Submission in advance of the consideration of the periodic report of Colombia, Human Rights Committee, 118th Session, 17 October – 04 November 2016

September 2016

1. Introduction

Dejusticia, Karisma and Privacy International ("the organisations") [1] note the written replies by the government of Colombia to the Committee's list of issues on Colombia's laws, policies and practices related to interception of personal communications and protection of personal data.[2]

The organisations remain concerned over the practices of surveillance by Colombian intelligence and law enforcement agencies. National legislation governing surveillance is inadequate, unclear as to the powers, scope and capacity of state surveillance activities and thus it falls short of the required human rights standards to safeguard individuals from unlawful interference to the right to privacy.

In this submission, the organisations provide the Committee with their observations to the written replies of the Colombian government and with additional, up to date information to that contained in the briefing submitted to the Committee in advance of the adoption of the list of issues in 2015 ("2015 Submission".)[3] Unless otherwise stated, the concerns expressed

1 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.

2 UN doc. CCPR/C/COL/Q/7/Add.1, 18 August 2016.

3 Available at: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fICO%2fCOL%2f22710&Lang=en

in the 2015 Submission are on going and if they are not repeated here it is solely for brevity sake.

2. General observations on the Colombian written replies to the list of issues

The organisations note that the Colombian government did not respond to the Committee's request for "updated information on the results of investigations into illegal intelligence activities allegedly conducted by officers of the former Administrative Security Department against human rights defenders, journalists, justice officials, politicians and international and regional organizations." Nor did it provide information on "whether there have been any complaints or reports of illegal surveillance activities by military, police or civilian bodies in the reporting period".[4]

This is a significant omission given past and present reports of unlawful surveillance in Colombia (see further the section below.)

As for the other issues identified by the Committee, the organisations note that the replies provided by the Colombian government focus only on the law, ignoring implementation obstacles and other difficulties, for example citing Articles from Act No. 1621 of 2013 and ruling by the Constitutional Court (C-540 of 2012), without providing additional information about their effective implementation.

3. Inadequacies of national legislation regulating domestic surveillance

The organisations reiterate their concerns about the scope of surveillance under the Intelligence Law (Law No 1621 of 2013) in which intelligence and counterintelligence activities are regulated, including "monitoring the electromagnetic spectrum".

The written replies of the Colombian government on this point (paragraphs 95-96) merely describe the scope of the law and the judgment of the Constitutional Court, without addressing the scope of monitoring, or providing any definition of what monitoring of the electromagnetic spectrum consists of.

To summarise the concerns of the organisations:

- The purposes under which information can be obtained (Article 4) are over-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;[5]
- 'Monitoring' the electromagnetic spectrum is not defined in the law (nor in the Colombian constitution). Without any definition provided, 'monitoring' the electromagnetic spectrum could include filtering, analysing and monitoring e-mails,

[4] UN Doc. CCPR/C/COL/Q/7, 26 April 2016.

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

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;[6]

- In fact the government accepts (in paragraph 95) that this 'monitoring' may include information that is not needed for the purposes of intelligence, but it fails to recognise that as a result, such 'monitoring' constitutes an interference with the individual's privacy that should be subject to the same strict test of legality, necessity and proportionality;
- The 2013 Intelligence Law only requires directors of the relevant security agencies to authorise the 'monitoring' of the electromagnetic spectrum.

New Police Code

In a significant development since the 2015 Submission, a new Police Code Law was enacted and will enter into force on 29 January 2017. This new Code gives far-reaching powers to the police without providing appropriate controls over police discretion. It includes several provisions, which would *prima facie* violate a range of human rights, including, for example, the right to peaceful assembly by allowing only protests with a "legitimate purpose".

The organisations focus here on those provisions that will have particularly negative implications with regards to the right to privacy.

Firstly, Article 32[7] contains a definition of privacy, which is unduly narrow. 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. 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) placed in public places, including bars, restaurants, etc.

[6] 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.

[7] "Artículo 32. Definición de Privacidad. Para efectos de este Código, se entiende por privacidad de las personas el derecho de ellas a satisfacer sus necesidades y desarrollar sus actividades en un ámbito que le sea exclusivo y por lo tanto considerado como privado.
No se consideran lugares privados:
1. Bienes muebles o inmuebles que se encuentran en el espacio público, en lugar privado abierto al público o utilizados para fines sociales, comerciales e industriales.
2. Los sitios públicos o abiertos al público, incluidas las barras, mostradores, áreas dispuestas para: almacenamiento, preparación, fabricación de bienes comercializados o utilizados en el lugar, así como también las áreas dispuestas para el manejo de los equipos musicales o Disc jockey, y estacionamientos a servicio del public".

Conversely, Article 139[8] defines public space in a very broad way, including notably "the electromagnetic spectrum".

The combined result of these definitions is of significant concern to the protection of privacy, particularly when considering that Article 237[9] states that: "(i) information, images and data of any nature captured and/or stored by video systems or technological means located in public place will be considered public and freely accessible; and (ii) video systems and technological means, of private or public property, located in the public space, common areas, places open to the public or that being private transcend to the public, will be permanently or temporarily linked to the network that for this purpose will be provided by the National Police." Thus, these provisions could even mean that communications travelling through the electromagnetic spectrum would be excluded from privacy protection.

Lastly, the new Police Code does not seem to take into consideration the complex technological changes which affect modern communication technologies. Hence, it is unclear

---

[8] "Artículo 139. Definición del Espacio Público. Es el conjunto de muebles e inmuebles públicos, bienes de uso público, bienes fiscales, áreas protegidas y de especial importancia ecológica y los elementos arquitectónicos y naturales de los inmuebles privados, destinados por su naturaleza, usos o afectación, a la satisfacción de necesidades colectivas que trascienden los límites de los intereses individuales de todas las personas en el territorio nacional.
Constituyen espacio público: el subsuelo, el espectro electromagnético, las áreas requeridas para la circulación peatonal, en bicicleta y vehicular; la recreación pública, activa o pasiva; las franjas de retiro de las edificaciones sobre las vías y aislamientos de las edificaciones, fuentes de agua, humedales, rondas de los cuerpos de agua, parques, plazas, zonas verdes y similares; las instalaciones o redes de conducción de los servicios públicos básicos; las instalaciones y los elementos constitutivos del amoblamiento urbano en todas sus expresiones; las obras de interés público y los elementos históricos, culturales, religiosos, recreativos, paisajísticos y artísticos; los terrenos necesarios para la preservación y conservación de las playas marinas y fluviales; los terrenos necesarios de bajamar, así como sus elementos vegetativos, arenas, corales y bosques nativos, legalmente protegidos; la zona de seguridad y protección de la vía férrea; las estructuras de transporte masivo y, en general, todas las zonas existentes y debidamente afectadas por el interés colectivo manifiesto y conveniente y que constituyen, por consiguiente, zonas para el uso o el disfrute colectivo.
PARÁGRAFO 1o. Para efectos de este Código se entiende por bienes fiscales, además de los enunciados por el artículo 674 del Código Civil, los de propiedad de entidades de derecho público, cuyo uso generalmente no pertenece a todos los habitantes y sirven como medios necesarios para la prestación de las funciones y los servicios públicos, tales como los edificios, granjas experimentales, lotes de terreno destinados a obras de infraestructura dirigidas a la instalación o dotación de servicios públicos y los baldíos destinados a la explotación económica.
PARÁGRAFO 2o. Para efectos de este Código se entiende por bienes de uso público los que permanentemente están al uso, goce, disfrute de todos los habitantes de un territorio, como por ejemplo los parques, caminos o vías públicas y las aguas que corren".

[9] "Artículo 237. Integración de Sistemas de Vigilancia. La información, imágenes, y datos de cualquier índole captados y/o almacenados por los sistemas de video o los medios tecnológicos que estén ubicados en el espacio público, o en lugares abiertos al público, serán considerados como públicos y de libre acceso, salvo que se trate de información amparada por reserva legal.
Los sistemas de video y medios tecnológicos, o los que hagan sus veces, de propiedad privada o pública, a excepción de los destinados para la Defensa y Seguridad Nacional, que se encuentren instalados en espacio público, áreas comunes, lugares abiertos al público o que siendo privados trasciendan a lo público, se enlazará de manera permanente o temporal a la red que para tal efecto disponga la Policía Nacional, de acuerdo con la reglamentación que para tal efecto expida el Gobierno nacional.
PARÁGRAFO. En tratándose de sistemas instalados en áreas comunes, lugares abiertos al público o que siendo privados trasciendan a lo público, se requerirá para el enlace a que hace referencia el presente artículo, la autorización previa por parte de quien tenga la legitimidad para otorgarla".

how the privacy of digital communications and of online spaces is protected given the definitions of privacy and public space included in the Code.

4. Absence of effective independent oversight of the intelligence agencies and the police with respect to unlawful surveillance

Regarding the efficacy of the systems used to monitor and oversee current intelligence activities raised in the Committee's list of issues, the government's reply only refers to the role of the Inspectors. These are internal oversight mechanisms within the relevant state security branch - which cannot be considered an independent mechanism and whose reports to the relevant ministers are not public.

On the role of the Inspectors the government claims that it has allowed the development of more transparent intelligence and counterintelligence activities (paragraph 92.) However, there is no concrete information on how this has been achieved, or how the government is monitoring and measuring such improvement (for instance, how many confidential annual reports have already been presented to the Ministry of National Defense Have they found that unlawful surveillance conducts are taking place?)

Regrettably, the written replies provide no information on the activities of the Legal Monitoring Commission of Intelligence and Counterintelligence Activities (see the 2015 Submission for additional information.)

According to the information available to the organisations, the Commission held a meeting with the intelligence agencies on 2 March 2016 to agree on the security required to conduct their oversight. As such security protocols (including in terms of receiving and holding reports from the agencies) have not yet been finalised, the Commission has been unable to carry out all the activities under its mandate.

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. We regret that the government failed to provide any information on the questions posed by the Committee on the investigations into DAS and on complaints of unlawful surveillance.

The 2015 Submission already contained information on some of these cases. That this is an on-going, significant concern is demonstrated by yet another report of unlawful surveillance which emerged in early 2016. Vicky Davila, a journalist investigating allegations of police cadets' involvement in a prostitution ring, was reportedly put under surveillance by the Colombian police.[10]

This lack of effective oversight and accountability goes hand in hand with lack of transparency and public scrutiny of the activities of the intelligence services. In this respect, it

10 See The Intercept – Police in Colombia accused of spying on journalist investigating prostitution ring, 17 January 2016 (https://theintercept.com/2016/01/17/police-in-colombia-accused-of-spying-on-journalist-investigating-prostitution-ring/)

is significant that the government written replies mention Decree 857 (2014) (see paragraph 93). The Decree provides for a total ban on disclosure of intelligence files, exceeding the appropriate limits of secrecy and enabling the intelligence agencies to maintain all their activities away from public scrutiny. Dejusticia has initiated legal proceedings against this Decree and has requested the Council of State to temporarily suspend its application till it reaches a final decision on the merits[11].

5. Data retention laws

Colombia has imposed the obligation of data retention upon telecommunications service providers for the purposes of criminal investigation and intelligence activities. Details of the applicable laws are contained in the 2015 Submission.

For criminal investigation, Decree 1704 (2012) provides that subscriber's information[12] and geolocalization[13] data must be kept for five years. Since the 2015 Submission, the Council of State reviewed article 4 of the Decree, related to subscriber's information. In its 18 February 2016 ruling, the Council of State 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. Therefore, according to the Council of State, the Colombian legislation clearly states that data retention should be done prior judicial order[14].

As noted in the 2015 Submission, the collection, retention and use of metadata/communication is an interference with the right to privacy.[15] The blanket, indiscriminate data retention provisions in Colombian law lack several safeguards needed to avoid unlawful interference with the right of privacy.

While the recent Council of State's decision addressed some of these concerns, it is yet to be seen how the decision will be applied in practice and in any case this decision only pertains to the data retention regime for criminal investigation purposes and not for intelligence activities, which remain regulated under Law 1621 (2013).

Further, the Ministry of ICT has implemented a strategy to counter cellphone theft which involves the creation of a database that associates IMEI numbers with SIM cards and personal information such as ID number, name and address.[16] The carriers must check the

---

[11] Lawsuit available at: http://www.dejusticia.org/#!/actividad/3157

12 Article 4 of Decree 1704 of 2012.

13 Article 5 of Decree 1704 of 2012.

[14] Ruling available at: http://190.24.134.67/documentos/boletines/PDF/11001-03-24-000-2013-00018-00.pdf

15 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.

[16] Resolución CRC 3128 de 2011, available at: https://www.crcom.gov.co/recursos_user/Normatividad/Normas_Actualizadas/Res_3128_11_Act_4986_16.pdf

user ID against any of several sources such as the National Archive of Identification, Civil Registry or financial databases.

Administrative, police and judicial authorities can access this information but there is not any provision on the reasons these authorities must provide to access the database or any oversight to this access which lays the ground for abuses of such a system and increases the risk of privacy violations.

6. Conclusions

Based on the above observations and those contained in the 2015 Submission, Dejusticia, Karisma and Privacy International propose the following recommendations to the Colombian government:

- Review the laws 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;
- Ensure that all interception activities including the monitoring of the electromagnetic spectrum, are only carried out in ways that comply with the principles of legality, necessity and proportionality;
- 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 fulfill 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 and how their acquisition and use is regulated and monitored.