Brazil

What is the legal framework that protects people's privacy in Brazil? Are my rights protected against State surveillance 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

What is the legal framework that allows for the 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 access to billing documents (article 11, Law no. 8.218/91).	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. 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).	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 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

Who has the authority to access stored information and intercept communications in Brazil and by what means?

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

How can I find out if I was a target of surveillance in Brazil?

You can't find out. The Code of Criminal Procedure (CPP) provides that a judge, upon an application for a "precautionary measure" [medida cautelar] (such as an application for a subpoena or warrant) shall notify the affected party, "except in cases of emergency or the possibility [that service may] compromise effectiveness of the measure" (article 282, § 3). While criminal investigations are conducted, this exception applies.

When criminal cases are brought to trial in courts, the accused shall be summoned by the judge when production or admission of evidence (such as those from interceptions and data confidentiality breaches) is requested (art. 370, CPP) so the accused learns that he or she was a target of surveillance.

With respect to intermediaries, most of the data requests and wiretap orders are accompanied by gag orders that forbid telephone companies and Internet service providers to provide notification. Despite the absence of a legal prohibition of notifying users in other circumstances, companies do not proactively engage in this practice.

Can the Brazilian government legally hack into our computers? Under what circumstances? What is its legal authority?

The legal scenario is uncertain. There is no specific regulation of government hacking in Brazil. However, news articles suggest that Brazilian police authorities claim authority to install spyware under the Interceptions Act, and that courts have accepted the applications and allowed the practice. Meanwhile, academics and civil society groups have argued that the practice is illegal in absence of a well-defined legal authority to perform such invasive actions.

One fact is clear: Brazilian law enforcement authorities have interest in hacking technologies. In July 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 citizens around the world—was hacked. Leaked internal documents were published online; they contained several references to intelligence agencies in Brazil, 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), Army's Intelligence Center (CIE), Cyberwar Instruction Center (CIGE), Rio de Janeiro Civil Police Department (CINPOL and DRCI), Rio de Janeiro Military Police Department, São Paulo Civil Police Department, São Paulo Military Police Department, Federal District Civil Police Department, Federal District Military Police Department, Ministry of Justice, and the Office of the Attorney General for the Republic.

The leaked documents raise questions about a growing surveillance market in Brazil and highlight the need for legal discussions about the kind of data that may be intercepted, taking into account the evolution of new surveillance technologies.

How many communications have been wiretapped by the Brazilian State?

According to provisions in Resolução no 59/08 issued by CNJ, criminal court judges all over the country are required to provide the Inspector-General of the National Judiciary Office with data on telephone interception operations, as well as interception of IT 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, VoIP phones and emails under surveillance.

Numbers obtained by InternetLab via FOIA request show that, on average, 18,000 telephone lines per month are wiretapped in Brazil. But Brazil does not have criteria or statistics on wiretaps like some other countries in the region do, so comparing Brazil to them is not helpful. We do know that in 2013, the United States, whose population is 120 million above that of Brazil's, authorized 3,576 wiretap orders. We do not know how many wiretap orders were authorized in Brazil, but 13,309 new criminal interception procedures were filed in 2013. In turn, Germany, a country with less than half the population of Brazil, issued 19,398 initial interception orders (*Erstanordnungen*) in 2013. In Brazil, 50,265 interception notices were sent to telecommunications companies over the same period of time.

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

Is the use of encryption legal in Brazil?

The short answer is yes. According to the Brazilian Constitution, no one shall be obliged to do or not to do something, except by virtue of law. The use of encryption is not prohibited per se by law in Brazil. Ergo, its implementation is lawful.

The most cautious answer, however, is it depends. The Brazilian National Telecommunications Agency (ANATEL) orders telecommunication 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 (art. 26, parágrafo único, Resolution nº 73/98; art. 90, Resolution nº 477/07; art. 24, Resolution nº 426/05). The Brazilian Interception Law also compels telecommunications providers to cooperate with law enforcement in wiretap proceedings authorized by law (art. 7, Lei n. 9.296/96). In practice, this constrains the use and type of encryption and similar technologies implemented by those actors.

While these ("CALEA"-type of) obligations do not directly extend to over-the-top applications that provide communications services, the huge popularity of encrypted messaging apps in Brazil has stirred intense debate around this technology in Brazil.