Fundación Karisma
www.karisma.org.co

Mr. David Kaye
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression
Palais des Nations
CH-1211 Geneva 10
Switzerland

February 10, 2015

Subject: State of Communications Encryption and Anonymity in Colombia

Hereby, Karisma Foundation presents its contribution on the state of the communications encryption and anonymity in Colombia.

Introduction

Karisma is a digital rights NGO that works in the defense of freedom of expression, privacy, access to knowledge and due process on digital spaces through research and advocacy. Karisma has worked with diverse communities, including: librarians, journalists, persons with visual disability, women's rights advocates to strengthen the defense of human rights in digital spaces. Karisma often works jointly with other NGOs and networks that support their actions and projects

Encryption

The legal status of communications encryption in Colombia is uncertain.

In 1993, the Congress passed Law 104, which provided some mechanisms for the reduction and eventual completion of the conflict between the State and rebel groups. Some of its provisions contain national security measures.

Title IV of that Law deals with communications systems. As such, Article 102 imposes some obligations to cell phone, pagers and radiotelephone users. Article 105 further specifies that those users shall not "send encrypted messages or in unintelligible language."

Act 104 of 1993 was abolished in 1997 and, in the same year, was replaced by Act 418. This standard contains the same provisions on mobile communications encryption as the one mentioned above. It also stated that it would be in force until 1999. In that year, Law 548 extended the period of validity for about three years.

In 2002, the text of Act 418 was modified. The new Law No. 782 of 2002, rather than mentioning cell phones, pagers or mobile radio, makes an abstraction in its Article 42 and prohibit sending "encrypted messages or in unintelligible language" in "all communication devices using the electromagnetic spectrum." Subsequently, through the Law 1106, 2006, those provisions were amended, but not as regards to the matter of encryption.

This temporary legislation has been constantly renewed since 2002. This happened in 2006 with Law No. 1106, in 2010 with the Law No. 1421, and in 2014 with Law No. 1738. As to the specific topic of encryption, despite the constant renewal, it has never been discussed.

The Constitutional Court reviewed the matter from the perspective of the right to freedom of expression and ruled that the prohibition against encryption is compatible with constitutional standards, since the State owns the electromagnetic spectrum and can impose rules on how to use it.[1] In addition, the rule banning the exchange of encrypted messages aims to prevent the use of communication devices in illegal activities. The Court also stated that there is no conflict between the right to privacy and the provisions in question because permission for the interception of communications is not provided.

In short, since 1993, there is in Colombia a law banning users of "communication devices that use the electromagnetic spectrum" to send "encrypted messages or in unintelligible language." The practice related to this provision is unclear. First, digital communication was not as important in 1993 as it is today, which, perhaps, is creating a problem about the mismatch between social, technical and legal realities. It is also blurred whether these provisions apply to digital communications, as it regulates mobile communications. In any case, the standards were drafted in a broad and ambiguous manner to the point that almost any communication device may be included in the ban. Furthermore, it is unclear whether encrypted communications on the internet are prohibited, especially if done from smartphones or cell phones. Finally, the review by the Constitutional Court does not consider methods of digital encryption and its ubiquitous use in online activities such as financial services, electronic commerce and secure web navigation. We understand that it is still needed a study and deeper debate

[1] Constitutional Court of Colombia. Sentence C–586 of 1995. M.P. Eduardo Cifuentes Muñoz.

on how the use of encryption helps protect vulnerable groups such as journalists and their sources, attorney-client or human rights defenders.

Apart from these provisions (Law No. 418 of 1997, Law No. 782 of 2002 and Law No. 1106 of 2006), the Intelligence and Counterintelligence Act provides that voice encryption service may be implemented "exclusively" for the intelligence agencies and "high government" officials by telecommunications service providers.[2] Thus, mobile voice encryption is prohibited for any citizen who is not part of the "high government" or intelligence agencies.

Fundación Karisma has sent information requests to relevant authorities in order to clarify some points regarding the enforcement of these provisions. At the time of the presentation of this contribution those requests are still pending.

Anonymity

The Colombian Constitution recognizes the right of freedom of expression and information (art.20) and the right to privacy (Art.15), gives constitutional rank to international treaties (Art. 93), and states that any omission to enunciation of rights and guarantees does not amount to its denial (Art.94). Thus, the following international instruments are part of the Colombian constitutional norms: American Declaration of the Rights and Duties of Man, 1948, Universal Declaration of Human Rights of 1948, the International Covenant on Civil and Political Rights and the American Convention 1966 on Human Rights, 1969.

The anonymous speech, especially in the digital environment, has not been subject of debate in the Constitutional Court or the legislature. However, it was affected in a recent criminal case.

In 2008, a person was found guilty of defamation for a comment he made in an abusive language in a digital newspaper in relation to an article on the financial mismanagement of a government official. The fact that the comment was signed with a pseudonym was considered by the Prosecutor as evidence of criminal intent. The matter of anonymity was not discussed during the court proceedings or by the media coverage of the decision. Additionally, through some public forums and reviews of opinion makers, Karisma Foundation has seen a social trend to reject anonymous expressions, as they are seen as illegal activities or opportunities to offend others.[3] It is possible that this

[2] Art. 44, par. 2 , Law. No. 1621 of April 17, 2013.

[3] *See* Caracol Radio (2014, July 21). Los insultos y falsas acusaciones en internet serán castigados con cárcel. *Caracol*. Available on http://www.caracol.com.co/noticias/judiciales/los-insultos-y-falsas-acusaciones-en-internet-seran-castigados-con-carcel/20140721/nota/2331715.aspx; Polémica por

trend motivated a bill intended to forbid anonymous expressions in the comments section of online newspapers.[4] Fortunately, this proposal failed. However, some op-ed pieces published in various media warned of the need to protect the anonymous speech.[5]

On the other hand, there are existing regulations that require the identification of mobile devices users and plans to build a system with mass surveillance capabilities.

According to Article 99 of Law No. 418 of 1997 and Resolution 0912 of 2008 of the National Police, telecommunications services providers must give remote access to the police to a database containing user data, such as name, ID number, place and residence address, mobile phone number and service activation date. The information provided by the user is given under penalty of perjury ("false witness" - Article 442 Penal Code.), which is punishable by a minimum of six years in prison. As for mass surveillance systems, the National Police and the Public Prosecutor's Office are advancing a program called "Single Platform of Monitoring and Analysis" (PUMA, in Spanish), which is going to increase the technological capabilities of the State communications surveillance. It is said that online communications may be intercepted as a result of this program, but there is a legal vacuum on the limits of such surveillance.[6]

Context

Colombia has a long history of breaches of the fundamental right to privacy of journalists, human rights defenders, judges and opposition leaders. In this context, the said laws and lack of clear regulations, especially in regards to the communications encryption, poses a great danger to human rights.

---

condena a autor de un comentario en internet (2014, July 21). *El País*. Available on http://www.elpais.com.co/elpais/judicial/noticias/primera-condena-colombia-por-injuria-internet.

[4] Proyecto de ley busca restringir opiniones en medios virtuales (2009, August 15). *El Espectador*. Available on http://www.elespectador.com/noticias/actualidad/articulo156403-proyecto-de-ley-busca-restringir-opiniones-medios-virtuales.

[5] *See* Botero, C. (2014, July 24). Nos Jugamos la libertad de expresarnos. *El Espectador*. Available on http://www.elespectador.com/opinion/nos-jugamos-libertad-de-expresarnos-columna-506516; Botero, C (2014, August 29). 18 meses de prisión por opinar en Internet. Digital Rights Latin American and the Caribbean, 14. Available on http://www.digitalrightslac.net/es/18-meses-de-prision-por-opinar-en-internet/; Cortés, C. (2014, July 21). *Cárcel para un comentarista ofensivo: revisando las paredes de los baños públicos*. Available on http://carloscortes.co/blog/2014/7/21/crcel-para-un-comentarista-ofensivorevisando-las-paredes-de-los-baos-pblicos.

[6] Valero, D. (2013, June 23). Policía podrá interceptar Facebook, Twitter y Skype en Colombia. *El Tiempo*. Available on http://www.eltiempo.com/archivo/documento/CMS-12890198.

In 2009, “Semana” magazine revealed the results of a six-month investigation in which a large illegal intelligence operation was found.[7] The former intelligence agency (DAS) was following judges, journalists, human rights defenders and opposition leaders, among other groups, as they were considered potentially dangerous to the former President Álvaro Uribe Vélez administration. External interception laboratories or facilities were the most common form of intelligence equipment deployment reported in illegal surveillance cases. Despite the adoption of a new 2013 Intelligence and Counterintelligence Act intended to prevent cases such as these, a year later a new case of illegal communications surveillance was known. In February 2014, “Semana” revealed that a undercover military intelligence unit not only executed an illegitimate operation, but also served as a center for the interception of electronic communications targeted to government and FARC representatives in the Peace Talks taking place in Havana, Cuba.[8]

According to information obtained by “Semana,” the intelligence operation was intercepting emails, Blackberry and WhatsApp instant messaging with the help of (young) civilians, who had been contacted by military agents in technology conventions (i.e. Campus Party). This operation is known as “Andromeda.”

This scandal brought to light that there are two branches of military intelligence: (1) one specialized in the interception of telephone communications, and (2) another devoted to the interception of digital communications. According to a “Semana” source, the branch dedicated to the interception of telephone communications operates within the Public Prosecutor's Office, which is subject to stricter controls. In contrast, due to the feeble legal framework on digital communications surveillance, the second one is more prone to commit abuses. However, it was reported that 115 out of 440 intercepted telephone numbers did not have a warrant issued by the competent authority.[9]

Conclusions

Consequently, Fundación Karisma kindly requests the Rapporteur to consider developing international principles and guidelines to serve the States in establishing regulations on communications encryption and anonymity on the Internet. In this sense, we believe it should be emphasized the need to highlight that any legislation in this regard must be clear and specific, as well as must unmistakably established the

[7] El DAS sigue grabando (2009, February 21). *Semana*. Available on http://www.semana.com/nacion/articulo/el-das-sigue-grabando/100370-3.

[8] ¿Alguien espió a los negociadores de La Habana? (2014, February 3). *Semana*. Available on http://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3.

[9] Chuzadas: así fue la historia (2014, February 8). *Semana*. Available on http://www.semana.com/nacion/articulo/chuzadas-asi-fue-la-historia/376548-3.

necessary balance between the protection of human rights and national security. Such international principles and guidelines should also emphasize the importance of encrypted communication and anonymity as part of the realization of the rights to privacy and freedom of expression. Finally, we believe it appropriate to emphasize that national security, while important, is not absolute; thus, it is not sufficient reason to prohibit both encrypted communication and anonymity on the Internet. On the contrary, it is a way we as ordinary citizens have of protecting our communications and identity from abuses or threats that can be caused by third parties, including the State.

Sincerely,

Carolina Botero Cabrera
Manager

Juan Diego Castañeda Gómez
Project Officer

Amalia Toledo Hernández
Project Coordinator