PRIVACY INTERNATIONAL

Stakeholder Report
Universal Periodic Review
27th Session – Brazil

The Right to Privacy in Brazil

Submitted by Coding Rights, Privacy LatAm and Privacy International

September 2016

PRIVACY INTERNATIONAL

CODING RIGHTS

Introduction

1. This stakeholder report is a submission by Coding Rights, Privacy LatAm and Privacy International (PI). PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. Coding Rights is a Brazilian based women-led civil society organization working to expose and redress the power imbalances built into technology and its applications. Privacy LatAm is a hub of Latin American academics who works and research the field of privacy and data protection. Coding Rights, Privacy LatAm and PI wishes to bring concerns about the protection and promotion of the right to privacy in Brazil before the Human Rights Council for consideration in Brazilian's upcoming review.

The right to privacy

2. Privacy is a fundamental human right, enshrined in numerous international human rights instruments. It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association.[1]

3. Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[2] As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection of personal data.[3] A number of international instruments enshrine data protection principles[4] and many domestic legislatures have incorporated such principles into national law.[5]

1 Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

2 Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

3 Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17)

4 See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72) As of December 2013, 101 countries had enacted data protection legislation.

5 See: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (January 28, 2014). Available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416 [1] A/HRC/WG.6/13/TUN/3, para 53 and 54

Follow up to the previous UPR

4. In Brazil's previous review, no express mention was made of the right to privacy in the context of communications surveillance in the National Report submitted by Brazil or the report of the Working Group.
5. However, Estonia did submit a recommendation on the right to privacy with regards to women calling on Brazil "to further develop the legislation that would allow women to exercise their rights to privacy and confidentiality during police investigations and guarantee the right to presumption of innocence, due process, and legal defence."[6]

6. Concerns on the right to privacy in relations to communications surveillance were expressed by stakeholders.[7] These concerns were raised with regards to the cybercrime legislation (Bill 84 of 1999) and the obligations it would impose on Internet service providers which would be obliged to collect and retain users' personal data for extended periods of time[8] and to inform authorities about any possible crime that may have been committed through their services.[9]

Domestic laws related to privacy

7. The Federal Constitution of Brazil of 1988 upholds the right to privacy under Article 5, X and XII. In addition, there are several other laws which protect the right to privacy including the Civil Code (Law No. 10.406 of 2002)[10], the Consumer Protection Code (Law No. 8.078 of 1990), the Credit Information Law (Law No. 12.414 of 2011), the Access to Information Law (Law No. 12.527 of 2011) and the Civil Rights Framework for the Internet (Law No. 12.965 of 2014)[11]. These statutes can be described collectively as the Data Privacy Legal Framework. Nevertheless, even though the country has been consulting on a draft bill on data protection since 2010, so far there is no comprehensive legislation on data protection, which represents a significative problem, once several different statutes propose different standards for data protection in different sectors and several areas are not covered at all if not for the general Constitutional provision. As of now, two Data Protection Bills are being considered by Parliament: Bill 330/2013, of the Federal Senate, and Bill 5276 of 2016, of the Executive.

International obligations

8. Brazil has ratified the International Covenant on Civil and Political Rights (ICCPR), which Article 17 provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or

6 A/HRC/21/11, Recommendation 119.116
7 A/HRC/WG.6/13/BRA/3
8 See Joint Submission 9 submitted by The Women's Networking and Support Programme, Instituto NUPEF, Sexuality policy watch and the Association for Progressive Communication, paras 13-14
9 See submission by Article 19, para, 7, p.2
10 Law No. 10.406 of January 10, 2002 (Civil Code; Código Civil)), http://www.wipo.int/wipolex/en/details.jsp?id=9615 (last accessed 26 June 2015).
11 Law No. 12.965 of 2 (Marco Civil da internet - Civil Rights Framework for the Internet; also called Internet Act), http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (last accessed 26 June 2015).

correspondence, nor to unlawful attacks on his honour and reputation". The Human Rights Committee has noted that states party to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."[12]

9. Since 25 September 1992, Brazil is a signatory to the American Convention on Human Rights or "Pact of San José de Costa Rica" (the "American Convention") but has not yet accepted the compulsory jurisdiction of the Inter-American Court of Human Rights. Brazil has also been leading many of the advancement made at the UN on the right to privacy. Together with Germany it introduced the UN Resolutions on the right to privacy in the digital age adopted by the UN General Assembly in 2013 and 2014, and it played a similar leading role with the creation of the mandate of the UN Special Rapporteur on the Right to Privacy by the Human Rights Council in March 2015.

Areas of Concern

Interception of communications and police infiltration in social networks

10. Interception of communications in Brazil is regulated by law No. 9.296/96[13] which allows for interception on both telephone and information technology systems. The purpose set by the law is for instructing criminal procedures or investigations. The requirements are a court order, which can be submitted directly by a court or requested by police authorities and the Office of the Public Attorney. The request must be founded within a reasonable suspicion that the person whose communications they are requesting to intercept has committed a crime, that there was no other way to obtain evidence of such crime and the interception should be runned under secrecy of justice.

11. Despite the safeguards presented in the law, there are concerns as to their implementation. For example, Article 5 of the law notes that the period may not exceed 15 days, but can be renewable for equal time once proven the indispensability of evidence. Therefore, this legislation leaves margin for interpretation regarding a time limit, a reason why there has been many cases of abuse. Indeed, in 2009, Brazil was found guilty by the Inter-American Court of Human Rights (IACHR) of having unlawfully subjected a farming cooperative associated with the Movimento Sem-Terra in the State of Paraná in 1999. It was revealed that the surveillance operations were undertaken for a period of 39 days, the request was submitted by an authority which did not have the power to make such request (i.e. Military Police, which does not have investigatory powers), it failed to meet the tests of reasonable suspicion as they were not undertaken within a criminal investigation procedure.[14]

12 General Comment No. 16 (1988), para. 1
13 Available at: http://www.planalto.gov.br/ccivil_03/leis/L9296.htm
14 See: Inter-American Court of Human Rights, Case Escher et al. vs. 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_ing.pdf

12. Trying to address the issues, in 2013, the Brazilian Supreme Court has considered the lack of clarity about the successively renewal of the authorization without time limit set as an issue subjected for general repercussion (meaning that a decision on the case shall be extended to all). The final understanding was that renewal would lawful if determined by court as the necessary and only means of proof to investigate a criminal fact.[15]

13. While it seems a good restriction, nevertheless, data from the National Council of Justice, acquired through an Freedom of Information Request submitted by Internet Lab,[16] shows a substantial increase in the judicial approval of requests for interceptions of communications. In June 2009 a total of 13965 phones and 282 electronic addresses were monitored, while in August, 2013, right after World Cup protests, the total increased to 21925 of phones and 1563 electronic addresses were under surveillance. All these data provided is not easily accessible in order to allow transparency and accountability. Further, the answers received to the FOIA request did not allow to establish the total number of requests for interception, neither of rejections through the National System to Control Interceptions. And for the format of the response, it is not possible to make a direct assessment about how many of these requests led to a criminal investigation.

14. Furthermore, while the number of interception of communications increase, we have also observed another trend from law enforcement agencies to use the expansion of digital communications to interfere with privacy even without having to go through the legal procedures for approving an interception: political monitoring and infiltrating on social networks.

15. As a blog from a police chief asserts: "the online data monitoring of internet for the purpose of criminal evidence is not something exactly "new". It is already common that the police gathers information on user profiles or communities in social networks to contradict witness statements or information provided by victims and investigated. However, the scope of the sites that the police, lawyers and judges can go for information has expanded rapidly, and many more are being added daily to the list of those already existing."

16. And so far, there is no single piece of legislation to set boundaries for the monitoring and data gathering on social media. Even so, law enforcement agencies have gone beyond web searching to compile this kind of information and have adopted practices of infiltration on digital platforms. According to Ponte Jornalismo and El País, an Army official of the Brazilian Armed Forces used, among other things, the Tinder application in order to meet women from social movements and activist groups and monitor their movements. This led to the arrest of members of one of these groups right before a planned political protest, where they were confronted by a huge operation with helicopters and lots of police officers. The group were released after a few hours with no charges. Infiltration of police agents is regulated by session III of Law 12850 from 2013,[17] which deals

15 http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=242810
16 http://www.internetlab.org.br/wp-content/uploads/2015/07/LAI-Intercepta%C3%A7%C3%B5es-para-o-site.pdf
17 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm

with organized crime, have no particular provision on infiltration on digital platforms but sets the need for court order to authorize such practice. Nevertheless, legal justification for these infiltrations, as well as the connection between the Army and the Military Police of São Paulo, is yet unclear, and both organizations deny that it exists.[18]

Blanket data retention

17. Resolutions No. 426/05[19], 477/07[20] and 614/13[21] of Anatel, the agency responsible to regulate the telecommunications industry and oversight of provision of related telecommunication services, require service providers to retain metadata pertaining to landline and mobile telephone services.

18. Article 22 of Resolution No. 426/05 requires landline service providers to retain data for at least 5 years and does not include details on the type of data, use limitation or purpose specification. Article 10, XX, of Resolution No. 477/07 disposes that mobile service providers must retain user account information and billing documents containing data on incoming and outbound calls, dates, time, duration, and price for a minimum of 5 years. Article 53 of Resolution No. 614/13 requires internet connection providers to retain data for at least 1 year.

19. Article 17 of the Law no. 12.850/13[22], about organized crime, provides that landline and mobile telephone companies are required to retain "identification logs of numbers of origin and destination of telephone connection terminals" for 5 years.

20. Law no. 12.965/14[23], also known as the Marco Civil, requires that internet connection providers retain Internet connection logs for 1 year under Article 13. For-profit application service providers are required to store logs of access to applications for a period of 6 months under Article 15. Paragraph 2 of both articles allow for the extension of retention periods in certain circumstances but there is no maximum time limit on the extension - which may be theoretically unlimited.

21. Such blanket data retention policies pose a significant interference with the right to privacy of users, as it was made clear in Digital Rights Ireland v Minister for Communications and Others[24], the Grand Chamber of the Court of Justice of the European Union (CJEU) concluded that the 2006 Data Retention Directive, which required communications service providers to retain customer data for up to two years for the purpose of preventing and detecting serious crime, breached the rights to privacy and data

18 Salvadori, F. (2016, September 9). "Infiltrado do Tinder" que espionava manifestantes é capitão do Exército. Ponte Jornalismo. Retrieved September 20, 2016, from ponte.org/infiltrado-do-tinder-que-espionava-manifestantes-e-oficial-do-exercito/
19 Available at: http://www.anatel.gov.br/legislacao/resolucoes/20-2005/7-resolucao-426
20 Available at: http://www.anatel.gov.br/legislacao/resolucoes/2007/9-resolucao-477
21 Available at: http://www.anatel.gov.br/legislacao/resolucoes/2013/465-resolucao-614
22 Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm
23 Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
24 http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN

protection. The CJEU observed that the scope of the data retention "entails an interference with the fundamental rights of practically the entire European population". The CJEU went on to note the Directive was flawed for not requiring any relationship between the data whose retention was provided for and a threat to public security, and concluded that the Directive amounted to a "wide-ranging and particularly serious interference" with the rights to privacy and data protection "without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary".

Access to stored data and blockage of applications due to jurisdictional conflicts to access user data

22. In case of investigations about money laundering (Law No. 9.613/98[25]) and organized crime (Law 12.850/13)[26] police authorities and the Public Attorney's Office can request directly to service providers to access users' subscription data, which comprises name, affiliation and address. Similarly, under Article 38 of ANATEL Resolution No. 596/12[27], the agency may request service providers directly for access to account information and call records of users.

23. In a similar way, paragraph 3 from article 10 of Law No. 12.965/14[28] provides that subscription data (name, affiliation and address) from connection and service providers can be access without court order by administrative authorities with legitimate competence. Paragraph 1 from article 10 of the same legislation also establishes that law enforcement authorities must require a court order to access both connection logs from service and connection providers, as well for accessing the content of private communications. So, unlike accessing logs and the content of digital communications, access to subscription data does not require a court order.

24. While access to subscription data without a court order is still problematic, the request for a court order for connection logs could, if effectively implemented, provide some safeguard against unlawful interference with privacy. Nevertheless, the application of such provisions has led to court orders blocking some of the most popular modern digital communicaitons applications.

25. In less than a year, judges in different States of Brazil have been issued court orders to telecommunications companies requiring them to cut off access to chat applications in the whole country due to services providers' denial of giving law enforcement agencies access to users' data.[29]

26. As a result of this trend, National Congress have been proposing several

25 http://www.planalto.gov.br/ccivil_03/leis/L9613.htm - article 17- B
26 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm - article 15
27 http://www.anatel.gov.br/legislacao/resolucoes/2012/308-resolucao-596
28 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
29 https://techcrunch.com/2016/07/19/whatsapp-blocked-in-brazil-again

draft bills that jeopardize the current status of protections, particularly changing Marco Civil, a text resultant of years of dialogue within different stakeholder groups. Proposals vary from provisions on blockage of applications; changing conditions for access to users' connection and application logs, location and subscription data (some of them require access points and service providers to collect them; another one mandates photo ID's on SIM card purchases). Many of these proposals have emerged from the Parliamentary Commission on Cybercrime,[30] while others are also part of the conservative agenda that informs recent activities National Congress. Most of them are being compiled in this database developed by Coding Rights to track legislative procedures pertaining to digital helm: codingrights.org/pls.

Surveillance Legacy from the Mega Events

27. Being the host of a series of major international mega events, from Rio+20 to the World Cup in 2014 and the Olympics in 2016, Brazil have become one of the main markets for surveillance technologies.[31] In the list of purchases by Military Police and Ministry of Defense departments are drones, facial recognition goggles and a face database system, video cameras and more integration of them to the Centro Integrado de Comando e Controle (CICC) bases (also built specially for the "Big Events" and left as "legacy" for the country), mobile CICC station vehicles (equipped with movable cameras and audio capture), high-quality video surveillance balloons (with 13 cameras each).[32] An investigation by VICE News discovered that a division of the Army (CCOMGEX, "Center of Communication and Electronic War") has bought a cell-site simulator ("IMSI catcher") from Harris Corporation, although it is not clear if its purchase was related to the Olympics.[33]

Limitations on anonymity

28. Subsection IV of article 5 of the Brazilian 1988 Federal Constitution prohibits anonymity in the context of freedom of expression. Furthermore, under Article 42 and 58 of the Regulation No. 477/07 of Anatel[34], users must provide a minimum set of personal data in order to be able to subscribe to a mobile telephone service. Such a ban on anonymity and mandatory registration of SIM cards raises serious concerns for the ability of users to freely and securely enjoy their fundamental right to privacy and freedom of expression.[35] As the UN Special Rapporteur on Freedom of Expression has noted, "encryption and anonymity provide individuals and groups with a

30 https://cpiciber.codingrights.org/
31 http://apublica.org/2013/09/copa-brasil-vira-mercado-prioritario-da-vigilancia/
32 Kayyali, D. (2016, June 13). As Olimpíadas estão transformando o Rio em um Estado de vigilância e repressão. VICE Motherboard. Retrieved September 20, 2016, from https://motherboard.vice.com/pt_br/read/as-olimpiadas-estao-transformando-o-rio-em-um-estado-de-vigilancia
33 Vicente, J.P. (2016, July 27). Como as Olimpíadas ajudaram o Brasil a aumentar seu aparato de vigilância social. VICE Motherboard. Retrieved September 20, 2016, from https://motherboard.vice.com/pt_br/read/como-o-brasil-aprimorou-seu-aparato-de-vigilancia-social-para-as-olimpiadas/
34 http://www.anatel.gov.br/legislacao/resolucoes/2007/9-resolucao-477
35 http://www.ohchr.org/Documents/Issues/Opinion/Communications/Jointcollaboration.pdf
36 A/HRC/29/32, para 16.

zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attack".[36]

Privacy, confidentiality during police investigations and addressing gender violence

29. Recalling Estonian recommendation "to further develop the legislation that would allow women to exercise their right to privacy and confidentiality during police investigations and guarantee the right to presumption of innocence, due process, and legal defence", we also want to stress that no particular change was achieved in the matter. In Brazil, there is no specific law that guarantees the right to privacy and confidentiality in gender related violence or any other crime. The only restriction is regarding minors (of any gender) that have their right to privacy and anonymity. According to some interviews carried out with victims of online violence (part of those interviews can be read in the newsletter on online violence, privacy and anonymity published by Antivigilancia platform[37]), one of the main reasons for victims to avoid reporting to the police has to do with the fear of being exposed and publicly criticized.

30. It has also been reported in the newsletter on anonymity and online gender violence published by Antivigilancia platform that the use of pseudonym and assumed name by transgender people is becoming more difficult on social networks that introduced real name policies, requiring the use of the real name in their IDs. These policies have the effect of limiting the capacity of individuals to use their social name, and are a cause of particular concerns for individuals that are the common target of online abuses and attacks.

31. Therefore, we should consider also the protection of privacy rights as a powerful tool in the context of balancing power struggles for gender balance and promoting the rights to sexual minorities. Some relevant bills that focus on gender violence in online and offline environments (regarding revenge porn and leaking intimate content without consent) are being discussed at the moment in the country, according to the analysis report on Law Bills developed by Coding Rights[38] and special attentions should be payed to those proposals that protect privacy of women without harming

37 https://antivigilancia.org/pt/boletim-14-es/
38 codingrights.org/pls

anonymity and privacy of internet users in general.

Recommendations

32. We recommend that the government of the Colombia to:

- Increase transparency in the use of court orders providing for interception of communications. Regular publication by the National Council of Justice (CNJ) regarding the number of requirements for interception of communications, as well as the rejections, acceptance and data about how many of these requests led to a successful criminal investigation shall be publicly disclosed;

- Ensure that monitoring and infiltration of social networks by law enforcement agencies is regulated by law and it is not used as a way to intercept communications and bypass legal procedures and limits for such practices;

- Amend requirements for blanket, indiscriminate data retention and ensure data retention ordered issued by a judge are limited in scope and time, and are necessary and proportionate to a legitimate aim;

- Ensure that requests to user data by authorities are targeted, necessary, and proportionate;

- Ensure that any new laws, particularly those proposed by the Parliamentary Commission of Cybercrime, comply and to not weaken the privacy standards assured in the Internet Civil Rights Framework (Marco Civil da Internet) and the Constitutional right to privacy;

- Ensure that the Data Protection Bills which are currently being considered by the Brazilian Parliament foster privacy and data protection practices among private and public sectors;

- Publicly avowal the surveillance capabilities of Brazilian law enforcement and other agencies and promote transparency about public expenditures in the purchase of surveillance equipment and as well as about limits, competencies and oversight of different authorities to use them within the boundaries of fundamental human rights;

- Recognize the importance of anonymity to guarantee the rights to privacy and freedom of expression online, particularly for minorities and voices of dissent and as a way to promote gender equality, the rights of LGBTs and prevent online abuse.