PRIVACY INTERNATIONAL

Human Rights Committee 116th Session

# The Right to Privacy in Colombia

**Suggestions for right to privacy-related questions to be included in the list of issues on Colombia, Human Rights Committee, 116th Session**

**March 2016**


PRIVACY
INTERNATIONAL


Fundación
Karisma
www.karisma.org.co


Dejusticia
derecho · justicia · sociedad

## 1. Main concerns on the right to privacy and communication surveillance in Colombia

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour or reputation. Any interference with the right to privacy can only be justified if it is in accordance with the law, has a legitimate objective and is conducted in a way that is necessary and proportionate. Surveillance activities must only be conducted when they are the only means of achieving a legitimate aim, or when there are multiple means, they are the least likely to infringe upon human right.[1]

Dejusticia, Karisma and Privacy International have on-going concerns on the practices of surveillance by Colombian intelligence and law enforcement agencies.[2] National legislation governing surveillance is inadequate, unclear as to the powers, scope and capacity of surveillance activities of Colombia's national intelligence and law enforcement agencies and thus it falls short of the required standards to safeguard individuals from unlawful interference to the right to privacy.

The shortcomings in legislation is accompanied by abusive practices of state surveillance. The main security and law enforcement agencies in Colombia that monitor communications compete for resources and surveillance capabilities.[3] This, in turn, created a patchwork of unregulated, overlapped systems of surveillance violating the right to privacy.

## 2. Inadequacies of national legislation regulating domestic surveillance

Article 15 of the Colombian Constitution expressly safeguards the privacy of communications and states that "[C]orrespondence and other forms of private communication are inviolable. They may only be intercepted or searched with a warrant, in the cases and with the formalities that the law establishes".[4] Nevertheless, with the constitutional amendments made in 2002[5], Article 250 of the Constitution was modified and the Attorney General was conferred upon the authority to carry out searches, seizures and interceptions of communications without a prior judicial authorisation as enshrined in Article 15

1 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); see also Report by the UN High Commissioner for Human Rights, the right to privacy in the digital age, A/HRC/27/37, 30 June 2014. See also International Principles on the Application of Human Rights to Communications Surveillance, available at https://necessaryandproportionate.org.

2 Dejusticia is a Colombian human rights organization that produces expert knowledge on human rights, influences public opinion and the design of public policies, and supports and strengthens community and civil society organizations, bolstering a democratic state governed by the rule of law. Karisma Foundation is an organization of the civil society dedicated to supporting and disseminating the good use of the technology available in digital environments, in social processes and in Colombian Public Policies and of the region, from a perspective of protection and promotion of human rights. During our coming up we have kept a constant interest in the convergence of the TIC and (our) rights, as well as in the promotion and participation of the people in relation to these topics. Privacy International is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world.

3 Privacy International, 'How Colombia built a shadow state, a new Privacy International investigation reveals' 31 August 2015, available at https://www.privacyinternational.org/node/636. As for the information on companies' dealings to build a surveillance infrastructure in Colombia see; Privacy International, 'Demand/Supply: Exposing the Surveillance Industry in Colombia', September 2015, available at https://www.privacyinternational.org/node/638.

4 Article 15 (3) of the Colombian Constitution. See; Carlos Cortés Castillo, 'Communications Surveillance in Colombia', Celeste Kauffman (trs), Dejusticia Working Paper 3, p. 24, available at http://www.dejusticia.org/files/r2_actividades_recursos/fi_name_recurso.683.pdf. See also; Colombia's Constitution of 1991 with Amendments through 2005, available at https://www.constituteproject.org/constitution/Colombia_2005.pdf.

5 Constitutional Amendment No. 3 of 2002.

of the Constitution but with later judicial control by the presiding judge as to the legality of its actions within 36 hours of the event.[6] This timeframe later was reduced to 24 hours by Law 1453 of 2011.

Article 235 of the Criminal Procedure Code stipulates the conditions under which the Attorney General's Office can order the interception of communications. Under this provision the Attorney General can only lawfully order interception of communication being transmitted via the electromagnetic spectrum (telephone, radio or fibre optic cables) for the sole purposes of seeking evidence, search and locate the accused or convicted person.[7] The order must be in writing and is valid for six months with the possibility for an extension if in the opinion of the Attorney General the reasons that originated it persist. Interception without a warrant, save the Attorney General's authority to perform such an interception in accordance with the Criminal Procedure Code, is a crime under the Criminal Code.[8]

The presiding judge is charged with examining the compliance of the Attorney General's actions with the law. The Constitutional Court of Colombia has ruled that the presiding judge must verify "whether the measure that affects the exercise of a fundamental right (i) is adequate to contribute to reaching a constitutionally legitimate goal; (ii) is necessary in that it is the least restrictive measure available to achieve the goal; and (iii) if the goal pursued by the rights affectation compensates the sacrifices that this affectation causes for rights holders and society".[9]

Outside of the surveillance powers pertaining to criminal investigation proceedings, in 2013, Colombia adopted the Intelligence Law (Statutory Law No 1621 of 2013) in which intelligence and counterintelligence activities are regulated, including "monitoring the electromagnetic spectrum". Article 4 of the 2013 Intelligence Law establishes that information may only be obtained for a lawful purpose. Those purposes are broad, namely 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.[10]

Article 17 of the Intelligence Law is entitled "Monitoring the Electromagnetic Spectrum and Intercepting Private Communications" and states that:

"(1) Intelligence and counter-intelligence activities include monitoring the electromagnetic spectrum when this is duly established in operational orders or work assignments. Information gathered during such monitoring in the context of intelligence and counter-intelligence activities that does not serve to achieve

6 Article 250 (2) of Colombian Constitution. See; Castillo's Working Paper 3 for Dejusticia (n 3) p. 25. See also; 'Mapping Laws on Government Access to Citizens' Data: Colombia' Electronic Frontier Foundation (EFF) available at https://www.eff.org/pages/mapping-laws-government-access-citizens-data-colombia.

7 Article 235 of the Criminal Procedure Code. See; Castillo's Working Paper for Dejusticia (n 3) p. 25. For the English translation of this Article see also; 'Mapping Laws on Government Access to Citizens' Data: Colombia' Electronic Frontier Foundation (EFF) available at https://www.eff.org/pages/mapping-laws-government-access-citizens-data-colombia; Privacy International, 'Shadow State: Surveillance, Law and Order in Colombia', September 2015, p. 33, available at https://privacyinternational.org/node/635.

8 Article 269C of the Criminal Code. See; Castillo's Working Paper for Dejusticia (n 3) p. 26.

9 Constitutional Court, decision C-591 of 2005, Presiding Magistrate Clara Inés Vargas. For the unofficial translation of the decision see: Castillo's Working Paper for Dejusticia (n 3) p. 26.

10 Privacy International, 'Shadow State: Surveillance, Law and Order in Colombia', September 2015, p. 33, available at https://privacyinternational.org/node/635.

the aims established in this Law shall be destroyed and may not be stored in intelligence or counter-intelligence databases. Monitoring does not constitute interception of communications. (2) Intercepting private mobile or land-line telephone conversations, as well as private data communications shall be subject to the requirements established in Article 15 of the Constitution and the Criminal Procedure Code and may only be conducted in the context of legal proceedings."[11]

This provision distinguishes monitoring the electromagnetic spectrum for intelligence and counterintelligence purposes, such for the purpose of maintaining national security, from the interception of communications. According to this Article, 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.

The term 'interception' in the context of communications surveillance has been interpreted to encompass any act involving the collection, control, acquisition, or taking custody of communications in the course of their transmission or while in storage. Regardless of the changes in the technological mechanisms by which those activities are effected, the term 'interception' should continue to hold the same meaning. Therefore, any technology that enables States to collect, acquire or take custody of communications is by its nature intercepting the communication and thus interfering with the right to privacy.[12]

'Monitoring' the electromagnetic spectrum is not defined in the law (nor in the Colombian constitution.) This in itself raises serious concerns about the powers attributed to the intelligence services in Colombia.

Further, monitoring the electromagnetic spectrum could include filtering, analysing and monitoring e-mails, text messages and phone calls that 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. 'Monitoring' the electromagnetic spectrum, thus, intrinsically, involves an interference with the right to privacy.[13]

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

10 Privacy International, 'Shadow State: Surveillance, Law and Order in Colombia', September 2015, p. 33-34, available at https://privacyinternational.org/node/635.

11 Privacy International, 'Shadow State: Surveillance, Law and Order in Colombia', September 2015, p. 33-34, available at https://privacyinternational.org/node/635.

12 Privacy International, Electronic Frontier Foundation, Access, APC, ARTICLE 19, Human Rights Watch et al, OHCHR consultation in connection with General Assembly Resolution 68/167 "The right to privacy in the digital age," 1 April 2014, p. 10, available at: https://www.eff.org/files/2014/04/17/ngo_submission_final_31.03.14.pdf.

13 Even if one contends that the means of 'monitoring' the electromagnetic spectrum without violating the privacy of communications exist, they pertain to an extremely narrow set of activities such as heat detection tools, and direction-finding tools and antenna. All other forms of 'monitoring' the electromagnetic spectrum necessitate an interference with a communication of a type that means that it is not possible to conclude anything other than that the monitoring has resulted in the communication being intercepted.

interference with the privacy of communication.[14] The 2013 Intelligence Law only requires directors of the relevant security agencies to authorise the 'monitoring' of the electromagnetic spectrum. By not requiring the 'monitoring' 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.

In fact, this loophole in the law is particularly concerning given the kind of surveillance technologies employed by the Colombian security and law enforcement forces.

### 3. Data retention laws

Colombia has imposed the obligation of data retention upon telecommunications service providers for the purposes of criminal investigation and intelligence activities. For criminal investigation, Decree 1704 (2012) provides that subscriber's information[15] and geolocalization[16] data must be handed to the Prosecutor immediately upon request and must be kept for five years. For intelligence activities, Law 1621 (2013) establishes that intelligence agencies may ask for the subscriber's data, "communications history" and location information.[17] The same law provides that those requests may be issued 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.

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.[18] 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.[19] These data retention provisions lack several safeguards needed to avoid unlawful interference with the right of privacy.

First, both regimes are far from clear in the terms they use and are unnecessary and disproportionate, specially because of the retention term which extends

14 Castillo's Working Paper for Dejusticia (n 3) p. 39. Dejusticia and Freedom of Press Foundation contented their arguments in their intervention before the Constitutional Court concerning the constitutional revision of the Intelligence Law. See; Constitutional Court, decision C-540 of 2012, Presiding Magistrate Jorge Palacio Palacio.
15 Article 4 of Decree 1704 of 2012.
16 Article 5 of Decree 1704 of 2012.
17 Article 44 of Law 1621 of 2013.
18 See report of the UN Special rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, and report of the UN High Commissioner for Human Rights, Right to Privacy in the Digital Age, UN doc. A/HRC/27/37, 30 June 2014.
19 See Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014.

up to five years. Because of its untargeted and indiscriminate scope, the data retention regimes in Colombia fail to comply with the test of necessity and proportionality. Secondly, there is no judicial oversight for the request or access to this data which amongst other things, closes the opportunity of defense for the user subject of these measures. Lastly, the Decree 1704 is not a law passed by Congress but a Decree issued by the President, which is not subject to the process of deliberation expected for such a restriction on fundamental rights.

**4. Prohibition of encrypted communications**

In Colombia, since 1993, a series of laws regulating the use of the electomagnetic spectrum prohibit sending "encrypted messages or in unintelligible language" in "all communication devices using the electromagnetic spectrum." It is unclear whether this law would also cover encrypted communications on the internet. The Colombian Constitutional Court reviewed this law and found it compatable with the Constitution.[20]

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.[21] Dejusticia, Karisma and Privacy International believe that the blanket prohibition of encrypted communication currently provided in Colombian law is not necessary nor proportionate.

**5. Surveillance technologies capabilities outside the legal framework**

Colombia's most visible communications interception system is Esperanza.[22] The Office of the Attorney General manages and administers 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.[23]

Esperanza suffered from various security vulnerabilities and has other technical limitations since voicemail messages, Blackberry messages and communications over internet cannot be intercepted through the system.[24]

These limits were among the key factors that triggered the efforts to set up systems with greater surveillance technology capabilities, namely the Single Monitoring and Analysis Platform (PUMA) in 2007. Unlike Esperanza, PUMA is linked directly to the service providers' network infrastructure, which enables the system to intercept communications of all individuals that go through this network and directs to the law enforcement monitoring facility without further facilitation from the service provider. Israeli companies Verint, and

20 See Constitutional Court of Colombia. Sentence C–586 of 1995. M.P. Eduardo Cifuentes Muñoz.
21 See report of UN Special Rapporteur on freedom of expression, UN doc. A/HRC/29/32, 22 May 2015.
22 Privacy International, 'Shadow State: Surveillance, Law and Order in Colombia', September 2015, p. 7, available at https://privacyinternational.org/node/635.
23 Article 2 of Decree 1704 of 2012.
24 'Acta de Comisión 06 de agosto de 2010 Cámara', 24 August 2010, available at http://www.camara.gov.co/portal2011/gestor-documental/doc_download/153-acta-06-comision-primera. See also; Privacy International, 'Shadow State: Surveillance, Law and Order in Colombia', September 2015, p. 26, available at https://privacyinternational.org/node/635.

later NICE provided PUMA's operational technology.[25] The former company sells monitoring centres that enable the interception, monitoring and analysis of target and mass communications over virtually any network.[26] It was reported in 2013 that the technology that Verint designs does not just conduct surveillance on a targeted basis, but it can be tailored to intercept phone calls and e-mails of millions of everyday citizens and store them on vast databases for later analysis.[27] Colombian police contracted with the former company, NICE, in 2013 to expand PUMA's interception capacity. Like Verint, NICE was also reported to supply surveillance technology to government conducting widespread communications surveillance and political repression to tightly monitor the opponent activists, journalists, lawyers and politicians.[28]

Another branch of the Police, DIPOL, 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 bulks and without assistance from the service providers.[29]

Mass interception of communications using the technologies employed in PUMA or IRS has no legal basis in the Colombian legal framework on surveillance. As mentioned above, the Constitution allows the interception of communications only on the basis of a judicial warrant and in an exceptional case on the basis of the Attorney General's order given in accordance with the Criminal Procedure Code. Even the 2013 Intelligence Law does not cover the type of surveillance activities carried through PUMA and IRS.

Further, Colombian authorities have acquired tactical interception technologies, such as mobile monitoring equipment (colloquially known as 'IMSI catcher') and computer network exploitation technologies (hacking.)[30]

According to reports, offensive malware products of Italian company Hacking Team is currently being used or has been used by the Colombian police.[31] An investigation by the Citizen Lab at the University of Toronto ascertained 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.[32] According to Privacy International's investigation Hacking Team had an active contract with the Colombian police in 2014.[33] Despite this compelling evidence on the deployment of offensive

25 Privacy International, 'Shadow State: Surveillance, Law and Order in Colombia', September 2015, p. 29-31, available at https://privacyinternational.org/node/635. See also; Privacy International, 'Demand/Supply: Exposing the Surveillance Industry in Colombia', September 2015, available at https://www.privacyinternational.org/node/638.

26 'Verint to supply new Swiss spying system', swissinfo.ch, 15 January 2014, available at http://www.swissinfo.ch/eng/telecom-tapping_verint-to-supply-new-swiss-spying-system/37740006.

27 Ryan Gallager, 'Meet the American Company Helping Governments Spy on "Billions" of Communications', 30 January 2013, available at http://www.slate.com/blogs/future_tense/2013/01/30/verint_the_american_company_helping_governments_spy_on_billions_of_communications.html.

28 Privacy International, 'Demand/Supply: Exposing the Surveillance Industry in Colombia', September 2015, p. 31, available at https://www.privacyinternational.org/node/638.

29 Privacy International, 'Shadow State: Surveillance, Law and Order in Colombia', September 2015, p. 47-48, available at https://privacyinternational.org/node/635.

30 By tactical technologies we mean to interception technologies where the communications data and content are taken directly from the device or by signals emitted by the device, rather than from the network architecture from the service provider.

31 Privacy International, 'Shadow State: Surveillance, Law and Order in Colombia', September 2015, p. 15, available at https://privacyinternational.org/node/635.

32 'Mapping Hacking Team's "Untraceable Spyware"', The Citizen Law, 17 February 2014. https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

33 Privacy International, 'Shadow State: Surveillance, Law and Order in Colombia', September 2015, p. 43, available at https://privacyinternational.org/node/635.

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, which is an intermediary for the distribution of those products.[34] 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.[35]

Hacking Team's Remote Control System can be used to hijack computer and mobile devices, whilst remaining undetectable to users, as it is designed to bypass common antivirus programmes and encryption. It can covertly collect, modify and/or extract data from the targeted device, including remotely turning on and control the microphone and camera of the device. As such it is a particularly intrusive form of electronic surveillance given the personal information that can be obtained from such access.[36]

In Colombia, "hacking" is a criminal offense and therefore its use for intelligence gathering purposes is a form of extra legal surveillance illegal under Colombian law. Whether equipment interference such as that provided by Hacking Team technology is ever justifiably deployed is still an open question. The privacy intrusion involved and the risk to security of communications raise serious human rights concerns.

**6. Reports of unlawful interference with the right to privacy in the context of interception of private communications**

Colombia recent history is characterised by the unlawful surveillance for political purposes.

According to an investigation led by the Attorney General's office in 2002 around 2,500 phone lines had been unlawfully tapped 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.[37] In 2007, eleven police generals from DIPOL were dismissed after it was disclosed that the agency had tapped the phone lines of influential opposition politicians, journalists, lawyers, and activists.[38] Yet the most notorious of the interception scandal involved now-disbanded Colombian security agency, DAS, when it was revealed in September 2009 that DAS had conducted unlawful surveillance of an estimated 600 public figures including parliamentarians, journalists, human rights activities, lawyers and judges among others. [39]

34 "Policía indicó no tener vínculos comerciales con firma Hacking Team," [Police declares that there are no commercial links with Hacking Team] El Tiempo, 8 July 2015, available at http://www.eltiempo.com/politica/justicia/policia-indico-no-tener-vinculos-comerciales-con-firma-hacking-team/16063640.

35 Digital Rights Latin America & The Caribbean, 'In Colombia, PUMA is not what it seems', 24 August 2015, available at http://www.digitalrightslac.net/en/en-colombia-el-puma-no-es-como-lo-pintan/

36 For a briefing on the activities of Hacking Team, see Privacy International, Briefing for the Italian government on Hacking Team's surveillance exports, April 2015, available at: https://www.privacyinternational.org/?q=node/561

37 'Informe Sobre Derechos Humanos: Colombia', US Department of State, 4 March 2002, available at http://www.acnur.org/t3/fileadmin/scripts/doc.php?file=t3/uploads/media/COI_53

38 'El DAS-gate y las 'chuzadas', vuelve y juega', El Espectador, 21 February 2009, Colombia', available at http://www.elespectador.com/noticias/judicial/articulo120226-el-das-gate-y-chuzadas-vuelve-y-juega.

39 'Más de 600 personas habrían sido 'chuzadas' ilegalmente por el DAS, según investigadores', Caracol Radio, 14 April 2009, available at http://caracol.com.co/radio/2009/04/17/judicial/1239945360_796294.html.

Privacy International spoke to confirmed former targets of DAS surveillance and persons who strongly believe that they are still targeted by state electronic surveillance.[40]

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. A member of CCAJAR, Reinaldo Villalba, said to Privacy International that they were certain that they had been spied on from the beginning. What they did not concretely know was the extent of spying and in 2009 they were truly surprised to see the vast amounts of files seized from the DAS, revealing the detailed information about the CCAJAR, each meeting they had, everyone they met abroad and even information about their families, including their children. Privacy International also interviewed Father Alberto Franco of the Inter-ecclesiastical Commission for Justice and Peace (CIJP). CIJP works in the restive Urabá region to represent peasant communities and expose the links between neo-paramilitary groups, private companies and the Colombian military. Father Alberto confirmed to Privacy International that they always assumed that they were under surveillance and they were occasionally tipped off of the ongoing interception of CIJP's communications. He shared his scepticism as to PUMA's value as a law enforcement tool and as to whether the intelligence agencies have truly changed their abusive practices, despite the disbanding of DAS.

Despite some reforms, reports of surveillance of independent journalists continue. A new scandal has recently emerged related to journalists investigating corruption by the police having had their communications intercepted.[41]

## 7. Absence of effective Independent oversight on the interferences by intelligence agencies with the right to privacy

There are significant shortcomings of the oversight regime of surveillance in Colombia. In any democratic state, the oversight of lawful security acts should be a combination of[42]: executive control; parliamentary oversight; judicial review and monitoring by expert bodies

Neither of these mechanisms works satisfactorily in Colombia, hence the grave violations of human rights by the security services.[43] Of particular concerns is the lack of supervision by data protection authorities and the failure to establish a parliamentary oversight.

40 Privacy International, 'Shadow State: Surveillance, Law and Order in Colombia', September 2015, p.53, available at https://privacyinternational.org/node/635.

41 See El Espectador (2015). "No hay duda de los seguimientos: Vicky Dávila": http://www.elespectador.com/noticias/judicial/no-hay-duda-de-los-seguimientos-vicky-davila-articulo-603572; El Espectador (2015). "El informante de las chuzadas": http://www.elespectador.com/noticias/investigacion/el-informante-de-chuzadas-articulo-604187?utm_source=Lyris&utm_medium=Email&utm_campaign=NewsletterEE&cmp=08%2F12%2F15

42 Surveillance by Intelligence Services: Fundamental Rights and Remedies in the EU. Mapping Member States´Legal Frameworks. European Union Agency for Fundamental Rights. Pg. 29. See: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf

43 El Tiempo. (2013). "Policía podrá interceptar Facebook, Twitter y Skype en Colombia", recovered on November 37, 2015 from: http://www.eltiempo.com/archivo/documento/CMS-12890198; Semana Magazine (2014). "¿Alguien espió a los negociadores de La Habana?" recovered on November 27, 2015 from: http://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3. El Espectador (2015) "Inteligencia en Colombia: El reino de las sombras," recovered on December 06, 2015 from: http://www.elespectador.com/noticias/investigacion/inteligencia-colombia-el-reino-de-sombras-articulo-582523 El Espectador (2015). "No hay duda de los seguimientos: Vicky Dávila". Recovered on December 6, 2015 http://www.elespectador.com/noticias/judicial/no-hay-duda-de-los-seguimientos-vicky-davila-articulo-603572

On one hand, data protection (habeas data) statutory law does not apply to databases containing personal data that "have as a purpose and are related to intelligence or counterintelligence activities".[44] Thus, even though the principles of data protection law apply, there is no independent regulator to control and protect personal data held by or for intelligence purposes. As a result, existing agencies with intelligence functions (at least 7 agencies in Colombia[45]) are not accountable to the data protection regulator.

This lack of accountability is exacerbated by the ineffectiveness of the independent commission to oversight intelligences activities. Intelligence Law 1621 of 2013 provides for the creation of the "Legal Monitoring Commission of Intelligence and Counterintelligence Activities" as the authority in charge of the oversight and political control over the surveillance practices carried out by state security and intelligence agencies.

As dictated by Article 20 of the law, the Commission has the duty to:
"(...) Perform control functions and political follow-up, verifying the efficiency of resources, respect for constitutional guarantees and compliance with the principles, limits and objectives set out in statutory law regulating the activities of intelligence and counterintelligence".

However, although the Intelligence Law came into effect on 17 April 2013, the Committee, that represents the only independent system of accountability to benefit citizens, has not yet been constituted, due to alleged security procedures that mask a lack of political will.

**8. Proposed questions for the list of issues**

Based on the above observations, Dejusticia, Karisma and Privacy International propose the following questions for the List of Issues:

Article 17:

- What measures is Colombia taking to ensure that its state security and intelligence agencies respect the right to privacy?

- In particular, how does Colombia ensure that all interception activities, including monitoring of the electromagnetic spectrum, are only carried out in ways that comply with the principles of legality, proportionality and necessity?

- What measures is Colombia planning to strengthen effective oversight over the surveillance practices of its state security and intelligence agencies?

- What type of surveillance technologies are employed by Colombian law enforcement and intelligence agencies and how their acquisition and use is regulated and monitored?

44 See article 2 of Statutory Law 1581 of 2012.
45 See article 1 of Decree 857 of 2014 that implements Law of Intelligence and Counterintelligence.