Colombia's compliance with the International Covenant on Civil and Political Rights
Suggested List of issues (LoI)
submitted to the UN Human Rights Committee
by Privacy International and Fundación Karisma
May 2022

This submission is for the 135th session of the Human Rights Committee that will take place between 27 June 2022 and 29 July 2022 in relation to Colombia's compliance with the International Covenant on Civil and Political Rights (ICCPR) before the adoption of the List of issues of issues (LoI).

Privacy International is a global advocacy and campaigning group that works at the intersection of technology and human rights. 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 digital rights NGO that works in the defence 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 defence of human rights in digital spaces. Karisma often works jointly with other NGOs and networks that support their actions and projects.

PI and Karisma call on the Human Rights Committee to include in the LoI the following issues:

- Colombia to provide explanations on the compatibility of social protection initiatives with the right to privacy.

- Colombia to provide information on current surveillance measures, the legal basis on which these are undertaken and to address how it is complying with Article 17 of the ICCPR.

- Colombia to provide further details on the current policy and legal framework in place to regulate Biometric ID systems and the use of facial recognition, including due diligence and procurement processes to oversee the acquisition of such technologies.

Further information is provided below.

## Covid-19 Pandemic social benefits initiatives and the use of beneficiaries' data

PI and Karisma are concerned that there is not sufficient regulation, oversight and transparency of data processing activities, particularly with regard to the use of individuals' data in the design and management of social protection initiatives.

In response to the Covid-19 pandemic, Colombia's welfare agency – the National Development Office – set up an unconditional cash transfer for 3 million citizens in just under two weeks. The Solidarity Income (in Spanish "Ingreso Solidario"), as the benefit was called, aimed to mitigate the impact of the pandemic on individuals in a situation of extreme poverty.[1]

Despite the legitimate aims behind the Solidarity Income, the process of determination of eligibility of beneficiaries was, and remains, shrouded in secrecy. As research by Fundación Karisma has documented,[2] the Solidarity Income was awarded to beneficiaries based on undisclosed criteria, with the chosen beneficiaries being notified of their entitlement without being given reasons.

The Solidarity Income, as every other benefit in Colombia, relies on the System of Possible Beneficiaries of Social Programs (SISBEN in Spanish), which was created to assist in the targeting of social programs in Colombia. Previous research undertaken by Fundación Karisma on the functioning of the SISBEN found that the system relied on the 34 public and private databases.[3]

Information about the determination of eligibility process which has been made publicly available indicates that beneficiaries were chosen based on a combination of almost 30 distinct databases (privately and publicly owned), and an algorithm, which remains undisclosed, to decide who is eligible to receive benefits. As a result, selected beneficiaries were not able to identify the basis on

[1] https://ingresosolidario.prosperidadsocial.gov.co/

[2] Fundación Karisma, Un experimento del estado para evitar discusión política sobre beneficios sociales por Covid 19. Available at: https://web.karisma.org.co/ingresos-solidario-o-una-barrera-mas-para-la-exigibilidad-de-beneficios-sociales-en-tiempos-de-pandemia/

[3] Fundación Karisma, Experimentando con la Pobreza: el SISBEN y los proyectos de analítica de datos en Colombia, February 2020. Available at: https://web.karisma.org.co/experimentar-con-los-datos-de-personas-en-situacion-de-pobreza-una-mala-practica-para-lograr-la-justicia-social-en-colombia/

which they had been deemed eligible for the benefit, nor the categories of personal data accessed and used to select them. There were documented instances, as reported by Fundación Karisma, of individuals being selected for the benefit despite not being in a situation of poverty. In recently published guidance,[4] the Bogotá administration - the entity responsible for disbursing the benefit to beneficiaries based in Bogotá - acknowledged the possibility of individuals having been allocated the benefit without needing it. The guidance states: "If you received the Solidarity Income, and do not need support, you can return the funds to the financial entity that made the deposit".[5]

By contrast, individuals who were not selected for the benefit and nonetheless were in a situation of poverty were unable to challenge the government's decision not to award them benefits, as they could not know on what basis they had been denied them.

These concerns reflect some of the systemic problems we have observed emerging from the increased digitalisation, automation and intrusive data collection in the "digital welfare state". As noted in the 2019 thematic report of the UN Special Rapporteur on extreme poverty and human rights, the risks of discrimination and exclusion triggered by the digitalisation, automation and intrusive data processing of social protection programmes need to be addressed.[6]

PI and Karisma recommend to the UN Human Rights Committee to include the following in the LoI and ask the Colombian government:

- To provide information on how the Solidarity Income complies with Article 17 of the ICCPR, and in particular for the government to clarify:
    - What measures and due diligence have been taken to ensure the privacy of individuals seeking state-provided benefits is protected or safeguarded in the process of allocating state benefits, including, for example 'human rights by design' and human rights impact assessments?

[4] Bogotá, Todo lo que debes saber sobre el ingreso solidario, 6 April 2022. Available at: https://bogota.gov.co/servicios/guia-de-tramites-y-servicios/informacion-general-sobre-ingreso-solidario

[5] Ibid.

[6] UN General Assembly, "Report of the Special Rapporteur on extreme poverty and human rights," A/74/493, 11 October 2019

- How these individuals are given access to due process and how automated decision-making processes are used to determine their eligibility to the programme?

- What effective accountability mechanisms are in place to guarantee meaningful access to redress and appeal mechanisms?

## Surveillance of human rights defenders

PI and Karisma are concerned that the unlawful surveillance of human rights defenders continues unabated in Colombia, despite years of outcry, at the expense of their rights to privacy and freedom of expression.

PI and Karisma raised concerns about unlawful surveillance practices by Colombian entities as early as 2015 in a report titled "Shadow State: Surveillance, Law and Order in Colombia".[7] Some of these concerns were also reflected in the concluding observations of the UN Human Rights Committee in 2016, when the Committee called on the Colombian government to adopt effective measures to prevent illegal surveillance activities.[8] PI and Karisma are disappointed that little has changed since then.

The fact that unlawful surveillance continues to take place in Colombia was recently acknowledged by the Inter-American Commission. The 2020 Annual Report of the OAS Special Rapporteur for Freedom of Expression recounts in detail various reported instances of surveillance against a range of actors.[9]

Specifically, PI and Karisma continue to be concerned about the following practices being undertaken in Colombia:

- Profiling: Profiling includes, among other practices, the online surveillance of individuals through the use of social media monitoring, either overtly through the use of "open" or publicly accessible sources or covertly through

[7] 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

[8] UN Human Rights Committee, Concluding Observations on the 7th periodic report of Colombia, CCPR/C/COL/CO/7, para. 32. Available at: https://digitallibrary.un.org/record/1313650

[9] OAS, Annual Report of the Office of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II, 30 March 2021, paras. 405-412. Available at: https://www.oas.org/en/iachr/expression/reports/ENGIA2020.pdf

surreptitious access of private profiles. Profiling is a highly intrusive practice which entails the systematic collection of personal data, and which can affect third parties, such as family members and minors. Following an investigation by Colombian newspaper *Semana*, there are concerns that Colombian authorities may be increasingly relying on profiling to gain insights into the lives of individuals who may be perceived to oppose government institutions, among other reasons.[10]

- Electromagnetic spectrum monitoring: Further to the concerns expressed by the Committee in their Concluding Observations on the seventh periodic report of Colombia,[11] it appears that "electromagnetic spectrum monitoring", as provided for in Article 17 of Act No. 1621 of 2013, is still relied upon by Colombian authorities. During the 2021 protests, the Unified Command Post of cybersecurity (Puesto de Mando Unificado de Ciberseguridad) conducted massive social media monitoring, trend-tracking and tagging of citizen content. We are particularly concerned that the Office of the Prosecutor mentioned in an answer to a freedom of information request submitted by Karisma that such activities were legal since their assessment is that the constant monitoring of networks does not constitute individual profiling.[12]

- Direct access to the internet and mobile network's service providers: Service providers have attested to the Colombian government's broad access powers to mobile networks. According to the 2020 Millicom Group Law Enforcement Disclosure (LED) Report:[13] "Procedures in Colombia require us to provide direct access for authorities to our mobile network. Regular audits ensure we do not obtain information about interception that is taking place. We are subject to strong sanctions, including fines, if authorities find that we have gained such information. As a result, we do not possess information regarding how often and for what periods of time communications are intercepted in our mobile networks in Colombia." In recent years, Movistar, Claro and Tigo have also stated that government

[10] Semana, Las Carpetas Secretas. Available at: https://especiales.semana.com/espionaje-desde-el-ejercito-nacional-las-carpetas-secretas-investigacion/index.html

[11] UN Human Rights Committee, Concluding Observations on the 7th periodic report of Colombia, CCPR/C/COL/CO/7, para. 32. Available at: https://digitallibrary.un.org/record/1313650

[12] La Silla Vacía. Carolina Botero. Poniéndole el ojo a los PMU-CIBER: ¿Qué son y para qué sirven? (Keeping an eye on PMU-Cybers: what are they and what are they for?). Available at: https://www.lasillavacia.com/historias/historias-silla-llena/poniendoles-el-ojo-a-los-pmu-ciber-que-son-y-para-que-sirven/. The response is quoted in this article and was the result of an initial FOIA request that was later denied.

[13] https://www.millicom.com/media/4402/final-millicom-led.pdf

authorities are technically enabled to carry out interceptions themselves as service providers are compelled to provide the relevant government authorities with direct access to their mobile network infrastructure, as opposed to interceptions concerning fixed network infrastructure, where service providers still act as intermediaries.[14] This means that by virtue of the direct access given to government authorities, which enables any oversight measure to be bypassed, any oversight capacity that intermediaries otherwise have in the interception of communications has been completely lost giving total power to law enforcement to undertake surveillance of mobile networks.

PI and Karisma recommend to the UN Human Rights Committee to include the following in the LoI and ask the Colombian government:

- Whether, and on what legal basis, profiling activities continue to take place to determine targets of surveillance?

- To what extent does the Colombian government continue to make requests for user information to service providers, and on what legal basis?

- To report on the legal basis for direct access, the oversight mechanisms, the frequency of instances of direct access to the providers' infrastructure for any purpose including interception, and the justification behind each direct access.

- To clarify how current communication surveillance policies and practices comply with Article 17 of the ICCPR.

[14] Movistar Informe de Transparencia en las Comunicaciones 2021, pp 20. Available at https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/08/Informe-de-Transparencia-en-las-Comunicaciones-2021.pdf
Claro, Informe de Sostenibilidad 2020, pp. 109-111. Available at: https://www.claro.com.co/portal/recursos/co/pdf/Informe_de_Sostenibilidad_Claro_2020-.pdf; Tigo, Políticas de Datos Personales y de Seguridad, Requerimientos de datos personales por terceros y bloqueos de contenido. Available at: https://www.tigo.com.co/legal-y-regulatorio/politica-de-datos-personales#politicas-de-datos-personales-y-de-seguridad-requerimientos-de-datos-personales-por-terceros-y-bloqueos-de-contenido

## Biometric ID systems and the use of facial recognition

Over the course of the last few years, we've seen the programme for biometric ID and registration grow in Colombia. Since 2018, the National Civil Registration Authority (Registraduría Nacional del Estado Civil - RNEC), without democratic discussion, implemented a facial recognition system in the National Identity System (Sistema Nacional de Identidad - SNI) by contracting the Multinational IDEMIA. This database, constructed and administered by the RNEC, which includes everybody above the age of 7, is expanding with new entries being uploaded every day, and its uses are yet to be regulated. It can be used for both identification (1:n) and authentication (1:1) tasks and can, at the time of writing, provide those services for public and private institutions on demand (in exchange for a fee), and with privileged access for law enforcement.

PI and Karisma are concerned with the possible abuses of such database and biometric systems for surveillance, security or commercial interest purposes. Such practices are especially concerning given the regulatory void that exists regarding both commercial and inter-institutional agreements. This means that such agreements can be signed between the RNEC and other public (such as Law Enforcement) or private actors, implying they can access and use the biometric databases constructed by the RNEC, without any risk assessments or prior consideration of the impact on human rights. This state of affairs translates into poor accountability and oversight, as well as poor visibility into the use of and level of access to the RNEC database of very sensitive personal data.

Specifically, PI and Karisma draw attention to the following findings and practices which are being deployed without the necessary safeguards and human rights due diligence:

- The acquisition of the multibiometric system ABIS by the Colombian police, which relies on accessing copies of the RNEC database, and the lack of regulation regarding its use and scope.[15]

- The differentiated use of biometrics based on the target population, illustrated by the use of three different biometric systems (facial

[15] El sistema multibiométrico ABIS de la Policía Nacional (The National Police's Multibiometric ABIS system). Available at: https://digitalid.karisma.org.co/2021/07/01/ABIS-reconocimiento-facial/

recognition, iris recognition and fingerprints) exclusively for the registration and surveillance of Venezuelan immigrants entering Colombia.[16]

- The use of biometric technology for the surveillance of public spaces such as the Transmilenio public transport system in Bogotá. [17]

PI recommends to the UN Human Rights Committee to include the following in the LoI and ask the Colombian government:

- To clarify what steps are being taken to ensure that the use of biometric databases established by the RNEC are effectively regulated and respect Colombia's national and international human rights obligations?

- What measures, if any, the government is taking to guarantee that the use of biometric technologies in various sectors are respectful of human rights and align with Colombia's national and international human rights obligations?

- What due diligence and procurement processes exist to regulate and oversee the acquisition of biometric technology by the government and its provision by the private sector?

[16] Biometría para entrar al país: el Estatuto Temporal de Protección a Migrantes Venezolanos (Biometrics for entering the country, the Temporal Statute for the Protection of Venezuelan Migrants). Available at: https://digitalid.karisma.org.co/2021/07/01/sistema-multibiometrico-etpmv/

[17] El Sistema Integrado de Videovigilancia Inteligente para Transmilenio (SIVIT) (The Integrated Intelligent Videovigilance System for Transmilenio (SIVIT)). Available at: https://digitalid.karisma.org.co/2021/07/01/SIVIT-reconocimiento-facial/