The Right to Privacy in Colombia

Stakeholder Report
Universal Periodic Review
30th Session - Colombia

Submitted by Dejusticia, Fundación Karisma and Privacy International

October 2017

I. Introduction

1. This stakeholder report is a submission by Dejusticia, Fundación Karisma and Privacy International (PI). Dejusticia is a Colombian human rights organization that provides expert knowledge on human rights. Fundación Karisma is a Colombian civil society organization that seeks to respond to the opportunities and threats that arise in the context of 'technology for development' for the exercise of human rights. PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world.

2. Dejusticia, Fundación Karisma and Privacy International wish to bring concerns about the protection and promotion of the right to privacy for consideration in Colombia's upcoming review at the 30th session of the Working Group on the Universal Periodic Review.

II. The right to privacy

3. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[1] 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.

4. 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]

5. A number of international instruments enshrine data protection principles,[3] and many domestic legislatures have incorporated such principles into national law.[4]

III. Follow up to the previous UPR

6. During Colombia's previous review in the second cycle in 2013, no express mention was made of the right to privacy in the context of data protection and communications surveillance in the National Report submitted by the government of Colombia or the report of the Working Group.

7. However, the compilation report of the OHCHR did raise the issue that "According to Working Group on Enforced or Involuntary Disappearances, Colombia still did not have a policy to rid the police and military and other State security and intelligence bodies of their links to paramilitarism".[5] Furthermore, the report[6] noted the concerns expressed by the UN Human Rights Committee in relations to their unlawful communication surveillance policies and practices in 2012[7] which were also raised at the last review of the Committee in 2016.[8]

8. Furthermore, the various stakeholders raised the issue of unlawful surveillance of human rights defenders and also the protection of freedom of expression online.[9]

9. Finally, extensive mentions and recommendations were made by government delegations on the protection of human rights defenders and journalists to report and investigate human rights abuses and violations.[10]

IV. Domestic laws related to privacy

10. The Colombian legal framework provides a number of essential protections for the right to privacy.

11. Article 15 of the 1991 Constitution provides that everyone has the right to personal and family privacy. It states:

    "Correspondence and other forms of private communication are inviolable. They may only be intercepted or recorded pursuant to a court order, following the formalities established by law."

12. Article 250 of the Constitution confers the Attorney General the authority to carry out searches, seizures and interceptions of communications without a prior judicial authorisation. Article 235 of the Criminal Procedure Code stipulates the conditions under which the Attorney General's Office can order the interception of communications. Interception without a warrant, save the described Attorney General's authority to perform such an interception, is a crime under the Criminal Code.

13. Financial personal data in Colombia is protected by Law 1266 of 2008. This law was originally intended to be the general legal framework applicable to the management of personal information. After a revision by the Constitutional Court (Decision C-1011 of 2008), its scope was reduced to only the financial, credit, commercial, and services information (and to such information coming from abroad for us in financial risk and credit risk assessment ("Financial Personal Data").

14. In 2012 the Colombian Congress enacted its own general data protection legislation: Law 1581 of 2012, which constitutes the general legal framework applicable to the management of personal data. This law was reviewed by the Constitutional Court in Decision C-748 of 2011, and regulated by Decree 1377 of 2013.

V. International obligations

15. Colombia has ratified a number of international human rights treaties with privacy implications. It has ratified the International Covenant on Civil and Political Rights (ICCPR), which upholds the right to privacy under Article 17. 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]."

16. On 28 May 1973, Colombia ratified the American Convention on Human Rights or "Pact of San José de Costa Rica" (the "American Convention") which under Article 11 establishes that "No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honour or reputation."

17. Furthermore, Colombia is a party to the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, and the International Convention for the Protection of all Persons from Enforced Disappearance.

18. All of these human right treaties ratified by Colombia are part of the Colombian Constitution in accordance with Article 92 of the Colombian Constitution, conferring upon them the higher status of constitutional law under paragraph 13.

VI. Areas of concern

i) Overly-broad purposes

19. Outside of the surveillance powers pertaining to criminal investigation proceedings and those of the Attorney General, Colombia has adopted an Intelligence and Counterintelligence Law (Statutory Law No. 1621 of 2013). This law regulates intelligence and counterintelligence activities, including "monitoring the electromagnetic spectrum".

20. The purposes under which information can be obtained as outlined in Article 4 of the Law No. 1621 of 2013, are overly-broad and vaguely defined, and include: ensuring national security, sovereignty, territorial integrity, the security and defence of the nation, the protection of democratic institutions and the rights of Colombian residents and citizens and the protection of natural resources and economic interests of the nation.

21. Such broad purposes allow for an expansive interpretation of the instances in which communication surveillance can be undertaken, failing to meet the tests of legality, necessity and proportionality.

ii) Lack of a definition of 'electromagnetic spectrum" monitoring

22. Article 17 of the Intelligence Law is entitled "Monitoring the Electromagnetic Spectrum and Intercepting Private Communications" and distinguishes monitoring the electromagnetic spectrum for intelligence and counterintelligence purposes, such for the purpose of maintaining national security, from the interception of communications. But 'monitoring' the electromagnetic spectrum is not defined anywhere in the Colombian law.

23. Without any definition provided, 'monitoring' the electromagnetic spectrum could include analysing and monitoring e-mails, text messages and phone calls that are carried upon the electromagnetic spectrum. Those acts constitute 'interception' of the communication and thereby interfere with the privacy of the person sending and receiving the information.

24. According to Article 17, the interception of communications is not authorised by the Intelligence Law, but rather must only occur under the lawful authority of the Criminal Procedure Code, on a targeted basis. However, the assertion that 'monitoring' does not constitute interception of communication leads to a significant legal loophole that raises serious concerns related to the protection of the right to privacy.

iii) "Monitoring of the electromagnetic spectrum" without prior judicial authorisation

25. In light of the above, the expression 'monitoring does not constitute interception of communication' under Article 17 of the Intelligence Law fails to recognise that monitoring the electromagnetic spectrum constitutes an interference with the privacy of communication.

26. By not requiring the 'monitoring' of the electromagnetic spectrum to be subjected to same or similar rules that regulate the interception of communication under the Criminal Procedure Code, the Intelligence Law fails to provide protection against interference with private communications.

27. This loophole in the law is particularly problematic given the kind of surveillance technologies employed by the Colombian security and law enforcement forces outlined elsewhere in our submission. As noted in the Concluding Observations on the Seventh Periodic Report of Colombia there are concerns that "instances in which private communications conveyed via the electromagnetic spectrum are intercepted without the benefit of a rigorous assessment of the legality, necessity and proportionality of such interceptions".[11]

iv) Far-reaching powers of the Police without appropriate controls

28. In January 2017, the National Code of Police and Coexistence (Código Nacional de Policía y Convivencia para Vivir en Paz) entered into force. This new Code gives far-reaching powers to the police without providing appropriate controls over police discretion. It includes several provisions that have particularly negative implications with regards to the right to privacy and their collective interpretation, which can lead to a state of surveillance.

29. Firstly, Article 327 contains an unduly narrow definition of privacy. By defining the right to privacy as the right of people "to meet their needs and develop their activities in an area that is exclusive and therefore considered private", the provision seems to confuse the right to privacy with the right to unhindered development of personality as well as with the right to the inviolability of the home.

30. Therefore, by linking the right to privacy with the existence of private physical spaces, it excludes from privacy protection any person or assets (such as cars, or electronic devices like portable computers or cellphones) placed in public places, including bars, restaurants, etc, while also leaving in a legal grey area private acts that may take place in a public space.

31. Conversely, Article 139 defines public space in a very broad way, including notably "the electromagnetic spectrum".

32. The combined result of these definitions is of significant concern to the protection of privacy, particularly when considering that Article 237 could be interpreted to mean that communications travelling through the electromagnetic spectrum would be excluded from privacy protection.

33. Lastly, the new Police Code does not seem to take into consideration the complex technological changes which affect modern communication. Hence, it is unclear how the privacy of digital communications and of online spaces is protected given the very restrictive definitions of privacy and public space included in the Code.

34. This shortcoming of the law was raised by the Human Rights Committee which highlighted concerns that the new Policy Code defines *"the concept of 'public areas' in a very broad sense that includes the electromagnetic spectrum, and by the fact that all the information and data gathered in public areas are considered to be in the public domain and to be freely accessible (art. 17)".*[12]

v) Surveillance technologies capabilities operating outside the legal framework

35. Colombia's most known communications interception system is called Esperanza. The Office of the Attorney General manages the platform, which can obtain mobile and fixed-line call data and content. Esperanza is used to obtain evidence for criminal investigation and prosecution by various law enforcement agencies in

Colombia. It relies on the collaboration of the telecommunications operators, which are obliged, under Colombian law, to cooperate with requests of interception by relevant authorities[13].

36. In 2007, the Police set up a system with even greater surveillance technology capabilities, known as the Single Monitoring and Analysis Platform (PUMA). Unlike Esperanza, PUMA is directly linked to the service provider's' network infrastructure, which enables the system to potentially intercept communications of all individuals that go through this network and to direct these communications to the law enforcement monitoring facility without further facilitation from the service provider. Israeli companies Verint, and later NICE provided PUMA's operational technology.

37. A branch of the Police, DIPOL (Dirección de Inteligencia Policial), also employs a mass surveillance system called the Integrated Recording System (IRS). Interception through IRS, just like in the case of PUMA, is done in bulk and without assistance from the service providers.

38. Whilst Decree 1704 (2012) requires telecommunications providers to set-up their infrastructure to enable "access and traffic capture" for crime investigation purposes, there is no explicit provision which either permits or prohibits measures of bulk surveillance as PUMA or IRS in the current legal framework which regulates the surveillance of communications in Colombia.

vi) Deployment of intrusive surveillance technologies

39. There are reports indicating that Colombian authorities had acquired intrusive surveillance technologies.

40. Hacking Team produces an intrusion system that was acquired by the Colombian police[14]. The company's Remote Control System (RCS) can be used to take control of a computer and mobile devices while remaining undetectable to users, as it is designed to bypass common antivirus programmes and encryption. By infecting a target's device, the RCS suite can capture data on a target's device, remotely switch on and off webcams and microphones, copy files and typed passwords. Besides, it can covertly collect, modify and/or extract data from the targeted device. As such it is a particularly intrusive form of electronic surveillance, given the personal information that can be obtained from such access.

41. A 2014 investigation by the Citizen Lab at the University of Toronto, concluded that since 2012 those technologies have been identified and associated with attacks on journalists, activists and human rights defenders, and showed evidence confirming suspected deployment of those technologies in at least 21 countries, including Colombia.[15]

42. In 2014, Hacking Team had a Colombia-based field engineer and an active contract with the Colombian police. According to Privacy International's investigation[16] Hacking Team had an active contract with the Colombian police in 2014. Despite this compelling evidence on the deployment of offensive malware products of Hacking Team, the Colombian police denied any direct relation with Hacking Team, admitting only contractual ties with a Colombian company called Robotec[17], which is an intermediary for the distribution of those products. However, the leaked document of July 2015 on Hacking Team showed that the Colombian police directly contacted with Hacking Team in order to activate the offensive malware products they bought in the first terms of 2015.

43. According with article 269A of the Colombian criminal code, "hacking" ("Abusive access to an information system") is a criminal offense, and therefore, in the absence of any law explicitly regulating its use for surveillance purposes, it is a form of extra-legal surveillance that is illegal under Colombian law. The privacy intrusion involved and the risk to security of communications raise serious human rights concerns. As a form of government surveillance, hacking presents unique and grave threats to both privacy and security. It has the potential to be far more intrusive than any other surveillance technique, permitting the government access to our personal devices and all the intimate information they store. It also permits the government to control the functionality of our devices, facilitating real-time surveillance through a device's microphone, webcam and GPS-based locator technology, or enabling the alteration, creation or deletion of data. At the same time, hacking has the potential to undermine not only the security of targeted systems, but also the internet as a whole.

44. Furthermore, many companies offer mobile monitoring equipment, also known as 'IMSI catchers' in Colombia, according to a Privacy International investigation.[18] An IMSI Catcher performs interception by presenting itself as a base station amongst the mobile network: the station that a phone connects to when it wants to place a call or send a message. Once connected to the IMSI Catcher's base station the Catcher it becomes possible to monitor the operation of the phone: the voice calls taking place, the messages being sent and the location of the phone and recover unique identifiers from the device such as its IMEI and IMSI numbers.

45. New Zealand-based Spectra Group, via Colombian company Microtel Ltda provided its Laguna IMSI catcher to the Police Intelligence Directorate (Dirección de Inteligencia Policial, DIPOL) in September 2005. The Laguna system is designed to monitor and record telephone conversations and data in mobile communication systems and could be mobile or assembled in fixed stations.

46. Bulldog and Nesie, manufactured by UK surveillance company Smith Myers, are two other popular IMSI catchers sold in Colombia. In 2010, the DAS was preparing to purchase a Bulldog interception system for over US$ 250,000 and a Nesie system for over US$ 320,000. The Fiscalía was also planning to buy a Bulldog system for just over US$ 280,000 as was the sectional division of DIJIN in Bogotá. In 2014, the Finnish branch of Canadian telecommunications company Exfo exported its NetHawk F10 IMSI catcher to Colombia.[19]

47. UN human rights mechanisms have expressed concerns about the use of hacking for surveillance purposes[20]. The UN Special Rapporteur on freedom of expression noted, in his 2013 report, that "Offensive intrusion software such as Trojans, or mass interception capabilities, constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information (…) From a human rights perspective, the use of such technologies is extremely disturbing. Trojans, for example, not only enable a State to access devices, but also enable them to alter – inadvertently or purposefully – the information contained therein. This threatens not only the right to privacy but also procedural fairness rights with respect to the use of such evidence in legal proceedings".[21]

vii) Reports of unlawful interceptions of private communications, including of journalists and human rights defenders

48. Communications interception scandals (sometimes called by the Colombian Spanish term 'chuzadas') have been a feature of Colombian security politics since the 1990s.

They include the unlawful surveillance of politicians, judges, journalists and human rights defenders and families of disappeared persons.

49. In 2014, the Colombian weekly magazine Semana reported that a Colombian army unit codenamed Andromeda was spying for more than a year on the government's negotiating team in ongoing peace talks with the country's FARC guerrillas.[22]

50. Stories of the illegal interception of private communications pervade accounts of extrajudicial disappearances and killings. Different agencies have been involved in these illegal interceptions such as:
    - The unlawful tapping of 2,500 phone lines by the joint military-police Unified Action Groups for Personal Liberty (Grupos de Acción Unificada por la Libertad Personal, GAULA), including a group representing the families of the disappeared, namely the Association for the Relatives of Detained-Disappeared (ASFADDES) among many other human rights organisations.[23]
    - The dismissal of eleven police generals from DIPOL after it was disclosed that the agency had tapped the phone lines of influential opposition politicians, journalists, lawyers, and activists.[24]

51. Yet the most notorious of the interception scandals involves the Administrative Department of Security (DAS) and was revealed by Semana in February 2009. Special strategic intelligence groups of the DAS conducted targeted surveillance of an estimated 600 public figures including parlamentarians, journalists, human rights activists and lawyers, and judges among others. According to files retrieved during an investigation by the Fiscalía, the DAS intercepted phone calls, email traffic and international and national contacts lists, using this information to compile psychological profiles of targets and conduct physical surveillance of subjects and their families, including children.[25]

52. Communications surveillance was central to the DAS abuses. Privacy International spoke to confirmed former targets of DAS surveillance and persons who strongly believe that they are still targeted by state electronic surveillance. DAS documents retrieved during the unlawful interception scandal in 2009 contained detailed descriptions of the Jose Alvear Restrepo Lawyers' Collective (CCAJAR) employees' and families' movements, list of their phone contacts and records of the DAS' attempts to link phone numbers with CCAJAR members.[26]

53. The phone lines of journalist Hollman Morris were under near-constant surveillance. Morris was later forced into exile on several occasions. Claudia Duque, a lawyer and journalist formerly working with the CCAJAR lawyers collective survived kidnapping attempts and received graphically violent phone threats; DAS files about her contained extensive evidence of communications and physical surveillance.[27] Such was the scale of the illegal interception that seven Supreme Court justices were recused from the 2011 trial of the former DAS head because evidence suggested that even they had been illegally spied on.[28]

54. The scandal-ridden DAS was disbanded in October 2011. Several former DAS heads were convicted for illegal interception and associated crimes. Fernando Tabares, former DAS director, was convicted for illegal wiretapping of government opponents in 2010. Jorge Noguera and Maria del Pilar Hurtado, who headed DAS in 2002 though 2008, are the highest-ranking officials to have been convicted for illegal surveillance. In 2011 a new agency, the National Intelligence Directorate (Dirección Nacional de Inteligencia, 'DNI'), was established to head the intelligence and counterintelligence sector within the overall structure of the state.

55. in the Concluding Observations on the Seventh Periodic Report of Colombia, the UN Human Rights Committee said that the government should *"expedite the investigations being carried out into suspected illegal surveillance activities allegedly conducted by officials of the former Administrative Department of Security and ensure that all responsible parties are held accountable for their acts"*.[29]

viii) Absence of effective independent oversight and transparency of intelligence agencies

56. In any democratic state, the oversight of lawful security acts should be a combination of executive control; parliamentary oversight; judicial review and monitoring by expert bodies.

57. Neither of these mechanisms works satisfactorily in Colombia, hence the grave violations of human rights by the security services. Of particular concerns is the lack of supervision by data protection authorities and the failure to establish parliamentary oversight.

58. On one hand, data protection statutory law (art. 2 of Law 1681 of 2012) does not apply to databases containing personal data that "have as a purpose and are related to intelligence or counterintelligence activities". Thus, even though the data protection law principles apply, there is no independent regulator to control and protect personal data held by or for intelligence purposes. As a result, the existing seven agencies with intelligence functions are not accountable to the data protection regulator of public agencies.

59. This lack of accountability is exacerbated by the ineffectiveness of the independent commission that was created within Congress to oversee intelligences activities. Although the Intelligence Law came into effect on 17 April 2013, the Legal Monitoring Commission of Intelligence, that represents the only independent system of accountability to benefit citizens, has been unable to carry out all the activities under its mandate due to alleged security and contracting procedures that mask a lack of political will. The failures of oversight are evident by the lack of any effective investigations in several reported cases of unlawful surveillance of communications of politicians, journalists and human rights activists.

ix) Data retention laws that lack safeguards against unlawful interference with the right to privacy

60. Colombia has imposed to telecommunications service providers the obligation of data retention for purposes of criminal investigation and intelligence activities.[30] According to the Council of State, the Colombian legislation clearly states that access to retained data should be done with a prior judicial order[31].

61. For intelligence activities, Law 1621 (2013) establishes that intelligence agencies may ask for the subscriber's data, "communications history" and location information. The same law provides that data may be retained for a period of five years. Finally, Resolution 0912 (2008) from National Police provides that the telecommunications service providers must allow the Police access to a database in which the following information of the subscribers must be registered: names and identification, location and residence address, cellphone number, and date and activation status.

62. The interception, collection and use of metadata interfere with the right to privacy, as it has been recognized by human rights experts, including the UN Special Rapporteur on freedom of expression, the UN Special Rapporteur on counter-terrorism and

human rights and the High Commissioner for Human Rights. The Court of Justice of the European Union noted that metadata may allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained" and concluded that the retention of metadata relating to a person's private life and communications is, in itself, an interference with the right to privacy.[32] The CJEU also held in a separate case that human rights law prohibits "national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data"[33].

63. The Human Rights Committee, in interpreting Article 17 of the ICCPR, has similarly adopted a position that data retention policies constitute an interference with the right to privacy and that as a general rule, countries should "refrain from imposing mandatory retention of data by third parties"[34]..[35]"

64. There is no regulator with the role of protecting personal data held by public agencies as the Inspector General (Procuraduría General de la Nación), that was given the task by the Constitutional Court, has not assumed this role.

x) Prohibition of encrypted communications

65. Article 102 of Law 418 (1997) prohibits sending encrypted messages in all communication devices using the electromagnetic spectrum. However, it is unclear whether these laws would also cover encrypted communications on the internet.

66. As the UN Special Rapporteur on Freedom of Expression noted restrictions on the use of encryption affect the right to privacy and freedom of expression, and therefore any such restriction needs to be lawful, necessary and proportional to the achievement of a legitimate aim.[36] Dejusticia, Fundación Karisma and PI believe that the blanket prohibition of encrypted communication currently provided in Colombian law is not necessary nor proportionate.

xi) Cellphone registry system

67. Since 2011 the Colombian government has been developing a cellphone registry system that aims to avoid and deter cellphone theft. A decree from the Ministry of ICT[37] established a measure to reduce the incentives for thieves to go after cellphones and thus reduce theft and related crimes. The decree was followed by a law and regulations established by the Telecommunications Regulator, which included a registry consisting of:
    a. lists of IMEI (International Mobile Subscriber Identity) numbers, or databases, as the legal documents call them, and
    b. a verification procedure

68. The objective behind the registry is that every device is allowed to work on mobile networks only if it is listed in a "positive database". Whenever a cell phone is stolen or lost, its IMEI is recorded in the "negative database". Mobile carriers should block any IMEI listed on this negative database to bar them from working on their networks. Also, a verification procedure was devised to keep both databases operational and effective. Based on communications metadata, the activity of each cellphone in Colombian networks is monitored to detect counterfeit or duplicated IMEI, along with devices that lack a certificate of conformity.

69. An in-depth policy and technical analysis of this registry conducted by Fundación Karisma found several problems from a human rights perspective.[38]

70. First, each IMEI is tied to a person's ID because the registry requires carriers to record IMEI, IMSI and telephone number along with the owner's name, ID and address. Mandatory identity registration requirements have been criticised by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression because they eliminate the possibility to communicate anonymously. This allows the tracking of people and facilitates the surveillance of communications[39].

71. Second, the verification procedure relies on communications metadata, which is collected and processed bypassing the constitutional protection recognised for communications content despite the interference with privacy noted above. As we mentioned in Section ix) above on data retention, the general and indiscriminate retention of all traffic and location data is contrary to international human rights law.

72. Finally, the system disproportionately affects human rights and is not necessary. The same aim of preventing cellphone theft can be reached without the registration of people's ID and the use of metadata. Sharing the "negative" list of presumed stolen cell phones may be as effective and less invasive than the current registry. Moreover, using only the "negative" list of IMEI is how it works generally in other countries and it is the way GSM Association, a trade body that represents the interests of mobile network operators worldwide, promotes the use of the system.

xii) Lack of access to intelligence archives relevant for the Peace Agreement implementation

73. According to the Peace Agreement, during the implementation of the agreement the access to the information held by the Government shall be given "in accordance with the laws in force at the time of implementing the Agreement". Currently enforceable laws regulating access to intelligence and counterintelligence information do not allow neither the Truth Commission, nor the Missing Persons Search Unit to have access to the archives that may be relevant for their investigations[40]. Access to such information is extremely important for these authorities in order to be able to determine human rights violations committed during the armed conflict, including the use of unlawful methods of surveillance or illegal processing of personal data by the intelligence agencies.

74. In 2013 the Intelligence and Counterintelligence Law (Statutory Law No 1621 of 2013) created a commission of private and public authorities to formulate criteria for purging the intelligence archives. It was noted that the Commission should consider various elements including the fundamental rights of citizens.[41] Whilst the process was concluded and a set of criteria were finalised, the Colombian government and the chairman of the Purging Commission did make these public, arguing confidentiality. If these criteria are not available to the public, it will hinder the ability to assess whether processing of personal data by intelligence agencies was lawful or not and, in case of unlawful processing, whether their actions have been corrected and citizens compensated.

xiii) Protection of sensitive databases related to the Peace Agreement

75. The Point 2.2.1 of the Peace Agreement provide for the creation of a register of all formal and informal social organisations and movements as a means for the authorities to assess their capabilities and respond to their needs as they undertake their functions in the peace process. [42] This register would involve the collection of sensitive personal data, which may reveal, for example, the racial or ethnic origin of individuals, their political orientation or their membership in social organisations. We

are concerned by the centralisation of this data and the risk that results when the necessary safeguards are not adopted to ensure the security of the data and the infrastructure. The unlawful use and sharing as well as breach of this type data, which is considered sensitive personal data in Colombia[43], may lead to discrimination or even endanger the lives or personal safety of the individuals concerned.

76. Our concerns are supported by evidence of prior incidences of unlawful access to sensitive personal data managed by the State in relation to the peace process and the reparation process. For example, in 2014 it was revealed that a network of individuals managed to unlawfully access the database managed by the Unit for Comprehensive Care and Reparation for Victims. [44] It was reported that these individuals managed to access the database using authorisation codes which had been leaked to them. This data was sold in order to enable unscrupulous people to impersonate real victims, to accelerate the payment of compensation to certain applicants, or to know the personal data of the complainants, among other offences.

77. We are concerned that similar unlawful access could occur with the registry of social organisations and movements. Therefore, if the government will proceed with the creation of this registry, it must ensure that it complies with the highest data protection standards to ensure the protection of the data and the security of its infrastructure.

VII. Recommendations

78. Based on these observations, Dejusticia, Fundación Karisma and Privacy International propose that the following recommendations be made to the Colombian government:

- Review the legal framework governing surveillance in Colombia, notably the Intelligence Law and the Police Code, to ensure they comply with the International Covenant on Civil and Political Rights, including Article 17 to ensure that any interference with the right to privacy is necessary and proportionate to the aim pursued;
- Ensure that all interception activities, including but not limited to the monitoring of the electromagnetic spectrum, are only carried out in ways that comply with the principles of legality, necessity and proportionality;
- Amend the law on data retention to ensure it does not impose indiscriminate obligations to retain communications data, and provide that any requests to access such data are subject to the principles of necessity and proportionality and authorized by judicial body.
- Conduct prompt and independent investigations into credible reports of unlawful surveillance of lawyers, journalists, human rights activists and others, with the view to bring to justice the perpetrators and provide reparations. Publish the results of these investigations;
- Strengthen effective oversight over the surveillance practices of the intelligence and law enforcement services, including by ensuring that the Commission of Intelligence and Counterintelligence Activities have the capacity to fulfil its oversight mandate in full;
- Ensure the full respect of the right to privacy by police procedures of the new Police Code;
- Disclose what type of surveillance technologies are employed by Colombian law enforcement and intelligence agencies, how their acquisition and use is regulated and monitored and how are they complying with the law and the Constitution;

- Strengthen effective guarantees related to the collection and treatment of sensitive databases related to the Peace Agreement;
- Disclose policies and procedures for data handling from law enforcement and intelligence agencies, in order to ensure that their content does not violate human rights and count with proper oversight.
- Ensure access to intelligence information files of violations of human rights as well as to intelligence information that contributes to the rights to truth justice and reparation in the implementation of the Peace Agreement.

[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] 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.

[4] As of December 2013, 101 countries had enacted data protection legislation. 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

[5] A/HRC/WG.6/16/COL/2, para. 30

[6]Ibid, para. 18

[7] CCPR/C/COL/CO/6, para. 27

[8] CCPR/C/COL/CO/7, para. 32-33

[9] A/HRC/WG.6/16/COL/3, paragraph 14 and 54

[10] A/HRC/24/6. See recommendations: 116.19, 116.73, 116.74, 116.75, 116.76, 116.77, 116.80, 116.81, 116.82, 116.83, 116.85,116.110

[11] CCPR/C/COL/CO/7, para. 32-33

[12] CCPR/C/COL/CO/7, para. 32

[13] Privacy International, Shadow State: Surveillance, Law and Order in Colombia, August 2015. Available at: https://www.privacyinternational.org/sites/default/files/ShadowState_English.pdf

[14] Privacy International, Shadow State: Surveillance, Law and Order in Colombia, August 2015. Available at: https://www.privacyinternational.org/sites/default/files/ShadowState_English.pdf

[15] The Citizen Lab, Mapping Hacking Team's "Untraceable" Spyware, 17 February 2014. Available at: https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/

[16] Privacy International, Shadow State: Surveillance, Law and Order in Colombia, August 2015. Available at: https://www.privacyinternational.org/sites/default/files/ShadowState_English.pdf

[17] Durán Núñez, D.C., El software espía de la Policía, 11 July 2015. El Espectador. Available at: https://www.elespectador.com/noticias/investigacion/el-software-espia-de-policia-articulo-571980

[18] Privacy International, Shadow State: Surveillance, Law and Order in Colombia, August 2015, pp. 42. Available at: https://www.privacyinternational.org/sites/default/files/ShadowState_English.pdf

[19] Ibid

[20] In 2017, the Human Rights Committee expressed concerns about the use of hacking for surveillance in Italy. See: Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, U.N. Doc. CCPR/C/ITA/CO/6 (28 March 2017)

[21] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40, para. 62 (17 April 2013).]

[22] Semana, *¿Alguien espió a los negociadores de La Habana?*, 3 February 2014. Available at: http://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/37607

[23] 'Informe Sobre Derechos Humanos: Colombia', US Department of State, 4 March 2002. Available at http://www.acnur.org/t3/leadmin/scripts/doc.php?le=t3/uploads/media/COI_53

[24] El Espectador, *El DAS-gate y las 'chuzadas', vuelve y juega*, 21 February 2009. Available at: http://www.elespectador.com/impreso/judicial/articuloimpreso120201-el-das-gate-y-chuzadas-vuelve-y-juega

[25] El Tiempo, *Un 'manual' para seguir y acosar a personas calificadas como opositores tenía el DAS*, 13 June 2009. Available at: http://www.eltiempo.com/archivo/documento/CMS-5436047

[26] Privacy International, Shadow State: Surveillance, Law and Order in Colombia, August 2015, pp. 53-54. Available at: https://www.privacyinternational.org/sites/default/files/ShadowState_English.pdf

[27] IFEX, *Former security operatives charged in journalist's torture in Colombia*, 18 March 2013. Available at: https://www.ifex.org/colombia/2013/03/18/security_charged/; Committee to Protect Journalists, *Colombian Official convicted of 'psychological torture' of journalist*, 22 December 2014. Available at: https://cpj.org/2014/12/colombian-of cial-convicted-of-psychological-tort.php

[28] Colombia Reports, *7 judges withdrawn from wiretap trial*, 12 August 2011. Available at: http://colombiareports.com/7-supreme-court-judges-victimized-in-wiretap-scandal-withdrawn-from-trial/

[29] Ibid, para 33

[30] For criminal investigation, Decree 1704 (2012) provides that subscriber's information and geolocalization data must be handed to the Prosecutor immediately upon request and must be kept for five years. On 18 February 2016, the Council of State reviewed Article 4 of the Decree, related to subscriber's information and declared the nullity of the expression "or other competent authorities", making it clear that subscriber's information can only be requested by the Prosecutor. Moreover, the Council of State indicated that the orders for interception of communications or data retention are supposed to be issued in accordance with the Constitution and the law.

[31]For further details, see: Submission in advance of the consideration of the periodic report of Colombia, Human Rights Committee, 118th Session, 17 October - 04 November 2016, available at: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fCSS%2fCOL%2f25208&Lang=en

[32] Judgement of 8 April 2014, *Digital Rights Ireland Ltd*, C-293/12 and *Kärntner Landesregierung*, C-594/12, EU:C:2014:238, paragraph 27. 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=635772

[33] Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al. (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (21 December 2016).

[34] Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, U.N. Doc. CCPR/C/USA/CO/4, para. 22 (23 April 2014)

[35] The Committee has also noted that Member States should review their data retention regimes with the view of ensuring: "that such activities conform with its obligations under article 17 including with the principles of legality, proportionality and necessity; [and that there exist] robust independent oversight systems [...] including by providing for judicial involvement in the authorization of such measures in all cases and affording persons affected with effective remedies in cases of abuse, including, where possible, an ex post notification that they were subject to [these] measures. See: Concluding Observations on the Sixth Periodic Report of Italy, UN Human Rights Committee, U.N. Doc. CCPR/C/ITA/CO/6, para. 37 (28 March 2017). See also: Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7, para. 24 (17 August 2015); Concluding Observations on the Initial Report of South Africa, Human Rights Committee, U.N. Doc. CCPR/C/ZAF/CO/1, paras. 42-43 (27 April 2016).

[36] A/HRC/29/32

[37] Colombian Ministry of ICT, Decreto 1630 de 2011 "Por medio del cual se adoptan medidas para restringir la operación de los equipos terminales hurtados que son utilizados para la prestación de servicio de telecomunicaciones móviles"

[38] Castañeda, J.D., *Un rastreador en tu bolsillo,* Fundación Karisma, July 2017. Available at: https://karisma.org.co/descargar/informe-investigacion-un-rastreador-en-tu-bolsillo/. An English summary is available at: https://karisma.org.co/descargar/a-tracker-in-your-pocket-executive-summary/

[39] A/HRC/29/32, para. 51

[40] See: Ramírez, A.M., Ángel, M.P., Albarracín, M., Uprimny, R. & Newman, V. (2017). Acceso a los archivos de inteligencia y contrainteligencia en el marco del posacuerdo. Bogotá: Dejusticia. Available at: https://www.dejusticia.org/wp-content/uploads/2017/04/fi_name_recurso_699.pdf

[41] Article 30 of Ley Estatutaria 1621 de 2013 "Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal.

[42] Gobierno Nacional de Colombia & Fuerzas Armadas Revolucionarias de Colombia-Ejército del Pueblo (FARC-EP). (2016). Acuerdo final para la terminación del conflicto y la construcción de una paz estable y duradera". Available at: http://www.altocomisionadoparalapaz.gov.co/procesos-y-conversaciones/Documentos%20compartidos/24-11-2016NuevoAcuerdoFinal.pdf

[43] See Article 5, Law 1581 of 2012.

[44] El Colombiano. "Siete capturados por supuesta venta de información de víctimas del conflicto", 05 August, 2014. Available at: http://www.elcolombiano.com/historico/siete_personas_capturadas_por_supuesta_venta_de_informacion_de_las_victimas_del_conflicto-OGEC_305487