



Right to Privacy

20

Implementation of recommendations from the previous period

No recommendations regarding the right to privacy were made to Colombia in the previous UPR. However, countries such as Bhutan and Azerbaijan recommended that the State work to eliminate gaps in the fulfillment of human rights in the country. Related to this issue, the Republic of Korea recommended increasing efforts to improve State transparency. Similarly, many countries (Germany, Bolivia, Austria, Belgium, Norway) made recommendations that Colombia adopt measures to protect its human rights activists and defenders.

Despite the general call to respect human rights and implement transparency measures, Colombia faces serious problems regarding the right to privacy due to a lack of regulation of technologies that permit citizen surveillance.

Current status

Continued profiling and surveillance of journalists and activists. During the last evaluation period, there were several cases of profiled activists and journalists. These include the Secret Files case, (1) as well as the profiling of journalists such as María Camila Villamizar (2) using open source intelligence (OSINT). (3) OSINT facilitates the collection and classification of information published on the Internet and demonstrates continued surveillance of civil society by the Colombian State.

The State has implemented technology to conduct mass surveillance without a clear legal framework. Both during the Covid-19 pandemic, (4) as well as during the 2021 social protests, (5) the Colombian Police and the Ministry of Defense undertook "cyber patrolling." This involved the live monitoring of content published by civil society, tracking social media trends, and reporting some publications posted by civil society members as fake news. (6)

(1) El Espectador. Las "carpetas secretas" de inteligencia militar: ¿para quién iban dirigidas y para qué? Available at:

<https://www.elespectador.com/judicial/las-carpets-secretas-de-inteligencia-militar-a-quienes-iban-dirigidas-y-para-que-article-917751/>. This article was also published in Semana Magazine. Available at: <https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpets-secretas-investigacion-semana/667616/>

(2) Fundación para la Libertad de Expresión (FLIP). Inteligencia Militar incrementa su capacidad para vigilar a periodistas y ciudadanía con tecnología de fuentes abiertas. Available at: <https://www.flip.org.co/index.php/es/publicaciones/informes/item/3007-inteligencia-militar-incrementa-su-capacidad-para-vigilar-a-periodistas-y-ciudadania-con-tecnologia-de-fuentes-abiertas>

(3) Open Source Intelligence (OSINT) consists of a series of techniques to collect and analyze data that is housed in open access information sources and is used for either offensive or defensive purposes (operation planning). For more information see: Karisma. Cuando el Estado vigila. OSINT y Ciberpatrullaje en Colombia. Available at: <https://web.karisma.org.co/cuando-el-estado-vigila-ciberpatrullaje-y-osint-en-colombia/>

(4) Índice de Derechos Digitales. Ciberpatrullaje de la Policía Nacional para identificar desinformación. 2023. Available at:

<https://indicederechos.digital/docs/CiberpatrullajeDesinformacion/>

(5) Karisma Foundation. Pistolas vs Celulares. Available at: <https://web.karisma.org.co/pistolas-contra-celulares/>

(6) This type of action was publicized through public reports known as General Balance Sheets that were periodically published by the Ministry of Defense. This report was published on 27 June 2021: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiFy4_ogIqAAxV3glQIHXLIAHMQFnoECC4QAQ&url=https%3A%2F%2Fwww.mindefensa.gov.co%2Ffirj%2Fgo%2Fkm%2Fdocs%2FMindefensa%2FDocumentos%2Fdescargas%2Festudios_sectoriales%2Finfo_estadistica%2Finforme_Corrido_Balance_Paro_2021.pdf&usq=AOvVaw0YdrW5-0VaAUJo1fDYRN2U&opi=89978449

There is no legislation that regulates the acquisition and use of surveillance technologies.

Entities such as the National Army, the National Intelligence Office, the Police, and the Attorney General's Office have tools to monitoring Internet content. They use these tools to gather intelligence, carry out surveillance, and conduct judicial investigations. Citizens are not allowed to know when this occurs or which laws permit these actions. (7)

These entities also purchase and use other technologies such as "jammers," (8) which allow for Internet and telephone signals to be blocked in a specific area, as well as SINGINT software (Signal Intelligence)(9) to intercept messages and conversations. These technologies are acquired confidentially using a "national security" argument. This means that it is not possible to know how they are being used nor what oversight is exercised on these tools. A number of civil society organizations have made public statements regarding their difficulties to access information about the purchase and use of technology by the Colombian State. As a result, it is very difficult for these organizations to exercise their right to access information. (10)

Impunity continues in cases of surveillance and citizen guarantees.

Impunity persists in cases involving State profiling or illegal interceptions against citizens, journalists, and activists. No progress has been made with internal and judicial investigations, sanctions, or reparations for the acts committed.

(7) Karisma. Cuando el Estado vigila. OSINT y ciberpatrullaje en Colombia. Available at: <https://web.karisma.org.co/cuando-el-estado-vigila-ciberpatrullaje-y-osint-en-colombia/>

(8) Carolina Botero. La Silla Vacía. El misterio detrás de los cortes de internet en Cali durante el paro de 2021. Available at: <https://www.lasillavacia.com/historias/historias-silla-llena/el-misterio-detras-los-cortes-de-internet-en-cali-durante-el-paro-de-2021/>

(9) ODIN. Osint e Inteligencia. Qué es SIGINT, Cómo se usa y ejemplos de la inteligencia de señales. Available at: <https://odint.net/sigint/>

(10) Karisma. La punta del iceberg. Los problemas de transparencia del OSINT en Colombia. Available at: <https://web.karisma.org.co/la-punta-del-iceberg-los-problemas-de-transparencia-del-osint-en-colombia/>

Recommendations

1. Design a regulation for the acquisition, use, and control of technologies that have the potential to affect citizens' rights.
2. Intensify the State's efforts to investigate and prosecute public officials involved in the illegal surveillance of citizens or the interception of citizens' personal communications.
3. Formulate a regulation that clearly lays out the functions of State entities when using specific technology and their obligation to notify the citizens involved.
4. Ensure that the use of surveillance technologies complies with the principles of legality, legitimacy of purpose, necessity, proportionality, and non-discrimination and does not inhibit the essential core of the right.
5. Conduct a rights impact analysis when the government purchases and uses surveillance technologies, which should take into account the risks of technology abuse.