Response to call for inputs on human rights challenges relating to the right to privacy in the digital age in Colombia

April 2018

The Center for Law, Justice and Society -Dejusticia, as part of the Privacy Network lead by Privacy International- PI and the International Network of Civil Liberties Organizations-INCLO shares and endorses both documents of recommendations submitted or to be submitted separately by PI and INCLO to the High Commissioner. In addition, we are enclosing the following diagnosis of the Colombian situation vis-à-vis privacy that answers the High Commissioner´s questionnaire and gives rise to recommendations of standards (highlighted in the beginning of each answer) that together with our endorsement to the principles, standards and best practices submitted by PI and INCLO to the High Commissioner should be considered for a new General Comment on the right to privacy under Article 17- ICCPR.

1. **Recent developments in national or regional legislation, case law, and practice concerning the right to privacy in the digital age.**

There is still a chasm between national legislation, technology and reality that requires the modernization of existing privacy and data protection legislation to ensure the effectiveness of the right to privacy in public and private places, on line and off line.

In 2012 the Colombian Congress enacted Law 1581 of 2012 (regulated by Decree 1377 of 2013) as the general legal framework applicable to the management of personal data. Basically, it is intended to protect individuals' right *to know, update and rectify information gathered about them in databases or files*. In Colombia this right is known as *habeas data* and is closely related to the right to privacy. However, a growing concern is the applicability of this legal framework to deal with emerging issues of the digital age. Law 1581 of 2012 is mainly focused on the protection and regulation of structured data residing in relational databases. This raises the question of its effectiveness to tackle with the new challenges of digital environments, where huge sets of unstructured data and big data tools prevail. Unfortunately, there has not been enough debate on this matter so far.

In recent years, legal developments on the right to privacy in the digital age have been limited. However, there are some factors that are worth noting. On 2017 a new Police Code Law entered into force (Law 1801 of 2016). Article 32 of this Code 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" and expressly excluding from the consideration of private places any asset or property in public spaces, private places open to public or used for social, commercial or

industrial purposes, 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 like portable computers or cell phones) 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. Conversely, Article 139 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 could be interpreted to mean that communications travelling through the electromagnetic spectrum would be excluded from privacy protection. Actually, this shortcoming of the law was raised by the Human Rights Committee in paragraph 32 of the Concluding observations on the seventh periodic report of Colombia, where it 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)". Lastly, the new Police Code does not seem to take into consideration the complex technological changes that 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.

On the other hand, there are relevant soft law mechanisms within the Colombian framework regarding privacy in the digital age. Firstly, the *online government strategy* (CONPES 3854 of 2016) included the protection of human rights as one of its pillars. Nevertheless, it still contains a call to increase the capacities of intelligence and law enforcement agencies without a corresponding call to increase controls and transparency duties. The effects of the new strategy are yet to be assessed as it will be implemented over the next years. On the other hand, the Telecommunications Sub-Directorate of the National Planning Department of Colombia will be soon issuing a new public policy (CONPES) on Data Exploitation, as part of a higher policy framework of Big Data, artificial intelligence and Smart Cities that will presumably generate tensions with the rights to privacy and data protection (habeas data) of Colombians[1].

National case law is starting to protect digital privacy but indicates lack of technical knowledge and of a modern legal and regulatory framework for the accountability of internet intermediaries/ algorithm and data set creators.

[1] Two bills were filed last year aiming to protect the right to privacy in social networks. On July 20, 2017 a Congresswoman filed a bill that seeks to prohibit the creation of false or anonymous accounts on social networks used to insult, slander or violate the privacy of another person, or to spread false news that may generate confusion or panic in the population. Similarly, on July 28 a Congressman filed a bill intended to formulate public policy guidelines for the prevention of crimes carried out against children and adolescents through computer or electronic means.

In recent years, court rulings have addressed issues such as the **processing of personal data in social networks**. For example, ruling T-260 of 2012 decided the case of a father who created a Facebook account for his 4 year-old daughter. In this case the Court declared that the principle of freedom in the handling of personal information had been breached. Therefore, given that the child was not aware of the creation of the account on Facebook, the Court considered that her right to data protection had been violated, and ordered her father to delete the account. Thereafter, the Court reviewed the case of a creditor who decided to publicly denounce her defaulting debtor on Facebook. In ruling T-050 of 2016 the Court decided that the message published on Facebook violated the right to privacy of the defaulting debtor, not only because it exposed part of her personal data, but also because the debtor did not give authorization for such information to be revealed. On this occasion, the Court concluded that "internet must be subjected to the same rules as the non-virtual world"; therefore, Facebook posts must consider the right to privacy and the right to dignity. By the time the Court decided the case, the post had already been deleted, so the Court deemed a public rectification on Facebook as a reasonable and just mechanism to repair the violation of the right to privacy. A similar decision was held in ruling T-145 of 2016, in which the Court dealt with a case of a woman who published a presumably false accusation of robbery against another woman on her Facebook personal profile.

The Court's position has not been as clear in regard to **personal data disseminated by mass media and the responsibilities of intermediaries**. In the rulings that have been recently adopted about personal data published on media, the Court has addressed the problem as a conflict between the right to freedom of expression and access to information, on the one hand, and the right to honor and a good name of the person involved, on the other hand. Therefore, it has not mentioned the right to habeas data, nor has it declared that the right to habeas data is not applicable to the case, since the discussion focuses on journalistic information disseminated by media in the exercise of freedom of expression, and not on information gathered in databases (T-040 of 2013). In ruling T-277 of 2015 the Court assessed a case in which a woman alleged the violation of her right to privacy by a national newspaper (El Tiempo) and Google as searching engine. The newspaper had reported her participation in acts constituting a crime and her name as a potential criminal would come up through the search engine Google, even though she had never been convicted for that act. In this case, the Court protected the right to privacy and ruled that El Tiempo had the obligation to correct the information. It is worth mentioning that both of these rulings –T-040/2013 and T-277/2015– estimated that internet intermediaries are not responsible for the contents published by mass media.

Lastly, the Colombian Constitutional Court **has decided cases related to the elimination, de-indexing and correction of information on digital platforms** in order to protect the right to privacy. For example, in ruling T-063A of 2017 the Court claimed that Google Inc. and Google Colombia Ltd., as the owners of the internet portal called "Blogger.com", had to permanently delete a blog post hosted on the Blogger platform, since its content violated the right to privacy. The Court found that the blog's owner was accusing the petitioner of committing fraud to his clients and, thus, violated his fundamental rights. This decision was

both criticized and supported by civil society and has built interest on the conflict between freedom of expression and the right to privacy.

2. **Surveillance and communications interception:**
    a. **Government surveillance, including, for example, communications interception and bulk data collection and processing, targeted intrusions in ICT systems and issues relating to cross-border surveillance and access to personal data.**

Lack of explicit provisions in the Colombian legal framework that prohibit measures of bulk surveillance and lack of control for targeted surveillance as well as for national and shared intelligence show that there is interference with the right to privacy, not subject to the principles of legality, necessity and proportionality:

Different Colombian agencies have been involved in Communications interception scandals (sometimes called by the Colombian Spanish term *chuzadas*). In 2007, there were revelations that the DIPOL had tapped influential opposition politicians', journalists', lawyers' and activists' phones. In February 2009, as revealed by Semana, interception scandals involved the Administrative Department of Security ('DAS') that estimated wiretapping of 600 public figures including parliamentarians, journalists, human rights activists and lawyers, and judges, using this information to compile psychological profiles of targets and conduct physical surveillance of subjects and their families, including children. 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. Maria del Pilar Hurtado, who headed DAS in 2008, is the highest-ranking official to have been convicted for illegal surveillance. In 2011 a new agency, the National Intelligence Directorate ('DNI'), was established to head the intelligence and counterintelligence sector.

In 2014, the Colombian weekly magazine Semana alleged 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. Lastly, in 2015, La FM editor-in-chief Vicky Davila had filed a complaint with evidence that the Police had been spying on her, and other journalists investigating irregularities within the National Police. On that same year, there was evidence in the news that the Police could have been involved in acquiring hacking devices from Hacking Team.

Finally, it is important to mention that intelligence sharing agreements are considered secret and cannot be monitored neither by civil society nor by the Legal Monitoring Commision that has been unable to carry out this and other oversight activities due to alleged security and contracting procedures that mask a lack of political will.

b. **Role of business enterprises in contributing to, or facilitating government surveillance activities, including:**
    1. **Sale of surveillance technology by business enterprises and ensuing responsibilities;**
    2. **Business enterprises' internal safeguards and remedial mechanisms.**

Various foreign and national business enterprises are involved in supplying services and devices that affect privacy by design for which there is no accountability from the buyer/acquirer nor from the seller/supplier:

For the input to this question please refer to the State of Privacy by Privacy International with collaboration from Dejusticia and Karisma in the the following web page: https://privacyinternational.org/state-privacy/58/state-privacy-colombia

3. **Encryption and anonymity as enablers for the enjoyment of human rights, including the right to freedom of expression and of opinion; challenges raised by encryption and anonymity and ways to address these challenges.**

The broad prohibition of encrypted communication in Colombia is not only unnecessary and not proportionate but unenforceable, naïve and out of date.

In Colombia, there is little discussion but old laws still prohibit encryption. **Law 104 of 1993** prohibited sending "encrypted messages or in unintelligible language" in "all communication devices using the electromagnetic spectrum". In ruling **C-586 of 1995** the Colombian Constitutional Court reviewed this law and found it compatible with the Constitution. Four years later the text of this statute was revived in article 103 of **Law 418 of 1997**, which regulates the use of the electromagnetic spectrum. Thereafter, this disposition has been continuously renewed, with **Law 1738 de 2014** extending its validity until 2018. It is unclear whether these laws would also cover encrypted communications on the internet. Besides, this total ban has an exception. **Law 1621 of 2013**, by means of which intelligence activities are regulated, provides that telecommunications services providers must offer encrypted voice call service to high government and intelligence officials. 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.

Finally, last year, the Colombian General Attorney (Fiscal General de la Nación) proposed that companies providing text messaging and voice services such as WhatsApp should not be allowed to operate through operators in Colombia if they do not sign an agreement to decrypt those forms of communication, when, prior judicial authorization, it is established that they are being used by criminal organizations.

4. **National legislative and regulatory frameworks concerning the collection, processing, retention or use of personal data by Governments and other actors, in particular business enterprises, related human rights protection gaps and ways to bridge those gaps.**

Data protection laws are not up to date with technology and not applicable to intelligence services or journalism leaving privacy unprotected in these realms as much as in the consideration according to which monitoring of the electromagnetic spectrum is not subject to the principles of legality, necessity and proportionality.

On the one hand, article 15 of the 1991 Constitution provides that everyone has the right to personal and family privacy as well as to data protection, including interception pursuant to a court order. On the other hand, article 250 of the Constitution confers the Office of the Attorney General the authority to carry out searches, seizures and interceptions of communications without a prior judicial authorisation. Accordingly, 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.

But outside of the surveillance powers pertaining to criminal investigation proceedings and those of the Attorney General, Colombia has also adopted an Intelligence and Counterintelligence Law- Statutory Law 1621 of 2013). Article 17 of the Intelligence Law is entitled, 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 the electromagnetic spectrum' 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. Even more, taking into account that 'monitoring' is not defined anywhere in the Colombian law and in practice includes analysing and monitoring e-mails, text messages and phone calls that are carried upon the electromagnetic spectrum. Therefore, the Intelligence Law fails to provide protection against interference with private communications in this event.

Moreover, article 44 of the Intelligence Law establishes that intelligence agencies may ask telecommunications service providers 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. Likewise, for criminal investigation Decree 1704 of 2012 provides that subscriber's information and geolocalization data obtained by telecommunications service providers must be handed to the Prosecutor immediately upon request and must be kept for five years.

Besides, article 163 of the new Police Code (Law 1801 of 2016) states that the police can enter without a court order a private or public establishment, under conditions including certain emergencies. In addition, Law 1266 of 2008 protects financial personal data in Colombia. Finally, in 2012 the Colombian Congress enacted its own general data protection legislation: Law 1581 of 2012. This law was reviewed by the Constitutional Court in Decision C-748 of 2011, and regulated by Decree 1377 of 2013. Nevertheless, this law explicitly provides that it does not apply to databases containing personal data that "have as a purpose and are related to intelligence or counterintelligence activities" or to databases of journalists. (although the Court made clear that the data protection law principles keep applying).

5. Growing reliance on data-driven technology and biometric data.

There is generalized and indiscriminate collection and retention of biometric data without passing the test of necessity, legitimacy and proportionality required for such conduct to be considered a lawfully interference of the right to privacy:

- **National Registry**

The National Civil Registry that includes footprints on birth and full ten-finger-print together with basic information like name and date of birth is the most important proof of the information it contains and will be demanded by any state agency accordingly. Even though the registry is public, the legislation imposes restrictions on issuing copies or certificates of it to protect privacy rights. However, upon agreement with the National Civil Registry, public and private parties can consult the National Identification Archive.

- **Identity card**

Since 1970, every newborn in Colombia has been assigned a unique identifier number. The age of majority in Colombia 18 years which means that the person has full legal capacity and can vote in public elections. The medium to validate this circumstance is the identity card ("cédula de ciudadanía"), which includes a photo and a fingerprint of the cardholder.

- **Biometric facial recognition technology**

In October 2016, it was announced that Medellin city had purchased biometric facial recognition technology from the Japanese company NEC. The arena operator has reportedly created a blacklist of disruptive football fans, which the NEC system will use to compare against the faces captured by surveillance cameras at the entrances. More generally, during 2017 the private entity that is responsible for organizing, managing and regulating the Colombian Professional Soccer Championships (DIMAYOR) pushed forward its strategy for security in the stadiums of the country. This strategy includes introducing

photo ID cards for fans, as well as the installation of facial recognition cameras and gates with biometric control and fingerprint recognition devices.

- **Biometric immigration system**

Migration Colombia has recently implemented a new-Colombian-developed immigration system for Colombian citizens, called Biomig. The mechanism, which will initially work in El Dorado International Airport in Bogotá, is based on the recognition of the traveler's iris and allows citizens to skip queues during immigration. Any Colombian citizen over 12 years old can voluntarily and for free enroll in this new system during emigration. To date there are more than 55 thousand Colombian citizens who are already registered.

6. Undue interferences with the right to privacy in the digital age that may have particular effects for women, as well as children and persons in vulnerable situations or marginalized groups, and approaches to protect those individuals.

The existence of sensitive databases under the protection of the State represent serious risks of criminalization and affectation of various rights, including the rights to privacy and to life of certain groups.

- **Personal data of victims of the armed conflict**

In 2014 it was revealed that a network of individuals unlawfully accessed the database managed by the Unit for Comprehensive Care and Reparation for Victims[2] reportedly using authorization 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.

- **Data of formal and informal social organizations and movements**

Point 2.2.1 of the 2016 Peace Agreement provides for the creation of a register of all formal and informal social organizations 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[3]. 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 organizations. We are concerned by the centralization of this data and

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

[3] 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

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 of data, which is considered sensitive personal data in Colombia[4], may lead to discrimination or even endanger the lives or personal safety of the individuals concerned. 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.

- **Personal data of voters who participated in the two interparty consultations that took place on March 11th, 2018**

The Colombian Electoral Observation Mission (MOE), together with the Inspector General and the National Electoral Council have requested the National Registry to eliminate the forms where the political inclination of the voters was collected in past elections[5].

7. Procedural and institutional safeguards, oversight mechanisms and remedies available to individuals exposed to domestic or extraterritorial surveillance, the interception of digital communications or other forms of processing of personal data by governments, business enterprises or private organizations.

Lack of oversight real –as opposed to nominal- mechanisms and remedies for extraterritorial and domestic surveillance, lack of capacities to regulate and control data protection and of transparency and accountability on data driven processes.

Data protection statutory law (Law 1581 of 2012) establishes the Office of the Superintendent of Industry and Commerce (Superintendencia de Industria y Comercio, 'SIC') as the national Data Protection Authority in charge of controlling the correct management of databases by private organizations. Under this role, before international business enterprises such a Google, Amazon, Facebook, Apple or Microsoft ('GAFAM'), there are three decisions that are worth mentioning. On 24 November 2014, the SIC published a legal concept stating that the processing of personal data on social networks does not fall within the purview of Law 1581 of 2012 , as in these cases the collection, use, circulation, storage or suppression of personal data is not made within the Colombian territory (since social networks are domiciled abroad). Nevertheless, on 3 March 2016, the SIC revised its position, arguing that the processing of personal data is carried out in Colombian territory not only when the data collector is domiciled in Colombia, but also when, in order to undertake the collection, use, circulation or storage of the personal data, it uses "means" that are located in the Colombian territory.

---

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

5 El Espectador. "MOE pide destruir material electoral que vulnera datos de votantes en la consulta", March 22. 2018. Available at: https://www.elespectador.com/elecciones-2018/noticias/politica/moe-pide-destruir-material-electoral-que-vulnera-datos-de-votantes-en-la-consulta-articulo-745949 and https://www.elespectador.com/elecciones-2018/noticias/politica/cne-ordenaria-destruir-material-electoral-con-datos-sensibles-de-votantes-articulo-748260

Finally, and in exercise of its legal obligation to guarantee the adequate protection of our data in international transfer of information (articles 21 and 26 of Law 1581 of 2012), the SIC issued the External Circular 005 of August 10, 2017, by which it defined the standards for international transfer of data which lack justification of certain prioritary matters[6].

Regarding the public entities, Law 1581 of 2012 provides that the office of the Inspector General (Procuraduría General de la Nación, 'PGN') will be in charge of sanctioning any misconduct that may occur in the management of databases within the public sector. However, the latter has not yet assumed entirely this role. Besides, Law 1581 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 authority in charge of regulating and sanctioning the public agencies.

Furthermore, besides the fact that the Parliamentary Legal Commission in charge of monitoring intelligence is inoperative, article 30 of the aforementioned Intelligence Law also created a commission of private and public authorities to formulate criteria for purging the intelligence archives to protect, among others, the personal data of the people there registered. Whilst the process was concluded, and a set of criteria was presented, the Colombian government and the chairman of the Purging Commission did not make these public, arguing confidentiality. Moreover, on December 2017 the government issued Decree 2149 of 2017, where a tripartite purging system was created. Nevertheless: i) the Decree adopted non of the recommendations of the Commission; ii) non of the three levels of the system includes a member with a human rights perspective, participation being solely restricted to members of the intelligence community; and, iii) the formulation of the criteria was delegated to the Board of Directors of the Purging System, whose decisions are said to be classified. Therefore, if these criteria are not going to be available to the public, this will hinder the ability of civil society 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.

[6] The Circular establishes a list of countries that Colombia considers to have an adequate level of data protection, including the countries of the European Union (which have been approved as adequate by the European Commission), Mexico, the Republic of Korea, Costa Rica, Serbia, Peru, Norway, Iceland and the United States, with no justification of the inclusion of the United States, criticized for not offering guarantees to foreigners. Moreover, it does not define how the adequacy of these countries will be maintained (as the laws change over time), nor how the level of protection of other countries will be evaluated in the future. By last, and contrary to the European model, the Circular does not provide a procedure to dispute the decisions of "adequate data protection".