COLOMBIA'S COMPLIANCE WITH THE ICCPR: PI's submission to the UN Human Rights Committee

June 2023

privacyinternational.org

Submission in advance of the consideration of the periodic report of Colombia, Human Rights Committee, 138th Session, 26 June to 28 July 2023

May 2023

Introduction

This submission is for the 138th session of the Human Rights Committee which will take place between 26 June 2023 and 28 July 2023 in relation to Colombia's compliance with the International Covenant on Civil and Political Rights (ICCPR).

Privacy International (PI) is a global advocacy and campaigning group that works at the intersection of technology and human rights. PI campaigns against companies and governments who exploit our data and technologies. We expose harm and abuses, mobilise allies globally, campaign with the public for solutions, and pressure companies and governments to change.

Fundación Karisma is a Colombian civil society organization dedicated to the defense of human rights in digital environments and arround new technologies, with a particular focus on public policy and the use of technology by the government.

Dejusticia is a think-tank that contributes to the strengthening of the rule of law and promotes social justice and human rights from a distinctly Global South perspective. As an action-research centre, Dejusticia has promoted positive social change for over 15 years by producing in-depth studies and fact-based policy proposals; carrying out effective advocacy campaigns; litigating in the most impactful forums; and designing and delivering training and capacity-building programs.

Privacy International has highlighted its concerns in its submission for the list of issues.[1] More recently, the organisation(s) have documented their concerns on a wide array of issues in Colombia, ranging from migrants rights and protest rights to health and social welfare in a joint stakeholder submission to the 44th session of the Universal Period Review working group, ahead of the Universal Periodic Review (UPR) of Colombia on 7 November 2023.[2]

The following submission expands on some of the issues previously commented on, and refers to our UPR submission where relevant.

[1] See Privacy International's and Fundación Karisma's joint civil society submission for the List of Issues. Available at: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/SessionDetails1.aspx?SessionID=2635&Lang=en

[2] Dejusticia, Fundación Karisma y Privacy International, Informe de actor interesado Examen Periódico Universal 44o periodo de sesiones – Colombia, April 2023 (online publication pending).

1. Digital ID and Colombia's biometric database

a. Increased processing by the RNEC of biometric data

The introduction by the National Civil Registry (RNEC, its acronym in Spanish) of a digital national ID[3] in Colombia raises significant privacy concerns, as described in our joint UPR submission.[4] The national ID is mandatory for anyone over 18, and it incorporates a nationwide biometric register both in its physical version and its electronic version.[5] Data collected allow the facial recognition and authentication of any Colombian without their express consent.

Crucially, this biometrics database was introduced and is evolving in the absence of regulation and without limits on the permitted uses for the data hosted within it, increasing the risk of unlawful surveillance, in violation of Article 17 of the ICCPR. For example, there are pilot programmes to introduce CCTV cameras with facial recognition capabilities in real-time in cities such as Bucaramanga and Medellin which will rely on the RNEC database.[6]

b. Implications in the context of elections

The civil register is an essential tool for the effective functioning of elections, and access to the register by selected actors monitoring the election is necessary to safeguard the fairness of the electoral process. At its core, however, a civil register is a nationwide centralised database storing a vast array of personal data about voters. The electoral register in Colombia ("censo electoral") is defined by law as the general register of the citizenship cards corresponding to Colombian citizens who are entitled to vote.[7] The electoral register acts as the civil register, as there is no other database which gathers the personal information of individuals at a nationwide scale. The Colombian citizenship cards – which are in the process of being replaced by national Digital ID - currently include information on a person's ID number, names and surnames, height, gender, blood group, date and place of birth, as well as the person's electronic signature and photograph.

Centralised electronic registers naturally raise concerns related to the safety of the personal data stored therein and the potential risks for unauthorised access, which is why Privacy International has been advocating for safeguards to ensure that the national framework is

---

[3] Fundación Karisma, La escalada funcional y tecnológica de la cédula de ciudadanía, 27 november 2022. Available at: https://digitalid.karisma.org.co/2022/11/27/la-historia-de-la-identificacio-n-en-Colombia/

[4] Dejusticia, Fundación Karisma y Privacy International, Informe de actor interesado Examen Periódico Universal 44o periodo de sesiones – Colombia, April 2023 (online publication pending).

[5] Registraduría Nacional del Estado Civil (29 January 2020). "Remisión documentos requeridos para la contratación del Fortalecimiento, mantenimiento y sostenibilidad del sistema de identificación y registro civil a nivel nacional vigencia 2020"; Registraduría Nacional del Estado Civil (2020)."Adición no. 01 y otrosí no. 03 al contrato electrónico de prestación de servicios no. 002 de 2020, sus condiciones adicionales y sus otrosíes no. 01 y 02 de 2020, suscrito entre la registraduría nacional del estado civil e idemia identity & security sucursal Colombia".

[6] La Vanguardia. *Así será el plan piloto de tecnología para la seguridad en Bucaramanga*, 16 March 2023. Available at: https://www.vanguardia.com/politica/asi-sera-el-plan-piloto-de-tecnologia-para-la-seguridad-en-bucaramangaYA6417364; El Espectador, *Los retos del reconocimiento facial que se usa para garantizar la seguridad*. 5 July 2022. Available at: https://www.elespectador.com/colombia/mas-regiones/los-retos-del-reconocimiento-facialen-la-seguridad/

[7] Law 1475 of 2011, Art. 47.

adequate to protect against the exploitation of data in the electoral process. [8] These concerns are heightened when the register includes sensitive personal data, such as biometric data, which is the case for Colombia's RNEC.

The current electoral landscape in Colombia adds to these concerns. Prior research conducted by Dejusticia around the transparency of actors involved in political campaigning revealed that Colombia's current platforms make it difficult to ascertain the involvement of companies specialising in data-intensive activities such as micro-targeting.[9] Specifically, *Cuentas Claras*, a monitoring tool created by the National Electoral Council to offer the public insights into campaign spending, failed to compel comprehensive information from political campaigns about companies contracted with for the purposes of providing digital marketing and political communication services. Crucially, Dejusticia found links between political campaigns and companies that had not been reported on the platform.[10] There is no specific regulation on the use of digital technologies for electoral purposes and little clarity on how the general regulatory framework of the Colombian electoral law and the data protection law apply in this context. Despite initiatives such as *Cuentas Claras*, there is a lack of transparency on the data processing of political parties and companies providing digital marketing and political communications services.

Further, new electoral legislation amending the Electoral Code is currently being debated by Colombian legislature. The bill seeks to overhaul the current electoral landscape, proposing major changes such as the introduction of electronic voting (e-voting) and including substantive provisions to regulate RNEC. Civil society organisations including Karisma have flagged the undesirability of addressing both electoral law and the civil register in a single legislative document, as each would require careful and distinct consideration. Discussions on voter identification at the polls and the national identification system as a whole must be held separately, and must specifically address the limits of the RNEC's authority to capture and manage personal data, including biometric data.[11] Further, increased reliance on technological solutions such as e-voting raises additional risks of abuse and specific challenges related to cybersecurity and the protection of anonymity of voters. These concerns have been articulated by some election observers' organisations, noting, for example, that "evoting systems linked to the Internet or other computer networks may be susceptible to hacking or outside manipulation".[12]

---

[8] Privacy International, Technology, Data and Elections: A Checklist on the Election Cycle, July 2019. Available at: https://privacyinternational.org/advocacy/3093/technology-data-and-elections-checklist-election-cycle

[9] Dejusticia, Digital Technologies and Political Campaigns, a risk for the 2022 elections? 30 November 2021. Available at: https://www.dejusticia.org/en/digital-technologies-and-political-campaigns-a-risk-for-the-2022elections/

[10] Ibid., p.30.

[11] Fundación Karisma, Concepto técnico sobre la reforma al código electoral y balance de la discusión durante el primer semestre del nuevo Congreso de la República, 15 December 2022. Available at: https://web.karisma.org.co/concepto-tecnico-sobre-la-reforma-al-codigo-electoral-y-balance-de-la-discusiondurante-el-primer-semestre-del-nuevo-congreso-de-la-republica/

[12] See EU third edition of the Handbook for European Union Election Observation. Available at: https://eeas.europa.eu/sites/eeas/files/handbook_for_eu_eom_2016.pdf

2. Unlawful surveillance

Unlawful surveillance, including through the widespread use of surveillance technologies, remains an ongoing concern of civil society and has been repeatedly raised in human rights monitoring processes, as noted in our submission to the List of Issues as well as the 2023 UPR Stakeholder report including the previous Universal Periodic Review.[13]

a. Open-source intelligence and cyber-patrolling

Online surveillance has flourished, with government entities increasingly turning to social media for intelligence-gathering activities.[14] Research carried out by Dejusticia documents the rise of online intelligence activities in Colombia.[15] Fundación Karisma, in separate research, documented the rise of "cyber-patrolling", a tactic coined by the National Police in 2015 in a resolution.[16] The practice, which remains undefined by the National Police or any other government entities, relies on open-source intelligence (OSINT) methods. The use of cyber-patrolling technologies was revealed during the 2021 protests, when law enforcement relied on these tactics, among other things, to categorise content shared by people on social media platforms, flagging as false content which often showcased instances of abuse of power at the hands of the police.[17]

Even as the meaning and limits of cyber-patrolling remain unclear, different entities within the Colombian government have entered into at least five contracts with private companies in order to obtain technology to be used for cyber-patrolling purposes.[18] However, finding information as to the extent of the contracting involved in order to expand the government's OSINT capabilities remains a difficult exercise, with the government typically relying upon national security grounds to object to the disclosure of information that would provide further insight into the government's increasing tech capabilities.[19]

b. Surveillance of human rights defenders

We note that the Colombian government has not addressed this issue in its reply to the List of Issues.[20] This omission adds to the grave concerns already shared by a wide section of civil society. According to research published in 2023, Colombia alone accounted for 46% of the total global killings of human rights defenders, making it the deadliest country for defenders

---

[13] Dejusticia, Fundación Karisma y Privacy International, Informe de actor interesado Examen Periódico Universal 44o periodo de sesiones – Colombia, April 2023 (online publication pending).

[14] Dejusticia, Inteligencia Estatal en Internet y Redes Sociales: El Caso Colombiano, December 2022. Available at: https://www.dejusticia.org/wp-content/uploads/2022/12/InteligenciaEstatalEnInternet-Web-Dic23.pdf

[15] Ibid., p. 22.

[16] Fundación Karisma, Cuando el Estado Vigila: Ciberpatrullaje y OSINT en Colombia, 27 February 2023. Available at: https://web.karisma.org.co/cuando-el-estado-vigila-ciberpatrullaje-y-osint-en-colombia/

[17] Fundación Karisma, Pistolas contra celulares, September 2021. Available at: https://web.karisma.org.co/pistolas-contra-celulares/

[18] Fundación Karisma, Cuando el Estado Vigila: Ciberpatrullaje y OSINT en Colombia, p. 11.

[19] Fundación Karisma, La punta del iceberg: los problemas de transparencia del OSINT en Colombia, 24 March 2023. Available at: https://web.karisma.org.co/la-punta-del-iceberg-los-problemas-de-transparencia-del-osinten-colombia/

[20] See UN Human Rights Committee, List of Issues in relation to the eighth periodic report of Colombia, 10 October 2022, CCPR/C/COL/Q/8, paras. 21 and 24. Available at: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/SessionDetails1.aspx?SessionID=2635&Lang=en

worldwide.[21] These human rights violations take place in a context where unlawful surveillance of human rights defenders has been historically widespread and continues to be pervasive.[22]

Interception of communications by intelligence agencies is not adequately regulated by national law and has been challenged before courts.[23] For example, a case currently pending before the Inter-American Court of Human Rights challenges the Colombian government's surveillance of various members of the Colectivo de Abogados José Alvear Restrepo (CAJAR) over many years.[24] In a joint amicus submission made to the Court, we argue that the law relied upon by the Colombian state to legitimise surveillance activity - Intelligence Law 1612 - does not explicitly authorize Colombian intelligence agencies to intercept private communications.

Surveillance by the National Protection Unit of beneficiaries in receipt of protective measures

There is worrying evidence to suggest that human rights defenders in particularly at-risk situations and in receipt of protection measures by the National Protection Unit (UNP, for its initials in Spanish) may be subjected to surveillance by the Unit itself. Journalist Claudia Duque, a former beneficiary of the UNP's protective measures, brought a case against the UNP to challenge the collection of her government-issued vehicle's GPS data by the UNP while she was a beneficiary of protective measures over a period of 209 days without her knowledge or consent.[25] Concerningly, when Duque opposed the continued collection of her GPS data and suggested the use of a less intrusive alternative – a digital tachograph[26] – the UNP refused to remove the GPS, ultimately leading Duque to entirely withdraw from her protection scheme.[27] The case's fact pattern raises concerns as to whether similar practices may have been used against other human rights defenders benefitting from protective measures, particularly as the UNP stated in early communications with Duque that although

[21] The total number of human rights defenders killed in 2022 was 186. Of these, 8 were environmental and indigenous land rights defenders. https://www.frontlinedefenders.org/en/resource-publication/global-analysis2022

[22] Privacy International, Colombia's record on privacy, surveillance, and human rights under renewed scrutiny at the United Nations, 17 October 2016. Available at: https://privacyinternational.org/pressrelease/1326/colombias-record-privacy-surveillance-and-human-rights-under-renewed-scrutiny

[23] Privacy International, Shadow State: Surveillance, Law and Order in Colombia, 1 September 2015. Available at: https://privacyinternational.org/report/991/shadow-state-surveillance-law-and-order-colombia

[24] Privacy International, Article 19, Electronic Frontier Foundation, and Fundación Karisma, Amicus curiae in *Members of José Alvear Restrepo Lawyers' Collective v. Colombia*, 24 May 2022. https://www.law.berkeley.edu/wp-content/uploads/2022/05/Amicus-Brief-CCAJAR-v.-Colombia.pdf

[25] The National Protection Unit confirmed it had records spanning 209 days, where it had collected 25,183 records through Duque's car's GPS, namely 120 daily information on her movements. More details about the case here: https://privacyinternational.org/video/5056/protecting-protectors-case-colombia.

[26] A digital tachograph is a device fitted to a vehicle that digitally records its speed and distance, together with the driver's activity. The activity information is stored in the tachograph's internal memory and a digital driver card inserted in the tachograph. Because the information is stored locally, it does not allow for electronic onward transmission in real-time, unlike GPS. See: https://transport.ec.europa.eu/transport-modes/road/tachograph_en

[27] El Tiempo, Corte revisa tutela de periodista contra UNP por recolección de datos personales, 30 August 2022. Available at: https://www.eltiempo.com/justicia/cortes/claudia-julieta-duque-seleccionan-tutela-contra-unp-pordatos-personales-698612

the GPS in and of itself was not considered a protective measure, it was installed by default in all of the vehicles operated by the UNP and given to beneficiaries of protective measures.

3. Conclusion and recommendations

As we noted in this and previous submissions and as already raised by this Committee in the previous concluding observations, surveillance by intelligence and other security agencies in Colombia is used to target human rights defenders and others. We also continue to witness an expansion of surveillance powers, including the proliferation of open-source intelligence. In this context, the development of national biometric databases as part of the Colombian ID system and its potential misuse, including in the context of elections, raises significant, novel concerns of Colombia's compliance with the ICCPR.

For these reasons, PI recommends the UN Human Rights Committee to make the following recommendations to Colombia:

1. The Electoral Law should ensure that the electoral register does not include personal data other than what is required to establish eligibility to vote. The law should define the minimum standards of security to protect the voters' register against unauthorised access; it should also define the conditions and limits of sharing and access to the personal data. In particular, biometric data (including photographs) must not be used for anything other than the stated purpose in law and subjected to additional protection against unauthorised access or other data breaches, including storing biometric data separately from other personal data.

2. Review and amend national legislation to ensure that interception of communications by intelligence agencies and other security and law enforcement forces comply with the principles of legality, necessity and proportionality and provide for effective, independent oversight, prior judicial authorisation and access to effective remedies for unlawful surveillance, in line with Article 17 of ICCPR.

3. Adopt precise legal framework to govern the collection, analysis and sharing of social media and open source intelligence (including the activities known as cyberpatrolling) that clearly define permissible grounds, prerequisites, authorization procedures and adequate oversight mechanisms.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org