State Surveillance of Communications in Brazil and the Protection of Fundamental Rights

Dennys Antonialli
Jacqueline de Souza Abreu

March 2016

ELECTRONIC FRONTIER FOUNDATION

INTERNET LAB

This report is part of the EFF "Surveillance and Human Rights" project carried out in eight countries in Latin America by the Electronic Frontier Foundation, an international nonprofit organization that, since 1990, defends freedom of expression and privacy in the digital age.

InternetLab is a nonprofit organization devoted to producing impactful research on internet law and policy in Brazil.

"State Surveillance of Communications in Brazil and the Protection of Fundamental Rights" by InternetLab and the Electronic Frontier Foundation is licensed under a Creative Commons Attribution 4.0 International License.

Authors

Dennys Marcelo Antonialli / PhD candidate in Constitutional Law at the University of São Paulo (Brazil), where he also earned his bachelor of laws degree (LL.B., 2008). He holds a Master of the Science of Law from Stanford Law School (J.S.M., 2011) and a Master of Law and Business from Bucerius Law School/WHU Otto Beisheim School of Management in Germany (MLB, 2010). Dennys has worked on the Policy Department of the American Civil Liberties Union of Northern California's (ACLU/NC) technology and civil liberties team and has acted as a legal consultant for the Timor-Leste Legal Education Project (Stanford Law School/Asia Foundation). He has been awarded the first place prize of the 2011 Steven M. Block Civil Liberties award for best written work on civil liberties at Stanford Law School and won the first place prize of the Brazil's Internet Framework Bill & Development Award (Google/FGV-SP). In 2013, he was a research fellow at the Alexander von Humboldt Institute for Internet and Society (Berlin). In July 2014, Dennys attended the Summer Doctoral Program at the Oxford Internet Institute. Currently, he is the coordinator of the Law, Internet and Society Nucleus of the University of São Paulo (NDIS-USP) and the executive director of InternetLab.

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

Collaborators

Francisco Brito Cruz (InternetLab)
Joana Varon Ferraz (Oficina Antivigilância)
Katitza Rodriguez (EFF)
Larissa Ribeiro (Oficina Antivigilância)
Luiz Alberto Perin Filho (Artigo 19)
Mariana Giorgetti Valente (InternetLab)
Paula Martins (Artigo 19)
Seth David Schoen (EFF)

Table of Contents

Purposes and Standards

The purpose of this report is to introduce relevant Brazilian laws and practices on State surveillance of communications, and the protection of fundamental rights. We have identified their strong points and main issues, and made recommendations based on the International Principles on the Application of Human Rights to Communications Surveillance.[1] For the purposes of this report, communications surveillance means interception, monitoring, review, usage, retention, and securing of information that includes, reflects, or stems from someone's past, present, or future communication.

This report analyzes the regulatory framework on State communications surveillance that was in force in Brazil up until March, 2016. After this report was written however, the parliamentary inquiry Commission on Cybercrimes (CPI dos Crimes Cibernéticos) issued a draft of its final report[2] which contained eight bills that may pose significant threats to several of the rights and guarantees laid out in this report such as the possibility of law enforcement to have warrantless access to IP addresses.

1.
Review: virtues and problems in surveillance practices in Brazil

1.1 Constitutional weaknesses in protecting against undue surveillance

The Brazilian 1988 Federal Constitution includes, in its list of fundamental rights, at least three subsections that are relevant to limitations on State surveillance of communications in Brazil. Subsection IV of article 5 protects positive freedom of communications as it assures freedom of speech ("IV – expression of thoughts is free, and anonymity is forbidden"). In turn, subsections X and XII of that same article protect negative freedom of communications, that is, the possibility of keeping them secret or, at least, limiting those to whom they are addressed, as it defines a right to privacy ("X – the privacy, private life, honor and image of persons are inviolable and the right to compensation for moral and property damages resulting from their violation is ensured") and secrecy of communications ("XII – the secrecy of correspondence and of telegraphic communications, data and telephone communications is inviolable, except, in the latter case, under court order, in the events and as provided for in Law for purposes of criminal investigation or penal prosecution").

Although the Brazilian Federal Constitution protects secrecy of communications and privacy, interpretation issues threaten the actual protection that such rights afford against undue surveillance of communications by State authorities.

Controversies: what kind of secrecy do we protect?

First of all, there is the dispute as to the scope of protection afforded under the unclear subsection XII of article 5 ("XII – secrecy of correspondence and telegraphic communications, telephone and data communications is inviolable, except, in the latter case, under court order in the events and as established in Law for purposes of criminal investigations and prosecution"). This subsection provides for the protection of communications secrecy, but its interpretation is all the more challenging given the absence of settled case law and legal scholarship that would allow for a clear determination of constitutional grounds for restrictions to fundamental rights; as a result, such determinations are ultimately made on a case by case basis.

In general, interpretative discussions on subsection XII are twofold: (i) there is dissent as to

whether the subject matter of protection of this fundamental right is information transmitted through the media so listed (correspondence, telegraph messages, data, and telephone calls) or *communication*, that is, the flow of such information while in transit; (ii) there is dissent about which categories, out of the four listed on that subsection, are included in the constitutional exception that allows for breach of secrecy[3] ("except, in the latter case").

Leading scholars[4] are of the view, endorsed in a decision of the Federal Supreme Court,[5] that the protection referred to in subsection XII of article 5 does not refer to information transmitted through correspondence, telegraph messages, data, and telephone calls in itself but rather to communication, and to the flow thereof as it is taking place. Moreover, only the secrecy of telephone communication, while underway, could be breached for purposes of criminal investigation and prosecution; this possibility would not apply to the flow of data, telegraph, or letters.

A large part of this dispute aims at identifying a core of *absolute* protection under article 5, subsection XII, on which any restriction would be unconstitutional: according to the above understanding, correspondence, while in transit, would be absolutely inviolable. Although that position is advocated by some legal scholars, it is not mirrored in case law, which has already accepted the "breach" of secrecy of communications flow of all types as long as it is "proportionate," whenever it is based on a fundamental right or the public interest.[6]

What's more, the limited interpretation that only information flows would be protected under article 5, subsection XII, would be insufficient to protect either the content of communications that have been stored, logged or recorded, or even information about the circumstances in which communications took place (metadata). This interpretation is also at odds with that of the Inter-American Court of Human Rights in the Case of *Escher et. al. v. Brasil* (as further explained in section 2.5 of this report).

Privacy grading: account information < metadata < content?

Even if case law and Brazilian legal scholarship hold that only the flow of communications enjoys protection under subsection XII of article 5, the right to privacy (provided for in a general fashion under subsection X of the same article) allows for protection of communications in a broader sense[7] including not only the content of communications, but also information about the circumstances in which they took place and between whom they happened (which may be revealed with account information[8] and metadata[9]).

As we will see below, ordinary legislation and case law grant different levels of protection to such different categories of information, that is, account information, metadata, and content of communications itself. This means that the degree of privacy afforded to information depends on the nature of the information.

For instance, recent legislative changes have provided less protection for account information since such information was perceived as less privacy-sensitive. In practical terms, these legal changes were made to facilitate authorities in obtaining such information simply by requesting it, without the need of a court order.[10] That provision might be partially explained as an inappropriate repercussion of the Brazilian "constitutional prohibition of anonymity," dictated in subsection IV to article 5, which, although it should apply only in instances of expression of thought, has been wrongly used to justify using data for identifying wrongdoers in any context.

Breach of secrecy of metadata has received a legislative treatment that varies depending on whether it relates to telephone or Internet data, and a court order is usually sufficient. Interception, that is, access to the content of communications, requires compliance with constitutional purposes and specific legal requirements, which must be assured by means of court orders.

Some may advocate the view that subsection XII, article 5 protects only the flow of communications and assume that account information and metadata are less relevant to privacy. This position fails to account for the central role that account information and metadata play in identifying users and inferring information about their interests, contacts, and activities. As a result, the limits on State surveillance in Brazil imposed by fundamental rights leave metadata and account information with less legal protection. As legal scholars and privacy experts from more than 70 countries around the world explained in the International Principles on the Application of Human Rights to Communications Surveillance,[11] it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information—but as technology evolves, it is now clear that metadata and other forms of non-content data may reveal even more about an individual than the content itself, and thus deserves equivalent protection.[12]

1.2 ANATEL: "unintentional" actual surveillance

Within its jurisdiction to pass regulatory provisions (article 19 of Law no. 9.472/97), which are *resoluções,* and in discharging its duties as a telecommunications regulatory agency, *Agência Nacional de Telecomunicações* (ANATEL) regulates and monitors the provision of services and enforces users' rights, not without creating significant surveillance potential. The lack of precision and clarity in ANATEL's resolutions, as well as insufficient transparency about the way they are enforced, expose telecommunications services users to unlawful State surveillance.

Telecommunications service providers' duties

Article 22 of *Resolução* no. 426/05 – *Regulamento do Serviço Telefônico Fixo Comutado*

[Fixed Switched Telephone Service Regulation] requires that "all data referring to provision of services, including phone records," shall be retained by fixed telephone service providers (such as Vivo and NET) "for a minimum of five years," without a precise description of what data is included, or by whom it may be used and for what purposes. There exists no specific security rules regarding the storage of this data: article 23 only establishes it is the providers' responsibility to protect the confidentiality of the data. Article 24 orders fixed telephone service providers to have technological resources and facilities sufficient to breach telecommunications secrecy within the scope of court orders, and that providers must bear the financial costs of maintaining such technology.

Resolução no. 477/07 – Regulamento sobre S*erviço Móvel Pessoal* [Personal Mobile Service Regulation] similarly establishes, in article 10, XXII, that mobile service providers (such as Vivo, Claro, Tim and Oi) shall keep, for a minimum of 5 years, "at the disposal of ANATEL and other parties in interest, billing documents (*documentos de natureza fiscal*) that contain data on incoming and outbound calls, dates, time, duration, and price, as well as account information of subscribers, in accordance with the provisions of article 11 of Law no. 8.218/91 [...]." That law requires legal entities to retain billing/tax documents at the disposal of Brazil's Federal Revenue Department for the period set forth in tax legislation to bring disputes to court (*prazo decadencial*), which is five years. Articles 42 and 58 also establish "minimum personal data" that users need to disclose to join a mobile telephone service (name, identity card number, and taxpayer number). In practice, that makes registration of a mobile dependent on a taxpayer number, which compromises anonymous usage.

The rationale of the five-year data retention obligation referring to telephone service, and justification thereof for purposes of billing audits and supervision by ANATEL are indicated under article 10, XXII of *Resolução* no. 477/07. However, both rules establishing data retention obligations for fixed and mobile telephone have long allowed for the convenience of keeping such records for the State's investigatory and prosecution purposes. Law no. 12.850/13 [Criminal Organizations Law], which required telephone companies to retain data expressly to that end, dates only to 2013. Moreover, provisions of these *resoluções* establish data retention obligations even for services under flat-rate plans, where a call's duration or the number called do not affect the amount paid by the user. It's thus reasonable to suppose that ANATEL regulations related to gathering data include purposes beyond those associated with its responsibilities.

Article 53 of *Resolução* no. 614/13 – *Regulamento do Serviço de Comunicação Multimídia* [Multimedia Communication Service Regulation] requires Internet connection providers (such as Vivo and NET) to retain connection logs and subscribers' account data for at least one year. The definition of connection logs is established in article 4, XVII (the set of information referring to date and time of use of a connection to the Internet and a given IP

address used at the terminal for incoming and outbound data packets, among other data that permits identification of the access terminal used). The shorter retention term compared to data retention obligations for telephone services, as well as the clear description of what data needs to be retained, might be attributed to the fact that the regulation was drafted while discussions on Law no. 12.965/14 (*Marco Civil da Internet*) were ongoing and to publicity concerning international decisions against data retention, which received particular attention from the academic community and civil society.[13]

Direct access to data

ANATEL's access to service providers' billing documents *(documentos de natureza fiscal)*, which, as we have seen, contain customers' account data, usage logs, and call prices, is generally available for inspection purposes whenever the agency requests it of a provider.

An article in the daily newspaper *Folha de São Paulo in* 2011[14] revealed the agency's intent to have direct and systematic access to such data by building infrastructure that enabled ANATEL to have unlimited *online* access with a view to modernizing its oversight capabilities. At that time, the agency stated that access to phone records would only take place with permission of users who requested the logs' disclosure,[15] and that the software to be installed would only allow access to providers' raw data, unrelated to account information.[16] Article 38 of ANATEL *Resolução* no. 596/12 established telephone service providers' obligations to provide data, allow access, and make available online access to applications, systems, technological resources, and facilities used by them "for collection, processing and submission of data, information and other features," thus confirming *Folha*'s reporting. ANATEL's previous pledges concerning limitations on its access to user data were not expressly implemented under this *resolução*.

1.3. Brazil's Federal Revenue Department: communications surveillance "in between the lines"

Article 10, XXII of the aforementioned ANATEL *Resolução* no. 477/07 reveals that the rationale behind the obligation to retain account information and telephone logs for at least five years is closely related to article 11 of Law no. 8.218/91, which requires legal entities to keep billing documents at the disposal of Brazil's Federal Revenue Department for the period set forth in the tax legislation. It means that not only ANATEL, but Brazil's Federal Revenue Department itself may, in the course of its tax management and auditing responsibilities duties, gain access to information on users' communications, by requesting billing documents that contain such data (in the case of mobile telephone, to which the *resolução* in question applies, at least number called, time, date, duration, and prices associated with the account or call).

Because the obligation to retain billing documents extends to all legal entities, Brazil's

Federal Revenue Department's prerogatives could potentially reach every telecommunication user in Brazil whenever such documents are capable of disclosing information on users' communication behavior, even if only from metadata and account information.

In July 2015, *Oficina Antivigilância* highlighted the recent execution of an agreement between the US Department of Homeland Security, US Customs and Border Protection, and Brazil's Ministry of Finance, through Brazil's Federal Revenue Department, for "mutual recognition" of the US agency's "Customs-Trade Partnership against Terrorism" program and the "Authorized Economic Operator" program of Brazil's Federal Revenue Department, which would involve transfer of data processing infrastructure, and development and usage of common information technology.[17] Since Brazil's Federal Revenue Department has potential access to detailed information on Brazilians' communications, such cooperation may lead to an expansion of communications surveillance.

1.4. Surveillance with and without checks and balances: telephone vs. Internet

Two recent federal laws have regulated State surveillance capacity for purposes of law enforcement: the signing of a new Criminal Organizations Law and of the *Marco Civil da Internet*. While the former gives rise to serious concerns about abuse of surveillance powers, especially in the telephone industry, the latter—developed in the context of broad and extensive public debate—both enables and limits surveillance on the Internet.

Criminal Organizations Law (Law no. 12.850/13)

Telephone log retention obligation

Article 17 of the Criminal Organizations Law establishes that "fixed or mobile telephone concessionaires shall keep, for five years, at the disposal of the authorities referred to in article 15 [chief of civil police and Public Attorney's Office], records for identification of incoming and outbound terminal numbers of international, long distance domestic and local calls." This obligation's presence in the Criminal Organizations Law suggests that it was intended for the legitimate purpose of investigating criminal organizations, but unfortunately the law contains no provisions that restrict the use of the retained data to investigations of organized criminal activities.

Inclusion of such a broad obligation in such a specific law may have concealed the enhancement of State surveillance power that it represents, all the more so since it went virtually unnoticed in public and academic debates, was not scrutinized for legality, necessity nor proportionality, and did not include detailed specifications of the data to be

logged, the entities to which it applied, access limitations and usage conditions, nor data security rules. The constitutionality grounds of this such provision was challenged under a *Ação Direta de Inconstitucionalidade* (ADI 5063/DF), which is awaiting trial and will be discussed further below.

Account information access prerogatives

Article 15 of the Criminal Organizations Law establishes that "the chief of civil police and the Public Attorney's Office shall have access, irrespective of court order, only to such account information of the accused that indicates personal qualification, parents and address retained by Electoral Courts, *telephone companies*, financial institutions, *Internet providers* and credit card administrators (emphasis added)." That provision repeats language existing in article 17-B of the Money Laundering Crimes Law (Law n. 9.613/99), which was recently added by Law no. 12.683/2012.

It should be noted that the rules that waived the requirement to obtain a court order for access to such information stem from a recent legislative reform. Previously, the possibility of breaching secrecy of account information without court order was a controversial matter among legal scholars and in case law. That was so because, although article 6, subsection III of the Code of Criminal Procedure allows Police authorities "to gather all evidence useful for clarification of the fact and circumstances" whenever informed of commission of a criminal offense, and article 8, subsection IV of Supplementary Law no. 75/93 allows the Federal Attorney's Office to require "information and documents from private entities" in performing its duties, which applies on a subsidiary basis to state entities (article 80 of Law no. 8.625/93), access to such information was rejected by companies based on the argument that the information would be protected under article 5, subsection X, of the Federal Constitution, and hence court orders were required for breach of secrecy.[18]

Recently enacted provisions changed these rules in response to investigative authorities' pressure for specific legislative authority granting them "free access"—merely upon a simple request—which would make investigations and legal proceedings much more efficient. Although legislation on organized crime and money laundering now allows them to access this information upon request, the authorities mentioned above are also working to expand their access to this data for other purposes, since the legislation did not expressly limit the purposes for which it could be used.[19] In practice, such authorities use these provisions to support data requests to telephone service providers; only if a company refuses to comply will the matter be submitted to a court for review.

Access prerogatives to telephone logs too?

Since the enactment of the Criminal Organizations Law, authorities with appropriate jurisdiction, but especially chiefs of civil police, have requested telephone logs from telephone companies without court orders, based on their combined interpretation of

articles 15, 17, and 21 of that law.

Under article 15, "chief of civil police and Public Attorney's Office shall have access, irrespective of court order, only to such account information of the accused that indicates personal qualification, parents and address" retained by telephone companies. Article 17, however, orders landline and mobile telephone companies to keep "identification logs of number of originating and destination telephone connection terminals" for five years "at the disposal of the authorities referred to in article 15". In turn, the main clause of article 21 criminalizes the refusal or failure to submit "account information, logs, documents and information demanded by the court, Public Attorney's Office or chief of civil police, in the course of investigation or proceedings," and establishes penalties ranging from six months to two years of incarceration, plus a fine. As a result, such authorities have demanded not only account information but also telephone logs (and even some location data), without court orders. Direct demands are made to companies under threat of punishment if they fail to comply.

Ação Direta de Inconstitucionalidade (ADI 5063/DF, referred to above), a constitutional challenge, was filed in the Federal Supreme Court by the *Associação Nacional de Operadoras Celulares* (ACEL), seeking to vacate these articles, on grounds that they violate the right to privacy and the principle of legality, since the rules' imprecision gives rise to legal uncertainty.[20] That action is still awaiting trial.

Marco Civil da Internet (Law no. 12.965/14)

Data retention obligations

With respect to connection logs, article 13 of *Marco Civil da Internet* establishes that "when providing an Internet connection, the relevant independent system provider (such as Embratel, Oi, UOL Diveo and many others like some universities for example) has the duty to keep connection logs, confidentially and in a secure, controlled environment, for a period of one year, pursuant to the applicable regulations." Subjects of the obligation, "independent system administrators" are, according to article 5, IV of the law, an "individual or legal entity that manages IP address blocks and relevant independent routing system, duly enrolled with the national agency in charge of recording and distributing IP addresses for the country," thereby reaching those Internet access providers that meet this definition.[21]

According to article 5, subsection VI, connection logs are "the set of information pertaining to date and time of beginning and ending of a connection to the Internet, duration thereof and IP address used by the terminal to send and receive data packets." Because of the risk to web users' privacy, article 14 forbids connection providers to retain logs of access to applications (that is, particular online sites or services).

In turn, article 15 of *Marco Civil da Internet* establishes that "Internet application providers organized as legal entities and engaged in business in an organized, professional manner and for purposes of profit shall keep records of access to Internet applications confidentially, in a controlled and secure environment, for six (6) months pursuant to the applicable regulation." According to article 5 subsection VII, an application is the "set of functionalities that may be accessed by means of a terminal connected to the Internet."

The subject of the obligation, here, is not every application provider, but only those engaged in such activity in a commercial capacity. Non-commercial application providers may, however, upon a court order, be required to retain data, "as long as it refers to logs pertaining to specific facts of a determined period of time," as provided for in § 1 of article 15. The particular data covered by the general data-retention obligation for application providers is, according to the definition of article 5 subsection VIII, "the set of information referring to date and time of use of a given Internet application on a given IP address."

With respect to the obligation to retain Internet connection logs and access to applications logs in general, three comments are also pertinent. First, § 2 of article 13 and § 2 of article 15 admit the possibility of motions, by means of injunctive proceedings, to extend data retention periods for particular entities in particular situations, and there is no rule about the maximum term for such extension. Second, article 10, § 4 and main clauses of articles 13 and 15, refer to security measures for retention and availability of logs while article 12 to penalties for violation thereof. Third, the regulation to which articles 13 and 15 refer, and which will probably introduce further specifications regarding those liable for retaining and for taking security measures is yet to be passed; it has, nonetheless, been through a preliminary stage of public inquiry, having gathered recommendations and debates, and is being structured. It is expected to enhance protection against undue surveillance.

Account information access prerogatives

Article 10, § 3 of *Marco Civil da Internet* establishes that protection to personal data and private communications as assured under the main clause "does not prevent access to account information that indicate personal identification, parents and address, as provided for by law, by administrative authorities that have appropriate jurisdiction to obtain such information." With regard to this provision, members of the academic community and civil society have argued that the regulatory Decree prescribed by *Marco Civil da Internet* should clarify the limits of such access to prevent abuse, and expressly identify the authorities with appropriate jurisdiction, be it by demanding a close relation between the requesting authority and the particular grounds for its data request, or by preventing access without court order and limiting it to the terms of the Criminal Organizations and Money Laundering Law.[22]

The Decree is also expected to deal with requests for account information made using data contained in application access logs (originating IP address and time), which, in principle, might circumvent the requirement for a court order in order to breach the secrecy of Internet connection logs.[23]

Access to Internet connection logs and access to applications logs

Article 10, § 3, of *Marco Civil da Internet* specifically establishes that access to Internet connection logs and access to applications logs will depend on court order, a protection that is reinforced by articles 13, § 5 and 15, § 3. In turn, article 22 limits its purposes to "production of the body of evidence in civil or criminal cases," and establishes the requirements that the "party in interest" must meet to be granted such a court order: solid indicia of wrongdoing; justification of the utility of the requested logs for the purposes of investigation or discovery; and the period to which such logs refer.

Finally, article 23 entrusts the court with "taking the necessary steps to assure confidentiality of information received and preservation of the user's privacy, private life, honor and image, and may order that cases be heard in camera, including with respect to motions for log retention."

Access to stored private communications

Breach of secrecy of electronic communications content in the possession of Internet application providers (such as Google and Facebook) is also covered by the *Marco Civil da Internet*, under articles 7, III and 10 § 2, which require a court order to that effect. These provisions, along with article 11, which demands compliance with Brazilian legislation by providers that gather, retain or process data in Brazil, were probably included in *Marco Civil da Internet* to build stronger legal grounds for turn over requests of data retained abroad.

Before the enactment of *Marco Civil da Internet,* it was allegedly more difficult to demand providers to turn over such data as providers could more easily claim that the data were subject to foreign legislation, requiring that specific international court proceedings were followed.[24] As a result, § 2 of article 11 expressly established that "the provisions of the main clause apply even where activities are performed by legal entities headquartered abroad as long as they provide services to Brazilians or at least one member of the same Brazilian economic group has operations in Brazil." Even if, on the one hand, *Marco Civil da Internet* more clearly established court order protection for some categories of evidence production, on the other hand, it expanded Brazilian State surveillance capabilities.

Moreover, the inclusion of such provisions in *Marco Civil da Internet* did not solve this question of jurisdiction as providers may still challenge the application of Brazilian law to data retained abroad, which has led to controversial and disproportionate court orders.[25]

Expanding surveillance absent regulation on telephone communications

Telephone surveillance for purposes of law enforcement is improvised in the Criminal Organizations Law. There is no systematic Law regulating safekeeping obligations, circumstances under which access is allowed, nor the purposes served by it. That is, there is no "Telephone Communications Bill of Rights" limiting surveillance. The application of international human rights law in this context has been ignored. For instance, there is no provision limiting breaches of confidentiality to criminal cases, and excluding civil cases, or narrowing down call logs (calls received and made, date, time, and duration) over which such safekeeping obligations shall apply and that it shall not apply to location data (Radio Base Stations, by way of example). In practice, the result is that confidentiality of *any* metadata generated over the telephone is breached *whenever* a Court order so determines.

A symptom of that is the case decided by the Court of Justice of Rio Grande do Sul in July 2007 that allowed breach of confidentiality of location data from a mobile user in default of alimony under the records of a proceeding to enforce this obligation. The defendant under the proceeding was ordered to pay alimony and failed to do so without cause, hence a warrant was issued for his arrest. Identification of his location was attempted many times without success. In view of that and "to fully protect children and teenagers," the Appeals Court Judge allowed "telephone tapping," as it was called, to gather data on the location of the defendant based on the number of his mobile phone.[26]

Marco Civil limiting surveillance on the Internet

The *Marco Civil da Internet* is, on the other hand, already yielding fruit in terms of limiting undue surveillance. In a ruling from April 2015,[27] the São Paulo Federal Court invalidated a request from a Federal Police officer to Twitter for "as much data as possible, such as applicable machine IP access, access dates, full identification and account information of user @EnkiEa666." The Federal Police argued that § 3, article 10, of *Marco Civil da Internet* "allows administrative authorities to request account information and Law no. 12.830/2013 expressly authorizes police officers, during the course of a police investigation, to request data and information relevant to the investigation," as determined by article 2, § 2, of that law.

In his ruling, the federal judge acknowledges that the request submitted by the police authority encompasses not only users' account information but also application access logs and states that "the law [*Marco Civil da Internet*] allows competent administrative authorities to request information from Internet providers concerning their users, provided such information is limited to account information, such as personal identification, parental information and address. Hence, it is my opinion that information relative to connection logs and Internet application access logs, as well as personal data and content of private

communications, is subject to court order as expressly determined by article 10, § 1 of Law no. 12.965/14." With regard to account information, the judge accepted the clarification provided by Twitter—that it did not have information such as user's full name, address and parental information—and, as to application access logs, concluded that Twitter did not have an obligation to make this data available due to the lack of a court order compelling its disclosure.

1.5. Interception: surveillance limited in theory but extensive in practice

Theory: Telephone Interception Law and CNJ and CNMP Resolutions (Resoluções)

Law no. 9.296/96 ("Telephone Interception Law") governs this traditional surveillance procedure in Brazil. Article 1, sole paragraph, of that law expands the scope of the regulation to "interception of communications flowing through information technology and telematics," thus including data communications flows over the Internet, such as emails. Within the context of the controversy about the proper interpretation of the constitutional provision protecting secrecy of communications, the constitutionality of this provision was challenged based on the understanding that only the flow of *telephone* communications, not other kinds of communications, could be intercepted limited for criminal investigation purposes.[28] However, the *Ação Direta de Inconstitucionalidade* was dismissed on procedural grounds. Currently, article 7, subsection II, of the *Marco Civil da Internet*, also allows for interception of the flow of communications over the Internet, by court order, "in the form required by law" (in reference to the Interception Law).

Interception of the flow of communications occurs, pursuant to the provisions of the main clause of article 1 of Law no. 9.296/96, for purposes of criminal investigation or discovery in a criminal proceeding, by court order, sua sponte ("*ex* officio") or upon request from a law enforcement officer or the Public Attorney's Office (art. 3). In light of such provisions, interception requested by authorities not expressly designated, such as the *Agência Brasileira de Inteligência* (ABIN), is prohibited. Article 2 limits even further the circumstance under which it may occur: it shall *not* be allowed in case there is no reasonable evidence of criminal responsibility or conspiracy to commit a crime; in case evidence can be obtained by other means; or when the act under investigation is subject to no more than an imprisonment sentence of the type "*detenção*" (common for misdemeanors).

The sole paragraph of article 2 and articles 4 and 5, in turn, ensure that interception shall only occur if duly justified: an interception request shall be supported by a clear description of what is being investigated, including naming and identification of the subjects, unless this is clearly shown to be infeasible; the request shall specify the grounds for the investigation

and the means to be employed; the ruling shall establish how it is to be carried out. Article 5 provides that the period of interception shall not exceed 15 days, subject to renewal by court order: it shall be "renewed for an equal period of time when its necessity is required for evidentiary purposes." Although article 5 could admit the interpretation that the maximum period of time for interception is 30 days, prevailing court precedents [29] are of the opinion that an interception order may be renewed for *as long as* it is required. Article 7 grants police authorities powers to request "services and specialized personnel from public utilities" to perform interception procedures. Article 8 requires confidential treatment of records of interceptions, and article 9 requires their destruction if they are not useful, or cease to be useful, for evidentiary purposes. Unlawful interceptions are deemed crimes under article 10. In view of the above, it may be argued that, as a general rule, the Telephone Interception Law contains provisions aiming to ensure that interception shall only occur in cases in which great public interest justifies the burden of the restriction on communications privacy.

A regulation issued by the National Justice Council (CNJ), *Resolução* no. 59/08, administratively provides for the procedure for requesting interception, establishes standards for court decisions on the matter, defines the form in which notices to companies of interest shall be submitted, and holds judges responsible for protecting the privacy of intercepted information. *Resolução* no. 36/09 of the Public Attorney's Office National Council (CNMP) contains similar provisions regarding request forms and execution of interception.

The purposes of such resolutions, which fill in a legislative void, are to limit the possibilities for abuse when issuing court orders, mitigate risks that may affect secrecy and, hence, success of the investigations, and increase the security of intercepted information. Furthermore, they also establish that members of the Public Attorney's Office and judges shall inform, respectively, the Inspector-General of the Public Attorney's Office (*Corregedoria-Geral do Ministério Público)* and the Inspector-General of the National Judiciary Office (*Corregedoria Nacional da Justiça*), on a monthly basis, of the number of ongoing interception operations (art. 10 of CNPJ *Resolução* no. 36/09 and art. 18 of CNJ *Resolução* no. 59/08), for statistical purposes.

Practice: diffuse use of interceptions

Case of Escher et al. v. Brazil – Inter-American Court of Human Rights

Brazil was found guilty by the Inter-American Court of Human Rights (IACHR), in July 2009, and ordered to compensate workers of farming cooperatives associated with the *Movimento Sem-Terra*, due to improper telephone interception operations carried out in the State of Paraná in 1999.[30] Such interception operations, which lasted 49 days, were ordered by a court without a proper legal basis, upon request from an inappropriate

authority (Military Police Department), outside the scope of any ongoing criminal investigation, and without notice to the Public Attorney's Office, all in violation of the Telephone Interception Law. In addition, excerpts of the interception protected by *in camera* proceedings were leaked and subsequently willfully disclosed in a press conference called by the State of Paraná Secretary of Public Security days after the recording—also in clear violation to the Telephone Interception Law.

To make matters even worse, the authorities involved in the unlawful interception were not held liable by any Brazilian court. According to the IACHR, Brazil violated the victims' right to private life, honor, and freedom of association, in addition to court protections and assurances of the Inter-American Convention on Human Rights. CNJ and CNMP *Resoluções* may be put into context by this case.

The IACHR has also expressly recognized that the right to privacy encompasses protection of not only the content of communications but also of metadata: "[The right to privacy] applies to telephone conversations irrespective of their content and can even include both the technical operations designed to record this content by taping it and listening to it, or any other element of the communication process; for example, the destination or origin of the calls that are made, the identity of the speakers, the frequency, time and duration of the calls, aspects that can be verified without the need to record the content of the call by taping the conversation. In brief, the protection of privacy is manifested in the right that individuals other than those conversing may not illegally obtain information on the content of the telephone conversations or other aspects inherent in the communication process, such as those mentioned."[31]

Police spy software on hacked mobiles?

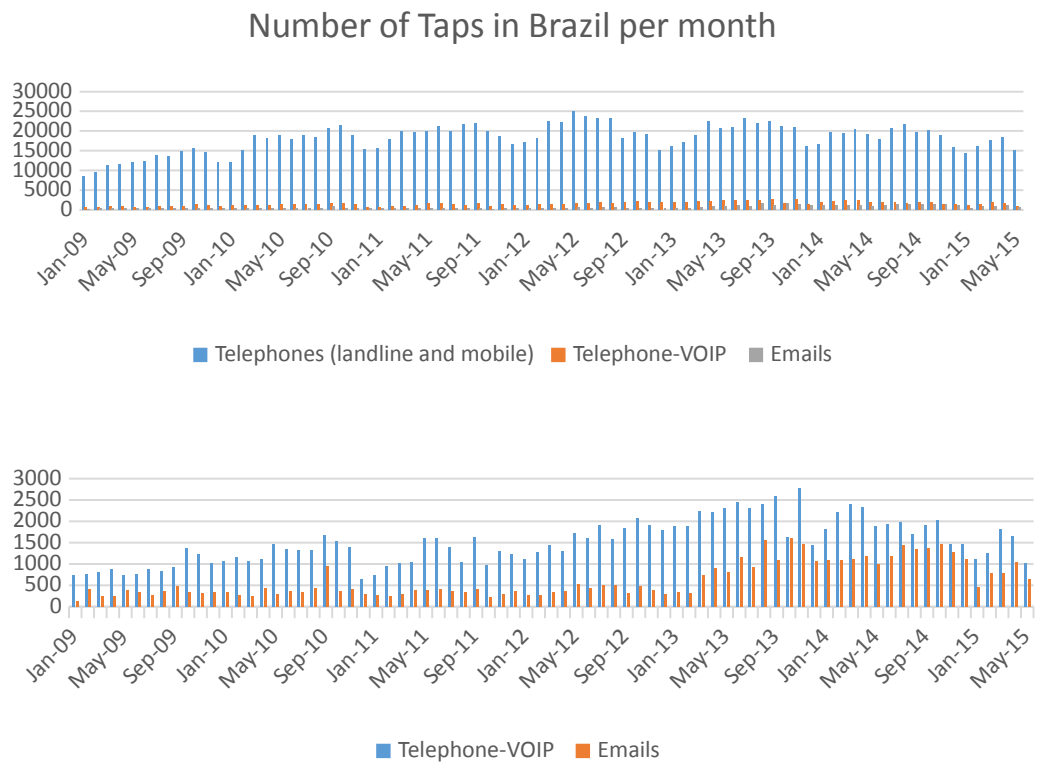
In April 2015, a news article published by *Folha de São Paulo* revealed that the Federal Police is trying to increase access to information stored in mobile telephones subject to court-ordered interceptions.[32] That is because, currently, the technology used in interception operations only allows access to SMS messages and calls, but not to messages exchanged using Internet-based applications, such as WhatsApp, whose use has been growing. The article indicates that the Federal Police "wants telephone companies to purchase spy programs," which is being opposed by such companies due to the high costs of purchasing these programs and using the subscriber's data package to transfer copied information from those under investigation. In addition, the article also mentions that during operation *Lava Jato*, which revealed the corruption scandal involving Petrobras, the Federal Police only managed to access messages from the black market dealer, Alberto Youssef, "because it convinced BlackBerry to grant access to conversations using BBM, an instant message service for BlackBerry devices."

The article highlights, on one hand, the need for regulation on the type of data to which

access shall be granted by interception, so as to comply with the legality and proportionality principles applicable to limitations to fundamental rights and, hence, impose limits that enable control over State power. Use of malware, even within the scope of court ordered interception operations under ongoing criminal investigations, such as those mentioned by the news article, raises concerns that go beyond secrecy of communications and affect integrity of communications and systems.[33] (On this matter, also see *Cooperating with Hacking Team?* below). On the other hand, the article also shows how a regulatory deficiency gives room to "non-statutory covenants" to obtain data protected by rights to secrecy of communications and to privacy.

National System for Interceptions Control

Due to the provisions of *Resolução* nº 59/08 issued by CNJ, criminal court judges all over the country are mandated to inform the Inspector-General of the National Judiciary Office about data relative to telephone interception operations, as well as interception of information technology and telematics systems using the National System for Interceptions Control (*Sistema Nacional de Controle de Interceptações*), which receives information on notices submitted to service providers, proceedings filed and numbers of telephones, telephones-VoIP and emails under surveillance. Such data is not available to the general public and was obtained by InternetLab through the Access to Information Law.[34]



The charts show that the average number of telephone lines under surveillance per month in Brazil exceeds eighteen thousand. It is also noted that the number of email addresses and telephones-VoIP has grown in the past months. To explain what these and other numbers gathered from the National System for Interceptions Control represent with regard to the application of the Telephone Interception Law by the courts in Brazil, it would be necessary to have access to the total number of requests for interception submitted or, alternatively, to the number of requests for interception dismissed by the judges.

Comparing Brazil to other countries does not help with this assessment, for there are not equivalent criteria to prepare comparative statistics. What is known is that in 2013, the number of authorized wiretap orders in the United States, a country whose population is 120 million above that of Brazil's, was 3.576.[35] There is no information as to the number of court orders authorizing interception granted in Brazil, but it is known that 13.309 new criminal interception procedures were filed in 2013.[36] In turn, Germany, a country with less than half the population of Brazil, issued 19.398 initial interception orders (*Erstanordnungen)* in 2013.[37] In Brazil, what is known is that 50.265 interception notices were sent to telecommunications companies during the same period of time.[38]

The statistics relative to interception in Brazil of the National System for Interceptions Control deserve a study of their own. If they are *high,* this fact may suggest, on one hand, that the theoretical protection expected (from the need of court order and definition of strict requirements for such procedure set forth by the Interception Law) does not apply in practice. On the other hand, it may also flag structural deficiencies in investigation capabilities of law enforcement authorities, rendering them highly dependent on this aggressive evidence-gathering method.

1.6. Non-transparent surveillance for intelligence and national security purposes

Sisbin's scope

Law no. 9.883/99 created the Brazilian System of Intelligence (Sisbin) to integrate planning and execution of intelligence tasks in Brazil so as to provide the Brazilian President with subsidies on matters of national interest, to obtain, review and disseminate knowledge relevant to government actions and decision making processes, as well as to ensure security to society and the State (article 1). Sisbin is comprised of all Federal Public Administration bodies responsible for producing knowledge relevant to intelligence activities (article 2) specified under article 4 of Decree no. 4.376/02, including the Office of the Chief of Staff, Institutional Security Cabinet of the Presidency of the Republic, Ministries of Justice, Defense, Foreign Affairs, Health, Finance, Science and Technology, among others, and related bodies, such as Federal Police Department, National Correctional Department, International Legal Cooperation Department, Brazil's Federal Revenue Department and

Central Bank. The core body constitutes the Brazilian Agency of Intelligence (ABIN), competent to plan, execute, monitor and control intelligence activities.

ABIN may have access to data obtained by other authorities through cooperation within the Sisbin. Article 6, item V, of Decree 4.376/02 regulating operation of Sisbin, determines that the bodies of this system shall exchange and provide the information required to produce knowledge of intelligence activities. Article 6-A of the same Decree, added in 2008, establishes that ABIN shall have representatives within Sisbin bodies at its Sisbin Integration Department, which "shall have the right to access, by electronic means, data bases of their bodies of origin, subject to the rules and limits of each institution and the laws governing security, professional secrecy and protection of confidential matters" (§ 4). Based on that, it is possible for ABIN to have access to information and data originally protected by the right to secrecy of communications, thus expanding the possibilities of surveillance by the Brazilian State.

Despite the fact that it is not competent to engage directly in interception activities, by way of example, because it was not granted intelligence purposes by the Constitution or by the Interception Law,[39] accessing data by means of cooperation should not be discarded. A case disclosed by *Folha de São Paulo* in 2008 revealed this kind of indirect access by ABIN to intercepted communications available in a Federal Police System (*Guardião*).[40] If Brazil's Federal Revenue Department holds billing documents of telephone companies in its data base, ABIN would be allowed access to users' telephone logs.

Under Law no. 9.883/99, Sisbin, as a general rule, and ABIN, in particular, are required to comply with Constitutional rights and assurances while performing their activities (article 1, § 1 and article 3, sole paragraph), subject to outside control and monitoring by the Joint Commission on Control of Intelligence Activities (*Comissão Mista de Controle das Atividades de Inteligência*), a permanent commission of the Brazilian Congress (article 6). Inadequate transparency as to how cooperation within the Sisbin takes place prevents a more accurate assessment from ABIN in terms of surveillance for purposes of intelligence and surrounds its activities in shadows and uncertainties.

COOPERATING WITH HACKING TEAM?

A contribution of Artigo 19 and Oficina Antivigilância

On July 5, 2015, the Italian company *Hacking Team—known* for developing and selling spy software and surveillance tools to governments and assisting law enforcement and military institutions to spy on computers, tablets, and mobile phones of citizens around the world—was *hacked*. As a result, 400 GB of internal documents, including private emails, invoices, client lists, and source code of commercial products were made available over the Internet.

The documentation leaked contained several references to Brazilian intelligence bodies, both civil and military, as well as to Brazilian companies that seem to be Hacking Team's local partners. Among the bodies mentioned in the files are: Brazilian Intelligence Agency (ABIN),[41] Army's Intelligence Center (CIE),[42] Cyberwar Instruction Center (CIGE),[43] Rio de Janeiro Civil Police Department (CINPOL[44] and DRCI[45]), Rio de Janeiro Military Police Department,[46] São Paulo Civil Police Department,[47] São Paulo Military Police Department,[48] Federal District Civil Police Department,[49] Federal District Military Police Department,[50] Ministry of Justice,[51] and the Office of the Attorney General for the Republic.[52]

The file is extensive and requires a careful review, including confirmation of authenticity of each document and, so far, it has not been possible to state that such agencies actually managed to purchase "solutions" from the Italian company. The only exception seems to be the Federal Police,[53] as a search through the files, even though cursory, revealed an exchange of emails between agents and Hacking Team's employees,[54] reports of trainings in Brasília,[55] and several documents, including a product delivery certificate,[56] confirming negotiation and purchase of the RCS (*Remote Control System*) system from Hacking Team for a three-month period pilot project.

Even if the documents are authentic, what is not clear, however, is what administrative proceeding followed to complete the purchase. In the emails, there is only one reference to Law no. 13.097, on January 19, 2015, which waives bidding procedures for purchases of "sensitive equipment required for police investigations." There is also a reference to a court order[57] that would have been issued in the first half of 2015, granting the Federal Police Department legal grounds to use the solutions purchased for 15 days (as of contamination) on 17 target telephones.

The RCS, according to Hacking Team, is a discreet spyware-based system, designed to attack, infect and monitor computers[58] (Windows, Mac OS, Linux) and smartphones (Android, BlackBerry, Windows Phone and jailbroken iOS). The tool allows for monitoring and control of an infected device's data and activities: it is possible to see stored files and which ones were opened recently, deleted or printed; to turn on the microphone and camera and capture images or sounds; to have access to chats, emails, SMS, and location; to listen to conversations via Skype (VoIP) and voice telephone calls; and to even capture every keystroke. The RCS employs several infection techniques that may be physical or remote: through USB flash drives; Wi-Fi networks; video streaming; email attachments; and simple links to fake sites.

Generally speaking, the leaked documents raised even more questions regarding the growing surveillance market in Brazil and pointed to the need of legal discussions about the kind of data that may be accessed by interception, in particular taking into account the evolution of new surveillance technologies. The 400 GB seem to further confirm the information published on April 2015 by *Folha de São Paulo* regarding the attempt of the Federal Police to use, with a court order, a "special application" to collect data from telephones under investigation.[59]

1.7. Surveillance of public communications

Below, three practical cases of communications monitoring publicly found on the Internet are presented. Even though it does not raise questions involving secrecy of communications and privacy, this kind of surveillance by different governmental entities has the potential to hinder exercise of freedoms, in particular, freedom of expression, freedom of assembly, and freedom of association.

Risk to freedom of speech: #HumanizaRedes

The National Pact Against Violations of Human Rights on the Internet ("Pacto Nacional de Enfrentamento às Violações de Direitos Humanos na Internet") - #HumanizaRedes is a program of the Brazilian Federal Government created by *Portaria Interministerial* nº 3, on April 8, 2015. Its purpose is to "foster the safe and responsible use of Internet features and applications, to receive and refer complaints involving crimes and violations of human rights and to promote a digital environment free from discrimination" (article 1). In addition to promoting education on human rights and safe use of networks through materials available on the #HumanizaRedes platform and related social media pages, the program also aims at "confronting violations of rights" through an online channel by receiving complaints of violations of human rights online and offline.

The program has been received with reservations. Bill of Decree Law no. 47/2015[60] proposed by the House of Representatives, still awaiting the opinion of the Human Rights and Minorities Commission, by way of example, proposes to eliminate the regulation that created #HumanizaRedes on the basis, among other things, that it does not provide criteria that define what sort of comments should be deemed a violation of human rights[61] and, in this sense, improperly gives the Executive Branch responsibility to define what comments would be deemed offensive.

The main concern raised by the initiative in terms of surveillance, however, is the fact that it will include use of software, to be developed with the Espírito Santo Federal University's Image and Cyberculture Laboratory to collect publicly-available profile data from social media based on subject matters predefined by the Human Rights Secretariat and map human rights violations online.[62] There are no express legal provisions regarding the operation of the program, only clarifications obtained through the Access to Information Law by NGO Artigo 19.[63] In these clarifications, the Human Rights Secretariat states that the software's operation, methodology, and scope, as well as the [definition of the] subject matters that it will attempt to identify, are still under discussion by the relevant working group.

It is worth mentioning that, in principle, #HumanizaRedes only handles information generally available to the public online, that is, information that may be accessed by any user (like the content of public profiles or blogs). Hence, it isn't a typical example of State

surveillance of communications; as a rule, such surveillance targets private communications. Nonetheless, whether through the complaint platform it creates or the monitoring software it uses, the program may generate *chilling effects* on freedom of expression, guaranteed by article 5, item IV, of the Federal Constitution, to the extent that it may affect citizens' freedom to post content online using their public profiles.

Virtual Raids: the Police on Facebook

A contribution of Artigo 19 and Oficina Antivigilância

In 2013 and 2014, several different criteria were used by police officers to identify individuals targeted in their investigations of the huge public protests that occurred during that time.[64]

The police investigation report that lead to the imprisonment or prosecution of more than 20 protesters in Rio de Janeiro, for example, reveals that a considerable part of the investigation was conducted by monitoring social media; an individual was considered a person of interest based on, in many cases, photographs, tags, and the individual's Facebook friends.[65]

Complaints and subpoenas within the scope of the investigation were based on information obtained by the so-called "Virtual Raids,"[66] under which the police department would screen and review not only personal profiles of people deemed to be of interest, but also relatives, friends, or Facebook contacts associated with these individuals, based on comments, likes, or tags on posts and photographs related to the protests.

The impression that remains is that most of the information collected came from public profiles whose owners did not limit access through their privacy settings, which made it easier for police officers to access profile information. However, based on the information mentioned in the investigation, it is not possible to determine if this was the only method used or whether fake profiles, sending friend requests to users of interest, were also used to review non-public information, a practice that was publicly opposed by Facebook[67] and is open to challenge under the Brazilian legal system.

In addition to monitoring data available on social media, under the same investigation, police sought to obtain court orders to gain access to access logs of at least of 46 profiles, one group, and three Facebook pages; specifically asking for "[...] account information containing creation and access logs, with date, time and time reference, IP, main and secondary e-mails, confirmation telephone numbers, as well as information contained in databases (credit card, if the profile manages any pages, etc.) [...]." The requests also encompassed communications made via private Facebook messages, including data such as "text, images, audio files, location, etc." (sic), logged from March 2013 through the "date the request is granted."

Social networks are important spaces through which citizens exercise their right to expression and association. Fundamental human rights considerations and the requirements of the Code of Criminal Procedure apply even to the monitoring of publicly-available profile data by the State. Important questions about this form of investigation include its adequacy and accuracy, and the basis on which authorities choose to begin investigations. These investigations may also lead officials to request access to non-public records; such requests also ought to meet thresholds of necessity and proportionality.

ABIN's "Mosaico": less transparency, more obscurity

In June of 2013, the newspaper *O Estado de São Paulo* disclosed that ABIN, through "an online system to monitor subject matters" defined by the Institutional Security Cabinet

(*Gabinete de Segurança Institucional*), the so-called "*Mosaico,*" would be monitoring social media, including Facebook, Twitter, Instagram and WhatsApp to check movements of protesters amid street protests then taking place across the country.[68] The system reportedly aimed to "predict the course and size of protests, infiltration of political parties, and even determine the events' funding sources." It is not unlawful for the State to gain knowledge of public communications and, at first glance, ABIN's monitoring is not clearly improper.

Nevertheless, two points deserve mention. First, the newspaper article alleges that private messages, such as those sent through WhatsApp, were also being monitored, thus constituting interception of flow of communications—for which ABIN does not have legal authority. Second, the article emphasizes the need for transparency in the operation of ABIN's "Mosaico" program and its scope and purpose, which is essential for meaningful control over State surveillance of communications in Brazil. [69]

2.
Recommendations

This report presented Brazilian communications surveillance laws and practices. Positive aspects of the laws were identified, and their most problematic aspects were highlighted, whether in the actual letter of the law or its deployment in practice. We conclude by presenting recommendations, using the 13 International Principles on the Application of Human Rights to Communications Surveillance as a reference for this purpose:[70]

2.1 International Principles on the Application of Human Rights to Communications Surveillance

Legality

Limits on the right to privacy must be set out clearly and precisely in laws, and should be regularly reviewed to make sure privacy protections keep up with rapid technological changes.

Legitimate Aim

Communications surveillance should only be permitted in pursuit of the most important state objectives.

Necessity

The State has the obligation to prove that its communications surveillance activities are necessary to achieving a legitimate objective.

Adequacy

A communications surveillance mechanism must be effective in achieving its legitimate objective.

Proportionality

Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Proportionate communications surveillance will typically require prior authorization from a competent judicial authority.

Competent Judicial Authority

Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent.

Due Process

Due process requires that any interference with human rights is governed by lawful

procedures which are publicly available and applied consistently in a fair and public hearing.

User Notification

Individuals should be notified of a decision authorising surveillance of their communications and be provided an opportunity to challenge such surveillance before it occurs, except in certain exceptional circumstances.

Transparency

The government has an obligation to make enough information publicly available so that the general public can understand the scope and nature of its surveillance activities. The government should not generally prevent service providers from publishing details on the scope and nature of their own surveillance-related dealings with State.

Public Oversight

States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions.

Integrity of Communications And Systems

Service providers or hardware or software vendors should not be compelled to build surveillance capabilities or backdoors into their systems or to collect or retain particular information purely for State surveillance purposes.

Safeguards for International Cooperation

On occasion, States may seek assistance from foreign service providers to conduct surveillance. This must be governed by clear and public agreements that ensure the most privacy-protective standard applicable is relied upon in each instance.

Safeguards Against Illegitimate Access

There should be civil and criminal penalties imposed on any party responsible for illegal electronic surveillance and those affected by surveillance must have access to legal mechanisms necessary for effective redress. Strong protection should also be afforded to whistleblowers who expose surveillance activities that threaten human rights.

2.2 Specific Recommendations:

1) To promote changes to the legal culture: train law students on privacy, secrecy of communications, and freedom of expression issues—in particular in connection with technology—and get current and future legal practitioners acquainted with international human rights law in the context of surveillance, including the International Principles on the Application of Human Rights to Communications Surveillance, its legal analysis, and its implementation guidelines.

One of the basic issues identified in this study was the adoption of restrictive interpretations of fundamental rights accorded by the Brazilian Constitution, which threatens the effectiveness of the protection guaranteed by such rights in practice. This leads to reduced protections for data of users of telecommunications services (even where court orders are required for access to the data).

Moreover, the statistics on telephone interception in Brazil and the growing number of emails monitored, despite the difficulty of drawing valid conclusions about the interpretation of these statistics without further information, suggest that concrete applications of international human rights law in the context of surveillance may not be fully reflected in practice. Promoting training, explanation, and debate would increase awareness of these matters and facilitate informed decisions on state surveillance, which is essential for actual compliance with the legal norms in question. This can be achieved by adding these topics to law school curricula and by providing continuing education courses and lectures to keep legal practitioners—including the members of the Judiciary and of the Public Attorney's Office—updated

2) To review the terms of ANATEL's Resoluções affecting surveillance of communications and request a more transparent form of oversight.

ANATEL's *resoluções* establishes obligations regarding users' identification, data retention, and surveillance infrastructure, as well as grants a prerogative of direct access to data, all of which limit fundamental rights. These provisions must be reviewed. ANATEL's Resolution no. 426/05, regulating landline telephones, does not meet the norms of transparency and accuracy with regard to its definitions of the data it requires to be stored and to the identification of the authorities that may have access to such data, which is a problem in light of the legality principle.

In addition, log retention for purposes of Telecommunications Regulation should be limited to those strictly required for such purposes so as to comply with the principles of legitimate aim and necessity. Obligations to retain data for five years should be reconsidered. In Europe, such periods are much shorter or non-existent: even under the already-superseded directive on Data Retention it varied from six months to two years.[71]

On that note, in 2014, the European Court of Justice (CJEU) declared the European Data Retention invalid.[72] In particular on the question of whether the interference caused by the directive is limited to what is strictly necessary, the court stated that "the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony" and that "entails an interference with the fundamental rights of practically the entire European population."[73] In July 2015, European

Digital Rights (EDRI), a coalition of more than 32 privacy and civil liberties organizations in Europe, asked the European Commission to investigate illegal data retention laws in the European Union after the adoption of the court decision.[74] At the international level, the UN High Commissioner for Human Rights, has expressly stated that "mandatory third party data retention, a recurring feature of surveillance regimes in many States, where governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access appears neither necessary nor proportionate."[75]

Regarding the possibility of granting direct access to telephone logs by integrating ANATEL systems with those of providers is at least questionable in the light of the transparency principle. The circumstances under which access shall be granted have to be clearly defined.

3) To monitor the progress of ADI 5063/DF, which challenges the constitutionality of articles 15 (access to account information by police authorities and the Public Attorney's Office upon request), 17 (telephone log retention obligation) and 21 (criminalization of refusal to provide access) of the Criminal Organizations Law, and to prepare amici curiae interventions.

The Criminal Organizations Law violates several international principles: legality (none of its terms are clear), necessity (it mandates telephone log retention for five years without empirical evidence support of its necessity), proportionality (it does not expressly limit the circumstances under which logs shall be accessed; imposes penalties of imprisonment and fine in case of failure to grant access to data), competent judicial authority (it allows broad interpretations regarding categories of data that may be demanded without court order) and user notification (it does not contain any provision on this matter).

The action challenging its constitutionality will face, at least, questions related to the necessity and proportionality of the obligation to retain telephone logs and the scope of the circumstances allowing access to data by the competent authorities without a court order. In view of the above, the decision regarding the constitutionality of this law will be an important precedent for the protection and confidentiality of communications in Brazil. Intervention in this process is vital. So far, only the National Association of Federal Police Deputies (*Associação Nacional dos Delegados de Polícia Federa*l) filed an *amicus curiae* brief.

4) To regulate access to telephone metadata through specific legislation that consider its sensitive nature;

Access to telephone logs cannot be subject to the informal treatment accorded to it by the Criminal Organizations Law, which has only made such access more susceptible to abuse and taken these rules even further away from compliance with international principles applicable to surveillance of communications. Ideally, access to telephone metadata in Brazil would be subject to a regulation of its own: a law establishing clear requirements for access (formal requirements, expressly delimiting the authorities competent to submit requests and determining the need for a court order, and substantive requirements, limiting such accesses to certain types of investigations), rules on user notification, and transparency about the number and frequency of requests. Requests for user location data should also be treated differently from requests for data about a user's telephone calls.

If surveillance is imposed by creating a data retention obligation, as the Criminal Organizations Law does, the legislation should at least be clear about the type of data to be retained, respect the necessity and proportionality principles in terms of duration of the retention, clearly define rules for access and use, and incorporate data security rules. Only then it would be closer to complying with international human rights standards. As the UN High Commissioner for Human Rights stated, "While concerns about national security and criminal activity may justify the exceptional and narrowly-tailored use of surveillance programs, surveillance without adequate safeguards to protect the right to privacy actually risk negatively impacting the enjoyment of human rights and fundamental freedoms."[76]

5) To monitor the application of Marco Civil da Internet, follow up on the process to draft its regulation, and review the constitutionality of article 15;

The *Marco Civil da Internet* establishes important rights and assurances to protect Internet users against unjust surveillance of their communications, in particular as it contemplates clear requirements on the circumstances and requirements for access to Internet connection logs, access to applications, and to stored private communications. While *Marco Civil da Internet* complies with the legality and competent judicial authority principles in these respects, these theoretical gains still have to become tangible. Monitoring the application of the *Marco Civil da Internet* is, therefore, vital.

On that note, the *Marco Civil da Internet* still has outstanding relevant issues: it provides for mandatory data retention, but does not determine a maximum period of time after which data shall be deleted—nor does it establish rules and standards for the security of stored data (which calls into question the proportionality of this obligation); it does not contain rules regarding user notification about third-party access to private data (in a clear violation of the user notification principle); it is not precise in identifying who is subject to

the obligation to maintain logs of access to Internet applications (a problem for the legality principle). As a result, civil society should closely follow and attempt to influence the drafting process of the *Marco Civil da Internet* regulations, which will govern these matters.

Furthermore, article 15 of the *Marco Civil da Internet*, providing for the obligation to retain logs of users' access to Internet applications, must have its terms reconsidered. The data to which this obligation refers to could reveal extremely privacy-sensitive information; it refers to their actual online behavior and can disclose their interests, habits, and relationships. The existence of means less restrictive of fundamental rights that may offer the same utility during investigations—such as the possibility of ordering data retention only upon reasonable suspicion of a particular Internet user's criminal activity—raises questions about the necessity of the existing measure. Data retention of every phone and internet user in Brazil may be ruled unconstitutional in principle.

If it is upheld as constitutional, the law should be amended to specify that access to retained data shall be available only in specific kinds of criminal cases related to serious crimes, the retention period shall be reduced, and the targets of the retention obligation shall be circumscribed to minimize harm to the rights to privacy and secrecy of communications.

6) To monitor application of the Telephone Interception Law to new surveillance techniques and new situations;

This report showed that the Telephone Interception Law is being applied not only to telephone wiretapping, but also to telecommunications. Moreover, it also described attempts to apply the law to new surveillance methods, such as malware infection on mobile phones and computers, an attempt which was demonstrated in the article and report on the apparent cooperation of the Brazilian authorities with Hacking Team. This effort to stretch the legislation to encompass radically different forms of surveillance violates the legality principle and has to be reviewed: this kind of technology not only breaches the secrecy of communications, limited by the Interception law, but also presents new issues regarding protection of the integrity and confidentiality of systems and, at a bare minimum, deserves its own regulation.

In the interim and to the extent parties outside of the government become aware of cases involving novel surveillance methods, the application and interpretation of the Interception Law may and must be influenced by participation in court cases, such as the filing of *amici curiae* briefs.

7) To perform empirical studies of requests for account information and breach of metadata privacy submitted by police authorities and the Public Attorney's Office; to compile statistics regarding breaches of metadata privacy; to expand and disclose information received by the National System for Interception Control (Sistema Nacional de Controle de Interceptações);

Recent legal changes grant police authorities and the Public Attorney's Office powers to access, upon mere request, users' telephone account information and other draft legislation proposes to expand these direct access powers to Internet users' account information and metadata.[77] This seems to suggest that *(i)* criminal investigations in Brazil rely substantially on breach of secrecy of account information and metadata, as a result of infrastructural deficiencies to deploy other methods of computer forensics investigations and lack of personnel; and/or that the *(ii)* slowness of the Brazilian judiciary system has led authorities involved in investigations to seek to circumvent the Judiciary by pushing for changes in the law that would give them easier and faster access to private information without involving the courts.

In both cases, the effective protection of the fundamental rights to secrecy of communications, privacy, and freedom of expression is at risk. Conducting empirical studies on practices involving requests for account information and metadata, compiling statistics on numbers of requests, and interviewing the agents involved may point to the underlying reasons for this scenario and lead to more broadly acceptable solutions.

At the same time, it is vital that data from the National System for Interceptions Control of the Inspector-General of the National Judiciary Office be *(i)* made generally available to the public without need to resort to the Access to Information Law, as was to obtain the statistics presented in this report; and *(ii)* expanded: the current system provides no information on the total number of requests for interception that were granted, only the number of proceedings filed, preventing a complete understanding of the surveillance picture. Meaningful transparency also demands that data on interceptions gathered by the system of the Public Attorney's Office National Council also be made available to the public.[78] Control over interceptions cannot be effectively exercised without disclosure of these numbers.

8) To push for transparency in intelligence and national security measures, create standards for the transfer of data within Sisbin, and increase oversight;

Little is known about ABIN's and Sisbin's operations in Brazil. Moreover, there is almost no information about the oversight exercised by the Joint Commission of the National Congress. A single ABIN program to monitor public communications—which came to

public attention due to the recent big events taking place in Brazil—is all that has come to light.[79] The most basic recommendation here seems to be to pay more attention to these bodies, demanding transparency about their activities so that they can be assessed and made subject to public scrutiny.

This report mentioned that ABIN does not perform interceptions, according to statute, court precedents, and ABIN's policy. This is hard to believe: Brazil has a national security authority that does not intercept communications—a surveillance authority that does not surveil. It seems that this inability is, or at least may be, circumvented by the existence of Sisbin. In light of that, to ensure compliance with international principles on surveillance, transparency about the activities performed by the agency and, in particular, on how it cooperates with Sisbin and other bodies, including the Federal Police and Brazil's Federal Revenue Department, is paramount. Standards must be created for the eventualities of such cooperation, since the purpose of the communications data collections—by the Federal Police in criminal investigation cases, or by Brazil's Federal Revenue Department, for tax control and audit matters—may be distorted and such data may be used for intelligence purposes.

3.
Legislative scenario

Chart 1 presents an overall picture of constitutional and general legal rules that impose boundaries on surveillance of communications in Brazil. In turn, Chart 2 shows the government institutions associated with surveillance practices and explains their roles. Chart 3 summarizes the scope of the Brazilian government's surveillance of communications and also summarizes the information that was detailed in this report. Chart 4 indicates how government surveillance practices may expand as a result of international cooperation in penal matters.

Chart 1: General limitations to surveillance of communications in Brazil

GENERAL LIMITATIONS TO SURVEILLANCE OF COMMUNICATIONS IN BRAZIL	
RIGHTS	Federal Constitution protects freedom of speech, privacy and secrecy of communications (article 5 subsections IX, X and XII).
	Laws no. 9.472/97 (articles 3, V and IX, and 72) and no. 12.965/14 (article 7) guarantee the rights to secrecy of communications and privacy when using of the telephone or Internet.
	There are no established tests applied in a uniform manner in case law and legal scholarship to assess constitutional grounds of limitations to such rights.
	Article 5, § 2 of the Federal Constitution establishes that the rights and guarantees therein do not exclude other rights stemming from the system and principles acknowledged by the Constitution, or international treaties to which Brazil is a party. However, the only human rights treaties that are considered as part of the Brazilian "constitutional block" are those approved by Congress under the same procedure necessary to amend the constitution, pursuant to article 5, § 3.
REMEDIES	In case of rights violations, a person may seek habeas corpus or *mandado de segurança* (similar to petition of writ of mandamus), as provided for in the Constitution (article 5, LXVIII and LXIX), or bring a lawsuit under the ordinary judicial process.
GUARANTEES	The Federal Constitution guarantees due process of law, an adversary system, right to a comprehensive defense, and presumption of innocence (article 5, LIV, LV and LVII). The Code of Criminal Procedure commands courts to abide by principles of adequacy, necessity and proportionality when ordering evidence-gathering (article 156). The same goes for rulings on motions that seek injunctive remedies on submission of evidence (article 282). Notice of subpoena should be served on the affected party "except in cases of emergency or the possibility [that service may] compromise effectiveness of the investigation at risk" (article 282, § 3).
	Under the Federal Constitution (article 5, LVI) and Code of Criminal Procedure (article 157) evidence secured by unlawful means, in violation of the law or Constitution, is inadmissible and void.
PENALTIES	Article 10 of Law n. 9.296/96 criminalizes illegal interception and breach of judicial secrecy and sets a penalty of incarceration from 2 to 4 years and a fine.
	Article 156-A of the Penal Code criminalizes breach of an information technology device with the intent to misappropriate data and sets a penalty of imprisonment from 3 months to 1 year and fine. If the action results in access to content of private communication, the penalty is increased to incarceration, from 6 months to 2 years, and a fine.

Source: InternetLab

Chart 2: Institutional Roles and their Powers

INSTITUTIONAL ROLES & THEIR POWERS: AUTHORITIES RELATED TO SURVEILLANCE PRACTICES	
ANATEL	Created under Law no. 9.472/97, ANATEL is the regulating agency in charge of organizing the operation of the telecommunications industry and overseeing provision of related services (article 8). It has authority to pass regulations (*resoluções*) (article 19).
	The agency performs its duties by passing regulations (*resoluções*) to create data retention, user identification obligations, and provisions on availability of funds for surveillance, apart from establishing its own prerogatives for access to retained data.
BRAZIL'S FEDERAL REVENUE DEPARTMENT	Agency of the Ministry of Finance in charge of administering internal and foreign trade taxes, by managing and enforcing collection, oversight and investigation, and also by engaging in international cooperation in tax and customs matters (article 15, Decree no. 7.482/11). It has access to tax documents of telecommunications providers.
POLICE AUTHORITIES	Law enforcement agencies. Under the Federal Constitution (article 144), State Civil Police and Federal Police comprise the Judicial Police. Under the Code of Criminal Procedure, the Judicial Police is in charge investigating criminal infractions (article 4). The Public Attorney's Office has external supervision over the proceedings (article 129, VII, CF).
	Code of Criminal Procedure establishes that, as soon as the police authority becomes aware of a penal infraction, it shall gather all evidence useful for investigation of the matter (article 6, III). Law no. 12.830/13 establishes that, in the course of a criminal investigation, the Chief of Police (*Delegado*) is in charge of requesting submission of evidence, information and data of interest for criminal investigative purposes (article 2, § 2).
PUBLIC ATTORNEY'S OFFICE	Pursuant to the Federal Constitution, the Public Attorney's Office is the State's independent entity intended to protect legal order, the democratic regime and individual rights (article 127). The duties of the Public Attorney's Office include the filing of class actions, service of notices in administrative proceedings within its jurisdiction, demanding information and documents to support them, and ordering investigations and police inquests (article 129).
	Supplementary Law no. 75/93 grants the Federal Public Attorney's Office the authority to demand information and documents from private entities and to perform inspections and investigations within the scope of its duties (article 8, IV and V); that also applies, on a subsidiary basis, to State Public Attorneys' Offices under article 80 of Law n. 8.625/93. This law also grants authority to demand information to members of Public Attorneys' Offices (article 26, III).
COURT AUTHORITIES	Courts may officially order production and submission of evidence pursuant to article 130 of the Code of Civil Procedure and article 156 of the Code of Criminal Procedure Courts rule on applications submitted by police authorities and Public Attorneys' Office for production of evidence in criminal investigations and criminal cases whenever they implicate rights protected under the Constitution, such as breach of confidential information.
CPIs	Parliamentary Commissions of Inquiry (CPIs) are created on a temporary basis within the Legislative Branch to ascertain a given fact; they hold the "powers of investigation that are proper to court authorities" pursuant to article 58, § 3 of the Federal Constitution. They are allowed to pierce confidentiality of stored data without the need to secure a court order.
ABIN & SISBIN	Pursuant to Law no. 9.833/99, it is incumbent upon ABIN, Brazil's central intelligence agency and operator of the Brazilian Intelligence System (Sisbin), to plan, execute, supervise and control intelligence activities. Under Decree no. 4.376/02, in addition to ABIN, Sisbin is also comprised by the Office of the Chief of Staff and Institutional Security Office of the Presidency of the Republic, apart from a number of Ministries and related agencies (such as Federal Police, associated with the Ministry of Justice and Brazil's Federal Revenue Department, associated with the Ministry of

	Finance). External supervision is performed by a permanent Joint Committee in Congress, in line with article 6 of Law no. 9833/99.
	ABIN does not have prerogatives to demand information, although it may be able to access data in possession of departments that comprise Sisbin, pursuant to Decree no. 4.376/02 (article 6-A). There are no impediments to monitoring of public communications.

Source: InternetLab

Chart 3: State surveillance of communications in Brazil

STATE SURVEILLANCE OF COMMUNICATIONS IN BRAZIL			
Purpose/ Authority	**Telecommunications Regulation (ANATEL)**	**Law Enforcement (Police, Public Attorneys' Office, Courts and CPIs)**	**Intelligence (Sisbin)**
DATA RETENTION OBLIGATIONS	ANATEL's *Resoluções* nos. 426/05, 477/07 and 614/13 require service providers to retain metadata pertaining to landline and mobile telephone services for at least 5 years and metadata pertaining to Internet connections for at least 1 year.	Law no. 12.850/13 (article 17) orders landline and mobile telephone companies to retain "identification logs of numbers of origin and destination of telephone connection terminals" for 5 years. Law no. 12.965/14 (articles 13 and 15) orders certain connection providers to retain Internet connection logs for 1 year and application providers operated for for-profit purposes to retain logs of access to applications for 6 months.	There is no specific retention obligation for intelligence purposes.
ACCESS TO DATA RETAINED (account information and metadata)	In performing its supervisory duties (article 8, Law no. 9472/97), ANATEL may access billing documents, which contain account information and call records, by requesting them from service providers. At present, there is infrastructure in place allowing direct and unlimited online access, pursuant to article 38, *Resolução* no. 596/12. Brazil's Federal Revenue Department may also request	Pursuant to Laws no. 9.613/98 (article 17-B) and no. 12.850/13 (article 15), access to account information of telephone users may take place simply upon request by police authorities or Public Attorney's Office's members to service providers. Access to telephone logs and other metadata generated by telephone use (e.g. location logs) has no specific legal regulation, and instead takes place through court orders to produce evidence. Under *Mandado de Segurança* 23452/RJ, decided by the Federal Supreme Court, access to telephone logs may also be ordered under CPIs.	ABIN has no authority to request and subpoena data. It is, however, possible to have Sisbin's agencies cooperate to that end (articles 6, V and 6-A of Decree no. 4.376/02).

	access to billing documents (article 11, Law no. 8.218/91).	Under Law no. 12.965/14, access to account information of subscribers of connection providers and users of Internet applications may take place whenever subpoenaed by authorities of appropriate jurisdiction (article 10, § 3). In the case of Internet connection and access to application logs, access requires a court order whenever there are grounded indicia of wrongdoing and logs may be useful to investigations or discovery; a specific time frame must also be established (article 22).	
ACCESS TO STORED COMMUNICATIONS RECORDS (content)	ANATEL's *Resoluções* allow access to recordings of calls made to telecommunications providers customers' services.	Law 12.965/14 allows access to private communications made by Internet applications upon court order (article 7, III). Under *Recurso Extraordinário* 418.416-8/SC, decided by the Federal Supreme Court, a warrant for search and seizure supports access to data stored on computers.	ABIN has no authority to request and subpoena data. It is, however, possible to have Sisbin's agencies cooperate to that end (articles 6, V and 6-A of Decree n 4.376/02).
INTERCEPTION	ANATEL has no prerogative to enforce and authorize interceptions.	According to Law 9.296/96, interception of telephone communications and information technology systems may take place upon court order, either at the court's own initiative or at the request of police authorities or Public Attorneys' Office's members, whenever there is reasonable suspicion that the perpetrator or accomplice committed a crime, punishable by imprisonment, as well as a lack of availability of other means to produce evidence (articles 1 and 2). Law no. 12.965/14 allows interception of Internet communication flow pursuant to Law no. 9.296/96. CNJ's and CNMP's Resoluções establish criteria to be complied with for applications and decisions.	ABIN has no prerogative to enforce or jurisdiction to request interception. Law no. 9.296/96 does not extend such authority to ABIN. It is, however, possible to have Sisbin's agencies cooperate to that end (articles 6, V and 6-A of Decree 4.376/02).

Source: InternetLab

Chart 4: International legal assistance on penal matters

MUTUAL LEGAL ASSISTANCE TREATIES ON PENAL MATTERS	
Brazil is a party to several international agreements dealing with mutual legal assistance. Such agreements have impact on communications surveillance to the extent they allow assistance in obtaining and producing evidence. Pursuant to the dual criminality principle, cooperation may only take place whenever the activity to which the request refers is defined as a crime in both jurisdictions.	
REQUIRES ENFORCEMENT OF THE DUAL CRIMINALITY PRINCIPLE	Bilateral agreements with China, South Korea, Cuba, France and Portugal

REQUIRES ENFORCEMENT OF THE DUAL CRIMINALITY PRINCIPLE IN EXCEPTIONS	Bilateral agreements with Colombia, United States, Italy, Mexico, Nigeria, Panama, Peru, United Kingdom, Switzerland, Suriname and Ukraine, and multilateral agreements within Mercosur and Organization of the American States
DOES NOT REQUIRE ENFORCEMENT OF THE DUAL CRIMINALITY PRINCIPLE	Bilateral agreements with Spain and Canada

Source: BELOTTO, Ana Maria de Souza; MADRUGA, Antenor; TOSI, Mariana Tumbiolo, Dupla incriminação na cooperação jurídica internacional, *in: Boletim IBCCRIM, n. 237, August 2012, available at: http://www.ibccrim.org.br/boletim_artigo/4678-Dupla-incriminao-na-cooperao-jurdica-internacional Accessed: 31 Jul. 2015.*

1 International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org/text Background and Supporting International Legal Analysis, https://necessaryandproportionate.org/legalanalysis, Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance. https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf Accessed on: 10 Sept. 2015.

2 Parliamentary Commission of Inquiry on Cybercrimes Draft Final Report. Available at http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=AB3F4BBA734C93D8C81D9B6DAA7AADE1.proposicoesWeb1?codteor=1447125&filename=REL+1/2016+CPICIBER+%3D%3E+RCP+10/2015. Accessed on: 4 Apr. 2016.

3 For the purposes of this report, the term "breach of secrecy" is used in a broad sense and refers to the consequences of any action of disclosure (following subpoenas or court orders or any type of request or turning over of data) of any kind of information related to communications (user account information, metadata or content). In the particular case regarding the interpretation of article 5, subsection XII of the Constitution, it specifically refers to any interception procedure that breaches the secrecy of communications.

4 With respect to protection of flow of communications, it is worth noting FERRAZ JR., Tercio Sampaio's work, "Sigilo de Dados: o direito à privacidade and os limites da função fiscalizadora do Estado," in: Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, 1993, p. 439-459. With respect to the reach of the exception, both SILVA, José Afonso da. Curso de Direito Constitucional Positivo. 32ª Ed. São Paulo: Malheiros, 2008, p. 438; and FERREIRA FILHO, Manoel Gonçalves. Curso de Direito Constitucional. 35ª Ed. São Paulo: Saraiva, 2009, p. 301 concur.

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

6 In habeas corpus 70814/SP (Case reported by the Justice Celso de Mello, tried on 1 Mar. 2004), for instance, the Federal Supreme Court accepted that a correctional administration may intercept an inmate's letter for reasons of public safety, correctional discipline or preservation of legal order, with a basis in the sole paragraph of article 41, of Law no. 7210/84, Criminal Corrections Law, which limits inmates' right "to have contact with the outside world through written correspondence" (article 41, XV of the same law). On this matter, refer to MORAIS, Alexandre. Direito Constitucional. 28ª Ed. São Paulo: Atlas, 2012, p. 59. More disputes about the validity of a narrow interpretation of subsection XII of article 5 will be presented in the course of this report

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

8 For the purposes of this report, account information refers to information included in the user's records with the telephone company, autonomous system operator, or application provider.

9 For the purposes of this report, metadata refers to all data and records generated from a given communication other than the communication's content, such as, for instance, the date, time, and duration of communication, sender, addressee, geographic location of the device, if known (such as identifiers or measurements by a radio base station), device identification codes (such as IMEI), and the like.

10 Recent legislative amendments have "circumvented" the need of court orders to obtain account information, as discussed below (section 2.4: Surveillance with and without checks and balances: Telephone vs. Internet), in violation of a position already expressed by the Federal Supreme Court. Please refer to Federal Supreme Court, Recurso Extraordinário 716795/RS, Case reported by the Honorable rel. Luiz Fux, tried on 31 Oct. 2012, on whether or not police would require a court order to obtain account information of telephone users; the Court decided that a court order is mandatory under the protection afforded by article 5, X. Available at: http://stf.jusbrasil.com.br/jurisprudencia/22599582/recurso-extraordinario-re-716795-rs-stf Accessed on: 17 June 2015.

11 See "Protected Information," International Principles on the Application of Human Rights to Communications Surveillance. 10 July 2013. Available at: https://necessaryandproportionate.org/text

12 See Luis Fernando Garcia, The Metadata Debate. A Latin American Perspective, 15 Sept 2015. Available at: https://www.eff.org/deeplinks/2014/09/metadata-debate-latin-american-perspective. Accessed on 10 Sept 2015. *See also* ACLU Vs Clapper. Declaration of Professor Edward W. Felten, 26 Aug 2015. Available at: https://www.documentcloud.org/documents/781486-declaration-felten.html. Accessed on: 10 Sept 2015. *See* Clifton Parker, Stanford students show that phone record surveillance can yield vast amounts of information, 14 March 2015. Available at: http://news.stanford.edu/news/2014/march/nsa-phone-surveillance-031214.html Accessed on: 10 Sept. 2015.

13 On that note, it is worth mentioning the landmark decision of the European Court of Justice, which invalidates the European data retention directive on the grounds that it disproportionately limited the rights to privacy and private life. *See* Judgment of the Court, In Digital Rights Ireland vs Ireland. Joined Cases C-293/12 and C-594/12, 8 April 2014. Available at: http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=1245760. Accessed on 10 Sept. 2015. *See also* Press Release N. 54/14, available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf. Accessed on: 27 March 2016.

14 FOLHA DE SÃO PAULO, "Anatel terá acesso total a dado sigiloso de telefones," published on 19 Jan 2011. Available at: http://www1.folha.uol.com.br/fsp/mercado/me1901201103.htm Accessed on: 17 June 2015.

15 FOLHA DE SÃO PAULO, "Agência diz que não há quebra de sigilo, published on 19 Jan 2011. Available at http://www1.folha.uol.com.br/fsp/mercado/me1901201104.htm Accessed on: 17 June 2015.

16 GAZETA DO POVO, "Quebra de sigilo continua a depender de mandado judicial, diz Anatel", published on 21Jan 2011. Available at: http://www.gazetadopovo.com.br/economia/quebra-de-sigilo-continua-a-depender-de-mandado-judicial-diz-anatel-da8drvp4kj7uyodcxir2ijw3y Accessed on: 17 June 2015.

17 Please refer to VARON FERRAZ, Joana., News Bulletin n. 11 by Oficina Antivigilância, available at https://antivigilancia.org/pt/2015/07/novas-revelacoes-do-wikileaks-sobre-vigilancia-no-brasil-dilma-

disse-que-nao-tem/. Refere-se a acordo available at http://www.itamaraty.gov.br/index.php?option=com_content&view=article&id=10389:atos-assinados-por-ocasiao-da-visita-da-presidenta-dilma-rousseff-aos-estados-unidos-washington-30-de-junho-de-2015&catid=42&Itemid=280&lang=pt-BR#neutrinos-port-8 Accessed on: 31 July 2015.

18 This position was once acknowledged by the Federal Supreme Court. See FEDERAL SUPREME COURT, Recurso Extraordinário 716795/RS, Case reported by the Honorable rel. Luiz Fux, tried on 31 Oct. 2012, which discusses the requirement of a court order to obtain telephone users' account information by chiefs of civil police, and concludes that it is indeed necessary. Available at: http://stf.jusbrasil.com.br/jurisprudencia/22599582/recurso-extraordinario-re-716795-rs-stf Accessed on: 17 June 2015.

19 Please refer to ARAS, Vladimir. A investigação criminal na nova lei de lavagem de dinheiro. Boletim 237 do IBCCRIM. Available at: http://www.ibccrim.org.br/boletim_artigo/4671-A-investigao-criminal-na-nova-lei-de-lavagem-de-dinheiro Accessed on: 17 June 2015.

20 ACEL's motion and examples of notices received by operators based on that (interpretation of the) law may be found at CONJUR, "Operadoras reclamam de pedidos de delegados para quebra de sigilo telefônico", of 29 Oct. 2014, available at http://www.conjur.com.br/2014-out-29/telefonicas-reclamam-quebras-sigilo-pedidas-delegados On the action brought by ACEL, please refer to news on the STF website, available at http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=254181 . Accessed on: 31 July 2015.

21 Francisco Brito Cruz, InternetLab's Director, reports that "in Brazil, Núcleo de Informação and Coordenação do Ponto BR (NIC.br), the operational arm of Comitê Gestor da Internet [Internet Management Committee] is in charge of creating rules on how connection providers may enroll as "independent systems," thereby participating in the assignment of IP number blocks made by NIC.br. According to NIC.br, entities must have, for instance, "a minimum infrastructure network" and "have 2 or more independent connections to the Internet or, alternatively, a connection to an operator and a connection to an Internet exchange point," apart from a series of technical standards and appropriate staffing. Sources: <http://registro.br/tecnologia/provedor-acesso.html?secao=numeracao> and <ftp://ftp.registro.br/pub/gter/gter28/07-Asbr.pdf>." As a result, not every Internet connection provider meets the definition in *Marco Civil da Internet* that creates the obligation to retain connection logs.

22 See BRITO CRUZ, Francisco, et. al., "What's at stake in the regulation of *Marco Civil da Internet*?, p. 32. Available at http://www.internetlab.org.br/wp-content/uploads/2015/08/Report-MCI-v2-eng.pdf Accessed on: 13 Sept. 2015.

23 Please refer to http://participacao.mj.gov.br/marcocivil/pauta/acesso-a-dados-cadastrais-por-autoridades-administrativas/, http://www.internetlab.org.br/pt/internetlab-reporta/internetlab-reporta-consultas-publicas-no-04/ and https://antivigilancia.org/boletim_antivigilancia/consultas/visualizacao. Accessed on: 17 June 2015.

24 This argument was advanced by Google in a number of cases. Before Marco Civil, the Superior Court of Justice (STJ) did, in Inquérito no. 784-DF (Case reported by the Justice Laurita Vaz, tried on 17 Mar. 2013) address the matter and ordered disclosure of data. More recently, a federal judge ruled in favor of Yahoo in a class action filed by the Public Attorney's Office demanding the company to turn over data retained in its parental company Yahoo INC. According to the court decision, Yahoo Brazil does not have control over the data stored abroad (in the parental company), being only compelled to turn over data which are

in its possession (users whose accounts are registered in yahoo.com.br and not in yahoo.com). See *26ª Vara Federal da Seção Judiciária de São Paulo, Ação Civil Pública n. 0012450-95.2014.4.03.6100 – Ministério Público Federal v. Yahoo! Do Brasil Internet LTDA*. Available at: http://www.internetlab.org.br/wp-content/uploads/2015/07/Y.SENTENÇA.ACP_.MPSP_.pdf Accessed on: 13 Sept. 2015.

25 In February 2015, Judge Luiz Moura Correia, presiding over Central de Inquéritos da Comarca de Teresina, ordered the WhatsApp application blocked throughout Brazil because the company was allegedly not cooperating with criminal investigations or abiding by breach of secrecy orders. Refer to O ESTADO DE SÃO PAULO, "Juiz exige a suspensão do Whatsapp in Brazil," published on 25 Feb. 2015, available at http://blogs.estadao.com.br/link/juiz-exige-a-suspensao-do-whatsapp-no-brasil/ (Accessed on 31 Jul. 2015). The decision was vacated by the Court of Justice of the State of Piauí soon thereafter. Refer to a case involving Yahoo Inc, dealt with on InternetLab Blog on newspaper Estado de São Paulo on 23 July 2015, available at http://blogs.estadao.com.br/deu-nos-autos/acesso-daqui-guardo-la-onde-estao-nossos-dados-na-internet/ Accessed on 31 July 2015.

26 COURT OF JUSTICE OF RIO GRANDE DO SUL. Agravo de Instrumento no. 70018683508, Appeals Court Judge Maria Berenice Dias. Ruling: 28 July 2007. Available at: http://jus.com.br/jurisprudencia/16757/tjrs-authoriza-interceptacao-telefonica-para-localizar-devedor-de-alimentos Accessed on: 17 June 2015.

27 FEDERAL COURT DIVISION – SÃO PAULO DISTRICT COURT. Mandado de Segurança no. 0001972-91.2015.4.03.6100. Federal Judge Djalma Moreira Gomes. Date of Ruling: 24 Apr.2015. Available at: http://www.omci.org.br/m/jurisprudencias/arquivos/2015/jfsp_00019729120154036100_24042015_KG45KXb.pdf. Accessed on 17 June 2015.

28 FEDERAL SUPREME COURT. Ação Direta de Inconstitucionalidade no. 1488-9/DF, Justice Néri da Silveira, Ruling of 7 Nov. 1999.

29 See for example, FEDERAL SUPREME COURT, habeas corpus 84.301-SP, Justice Joaquim Barbosa, ruling of 9 Nov .2004 (available at http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=79542; accessed on 3 Aug. 2015) and Habeas Corpus 83.515-RS, Reporting Justice Nelson Jobim, ruling of 16 Sept. 2005 (available at http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=79377; accessed on 3 Aug. 2015).

30 INTER-AMERICAN COURT OF HUMAN RIGHTS. *Case Escher et al. v. Brazil.* Ruling of 6 July 2009. Available at http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf Accessed on: 17 June 2015.

31 INTER-AMERICAN COURT OF HUMAN RIGHTS. Case *Escher et al. v. Brazil* Preliminary Objections, Merits, Reparations and Costs. Judgement of 6 July 2009. Series C No. 200, para. 114. Available at http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf Accessed on: 17 June 2015.

32 FOLHA DE SÃO PAULO, "PF quer instalar vírus em telefone grampeado para copiar informações," published on 27 Apr. 2015. Available at: http://www1.folha.uol.com.br/poder/2015/04/1621459-pf-quer-instalar-virus-em-telefone-grampeado-para-copiar-informacoes.shtml Accessed on 17 June 2015.

33 On this subject, see MENDES, Laura Schertel, "Uso de softwares espiões pela polícia: prática legal?," in: Jota, published on 4 June 2015, available at http://jota.info/uso-de-softwares-espioes-pela-policia-pratica-legal, Accessed: 3 Aug. 2015. Mendes emphasizes that infection of electronic devices by trojan horses is capable of gathering all pieces of information stored in the device. This goes beyond interception of flow of communications, regulated by the Telephone Interception Law. She further highlights that, in Germany, a review of the constitutionality of this type of procedure lead the German Federal Constitutional Court to rule for the existence of a fundamental right to reliability and integrity of information technology systems. *See also* Principle 11 - Integrity of Communications and Systems, International Principles on the Application of Human Rights to Communications Surveillance. Available at: https://en.necessaryandproportionate.org/text#principle_11. Accessed on: 10 Sept. 2015.

34 Ombudsman Record/CNJ: 147763. Request filed by the InternetLab to the CNJ and respective answer, including full data on the system, available at http://www.internetlab.org.br/wp-content/uploads/2015/07/LAI-Interceptance-para-o-site.pdf, (Accessed on: 3 Aug. 2015).

35 See statistics available at http://www.uscourts.gov/statistics-reports/wiretap-report-2013 Accessed on 3 Aug. 2015. Each wiretap order may involve, however, more than one person and, consequently, more than one telephone line.

36 See data of the Sistema Nacional de Interceptação available at http://www.internetlab.org.br/wp-content/uploads/2015/07/LAI-Interceptance-para-o-site.pdf. This figure refers to the number of criminal proceedings filed in 2013, so called "initial," as mentioned in the chart, that is, does not refer to the total number of proceedings filed during the month, which may include data from the previous month. The chart refers to monthly information in 2013 regarding item "Total 3," relative to telephone interception added to that of item "Total 9" relative to telematics interception.

37 See statistics available at: https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2013.pdf?__blob=publicationFile&v=3 Accessed on 3 Aug. 2015.

38 See data of the Sistema Nacional de Interceptação available at http://www.internetlab.org.br/wp-content/uploads/2015/07/LAI-Interceptance-para-o-site.pdf. This figure refers to the number of notices issued in 2013, so called "initial," as mentioned in the chart, that is, does not refer to the total number of notices issued during the month, which may include data from the previous month. The chart refers to monthly information in 2013 regarding item "Total 1," relative to telephone interception added to that of item "Total 7" relative to telematics interception.

39 This opinion is stated in court precedents. See SUPERIOR COURT OF JUSTICE, habeas corpus 149250-SP, Justice Adilson Vieria Macabul, ruling of 16 May 2012, which also reviewed unlawful interception operations performed with ABIN's agents within the scope of Operação Satiagraha. It has also been mentioned by ABIN in public. Answering the question "A ABIN faz escuta telefônica?" (Does ABIN intercept telephone conversations?) on its site, the agency states: "Law no. 9.296, of July 24, 1996, regulating art. 5, item XII, of the Federal Constitution, determines the bodies competent to perform, subject to court order, telephone interception operations. ABIN is not mentioned by this legal provision." available at: http://www.abin.gov.br/modules/mastop_publish/?tac=Perguntas_Frequentes (Accessed on: 31 July 2015). The agency, however, was publicly accused of intercepting the telephone of Federal Supreme Court Justice Gilmar Mendes, in a scandal made public in 2008. See FOLHA DE SÃO PAULO, "Divulgação de grampo a presidente do STF derruba diretoria da Abin", published on 7 Nov. 2008, available at http://www1.folha.uol.com.br/fsp/corrida/cr0709200802.htm (Accessed on: 31 July 2015).

40 FOLHA DE SÃO PAULO, "Acesso ao Guardião pela Abin gera polêmica," published on 12 Nov. 2008. Available at: http://www1.folha.uol.com.br/fsp/brasil/fc1211200805.htm Accessed on: 17 Jun. 2015. Accessed on: 13 Sept. 2015.

41 See results of the search at https://www.wikileaks.org/hackingteam/emails/?q=%22ABIN%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult Accessed on: 13 Sept. 2015.

42 See results of the search at https://www.wikileaks.org/hackingteam/emails/emailid/446716 Accessed on: 13 Sept. 2015.

43 See results of the search at https://www.wikileaks.org/hackingteam/emails/?q=%22CIGE%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult Accessed on: 13 Sept. 2015.

44 See results of the search at https://www.wikileaks.org/hackingteam/emails/?q=%22CINPOL%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult Accessed on: 13 Sept. 2015.

45 See results of the search at https://www.wikileaks.org/hackingteam/emails/?q=%22DRCI%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult Accessed on: 13 Sept. 2015.

46 See results of the search at https://www.wikileaks.org/hackingteam/emails/emailid/7264 Accessed on: 13 Sept. 2015.

47 See results of the search at https://www.wikileaks.org/hackingteam/emails/emailid/7264 Accessed on: 13 Sept. 2015.

48 See results of the search at https://www.wikileaks.org/hackingteam/emails/?q=%22policiamilitar.sp.gov.br%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult Accessed on: 13 Sept. 2015.

49 See results of the search at https://www.wikileaks.org/hackingteam/emails/emailid/237181 Accessed on: 13 Sept. 2015.

50 See results of the search at https://www.wikileaks.org/hackingteam/emails/emailid/446822 Accessed on: 13 Sept. 2015.

51 See results of the search at https://www.wikileaks.org/hackingteam/emails/?q=%22mj.gov.br%22+!LISTA+!%22Progetto+Polizia+Federal%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=2#searchresult Accessed on: 13 Sept. 2015.

52 See results of the search at https://www.wikileaks.org/hackingteam/emails/emailid/446919 Accessed on: 13 Sept. 2015.

53 Please refer to http://apublica.org/2015/07/hackeando-o-brasil/ Accessed on: 13 Sept. 2015.

54 Please refer to http://htbrasil.pen.io/ Accessed on: 13 Sept. 2015.

55 See https://www.wikileaks.org/hackingteam/emails/emailid/921981 Accessed on: 13 Sept. 2015.

56 See file attached at https://www.wikileaks.org/hackingteam/emails/emailid/921981 (file attached) Accessed on: 13 Sept. 2015.

57 See https://www.wikileaks.org/hackingteam/emails/emailid/921908 Accessed on: 13 Sept. 2015.

58 See https://www.wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf Accessed on: 13 Sept. 2015.

59 See FOLHA DE SÃO PAULO, "PF quer instalar vírus em telefone grampeado para copiar informações," published on 27 Apr. 2015. Available at: http://www1.folha.uol.com.br/poder/2015/04/1621459-pf-quer-instalar-virus-em-telefone-grampeado-para-copiar-informacoes.shtml Accessed on: 13 Sept. 2015.

60 With grounds on http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=1214850. Accessed on 17 Jun. 2015.

61 The Work Group managing #HumanizaRedes was created by Portaria Interministerial no. 2, of November 20, 2014. Its purpose is "to receive complaints regarding online comments posted on social media regarding web pages and groups inciting or promoting crimes against human rights, in particular those fostering violence of a discriminatory nature" (main clause of art. 1). The sole paragraph of art. 1 defines incitement or promotion of crimes against human rights any comment fostering practice of any of the crimes set forth by Law no. 7.716, of January 5, 1989 or article 40, paragraph 3, of the Criminal Code." The scope of #HumanizaRedes activities, therefore, refers to this definition.

62 BRAZILIAN FEDERAL GOVERNMENT, "Governo vai usar software contra crimes de ódio na internet,"published on 12 Dec. 2014. Available at: http://www.brasil.gov.br/cidadania-e-justica/2014/12/governo-vai-usar-software-contra-crimes-de-odio-na-internet Accessed on 17 June 2015.

63 Requests and answers to ARTIGO 19 are available at: (i) http://www.artigo19.org/centro/esferas/detail/706; (ii) http://www.artigo19.org/centro/esferas/detail/701 and (iii) http://www.artigo19.org/centro/esferas/detail/702, accessed on 17 June 2015.

64 Regarding the protests, read further details at http://www.artigo19.org/protestos/

65 The Public Agency had access to the details of the investigation and highlighted these aspects in this article: http://apublica.org/2015/05/um-preso-politico-no-brasil-democratico/

66 "Virtual Raid" is basically a manual work to check profiles of individuals associated with pages supporting protests and inciting destruction of property, against law enforcement, etc. Practice already mentioned in other cases mentioned by the police (e.g. http://oglobo.globo.com/sociedade/oab-rj-aciona-ministerio-publico-estadual-policia-civil-para-investigar-paginas-consideradas-racistas-13953005).

67 http://www.techtudo.com.br/noticias/noticia/2014/10/facebook-veta-uso-de-perfil-falso-pela-policia-apos-polemica-com-nomes.html

68 ESTADO DE SÃO PAULO, "Abin monta rede para monitorar internet." Available at: http://sao-paulo.estadao.com.br/noticias/geral,abin-monta-rede-para-monitorar-internet,1044500 Accessed on: 17 June 2015.

69 These concerns were discussed by experts in an article by REVISTA GALILEO, "Mosaico, o 'Prism' brasileiro," with no publication date. Available at: http://revistagalileu.globo.com/Revista/Common/0,,EMI339490-17770,00-MOSAICO+O+PRISM+BRASILEIRO.html Accessed on: 17 June 2015.

70 https://pt.necessaryandproportionate.org/text

71 See Directive 2006/24/EC on retention of data generated and processed during the provision of telecommunications services, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF. Accessed on 03 Aug. 2015.

72 Judgment of the Court, In Digital Rights Ireland vs Ireland. Joined Cases C-293/12 and C-594/12, 8 April 2014. Available at: http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=1245760. Accessed on 10 Sept. 2015.

73 EDRI. European Digital Rights asks the European Commission to investigate illegal data retention laws in the EU. 2 Jul 2015. Available at: https://edri.org/edri-asks-european-commission-investigate-illegal-data-retention-laws. Accessed on 10 Sept. 2015.

74 See EDRI, Non-exhaustive list of EU Member States with national legislation contrary to the Digital Rights Ireland Ltd (C-293/12) CJEU ruling. Available at: https://edri.org/files/DR_EDRi_letter_CJEU_Timmermans_20150702_annex.pdf

75 Office of the United Nations High Commissioner for Human Right, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary – General. Paragraph 26, 30 June 2014. Available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf Accessed on 10 Sept. 2015.

76 Navy Pillay, UN rights chief urges protection for individuals revealing human rights violations, 12 July 2013, Available at: http://www.un.org/apps/news/story.asp?NewsID=45399. Accessed on 10 Sept. 2015.

77 See Bill of Law no. 8.040/14, originating in the House of Representatives, which includes the right to direct access to Internet users' account information by the Federal Police, available at http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=623798, and Bill of Law no. 494/08, originating in the Federal Senate, which expands the retention obligation to Internet connection logs and allows access, upon a simple request by the police department or Public Attorney's Office, to account information and "connection data" in investigations of cases "involving children and teenagers," available at http://www.senado.gov.br/atividade/materia/getPDF.asp?t=55354&tp=1. Accessed on 31 July 2015.

78 InternetLab also requested to the National Ombudman Council of the Public Attorneys' Office access to information on interceptions gathered by the CNMPInd system. Access, however, was denied based on an allegation of a formal deficiency of the request and because the "information requested is protected by

confidentiality under the terms of the Law." It is worthwhile reminding that such numbers are mere statistics and do not give rise to any disclosure about specific cases, what poses a question over the alleged confidentiality protection. See request and answer at http://ouvidoria.cnmp.gov.br//ticket.php?track=AD7GASR276&Refresh=40756 . Accessed on: 31 July 2015.

79 The intelligence sector became more relevant with the 2014 World Cup in Brazil and will remain important during the 2016 Summer Olympics in Rio de Janeiro. On its effectiveness, see FOLHA DE SÃO PAULO, "Ameaça de bomba na Copa mobilizou inteligência e deixou Dilma apreensiva," published on june 14, 2016 . available at http://www1.folha.uol.com.br/esporte/2015/06/1641861-ameaca-de-bomba-na-copa-mobilizou-inteligencia-e-deixou-dilma-apreensiva.shtml . Accessed 31 July 2015.