to constitutional control), but would be hierarchically above ordinary federal laws: ordinary laws are subject to conventionality control (controle de convencionalidade) and, therefore, need to comply with supra-legal human rights norms.

---

[2] See, for instance, Júnior, T. S. F. (1993). Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito, Universidade de São Paulo, 88, 439-459. Available at: <http://www.revistas.usp.br/rfdusp/article/view/67231>..

[3] Universal Declaration of Human Rights, art. 12. "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Available at: <http://www.un.org/en/documents/udhr/index.shtml#a12>.

[4] International Covenant for Civil and Political Rights, art. 17. "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks." Available at: <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

[5] American Convention on Human Rights, art. 11. " 1. Everyone has the right to have his honor respected and his dignity recognized. 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. 3. Everyone has the right to the protection of the law against such interference or attacks." Available at: <http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm>.

[6] This understanding was expressed by the Brazilian Supreme Court when it ruled on Special Appeal (RE) 466.343.

The shift that took place on the last decades, based on the evolution of law and jurisprudence, shows the efforts to increasingly harmonize Brazilian national laws with international standards on human rights.

2. Law 9.296/1996 and the exceptions to the confidentiality of communications

As mentioned above, the Constitution lays down an exception from the right to the confidentiality of communications. This derogation is regulated by Law No. 9.296/1996, stipulating the criteria for the interception of telephone communications which may only be requested by the chiefs of police or the Public Prosecutor's Office for the purposes of both the pre-trial and trial stages of a criminal case.[7] The requesting authority must (i) provide reasonable indications that the individual concerned has committed an offence punishable by reclusion under the Brazilian Penal Code[8] and (ii) prove that the evidence cannot be obtained by other means.[9]

The procedure for intercepting telephone communications is subject to judicial control. Interception may be permitted for a maximum period of 15 days which may be extended for another 15 days provided that the requesting authority demonstrates that extension is essential for obtaining evidence related to the investigation.[10] The Public Prosecutor's Office must always be notified by the police of the execution of any interception that has been authorized.[11]

The conditions laid down in Law 9.296/1996 seek to follow the jurisprudence set by international human rights courts concerning the confidentiality of communications and the requirements for wiretapping. The Inter-American Court of Human Rights, for instance, has acknowledged that "taking into account that telephone interception can represent a serious interference in the private life of an individual, this measure must be based on a law that must be precise and indicate the corresponding clear and detailed rules, such as the circumstances in which this measure can be adopted, the persons authorized to request it, to order it and to carry it out, and the procedure to be followed".[12] The Court further held that "to conform to the American Convention any interference [in telephone communications] must comply with the following requirements: (a) it must be established by law; (b) it must have a legitimate purpose, and (c) it must be appropriate, necessary and proportionate".[13]

A. The interpretation of Law No. 9.296/1996 by courts

In spite of the fact that the right to privacy and the confidentiality of communications enjoy constitutional recognition and that the wording of Law 9.296/1996 is in line with the relevant international standards on human rights, Brazilian courts appear to have adopted a rather broad interpretation of the limitations on telephone interceptions. A good example concerns the duration of the interception: on at least two different occasions, the Brazilian Supreme

[7] Law No. 9.296/1996, art. 3°.
[8] The Brazilian Penal Code differentiates between different types of imprisonment like reclusion and detention, being the first the most severe and applicable to offenses considered to be more serious. See Decree-law No. 2.848/1940, art. 33.
[9] Law No. 9.296/1996, art. 2°.
[10] Ibid, art. 5°.
[11] Ibid, art. 6°.
[12] Escher and others v. Brazil at paragraph 131. 2009. Available at: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_ing.pdf.
[13] Ibid.

Court ruled that the law allows for an extension of the duration of the interception multiple times.[14] It bears noting that in one of these two cases, the order remitting the interception was renewed for a period of 7 months.[15] The judgment, authored by Justice Jobim, considered the renewal of authorizations for the interception of telephone communications legal especially in complex cases which demand lengthy investigations.[16]

In both cases, Justice Mello authored a dissenting opinion in which he took the stance that the law allows for interception for a maximum period of 30 days, that is, that extension of the 15-day period may be renewed only once. According to Justice Mello, the exception to the confidentiality of telephone communications should be narrowly interpreted.

In order to point out the disproportionate nature of the decision made in a previous stage of the judgement (which reached the same conclusion on the legality of the extensions in a lower court[17]), Prado (2006) compared the provisions of the Federal Constitution regarding the duration of permissible interception for the purposes of criminal investigation (see above) with the duration for the state of emergency situations established by the Constitution (state of defense and state of siege). According to the Constitution, the state of defense can be declared when there is a threat to the public order or the social peace and it may last for up to **60 days** during which the confidentiality of communications will be restricted.[18] The state of siege in turn can be declared for **30 days** in case the state of defense is not effective or if there is a war or international attack in place.[19] Prado argues that if the Constitution limited restrictions on fundamental rights for serious national crisis, it would seem disproportionate to allow for unlimited wiretapping for criminal prosecution, a possibility that the aforementioned judgments of the Constitutional Court appear to have left open.

In 2009, the Inter-American Court of Human Rights condemned Brazil for having violated the right to privacy in *Escher et al*. This case concerned the monitoring of telephone conversations of land rights activists in the state of Paraná. The interception of telephone communications lasted for 49 days and, according to the Inter-American Commission on Human Rights (IACHR), the State failed to provide evidence that it followed the established legal proceedings for the extension of the duration of the interception.[20] The judgment stated that "the telephone conversation interceptions and recordings that [were] the object of this case did not comply with Articles 1, 2, 3, 4, 5, 6 and 8 of Law No. 9,296/96 and, therefore, were not based on the law". As a result, the Court ruled that the State violated the right to privacy established in Article 11 of the American Convention.

[14] HC 83515/RS, rel. Min. Nelson Jobim, 16.9.2004 and Inq 2424/RJ, rel. Min. Cezar Peluso, 19 e 20.11.2008.
[15] HC 83515/RS, rel. Min. Nelson Jobim, 16.9.2004.
[16] The same decision also softened the legal text that says in article 2º that telephone interception would only be accepted for crimes punishable with reclusion by stating that crimes that are punished with detention but are similar to the first ones can also justify the interception (Nucci, 2009).
[17] RHC 13274 RS 2002/0104866-6, rel. Min. Gilson Dipp, 19.8.2003.
[18] Brasil. Constitution of the Federative Republic of Brazil: constitutional text of October 5, 1988, with the alterations introduced by Constitutional Amendments no. 1/1992 through 64/2010 and by Revision Constitutional Amendments no. 1/1994 through 6/1994. – 3. ed. – Brasília: Chamber of Deputies, Documentation and Information Center, 2010. Art. 136.
[19] Brasil. Constitution of the Federative Republic of Brazil: constitutional text of October 5, 1988, with the alterations introduced by Constitutional Amendments no. 1/1992 through 64/2010 and by Revision Constitutional Amendments no. 1/1994 through 6/1994. – 3. ed. – Brasília: Chamber of Deputies, Documentation and Information Center, 2010. Art. 137.
[20] Escher and others v. Brazil. 2009. Available at: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_ing.pdf.

B. Administrative rules on the confidentiality of communications

The confidentiality of communications is also guaranteed by several resolutions[21] issued by the National Telecommunications Agency (Anatel), which regulates the provision of services of landline telephony, mobile telephony and data communications.[22] Anatel was created by the General Telecommunications Act (Law No. 9.472/1997), which also provides that users of telecommunications services have the right to their privacy in the billing documents and on the use of their personal data by the service provider.

Anatel Resolution No. 73/98 on telecommunication services establishes the duty of the providers to safeguard the confidentiality of data and information, but states that the providers must also make available the technological tools needed for the suspension of the confidentiality when ordered by an authority vested with such powers. It also obliges the providers to control the interception and follow through its implementation in order to ensure that the prescribed limits are respected.[23]

Anatel Resolution No. 426/2005 on the regulation of land switched telephone services enshrines the right to the confidentiality of communications and to the privacy of their billing documents and lays down conditions for the use of personal data by the providers. According to the Resolution, this data cannot be shared with third parties without previous and express authorization from the data subject, except the necessary for the sole purposes of billing.[24] Similar to Resolution No 73/98, it states that the provider is responsible for ensuring the secrecy of communications over the network and the confidentiality of data and information[25] and for having the necessary technological resources for its suspension[26].

Similar provisions are laid down in Anatel Resolution No. 477/2007 on mobile services[27] and Anatel Resolution No. 614/2013 on multimedia communications services which extends confidentiality to connection logs and information from the subscriber. This later act lays down that providers must disclose data related to the suspension of the secrecy of telecommunications to the competent authorities[28] and establishes that connection logs should be retained for the minimum period of one year.[29] [30]

[21] Resolutions are a type of administrative act issued by public bodies that are administrated by a group of agents (e.g. commissions, councils, etc.) and not individually by one specific person (Bandeira de Mello, 2002). The competence of the National Telecommunications Agency (Anatel) to issue norms that discipline matters related to telecommunications was determined by article 22 of Law No. 9.472/1997.

[22] Anatel was created by Law No. 9472/1997 and it is responsible for, among other activities, adopting rules on the telecommunication services and interpreting the telecommunication law on the administrative sphere. The General Telecommunications Act (Law No. 9.472/1997) also enshrines in article 3º the right to privacy on billing documents and on the use of their personal data by the service provider.

[23] Anatel Resolution No. 73/98, art. 26.

[24] Anatel Resolution No. 426/2005, art. 11, VI and XI.

[25] Ibid, art. 23..

[26] Ibid, art. 24.

[27] Anatel Resolution No. 477/2007, art. 6, 89 and 90.

[28] Ibid, art. 52.

[29] Ibid, art. 53.

[30] As we will see below, this provision contradicts the Marco Civil da Internet which establishes that connection logs will only be made available for the authorities when determined by a court order.

3. Secrecy of data

Article 5º, XII, of the Constitution[31] has raised a debate among scholars regarding the reach of the inviolability of the secrecy of correspondence, telegraphic, data and telephone communications (Nucci, 2009).

For some scholars the text is clear in protecting the inviolability of (i) correspondence and telegraphic communications and (ii) data and telephone communications, in the later case (ii) except by court order in criminal investigations or pre-trial procedures.

Ferraz Júnior (1993)[32] and others, on the other hand, have interpreted the word "communications" narrowly. Secrecy would be restricted to **communications** - in other words, to the transmission of information -, made by correspondence, telegraph, data and telephone. In the case of data, this would imply that the secrecy would only be protected while data is being transmitted and not when it is stored. For him, stored data can be obtained through search and seizure warrants as predicted by the Brazilian law for other types of evidence. That's why the only exception to the secrecy of communications would refer to telephone communications which leave no type of evidence after they end.

The first interpretation means that the confidentiality of telephone and data would only be broken for "the purposes of criminal investigations or criminal procedural finding of facts", the second affords a lower level of protection to data: the secrecy of stored data may be waived irrespective of whether the request is related to a criminal case or not.

The last interpretation has prevailed in the jurisprudence with at least two decisions by the Supreme Court holding that the clause refers to the ***communication*** of data to justify the legality of seizure of equipment containing data after a judicial authorization was granted for that purpose.[33]

4. Remedies for violations of privacy

The Constitution lays down that "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"[34]. The Civil Code also assures the inviolability of the private life and the protection of the image and honor.[35] It also establishes indemnification as a remedy for the damages resulting from defamation, slander and injury which will be determined by a judge in case the victim cannot prove material damages.[36]

[31] Brasil. Constitution of the Federative Republic of Brazil: constitutional text of October 5, 1988, with the alterations introduced by Constitutional Amendments no. 1/1992 through 64/2010 and by Revision Constitutional Amendments no. 1/1994 through 6/1994. – 3. ed. – Brasília: Chamber of Deputies, Documentation and Information Center, 2010. Art. 5º, XII, "[t]he 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".

[32] Júnior, T. S. F. (1993). Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito, Universidade de São Paulo, 88, 439-459. Available at: <http://www.revistas.usp.br/rfdusp/article/view/67231>.

[33] MS 21.729, rel. Min. Marco Aurélio, 5.10.1995 e RE 418.416-8 SC, rel. Min. Sepúlveda Pertence, 10.05.2006.

[34] Brasil. Constitution of the Federative Republic of Brazil: constitutional text of October 5, 1988, with the alterations introduced by Constitutional Amendments no. 1/1992 through 64/2010 and by Revision Constitutional Amendments no. 1/1994 through 6/1994. – 3. ed. – Brasília: Chamber of Deputies, Documentation and Information Center, 2010. Art. 5º, X.

[35] Law No. 10.406/2002, art. 20 and 21.

[36] Ibid., art. 953.

Under Law 9.296/1996, which was examined in more detail above, the act of (i) intercepting telephone and informatics communications or (ii) violating legal confidentiality[37] without a court order or for purposes that are not predicted by law is considered a crime that can be punished with detention from 2 to 4 years and fine.[38]

Marco Civil da Internet (Law 12.965/2014) also establishes sanctions in case of violations of rules on privacy and data protection by internet service providers (ISPs) and online application providers[39]. It also states that the latter must provide (i) information regarding the security measures they apply to protect users' private communications and personal data and (ii) information that allows the verification of the fulfillment of the rules related to the collection, storage and processing of data and respect to privacy and the confidentiality of communications. The law does not specify how this will be operationalized and the details should be defined in the implementing regulation[40].

When it comes to actions undertaken by the State authorities, it is difficult for most citizens to identify if their privacy has been violated. A good example that illustrates this point is in *Escher et al. v. Brazil*: "[the representatives] stated that, owing to the confidential nature of the telephone interception and recording procedure established in Act No. 9.296/96, 'at no time, during the proceedings before the [Commission], had they identified the [presumed] victims of the violations by naming them[, since] in 2000, when the petition was submitted, the petitioner organizations did not know the scope of the illegal telephone interceptions [and] all the people whose telephone conversations had been intercepted and recorded by the Military Police of the state of Paraná. [They merely knew] of a small group of members and leaders of COANA and ADECON whose telephone calls had been intercepted because their conversations were disseminated in the local and national newspapers [...]. It was only in 2004 [... that they] were able to learn about and have access to all the transcripts of the recordings'".

5. The protection of personal data

Brazil does not have a unified act that deals with data protection specifically. Sparse norms regulate data protection like the Consumer Protection Act (Law No. 8.078/1990) and Law No. 9.507/1997 on *habeas data,* which is a type of legal action that, as seen before, enjoys constitutional status and enables the individual to exert the right to access personal information retained by governmental authorities or in public databases and to rectify them.[41]

The absence of a unified framework that regulates data protection gives a wide margin of discretion when dealing with citizens' personal data. One example can be found in the control that the Ministry of Social Development exerts over the database of all the beneficiaries of the Bolsa Família, a welfare program created in 2004 to assist poor families. According to Law No.

[37] Article 1º of Law No. 9.296/1996 establishes that it applies to telephone, telematics and informatics communications.
[38] Law No. 9.296/1996, art. 10.
[39] Marco Civil considers an online application any functionality that can be accessed through a terminal connected to the Internet. Law No. 12.9652014, art. 5º, VII.
[40] The Ministry of Justice opened a call for contributions on the text of the regulation and received the inputs from civil society – including academic – organizations and the private sector, however more than one year since the Law came into force, the decree was not published.
[41] Brasil. Constitution of the Federative Republic of Brazil: constitutional text of October 5, 1988, with the alterations introduced by Constitutional Amendments no. 1/1992 through 64/2010 and by Revision Constitutional Amendments no. 1/1994 through 6/1994. – 3. ed. – Brasília: Chamber of Deputies, Documentation and Information Center, 2010. Art. 5º, LXXII.

10.836/2004, the list of beneficiaries should be public and accessible through the web;[42] as a result, it is possible nowadays to easily find the full name, identity number, city and amount received by each person receiving funds under the program in question (Córdova & Gonzalez, 2015). Furthermore, additional information about the beneficiaries of the program, including about whether they belong to a specific minority or vulnerable group of the populations is collected. This data is considered private, but according to a Portaria[43] of the Ministry of Social Development (MDS) they might be shared for (a) "research purposes", without further specification, and (b) with other institutions of the public administration for the development of public policies.[44]

The Constitution is not clear, however, as to whether the right to *habeas data* applies to private entities. Legal scholarship and jurisprudence answer this question in the affirmative (Doneda, 2006).[45]

Also, the Consumer Protection Act enshrines the right (i) to access all registers that include information about the consumers' activities as well as the sources from which the data was collected, (ii) to be notified in cases where retention of their personal data may take place without their consent and (iii) to correct personal data that is stored in databases. It also establishes the obligation to notify consumers in writing in cases where a file is created that contains their personal data.[46] By establishing these rules, the Consumer Protection Act aims at ensuring that private entities do not exploit consumer data in an abusive manner.

Although the above mentioned provisions are usually applied on credit reporting[47], it has been suggested that the Consumer Protection Act can be interpreted broadly so as to ensure that some principles of data protection apply to other situations. For example, Doneda (2006) argues that the principle of good faith[48] can serve as the basis for the incorporation of the purpose limitation principle.[49]

Article 154-A of the Penal Code, which binds both private and public bodies, prohibits the violation of security mechanisms of electronic devices of others in order to obtain, tamper or destroy data without an authorization from the owner and establishes a penalty of 1 to 12 months detention plus fine. If the violation results in access to private communications,

[42] Law No. 10.836/2004, art. 13.
[43] Portarias are administrative acts issued by chiefs of public bodies or departments to transmit decisions of internal effects (i.e. inside the body where it was issued) to their subordinates (Bandeira de Mello, 2002).
[44] Portaria No. 10/2012 of the MDS, art. 4º.
[45] "A ambiguidade da expressão "de caráter público" motivou uma atuação positiva da doutrina e da jurisprudência para estender a abrangência da ação além dos órgãos públicos [...]."
[46] Law No. 8.078/1990, art. 43.
[47] See, for instance, TJSP, 14ª C. Civil, AC n.º 254.356-2, j. em 21.3.95, rel. des. Ruiter Oliva, v.u., JTJ-Lex 170/35-39, (1º TACSP, 2ª C., AI n.º 486.629-1, j. em 2.10.91. rel. juiz Roberto Mendes de Freitas, v.u., JTACSP-Lex 133/37-39, STJ , 3ª T., REsp n.º 30.666-1-RS, j. em 8.2.93, rel. min. Dias Trindade, v.u., RT 696/249-250 and STJ, 3ª T., REsp n.º 14.624-0-RS, j. em 22.9.92, rel. min. Eduardo Ribeiro, v.u., JSTJ e TRF-Lex 41/188-192.
[48] Law No. 8.078/1990, art. 51. Law 10.406/2002, art. 113.
[49] "(…) in the [legal] doctrine we can find support for an expansive interpretation of Consumer Protection Code norms, so that it would be possible to identify principles of personal data protection that apply to other situations. Thus, for example, the principle of purpose in our legal system gets extended through the application of the good faith clause coupled with the constitutional guarantee of privacy. As a consequence, data provided by the consumer should be used only for the purposes that motivated its collection - which may serve as grounds for recognizing a principle that forbids the collecting of sensitive data and commercialization of databases of consumers' data." (Doneda, 2006, p. 339)

commercial or industrial secrets or confidential information, punishment is more severe: conviction may lead to reclusion (6 months to 2 years) and a fine.[50] [51]

6. The Freedom of Information Act and Marco Civil

In the absence of a unified framework for data protection, the recently approved Freedom of Information Act and Marco Civil da Internet also contain provisions on the matter.

A. Brazilian Freedom of Information Act

The Freedom of Information Act (Law No. 12.527/2011) regulates the right to access to information enshrined in the Constitution[52] and establishes the procedures for processing access to information requests as well as the obligations concerning proactive disclosure of public interest information such as contact, budget and expenditure. It applies to both public entities and nonprofit organizations that are publicly funded.

With regard to the processing of personal information, the law provides that the controller must respect the intimacy, private life, honor and image of the data subjects according to the following rules: (i) access to personal information from public databases is restricted to legally authorized public servants and to the data subjects for a maximum period of 100 years after its production; (ii) personal information can only be published or accessed if it is permitted by law or there is an express consent by the data subject.[53] According to the Freedom of Information Act, any natural or legal person that acquires unlawful access to personal information will be deemed responsible for its misuse.[54] The Act also provides for certain derogations from the general rules whereby access to third parties' information might be disclosed without consent. These are (i) for medical purposes - when the data subject is incapable of giving consent, (ii) for the development of public interest statistics and scientific research; (iii) to comply with the law and (iv) for the defense and protection of human rights and the public interest.

Despite regulating processing of personal data, the Act is limited to situations in which data protection conflicts with access to information and to the activities of public bodies or public funded nonprofits.

B. Marco Civil da Internet

The Civil Rights Framework for the Internet in Brazil (Marco Civil da Internet), Law No. 12.965/2014, emerged as an alternative to some legislative proposals aiming to criminalize certain practices on the Internet, many of them considered socially acceptable or trivial.[55] The law is considered an important international reference, not only for encompassing some progressive provisions, such as the principle of network neutrality, but also because extensive

[50] The penalty is increased from one third to half of the original one if the crime is perpetrated against governmental authorities.
[51] Decree-Law No. 2.848/1940, art. 154-A.
[52] Brasil. Constitution of the Federative Republic of Brazil: constitutional text of October 5, 1988, with the alterations introduced by Constitutional Amendments no. 1/1992 through 64/2010 and by Revision Constitutional Amendments no. 1/1994 through 6/1994. – 3. ed. – Brasília: Chamber of Deputies, Documentation and Information Center, 2010. Art. 5º, XXXIII.
[53] Law No. 12.527/2011, art. 31.
[54] Public servants and militaries will be subjected to a specific laws and will be penalized at least with suspension (Law No. 12.527/2011, art. 32). Natural or legal people will be penalized with warnings, fines or other measures predicted in art. 33 of Law No. 12.527/2011.
[55] This was the case of bill 84/99, known as "bill Azeredo", which would establish, for example, penalties of up to four years of imprisonment for unblocking or "jailbreaking" a mobile phone, or for transferring songs from an MP3 player back into a computer.

rounds of public consultation shaped the drafting of the bill that was sent to the Brazilian Congress. [56]

While the bill was awaiting Congress deliberation, several documents leaked by the former NSA contractor Edward Snowden and published by The Guardian and The Washington Post revealed details on global surveillance activities performed by the United States National Security Agency (NSA) and closely aligned governments. The leaks continued during the year of 2013 and indicated that the NSA had intercepted Brazilian communications including those of president Dilma Rousseff. The Agency also targeted Brazilian state-owned oil company, Petrobrás.[57] In the aftermath of these revelations, the provisions related to privacy on Marco Civil were strengthened as a response to international scandals on mass surveillance.[58]

Marco Civil da Internet regulates certain important aspects of data protection, seeking to grant to Internet users a higher level of protection. Following the same approach as Law 9.296/1996, Marco Civil provides that private communications are in principle inviolable and that this inviolability may only be waived by means of a court order. It also provides that: (i) users' personal data should not be transferred to third parties without the users' freely given, informed and specific consent; (ii) users have the right to access clear and complete information about the collection, use, storage, processing and protection of their personal data which can only be used to purposes that (a) justify collection, (b) are not forbidden by law and (c) are explicitly laid down in services contracts or terms of use; (iii) users have the right to consent about the collection, use, storage and processing of personal data and (iv) users have the right to request the complete deletion of their personal data upon the expiry of the contract except when predicted by law. Marco Civil also determines that any contractual clause that undermines the confidentiality of private communications on the Internet should be declared null.[59]

By establishing the above rights, Marco Civil explicitly incorporated two internationally recognized principles of data protection: transparency and purpose[60], and consolidated rights that were already part of the consumer protection.

Given the global reach of the Internet, Marco Civil also contains a clause stating that relevant Brazilian law will apply to entities that collect, store and process logs, personal data and

[56] The Office of Legislative Affairs of the Ministry of Justice (MJ-SAL) and the Center for Technology and Society at the Getulio Vargas Foundation (CTS-FGV) developed a partnership to conduct the public consultation and created a platform in Digital Culture website to receive comments. The public consultation process was divided into two phases. In the first, which began in October 2009 and lasted just over 45 days, a text containing general principles for the regulation of the Internet was put under consultation. Participants were able to detail these principles and propose new topics to be embraced in future legislation. In the second phase, a draft bill, based on the suggestions received, was put under consultation. Comments were incorporated by MJ-SAL and CTS and the draft bill was sent to Congress. During the time the bill was in Congress, 7 public hearings were held with the participation of 62 members of civil society and 374 suggestions were collected from the public and considered in the draft of the final text in the Chamber of Deputies.

[57] Watts, J. (2013). "NSA accused of spying on Brazilian oil company Petrobras". The Guardian. Available at: <http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras>

[58] At the opening of the 68th Session of the United Nations General Assembly, the Brazilian president, Dilma Rousseff, defined mass surveillance as "a breach of international law", "a disrespect for national sovereignty" and a "grave violation of human rights and civil liberties". The president also mentioned the need to develop a framework for the governance and use of the Internet and to create mechanisms to ensure basic principles are guaranteed, such as privacy, freedom of speech and net neutrality. Subsequently, Germany and Brazil have jointly proposed a resolution at the UN General Assembly on the right to privacy on the digital age.

[59] Ibid, art. 7º.

[60] Contribution from the Brazilian government to the report of the United Nations High Commissioner of Human Rights on the right to privacy in the digital age (2014). Available at: http://www.ohchr.org/EN/Issues/DigitalAge/Pages/Contributions.aspx.

communications if at least one of these actions occurs in the national territory. The law covers the operations of collection where at least one of the terminals is located in Brazil and applies to providers that are located abroad but offer services to Brazilian consumers or if at least one of its subsidiaries is located in Brazil.[61]

Marco Civil establishes that ISPs and online application providers that infringe the right to privacy or to data protection are subject to penalties, which are still to be defined in implementing regulation. Hence, until such legislation is enacted, the effective exercise of the rights enshrined on this article is surrounded by uncertainty.

It bears noting that Marco Civil only applies to activities on the Internet.[62] Moreover, it does not provide for a detailed definition of the term "personal data", thereby leaving room for different, perhaps contradictory, interpretations by the courts.

While Marco Civil represents in many aspects an improvement to the protection of personal data of Internet users, it is not - and was not meant to be - a law on data protection. The articles on data protection were a quick fix adopted in a context of public commotion with the revelations on mass surveillance. Brazil still needs a comprehensive legal instrument on privacy and data protection.

The vague terms of Marco Civil and the fact that it leaves to implementing regulation important definitions restrict the possibilities of its application. As a result, it remains to be seen how courts will interpret the above-mentioned provisions.

As new challenges are posed to data protection, legislators from both the Chamber of Deputies and the Senate have developed bills on data protection that are currently being discussed separately: PL 4060/2012 and PLS 330/2013. The Ministry of Justice has also conducted a public consultation from January to July 2015 on a draft bill that should be presented to the Congress once there is consensus on the final text.

7. Data retention

Following an international trend that led to the approval of data retention mechanisms in different countries[63], Brazil gradually introduced in its legal framework provisions compelling private companies to store users data for law enforcement purposes.

While data retention was perhaps more feverishly debated in the context of the adoption of the Marco Civil, it must be pointed out that it was already regulated by several laws that came into force before the Marco Civil. More particularly, Law No. 12.850/2013 on organized crime establishes that telephone companies should keep for a period of five years all data regarding the origin and destination of telephone calls available to Chiefs of Police and to the Public Prosecutor's Office without specifying if the access is subject to court authorization.[64] Law 12.850/2013 on organized crime also determines that transport companies must provide

[61] Law No. 12.965/2014, art. 11.
[62] Ibid, art. 1º.
[63] Europe for instance approved in 2006 a Data Retention Directive (Directive 2006/24/EC) which was implemented in countries like Romania and Germany (in both cases the data retention laws were declared unconstitutional). The Directive was finally annulled by the Court of Justice of the European Union in 2014.
[64] Law 12.850/2013, art. 17.

direct access to databases on travel reservations to judges, the public prosecutors and chiefs of police.[65]

Marco Civil establishes a 12 month-period for the retention of connection logs[66] and a 6-month period for the retention of access to online applications logs[67]. The law defines connection logs as information related to the time and date of connections to the Internet, their duration and the IP addresses used for the access.[68] Applications logs in turn are defined as information related to the time and date of use of applications from certain IP addresses.

According to Marco Civil, providers are only obliged to give access to the retained logs if there is a court order to that effect. To obtain the order, the interested party must present indications of the alleged offence, the need of the requested information for the investigation concerned and the specific period of time. The judge is responsible for safeguarding the secrecy of the received information as well as the subject's intimacy, private life, honor and image.

The only exception provided for under Marco Civil relates to users information on personal qualification, affiliation and address that may be handed over to administrative authorities without a court order.[69] The same can be found on Law No. 9.613/1998 on money laundering which states that the Public Prosecutor's Office and the police authority will have access to subscription data personal qualification, affiliation and address from the Electoral Justice, telephone companies, finance institutions, Internet providers and credit card administrators regardless of a court order.[70] Law No. 12.850/2013 on organized crime contains a similar provision.

The logs Marco Civil makes reference to constitute what is often defined as "metadata". According to Article 29 Working Party

> "Metadata are all data about a communication taking place, except for the content of the conversation. They may include the phone number or IP address of the person placing a call or sending an e-mail, time and location information, the subject, the addressee, etc. Its analysis may reveal sensitive data about persons, for example because certain information numbers for medical or religious centres are dialed."[71]

Although Marco Civil does not define metadata, it is possible to draw a distinction between logs, personal information and the content of private communications in its text[72]. Given the fact that there is no clear definition on personal data and that Brazil lacks a specific framework

[65] Ibid, art. 16.
[66] Ibid, art. 13.
[67] Ibid, art. 15.
[68] Ibid, art. 5º.
[69] Ibid, art. 10, § 3º. A bill pending approval on the Deputies Chamber aims at changing this provision to extend the type of information that could be accessed without a court order to include e-mail address, telephone number, and the national identity number of any user. For more information see: O'Brien, D. (2015). "Brazil's Politicians Aim to Add Mandatory Real Names and a Right to Erase History to the Marco Civil". Available at: https://www.eff.org/deeplinks/2015/10/brazils-terrible-pl215.
[70] Law No. 9.613/1998, art. 17-B. This text was given by Law No. 12.683/2012, art. 3º.
[71] Article 29 Data Protection Working Party. Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes. 2014. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.
[72] See for instance Law No 12.965/2014, art. 10.

on data protection, the question whether logs are considered personal data or not will be answered by the courts. This answer will be particularly relevant to clarify the treatment of metadata, especially considering the data retention provisions existing in the country.

8. Intelligence activities

The Brazilian intelligence system was created by Law No. 9.883/1999 with the purpose of preserving the national sovereignty, defending the democratic State and the human dignity.[73] The law defines intelligence as "the activity that aims at the collection, analysis and dissemination of knowledge within and outside the national territory about facts and situations of immediate or potential influence on decision-making and government action and on the protection and security of society and the state".[74] Information is acquired by the intelligence system and transformed into intelligence.[75]

Although there is not a unified international definition of intelligence, Sherman Kent (1966) identified three main aspects of it: a) intelligence as knowledge would be the product of the analysis of information that serves as input to the decion-making process; b) intelligence as organization would encompass the governamental bodies that contribute to intelligence; c) intelligence as an activity would be the process of obtaining, analysing and disseminating information.

The organizational aspect of intelligence is well defined by national laws. Law No. 9.883/1999 created the Agency of Intelligence (ABIN)[76] to be responsible for planning, executing, coordinating, supervising and controlling the intelligence activities in the country. The oversight of ABIN's activities is the responsibility of a Legislative commission composed by 12 members (6 from the Senate and 6 from the Chamber of Deputies).[77]

Decree 4.376/2002 further detailed the organization and functioning of the Brazilian intelligence system especially with regard to its composition.[78] Four amendments were made in order to change or include new members on the system that nowadays is composed by 19 bodies.[79] According to the decree, each of the members should, among others: (i) plan and execute actions related to the collection and integration of data and information; (ii) exchange information necessary to produce knowledge related to intelligence and counterintelligence activities; (iii) provide ABIN with information related to the defense of national institutions and interests.

While the definition of intelligence is similar to what is already enshrined in article 1º of Law No. 9.883/1999[80], the decree defines counterintelligence as activities that aim at neutralizing

[73] Law No. 9.883/1999, art. 1º.
[74] Law No. 9.883/1999, art. 1º, paragraph 2
[75] According Gonçalves (2001), information is something that is known, regardless of how it came to knowledge; intelligence, meanwhile, is information specially geared towards the needs of decision makers. Therefore, all intelligence is information, but not all information is intelligence. Intellegence is a form of elaborated knowledge, produced through the analysis of raw information.
[76] Ibid, art. 3º.
[77] Ibid, art. 6º.
[78] Decree No. 4.376/2002, art. 4º.
[79] Decrees No. 4.872/2003, 6.540/2008, 7.803/2012 and 8.149/2013.
[80] Decree No. 4.376/2002, art. 2º.

adverse intelligence or any action that may threaten the safety of sensitive information to the national security.[81]

Some relevant parameters for the activities of the intelligence system are laid out in Decree 3.505/2000 that establishes the Information Security Policy in the organs and entities of the Federal Public Administration, Law 8.159/91, which provides for the national policy of public and private archives and Decree 7.845/2012, which regulates procedures for security accreditation and treatment of classified information in any degree of confidentiality, and provides for the Security and Accreditation Center.

Despite being explicitly mentioned in both norms, Brazil lacks a specif national policy on intelligence for more than two decades.[82] The lack of a comprehensive framework to deal with intelligence activities reveals shortcomings in the Brazilian Intelligence System related to the need to develop frameworks for day-to-day operations and the need to modernize the mechanisms of oversight, which is carried out by the Parliament.

It is important to highlight that art. 3 of Law 9.883/99 provides that intelligence activities cannot be held on the sidelines of the Constitution or of individual human rights and guarantees.

> "Intelligence activities will be developed, with regard to the limits of its extension and the use of techniques and secret means, in unrestricted compliance with the individual rights and guarantees, loyalty to institutions and ethical principles that govern the interests and security of the State"

This means, for example, that intelligence activities need to abide by the aforementioned Law 9.296/96, which regulates art. 5, item XII of the Constitution. The law establishes the bodies that are allowed to carry out telephone interception and ABIN is not included among them. This is one of the provisions that members of ABIN and some Brazilian specislists on Intelligence are willing to reform in order to streghten the Brazilian Agency.[83]

Consistent with the Constitutional provision of Habeas Data, any individual may request information stored about himself by ABIN. The person concerned shall send a signed request to the Director General of the Organization. Nevertheless, this possibility may, in practice, be mitigated by provisions of the Freedom of Information Act establishing restrictions to the access to information. Article 23 deals with information considered essential to the security of society or the state, which can be classified. This includes information that may compromise intelligence activities, as well as research and monitoring in progress, related to the prevention or prosecution of offenses.

When it comes to ABIN's activities online, the street demonstrations that took place in Brazil in 2013 prompted the organization to monitor social networks, such as Twitter, Facebook, Instagram and also WhatsApp. The likelihood of street protests was measured on a daily basis

[81] Ibid, art. 3º.
[82] Brazilian Senate. Brasil está há duas décadas sem política nacional de inteligência, alertam especialistas. 14 de julho de 2015. Available at http://www12.senado.leg.br/noticias/materias/2015/07/14/brasil-esta-ha-mais-de-duas-decadas-sem-politica-nacional-de-inteligencia-alertam-especialistas
[83] Ibidem.

by a system called Mosaico, which monitored 700 topics defined by the minister in chief of the Cabinet of Institutional Security of the Presidency of the Republic (GSI). ABIN officers aimed to identify the itinerary, the size of manifestations and their sources of financing.[84]

EBC news sought further information by means of a formal request presented to ABIN, legally based on the Freedom of Information Act. The Agency responded that "when necessary, the Brazilian Intelligence Agency conducts research on open sources [of information], including social media, to eventually gather input to their work".[85]

Bibliography

Brandão, P. (2014). A Atividade de inteligência e a Cooperação Internacional: o desafio da integração no combate ao crime organizado nas Américas e a imposição da agenda estadunidense. 2014. Paper presented at the XII International BRASA Congress.

Córdova, Y. & Gonzalez, C. (2015). Unchecked and unintended effects of Open Data policies in Brazil. Paper presented at the 2015 Open Data Research Symposium, 27th May 2015, Ottawa, Canada.

de Souza Nucci, G. (2006). Leis penais e processuais penais comentadas. Editora Revista dos Tribunais.

Doneda, D. (2006). Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar.

Júnior, T. S. F. (1993). Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito, Universidade de São Paulo, 88, 439-459.

Kent, S. (1966) Strategic Intelligence for American World Policy. Princeton University Press.

Mello, C. A. B. D. (2002). Curso de direito administrativo. refund. ampl. e atual. até a Emenda Constitucional 35, de 20.12. 2001. São Paulo: Malheiros.

Brasil. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. (2013) Roteiro de atuação sobre crimes cibernéticos. Brasília: MPF/2ªCCR.

Maciel, M; Zingales, N.; Fink, D (2014). The Global Multistakeholder Meeting On The Future Of Internet Governance (Netmundial). In NoC Internet Governance Research Project: case studies. Moncau, L.F.M.; Maciel, M.F (2014). Internet Governance and the the Brazilian Civil Rights Framework. LACTLD Report. Ed 4. Year 3.

Prado, G. (2006). Limite às interceptações telefônicas e a jurisprudência do superior tribunal de justiça. Ed. Lumen Juris.

Vasconcellos, H. (2013). Cooperação jurídica internacional em matéria penal: uma análise do mutual legal assistance treaty Brasil/Estados Unidos.

[84] Alana Rizzo; Tânia Monteiro. O Estado de São Paulo. ABIN monta rede para monitorar a Internet. 19 June 2013. Available at http://sao-paulo.estadao.com.br/noticias/geral,abin-monta-rede-para-monitorar-internet,1044500

[85] Edgard Matsuki; Leyberson Pedrosa. Abin admite monitorar dados de redes sociais para informações. Portal EBC. 28 August 2013. Available at http://www.ebc.com.br/tecnologia/2013/08/abin-monitora-dados-de-redes-sociais

GERMANY

1. The Protection of Privacy

In Germany, the right to privacy is a fundamental right – although is not named explicitly in the constitution but has been created by the constitutional court and can be seen as part of the fundamental right to self-fulfillment. It is based on Article 2 Para. 1 (self-fulfillment) in connection with Article 1 Para. 1 GG86 (human dignity), which constitute the common personal law. It is complemented by the privacy of correspondence, posts and telecommunications (Article 10) and the privacy of the home (Article 13).

On the European level, the right to privacy (as a fundamental right) is codified in Article 8 of the European Convention on Human Rights (right to respect for private and family life), and has been further development by the European Court of Human Rights.

Furthermore, the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights apply.

2. Restrictions of the Right to Privacy

The privacy of correspondence, posts and telecommunications can be restricted by law: the code of criminal procedure (StPO), the G10 Law and law of the German Federal Office of Criminal Investigation (BKA). Besides measures under the G10 Law, telecommunication and service providers have to hand over the data to relevant agencies and policies following an ordinance of a competent judge. Under urgent circumstances (imminent danger) data can be handed over without ordinance by a judge.

The StPO allows the surveillance of German citizens by the police if it is authorized by a judge with probable cause for certain crimes (§100a StPO). Another tool is the radio cell query (§100g Para. 2,2 StPO), which allows law enforcement agencies to collect data about all mobile devices registered in a specific mobile network cell. It is highly disputed and there is evidence, that public authorities often violate the rules for deletion and notification.87 § 100a StPO names the probable cause for severe crimes (as listed in § 100a Para. 2 StPO) and the approval of a judge as legal requirements. The use of the collected data is only allowed in case of severe crimes named in § 100g StPO. They can be accessed by all law enforcement agencies.

The G10 Law88 allows the restriction of Article 10 GG without the permission of a judge by the German intelligence agencies (Federal Intelligence Service, BND; Office for the Protection of the Constitution; Military Counterintelligence Service, MAD) in case of severe crimes. The so-called G10 Commission supervises the measures. The G10 Commission consists of four regular members and four deputies that are named by the parliamentary parties and are funded by the Parliament. A small office supports the commission. The commission is informed about surveillance measures by the government on a monthly basis and meets in secrecy.

[86] GG means *Grundgesetz*, the German constitution.

[87] Cf. Andre Meister (18.02.2015), Funkzellenabfrage: Ob Betroffene benachrichtigt werden wollen, entscheidet die Staatsanwaltschaft, nicht Betroffene, retrieved 01.10.2015 from <https://netzpolitik.org/2015/funkzellenabfrage-ob-betroffene-benachrichtigt-werden-wollen-entscheidet-die-staatsanwaltschaft-nicht-betroffene/>.

[88] The term "G10 Law" or "Article 10 Law" is a short form of *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*.

Besides the G10 Commission, the intelligence agencies have to report to a Parliamentary Committee.89 It consists of nine members of Parliament. The committee is bound to secrecy, but can give general public statements and issues a general annual report. The actual usefulness of this information is debatable, though. The committee has the right to inspect records and conduct enquiries, but the members can only refer to problematic practices if they have the relevant information about it – a fact that has been criticized by the German civil society and media over the course of the parliamentary inquiry commission on the NSA activities in Germany ("NSA Untersuchungsausschuss").

The law of the German Federal Office of Criminal Investigation regulates further measures of surveillance. The constitutional court is currently reviewing this law, though. A main point of criticism is the permission to monitor lawyers, doctors and journalists during confidential conversations with their clients. The BKA also plans the use of a spy software called "Bundestrojaner" which enables the direct monitoring of the communication of computers and other electronic devices before they can encrypt the data ("Quellen-Telekommunikationsüberwachung", TKÜ) and a forensic search on these devices ("Online-Durchsuchung"). The BKA announced the upcoming release for autumn 2015.90 Earlier versions of this software are in use already.91

The German Constitution has got an amendment of 1968 that allows exceptional laws during a state of emergency like war (case of defense) or natural disasters. It includes the possibility of restrictions of Article 10 GG but has not been used yet.

The German law does not restrict the use of encrypted or anonymous communications and – in contrast to some other European countries – the broad public and political opinion is currently not in favor of such restrictions. There are even (if limited) approaches to enhance encryption: The federal data protection commissioner and consumer advice centers publish information brochures and inform the public about data protection and security. Furthermore, the Federal Office for Information Security (BSI) fosters cyber security.

3. Communications v. Data

While some laws on the surveillance of specific suspects allow to access the content of communication (e.g. § 100a StPO, § 1 G10 Law as well as the specific police laws of the federal states), the regulations on mass surveillance only cover traffic data (e.g. § 100g Para 2,2 StPO, but also the law on data retention).

However, even with regard to specific surveillance, the StPO restricts the content: Findings regarding the core area of private life ("Kernbereich privater Lebensgestaltung")92are inadmissible and have to be deleted immediately.

[89] As a side note: The recent case of the Blog Netzpolitik.org is linked to another commission ("*Vertrauensgremium"*). It consists of a few members of parliament, meets – as both of the other commissions – in private, and decides on the budget of the German intelligence services. Netzpolitik.org leaked information about the budget and therefore two of its reporters were accused of treason. The prosecution was stopped, the Federal General Attorney was released

[90] Cf. Spiegel Online (25.04.2015), BKA-Chef: Bundestrojaner im Herbst einsatzbereit, retrieved 29.10.2015 from <http://www.spiegel.de/netzwelt/netzpolitik/bundestrojaner-des-bka-im-herbst-einsatzbereit-a-1030485.html>.

[91] Cf. Chaos Computer Club (08.10.2015), Chaos Computer Club analyzes government malware, retrieved 29.09.2015 from <http://ccc.de/en/updates/2011/staatstrojaner>.

[92] The actual definition of this concept is disputed among lawyers, the Federal Constitutional Court includes, for example, the sexuality of a person (Decision 75, 369 (380)) and a person's diary (Decision 80, 367 (374, 383)).

4. Remedies for Violations of Privacy

The implementation of data protection is supervised by data protection commissioners – one for every federal state and one for the whole of Germany, funded by the Ministry of the Interior. Companies processing a lot of data are also obliged to appoint a commissioner from their staff. The commissioners work independently and function as ombudsmen for citizens. In cooperation with the consumer advice center, the commissioner also informs citizens about the current legislation and ways to enhance their data protection and security. These efforts are accompanied by the Federal Office for Information Security (BSI).

German companies that store data too long or process it incorrectly can be punished with a fine of up to € 50 000, € 300 000 or even more depending on the economic advantage the company gained (§ 43 BDSG). The place of business constitutes the relevant factor for the applicability of the German data protection law, as long as the company concerned is not seated in another EU Member State (§ 1 BDSG). This also holds true for the Telecommunications Act, which leaves the jurisdiction of the German authorities at least unclear.

If the restriction of the right to privacy falls under the G10 Law, the person concerned has to be informed about the measures three months after their end. The G10 Commission can allow for exceptions, though, to delay or hamper the notification. Legal actions by the person concerned, e.g. a complaint at the Constitutional Court, can only be taken after the official notification (§ 13 G10 Law).

5. The Protection of Personal Data in Germany

In Germany, the most important legislation on the use of personal data is the national law on data protection (Bundesdatenschutzgesetz, BDSG) and its federal counterparts as well as the Telecommunications Act with regard to telecommunication. In February 2015, the government issued a draft law linking data protection closer with consumer protection.93 The BDSG will presumably be replaced by the EU General Data Protection Regulation in the beginning of 2018 (see below).

The law on data protection names several requirements for public bodies to process personal data. First of all, the rule applies that every processing of data is forbidden until it has been explicitly allowed by law or by the concerned person. The consent can be withdrawn later and everyone (regardless of his/her nationality) has the right to request information on his/her processed data (§§ 4, 4a, 28 BDSG). A second important requirement is the appropriation, meaning that the processing of data must be really necessary and used for the originally intended purpose (§§ 14, 28, 29, 31 BDSG). There are a few exceptions to the rule, though, e.g. a law, the consent of the person concerned, law enforcement, matters of common welfare or hazard control. The case of unifying data from different sources by reference or content in a single database is contentious and has been discussed on different occasions by Federal Courts.

The collection of some specific kinds of data is restricted, e.g. on religion, ethnos, political opinion, sexual orientation, health and labor union membership.

[93] Cf. German Government (04.02.2015), Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts, retrieved 28.09.2015 from <http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/RegE-UKlaG.pdf?__blob=publicationFile>.

The term personal data includes all data that can be related to a natural person. Data of legal entities are not regulated by the BDSG. Several decisions by the German Constitutional Court define the term “personal data” and extend it to the digital world.

The law on data protection regulates every processing of personal data, including electronic communication. Nevertheless, some norms relate to electronic communication specifically. For example, the Telemedia Act regulates tracking of users on websites since the data collected and merged through several websites can become a threat to privacy (§ 15 Para. 3 Telemedia Act). Furthermore, the Telecommunications Act and the Telecommunications Interception Ordinance protect personal data of telecommunication users from the relevant companies and regulate the companies’ duties with regard to surveillance measures.

The general laws of data protection apply for technologies like security cameras and drones, too. However, the law on data protection mentions video surveillance and the design of technologies dealing with data. Amongst other aspects, technologies and processes must be implemented in a way that hampers the – unauthorized – aggregation of data (privacy by default).

Video surveillance is allowed for three reasons (§ 6b BDSG): the task fulfillment of public authorities, the enforcement of domestic protections and the enforcement of “eligible causes”94. Besides that, the use of cameras has to be indicated, so that people are aware that their actions are being recorded. The enquiry, use and storage of the video data have to be necessary, and if the data is assigned to a specific person, the person concerned has to be notified.

On the European level, Germany is bound to the Data Protection Directive (Directive 95/46/EC) of 1995. It will be superseded by the General Data Protection Regulation soon: After three years of negotiations, the EU Commission, the EU Parliament and the EU Council of Ministers currently in the phase of fine tuning the document. The new regulation will introduce a single set of rules to all EU Member States and will apply to every company based in the EU or processing data of EU citizens. The Regulation includes elements like Data Protection Officers who - similar to the current German law - have to be appointed by all public authorities as well as by companies processing more than 5000 data subjects within 12 months. It also defines fines for companies: a warning in cases of first and non-intentional non-compliance, regular periodic data protection audits or a fine up to one million Euro or up to 5% of the annual worldwide turnover.

6. Data Retention

In October 2015, the German Parliament approved a new bill introducing data retention. There was an earlier attempt to introduce a law to allow data retention that was suspended by the German constitutional court in March 2010. A EU Directive introducing data retention was suspended by the European Court of Justice in April 2014. The new version of the German law has been introduced in May 2015, reacting on the courts’ critique. It changes the StPO, the Telecommunications Act, the criminal code, as some other laws/acts.

[94] These causes are not defined by law, but have to be determined after a weighting to the respective interests of the public and of the parties concerned.

The data retention law targets telephone operators and internet service providers. The relevant data on telecommunication (including text messages) contain the caller, the called person, the timeframe, and the location. With regard to the internet access, user, IP address, and timeframe of the internet access are of relevance. Data regarding e-mails – content as well as meta data – is not part of the law.

The use of the collected data is only allowed in case of severe crimes named in § 100g StPO. The data has to be properly secured by the companies, which will be monitored by the Federal Network Agency. Violations can evoke claims for indemnity and compensation for immaterial damage.

As for the topic of data retention telecommunication providers are obliged to store meta data by own technical means for ten weeks (data on location for four weeks) and hand it over for prevention and prosecution purposes to law enforcement agencies after a formal decision by a judge.

A complaint against the law at the Constitutional Court is very likely and polls indicate a public majority against data retention.95

7. The Exchange of Data

With regard to the exchange of data, the law on data protection determines that Member States of the European Union have to be treated like German authorities. The exchange of data with non-EU countries is only permitted if the concerned person does not have interests requiring protection.

On the European level, an important basis for data exchange with regard to terrorism and cross-border crime is the Prüm Convention. It was signed in 2005 and was partially integrated in EU law in 2008. Amongst other things it enables the signatories to exchange data regarding DNA, fingerprints and vehicle registration.

The G10 Law (§ 7a) allows the international exchange of data and information gained from surveillance under three preconditions: a valuable security issue, a comparable level of data protection and reciprocity. The federal chancellery has to permit the exchange; the G10 Commission and the Parliamentary Commission have to be notified. Especially with regard to the cooperation of BND and the US National Security Agency, the G10 Commission publicly expressed their displeasure about the quality of information provided by the government. Due to a lack of useful information, the commissioners can hardly assess the actual measures and the extent of cooperation. The remedies are limited, at best, since the commissioners, just like the members of the Parliamentary Committee, cannot ask for information on actions unknown to them.

In addition, there were and probably are secret cooperation projects between German and foreign intelligence services. Their legal basis is often disputable.

[95] Cf. YouGov (30.06.2015), Mehrheit gegen Vorratsdatenspeicherung – selbst, wenn sie hilft, retrieved 28.09.2015 from <https://yougov.de/news/2015/06/30/mehrheit-gegen-vorratsdatenspeicherung-selbst-wenn/>.

Conclusion

To some extent, Brazil and Germany have different legal approaches to upholding privacy and data protection and to perform intelligence activities. On the international level, both countries adhere to the main instruments that protect the right to privacy, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. On the national level, Brazil protects privacy as a fundamental right in the Constitution together with the inviolability of home and communications. In Germany, although the right to privacy is not named explicitly in the Constitution, it has been consolidated by decisions of the constitutional court and complemented by the privacy of correspondence, posts and telecommunications and the privacy of the home.

The implementation of these rights at the infra-constitutional level in both countries has some particularities. Different norms regulate the right to privacy and its several aspects in both countries. However, Germany seems to have more specific rules on surveillance activities while the main regulation on privacy in Brazil is related to the interception of telephone communications. The main points of similarities and distinctions can be seen below:

- The Brazilian Constitution protects the inviolability of communications and a specific law regulates the interception of telephone communications, which is allowed only for criminal prosecution purposes and if there is a judicial order. It is worth noting that intelligence bodies are not included among the ones that are allowed to intercept communications according to the Brazilian law. Germany follows a similar approach when it comes to the need of a judicial order as precondition for law enforcement agencies to access personal information from telecommunications and service providers, but the law allows the restriction of privacy of citizens for intelligence agencies with a prior approval by the G10 commission .

- Intelligence agencies in Germany are supervised by a special commission (G10 commission) and have to report to a Parliamentary Committee. Furthermore, affected individuals need to be informed about surveillance measures three months after their end. The Brazilian Intelligence Agency is also under Parliamentary oversight. No provision on notification of individuals was found in the Brazilian law, although the Telephone Interception Act sanctions illegal wiretapping.

- In general, there is a clear distinction of competencies and regulations between police and intelligence agencies in Germany. Even though, privacy-related rights and their constraints are defined in a detailed way, this distinction is about to blur increasingly with new inter-agency competencies and cooperation between law enforcement and intelligence agencies. The Brazilian National Agency of Intelligence (ABIN) was created only in 1999, but unlike Germany, Brazil lacks specific national plan to guide intelligence activities, which could be an important element to more clearly define the framework in which intelligence activities could

operate and that would protect citizens affected by surveillance activities.[96] The difference might reflect a characteristic of Latin American recent democracies where the distinction between the repressive function of the police and intelligence tasks are historically unclear. As Brandão (2014) points out, issues and agents related to internal politics were usually the target for the intelligence agencies during recent authoritarian governments in the region and civil or military bodies gathered enough power and autonomy to centralize both the identification and the neutralization of the so considered "State enemies".

- As part of the European Union, which has a specific directive on data protection, Germany ensures the right to determine the use of one's personal data by the Federal Data Protection Act or the applicable state (Länder) data protection act. Brazil lacks a unified law on data protection and some of its principles were incorporated by jurisprudence through the application of the Consumer Protection Act or other sparse provisions. The role of the judiciary in this case has been central in filling gaps left by the legislation.

- With regards to the processing of data by public bodies, the German law on data protection names several requirements. First of all, the rule is that every processing of data is forbidden until it has been explicitly allowed by law or by the concerned person. The consent can be withdrawn later and everyone (regardless of nationality) has the right to request information on the processed data. A second important requirement is the appropriation, meaning that the processing of data must be really necessary and used for the originally intended purpose. There are a few exceptions to the rule if e. g. the following applies: a specific law, the consent of the person concerned, law enforcement matters, hazard control or matters of common welfare. The case of unifying data from different sources by reference or content in a single meta data base is contentious and has been discussed on different occasions by Federal Courts. Finally, the collection of some specific kinds of data is restricted, e.g. on religion, ethnos, political opinion, sexual orientation, health and labor union membership. In Brazil, the Freedom of Information Act only regulates how personal information can be accessed or disclosed with no formal limitation to what can be collected.

- The recently approved Civil Rights Framework for the Internet in Brazil (Marco Civil da Internet) regulates important aspects of data protection, seeking to grant to Internet users a higher level of protection. Concretely, Marco Civil da Internet brought some limitations on the access to connection and access to application logs by state authorities, such as that they will only be accessible if there is an authorization through a court order. Although such special regulations do exist in Germany, too, basic principles in the online-world have been developed through jurisprudence, particularly by the Federal Constitutional Court. In addition, European law and the European Convention on Human Rights set basis for digital data and communication and the law on data protection regulates every processing of personal data, including electronic communication. While Marco Civil represents in many aspects an improvement to the protection of personal data of Internet users, it is not - and was not meant to be - a law on data protection. Moreover, it leaves to implementing regulation important definitions restrict the possibilities of its application, which means that Germany still has more specific rules for the processing of personal information in the online environment.

[96] The oversight of ABIN's activities is under the responsibility of a Legislative commission composed by 12 members (6 from the Senate and 6 from the Chamber of Deputies).

- Both Brazil and Germany have incorporated provisions on mandatory data retention to their legal framework in the past years. Although the German version has more safeguards and shorter timeframes for retention, the public opposition seems to be stronger than in Brazil. A new complaint at the German Constitutional Court is expected, while no questioning of the constitutionality of the data retention mechanism was formally presented to the Brazilian Constitutional Court until the moment. It is worth noting that Brazilian policymakers started to introduce data retention provisions shortly after the approval of a Data Retention Directive in Europe in 2006. While some of the EU Member States that implemented data retention laws have gradually declared them unconstitutional and the Directive was finally annulled by the Court of Justice of the European Union in 2014, this didn't reverberate in Brazilian courts.

- The exchange of data is regulated through several mechanisms in Germany. Member States of the European Union are treated like German authorities and the exchange of data with non-EU countries is only permitted if the concerned person does not have interests requiring protection. On the European level, the Prüm Convention enables the signatories to exchange data regarding DNA, fingerprints and vehicle registration. The international exchange of data and information gained from surveillance is allowed under three preconditions: a valuable security issue, a comparable level of data protection and reciprocity. Brazil has concluded a number of Mutual Legal Assistance Treaties (MLATs) with different countries to facilitate the process of obtaining evidence for criminal investigations or prosecutions. The countries with which Brazil has MLATs include the United States, Spain, France, Peru, Portugal, Canada, Cuba, Colombia, China and South Korea. The authority responsible for making and receiving requests on these treaties is the Ministry of Justice.

Although a simple transposition of the German model in the Brazil legal scenario would not be suitable, the comparison between the two countries evidences that the regulation of data protection and some of the limits introduced to intelligence in Germany could serve as reference to current legislative efforts in Brazil. This is even more important considering the extraterritorial aspect of the collection, processing, storage and disclosure of data in the digital age.

The comparison of the German and Brazilian legal framework also offers several starting points for an international agreement to foster privacy and data protection. Especially in issues where both countries lack regulations such as the development and use of technologies enabling encryption, anonymity and privacy by the design of software that can support the technological sovereignty of the citizens. Besides that, both countries should work towards international regulations that incorporate the specifics of cyberspace beyond classic international law. It is clear that when it comes to foreign affairs, Brazil and Germany appear to have more proximities than in their domestic legislation. For instance, despite the implementation of data retention in both countries, the foreign ministries have endorsed the restriction of surveillance to a reasonable and effective level and supported the appointment of the UN Special Rapporteur on privacy in 2015.

Considering that several legislative issues are still to be addressed in both countries, especially regarding new challenges both by the evolution of technology, international cooperation can be key in developing solutions in both domestic and international field.