Regional Report

Digital Identity in Latin America and the Caribbean: Current Situation, Trends, and Issues

Greater Internet Freedom

Derechos Digitales

June 2023

Acknowledgments

We would like to express our gratitude to Derechos Digitales (DD) and DD researchers, Carlos Guerrero, and Paloma Lara Castro, who conducted this research and authored this report.

Derechos Digitales is an independent, non-profit organization with a Latin American scope, founded in 2005, whose main objective is the development, defense and promotion of human rights in the digital environment. The work of the organization focuses on three fundamental axes:

- Freedom of expression.
- Privacy and personal data.
- Copyright and access to knowledge.

We are also grateful to all the communities and individuals who generously shared their time, experiences, and perspectives with us, and contributed to the research process. Specifically, we would like to thank the following individuals who participated in the interviews and/or provided feedback on the different versions of the report: Daniel Vizuete (CTS-Lab of FLACSO); Diego Alvarez (Niubox Legal); Rafael Bonifaz (DD); and Ricardo Chica Reino (Citizenship and Development Foundation).

This report is published under the USAID Greater Internet Freedom (GIF) project implemented by Internews and the GIF consortium.

This report is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of the DD and do not necessarily reflect the views of USAID or the United States Government.

Table of Contents

Executive Summary

This report focuses on the Latin America and the Caribbean (LAC) region and is part of a multi-region research seeking to identify and compare the state of biometrics and digital identity threats, usage, and impact in Africa, the Balkans, Central Asia, Latin America and the Caribbean, and South and Southeast Asia.

The report provides an overview of the level and nature of digital identity (ID) adoption in four LAC countries, namely Bolivia, Brazil, Colombia, and Ecuador, with a focus on three types of digitalized ID systems. These include: (a) foundational digital identity systems; (b) digital identity systems based on the mandatory registration of mobile lines or equipment for police purposes; and (c) functional digital identity systems used in specific areas, such as health and social security.

We align with the *Instituto de Tecnologia & Sociedade do Rio* (ITS Rios) statement in its report "*Good ID in Latin America: Strengthening appropriate uses of Digital Identity in the region"*[1] that there is no basic difference between digital identity (ID) systems and state surveillance systems. While these two systems pursue different theoretical objectives, in practice they can overlap, giving raise to human rights concerns, particularly on the protection of the right to privacy.

The most notable concern noted in this report is the potential of digital ID systems to be integrated into broader state surveillance infrastructure, resulting in the consolidation of personal data, and increasing surveillance potential. As examined below, digital ID databases are accessible by a wide range of state and private entities, raising concerns about the scope, safeguards, and transparency of these exchanges.

The key findings are summarized in detail below and explored extensively in the report.

[1] ITS Río (2020). Good ID in Latin America: Strengthening appropriate uses of Digital Identity in the region (Page 11). See: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf.

Key Findings

This report details the following findings:

- **Finding 1:** all four researched LAC countries have implemented digital ID systems and deployed biometric technologies for foundational and/or functional purposes.
- **Finding 2:** most LAC countries favor centralized digital ID models, instead of decentralized, federated, or open market digital ID systems.
- **Finding 3:** all four researched LAC countries are collecting and processing biometric data in one or multiple digital ID databases without prior human rights assessment.
- **Finding 4:** some suppliers of surveillance technologies to LAC governments are similar to the suppliers of digital ID and biometric technologies.
- **Finding 5:** ambiguity latent in the 'digital ID' concept has enabled LAC countries to continuously expand the legal remit of their digital ID databases beyond identification to encompass any purposes marked as a state need, including migration control, and the delivery of social security programs. The failure to impose limits on the purpose and scope of digital ID systems prevents stakeholders, such as CSOs, charged with ensuring transparency, accountability, and the protection of individuals' rights from assessing the level of threats and risks to human rights against pre-set limits.

Recommendations

States and national governments in the LAC region are urged to:

- Conduct human rights impact assessments (HRIAs) prior to the implementation of digital ID systems and monitor their implementation to respond to human rights impact;
- Develop mechanisms of accountability and participation of multiple stakeholders prior to and during the implementation of digital ID systems and processes;
- Amend identity laws to make collection of biometric data optional and delink individuals' access to public and private services from the mandatory provision of biometric data.

Civil society organisations in the LAC region are urged:

- Conduct further and deeper research on digital ID in the broader LAC region;
- Pursue advocacy campaigns and undertake strategic litigation contesting digital ID systems that impact human rights.

This document provides an overview of digital ID in four researched LAC countries with the additional hope that these findings inspire governments and civil society to coordinate for rights-respecting digital ID systems.

Introduction

In the last decades, the global trend of implementing digital identity (ID) systems has consolidated under techno-solutionist arguments that present technologies as "solutions" to different social problems, often canvassed as part of digitalization and digital transformation efforts. Digital identity systems have been embraced by the public sector, allowing for their integration into the digitalization of vital services, such as healthcare, tax payments and social security.

States argue that the current technology allows the development of more reliable, resilient, and sustainable systems compared to traditional systems based on paper. In the LAC region, states have integrated digital ID into their identification systems for varying purposes, including streamlining their service delivery through the unique identification of people. Notably, many LAC countries rely on centralized identification registries or databases that capture, and process data associated to individual's identity, and that, in many cases, condition their access to social benefits.

Guided by Target 16.9 of the Sustainable Development Goals (SDGs) encouraging states to 'provide legal identity for all, including free birth registration,'[2] some LAC governments have expressed their interest in providing legal identity through digitized ID systems. These efforts continue to be supported by international development organizations and financial institutions, such as the World Bank,[3] which support and, in some cases, have actively collaborated in the development of digital ID systems.

The right to be recognized as a person before the law is an inalienable, universal right under Article 6 of the Universal Declaration on Human Rights (UDHR) and Article 16 of the International Covenant on Civil and Political Rights (ICCPR).[4] Despite this, we reiterate that

[2] UN. Sustainable Development Goals, Goal 16, Target 16.9. See: https://sdgs.un.org/goals/goal16.
[3] Examples include the ID4D project of the World Bank. See: https://id4d.worldbank.org/about-us
[4] OHCHR. UDHR. See: https://www.ohchr.org/en/universal-declaration-of-human-rights#:~:text=The%20Universal%20Declaration%20of%20Human%20Rights%20(UDHR)%20is%20a%20milestone,rights%20to%20be%20universally%20protected. OHCHR. ICCPR - General Assembly resolution 2200A (XXI). See: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

the right to identity does not equate to making identification a mandatory requirement.[5] Further, while identity and biometric technologies can simplify processes and expedite the delivery of public and private services, it is important to note that the requirement to have a legal identity is not contingent upon the implementation of digital identification systems. Additionally, there is no unique, standardized system that is applicable to all countries and contexts, noting that each country must assess its own internal needs and objectives prior to the deployment of digital ID systems.

Critically, digital ID systems are promoted as beneficial for developing counties with weak or ineffective identification systems. However, these broad and technology-centric assertions fail to promote simultaneous solutions to address substantial disparities in Internet and Information and Communication Technologies (ICT) access across different generations, geographical locations, socio-economic statuses, and gender. These disparities highlight existing inequalities that must be tackled through alternative public policy measures. [6]

This report observes that digital ID systems have gone far beyond the sphere of identification, generating potential impacts on human rights associated with state surveillance and the deepening of pre-existing discrimination situations. Through an open letter, an international digital rights non-profit organization, Access Now, and 73 signatories urged the World Bank and other international organizations to "take immediate action to end activities that promote harmful models of digital identification (digital ID) systems."[7]

[5] ITS Río (2020). Good ID in Latin America: strengthening appropriate uses of Digital Identity in the region. See: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf.
[6] Barbosa, A. Carvalho, C. Machado, C. Costa, J (2020). Good ID in Latin America: strengthening appropriate uses of Digital Identity in the region. See: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf
[7] Access Now (2022). Open Letter: The World Bank and its donors should protect human rights in the digital ID systems. See: https://www.accessnow.org/press-release/carta-abierta-el-banco-mundial-sistemas-de-identificacion-digital/.

This underscores the urgency of taking immediate action against the human rights risks posed by digital identity systems, including:[8]

Broad Justification and Insufficient Legal Frameworks: The incorporation of digital and biometric technologies is broadly justified as beneficial without sufficient and compelling evidence, and without an accompanying comprehensive legal framework.

Poor Stakeholder Engagement: Digital ID systems are deployed in an exclusionary manner, without the participation of multiple stakeholders.

Deployment of Digital ID Systems without Proper Safeguards: States in the LAC region have deployed various technologies, including biometric technologies, with the capacity to process personal data, albeit with inadequate data security and protection measures, limited transparency, and insufficient human rights safeguards, such as prior human rights assessments, and independent oversight mechanisms.

Failure to Mitigate and Address Human Rights Risks Posed by Digital ID Systems: This was illustrated in the cases of Aadhaar in India; Huduma Namba in Kenya; and the Sistema Patria in Venezuela. As Derechos Digitales has mentioned in previous research,[9] the use of digital ID systems, especially those integrating biometric technologies, for access to basic resources not only affects the right to privacy, but also directly harms the right to integrity, autonomy, and dignity. Digital ID systems can foster, reinforce, or deepen situations of discrimination and the exclusion of vulnerable and historically excluded groups, particularly in the context of social protection programs. This is most glaring in the health context, where risks are exacerbated for vulnerable and marginalized populations, such as women, persons with disabilities, the elderly and the LGBTIQ+ community.

[8] Center for Human Rights & Global Justice, NYU School of Law (2022). Paving a Digital Road to Hell? A primer on the role of the World Bank and Global Networks promoting Digital ID. See: https://chrgj.org/wp-content/uploads/2022/06/Report_Paving-a-Digital-Road-to-Hell.pdf.

[9] Díaz, M. (2018). El cuerpo como dato. Derechos Digitales. See: https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf *y* https://www.derechosdigitales.org/wp-content/uploads/sistemas-de-Identificacion_ES.pdf.

In the digital age, the right to privacy has become an access door to the protection of many other rights.[10] The UN's Resolution 68/167 of 2014 on the right to privacy in the digital age states that the right to privacy requires strong protection as "a necessary precondition for the protection of values such as freedom, dignity, and equality from government intrusion," and "an essential ingredient for democratic societies….". Despite this access door, digital ID systems threaten the right to privacy, with an impact on the protection and fulfilment of other human rights.

Instructively, data collection never takes place in a neutral environment and must be framed within a country's operating environment, particularly its social environment. The processing of sensitive data poses risks to communities in vulnerable situations. For example, women, and particularly lesbian, gay, bisexual, intersex, and transgender (LGBTQI+) people, may experience stigma, marginalization, and violence following the exposure of private information related to their sexual and reproductive history, sexuality, and/or identity.

Human rights organizations and mechanisms have expressed their concern about the growing use of technologies, which do not comply with the three-part test on legality, necessity, and proportionality, or the purpose limitation in data protection laws.[11] One of the core concerns raised by actors in the digital ID space is 'mission creep,' which carries surveillance implications.[12] LAC states have been going beyond the original purpose of digital ID systems, raising queries about their differentiation from surveillance systems.

This situation is particularly alarming, given the historical context of surveillance in the LAC region, and the absence of independent oversight mechanisms due to institutional vulnerabilities. In some cases, states implementing digital ID systems do not have laws on

[10] UN. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32 (2015) and UN. General Assembly Resolution 68/167, A/HRC/13/37 and Human Rights Council resolution 20/8). See https://undocs.org/A/HRC/29/32.

[11] Office of the United Nations High Commissioner for Human Rights (2014). The right to privacy in the digital age, A/HRC/27/37. See: https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

[12] Omidyar Network (2019). Five Surprisingly Consequential Decisions Governments Make About Digital Identity. See: https://omidyar.com/five-surprisingly-consequential-decisions-governments-make-about-digital-identity/.

the protection of personal data capable of comprehensively governing data collection and processing, including the exchange of data amongst public-public and public-private entities. This can impact specific groups, namely human rights defenders, activists, and journalists.

Globally, actors are querying the relevance and need for digital ID systems and the adoption of biometric technologies. This report notes that some of the biometric technologies being deployed in digital ID systems are similar in nature to those used in state-surveillance systems. This suggests that the specific issues and risks present in surveillance systems are likely to arise in digital ID systems, with these risks being intensified further by the historical context of continuous state surveillance in the LAC region. The potential for mass surveillance latent in digital ID systems and biometric databases was highlighted by the United Nation's Office of the High Commissioner for Human Rights (OHCHR), as follows:

> *"Across a range of countries, identity systems are linked to extensive central storage of personal data, including biometric information such as fingerprints, facial geometry, iris scans and DNA. Moreover, databases are often interlinked and made available for searching by other agencies. As a consequence, identifying individuals wherever they are located has become easier and easier."*[13]

Actors have called for a range of solutions to the challenges of a burgeoning surveillance industry, ranging from a review of adoption and governance processes to the establishment of moratoriums on the use of biometric technologies.[14] While the United Nations High Commissioner for Human Rights call for a moratorium on the production and sale of surveillance systems did not focus on digital ID systems, we argue that the OHCHR's argument above expands this call to cover digital ID systems, in recognition of the human rights risks latent in these systems.[15]

[13] OHCHR (2022). The right to privacy in the digital age. See: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F51%2F17&Language=E&DeviceType=Desktop&LangRequested=False.

[14] UN News (2021). Urgent action needed over artificial intelligence risks to human rights. See: https://news.un.org/en/story/2021/09/1099972.

[15] *Ibid.*

Methodology

Table 1: *Research Topic and Research Question (by DD)*

Research Topic	Exploratory Study: The Level of Adoption and Use of Digital Identity Systems and Biometrics in Latin America & the Caribbean (LAC)
Research Questions	a. What digital ID systems have been adopted in Bolivia, Brazil, Colombia, and Chile? b. What are the emerging trends on the development and adoption of digital identity systems and biometrics in the Latin American region? c. What risks do digital identity systems pose to human rights?

This report consolidates information in the LAC region and offers an exploratory analysis on the current state of digital ID systems and specific human rights risks latent in these systems. Given its exploratory nature, this report adopted a qualitative approach restricted to a desk review of secondary and tertiary sources, mainly documents produced by civil society organizations, private sector, and international organizations.[16] This research methodology is appropriate for exploring complex and nuanced topics in a region with varying levels of digital ID deployment for functional and foundational purposes.[17]

The researchers selected four countries for exploration, informed by digitization initiatives at the government level, digital divide considerations, and the amount of information available on the implementation of digital identity systems.

To analyze collected information we relied on the guide *'¿Qué buscar en los sistemas de Identidad Digital? Una tipología de etapas,'*[18] proposed by the Engine Room (a non-profit organisation), and used several concepts located in '*Governing ID: Principles for Evaluation'*[19] developed by the Centre for Internet & Society (a non-profit organisation), which outlines

[16] The complete list can be consulted in the Literature Review document.

[17] Following the terminology proposed by the World Bank, the main difference between a foundational digital identity system and a functional one is that the former is usually always a mandatory record that, in addition to identification, can serve other purposes, while the latter is created for sole purpose.

[18] The Engine Room (2019). ¿Qué buscar en los sistemas de Identidad Digital? Una tipología de etapas. See: https://www.theengineroom.org/wp-content/uploads/2019/11/Digital-ID-Typology-Espan%CC%83ol-The-Engine-Room.pdf.

[19] Centre for Internet and Society India (2020). Governing ID: Principles for Evaluation. See: https://digitalid.design/docs/CIS_DigitalID_EvaluationFrameworkDraft02_2020.01.pdf.

parameters for evaluating digital identity systems. The final text of this report has been reviewed by members of other allied organizations and experts from the region to correct errors and inconsistencies. This report is the sum of all these efforts.

Research Limitations

This research report was limited by the following:

- **Assumptions in sources**: this report relied on publicly accessible material, with the reviewed studies and reports containing the assumptions of respective authors in their individual and professional capacities.

Glossary of Terms

Biometrics	This document relies on the World Bank's definition of biometrics as "the use of electronically captured facial features, iris patterns or fingerprints to authenticate a person's identity."[20]
Digital Identity (ID)	This document relies on the World Bank's definition of digital identity as "a set of attributes and/or credentials collected and stored electronically that uniquely identifies a person."[21]
Digital ID System	This document relies on the World Bank's definition of digital identity systems as "an identification system using digital technology during the whole life cycle of the identity, even for data collection, validation, storage and transference;

[20] World Bank Group, 'Brief on Digital Identity,' https://thedocs.worldbank.org/en/doc/413731434485267151-0190022015/render/BriefonDigitalIdentity.pdf, accessed 24 April 2023.
[21] Digital identity: See: https://id4d.worldbank.org/guide/glossary

> management of credentials; and verification of identity and authentication."[22]

Results: Current Situation of Digital ID Systems in LAC

This section provides an overview of three digital ID systems in four LAC countries, namely Bolivia, Brazil, Colombia, and Ecuador. The three digital ID systems include: (a) Foundational digital ID systems; (b) Digital ID systems created via the mandatory registration of mobile lines or digital equipment; and (c) Functional digital ID systems used for specific purposes, including health, social security, and migration control.

1. Bolivia

In *República de Bolivia* (Republic of Bolivia or Bolivia), the two core digital ID systems that capture individuals' digital identity data include the *General Personal Identification Service* (SEGIP) and the *Civil Registry Service* (SERECI).[23] The SEGIP is supervised by the Ministry of Government and is charged with issuing identity cards, whereas SERECI is administered by the Supreme Electoral Court.[24] Some features of these systems are: mandatory registration, biometric data collection, and, in the case of SEGIP, availability of a digital version of the identity document via mobile application.[25]

[22] Digital identity system: An identification system using digital technology during the whole life cycle of the identity, even for data collection, validation, storage and transference; management of credentials; and verification of identity and authentication (free translation). See: https://id4d.worldbank.org/guide/glossary

[23] Venturini, Jamila; Díaz, Marianne (2021). Identification and social protection systems in Venezuela and Bolivia: surveillance, gender and human rights (Pages 26-28). See: https://www.derechosdigitales.org/wp-content/uploads/sistemas-de-Identificacion_ES.pdf.

[24] UNHCR, OAS, CLARCIEV (2020). Regional Study on Late Birth Registration, Issuance of Nationality Documents and Statelessness. See: https://www.refworld.org.es/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=61a9765b4.

[25] Diario La Razón (2023). Segip activates 'My Identity' to carry the identity card and license digitally. See: https://www.la-razon.com/sociedad/2023/02/24/el-segip-presenta-mi-identidad-para-facilitar-tramites-y-portar-el-carnet-de-identidad-y-la-licencia-de-forma-digital/.

In 2009, the *Registry of Ownership of Mobile Terminal Equipment and Registry of Account Holders* was created under the Supreme Decree No. 0353. This registry incudes, among others, data of the account holder, IMEI code, mobile number. Some features of this system are mandatory registration, prevention of mobile theft, and accessibility of the database to public and private entities.

Further, there are several functional digital ID systems in specific areas, particularly for social security. Digitized databases are used for the monetary transfer of economic assistance, including the *Bono Juana Azurduy,* and pension schemes such as *Renta Dignidad*. Registration in these databases is voluntary and accessible to both public and private entities.[26]

2. Brazil

In *República Federativa do Brasil* (Federative Republic of Brazil or Brazil), three core digital ID registries that capture individuals' digital identity data include the *Sistema Nacional de Informações de Registro Civil* (National Civil Registration Information System or SIRC) maintained by the *Instituto Nacional do Seguro Social* (National Institute of Social Security or INSS), the Elective Terms in Office – Higher Electoral Court maintained by the *Tribunal Superior Eleitoral* (Higher Electoral Court or TSE and *Receita Federal do Brasil* (Brazilian Internal Revenue System or RFB) maintained by the *Receita federal do Brasil* (Federal Revenue Secretariat of Brazil).[27] Some features of these systems are that registration in the SIRC and the TSE systems is mandatory, that TSE always collects biometric data, and that all three provide a physical or digital card that can be used as an identity document.[28]

[26] Venturini, Jamila; Díaz, Marianne (2021). Identification and social protection systems in Venezuela and Bolivia: surveillance, gender and human rights (Pages 29-42). See: https://www.derechosdigitales.org/wp-content/uploads/sistemas-de-Identificacion_ES.pdf.
[27] World Bank (2021). Enrollment and eligibility process of Brazil's Auxílio Emergencial: Data processing and use of administrative registries. See: https://documents1.worldbank.org/curated/en/099255012142136232/pdf/P1748360d7131402e086730fbce1d687fa1.pdf.
[28] Data Privacy BR (2022). Between visibility and exclusion: Mapping the risks associated with the National Civil Identification System and the usage of its database by the GOV.BR platform. See: https://www.dataprivacybr.org/wp-content/uploads/2022/11/Policy-paper-Data-Privacy-Brazil-Research-BETWEEN-VISIBILITY-AND-EXCLUSION.pdf

In 2017, the creation of a new digital ID system called the *National Civil Identification* (ICN) was approved under Law No. 13.444, which establishes the launch of a database composed of different registrations such as the SIRC, TSE, among others, and the issuance of a new identity document. One of the immediate objectives of this system is to offer access to government services through the Portal of the Government of Brazil, *Gov.br.*[29]

Finally, there are several functional systems, with the most relevant system being used for social security purposes. The *Cadastro Único* (CadÚnico) is a database maintained by the federal government of Brazil and managed by the governments of each state, from which beneficiaries of economic assistance such as *Bolsa Família*, *ID Jovem*, *Carteira do Idoso*, among others, are identified. The registration in these databases is voluntary and the database is accessible to public entities.[30]

3. Colombia

In *la República de Colombia* (the Republic of Colombia or Colombia), the most important digital ID system that captures individuals' digital ID data, the unique identification register, is maintained by the *Registraduría Nacional del Estado Civil* (National Civil Registry or RNEC), which is charged with managing and organizing civil registration and identification of persons.[31] Some features of this system are mandatory registration, collection of biometric data and availability of a digital version of the identity document via mobile application.[32]

In 2011, Decree No. 1630 mandated registration of all mobile equipment acquired for the first time, creating the International Mobile Equipment Identity (IMEI) registry. This database is comprised, among others, of the data of the equipment holder, IMEI code, and

[29] *Ibid.*
[30] ITS Río (2020). Good ID in Latin America: Strengthening appropriate uses of Digital Identity in the region (Páginas 49-50). See: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf
[31] Registraduría Nacional del Estado Civil, Corporación Opción Legal & UNHCR (2013). Strengthening the National Civil Registry to assist displaced populations or those at risk of displacement. See: https://www.acnur.org/fileadmin/Documentos/Publicaciones/2013/9159.pdf?file=fileadmin/Documentos/Publicaciones/2013/9159.
[32] Fundación Karisma (2021). The facial recognition system of the National Registry. See: https://digitalid.karisma.org.co/2021/07/01/sistema-reconocimiento-facial-registraduria/.

mobile number. Some features of this system are mandatory registration, prevention of mobile theft and accessibility of the database to public entities.[33]

Finally, there are several functional systems, with the most notable system being used for migration control purposes. The *Registro Único de Migrantes Venezolanos* (Single Registry of Venezuelan Migrants or RUMV) is a database maintained by the Ministry of Foreign Affairs through the *Special Administrative Unit for Migration Colombi*a. The RUMV seeks to identify Venezuelan migrants in Colombia and determine their immigration status.[34] The registration in this database is mandatory and collects biometric data.[35]

4. Ecuador

In *República del Ecuador* (Republic of Ecuador or Ecuador), the government has developed multiple digital ID systems (*see Annex 1 below for a more detailed exploration*). Ecuador's foundational ID system is managed by the *Dirección General de Registro Civil, Identificación y Cedulación* (DIGERCIC, or the *General Directorate of Civil Registration, Identification, and Identification Card Issuance,* or Civil Registry). The foundational ID system is comprised of three databases, including births and deaths, civil registration, and identification. These centralized databases contain biometric data and are used to provide different identification services for both public and private sector.[36]

The government has also launched functional identification systems for policing purposes. A few examples include the Register of Lost, Stolen or Robbed Mobile Devices, and,

[33] Fundación Karisma (2020). Ensayo y error: Análisis de la efectividad del registro de celulares. See: https://ia801700.us.archive.org/9/items/karisma-ensayo-error-2020-1/Karisma-Ensayo-Error-2020-1.pdf.

[34] Paula Rossiasco and Patricia de Narváez (2023). Adapting public policies in response to an unprecedented influx of refugees and migrants: Colombia case study of migration from Venezuela - Background paper to the World Development Report 2023: Migrants, Refugees, and Societies. See: https://thedocs.worldbank.org/en/doc/7277e925bdaa64d6355c42c897721299-0050062023/original/WDR-Colombia-Case-Study-FORMATTED.pdf.

[35] Fundación Karisma (2021). Biometría para entrar al país: el Estatuto Temporal de Protección a Migrantes Venezolanos. See: https://digitalid.karisma.org.co/2021/07/01/sistema-multibiometrico-etpmv/.

[36]Dirección General de Registro Civil Identificación y Cedulación. Trámites y Servicios Institucionales. See: https://www.gob.ec/dgrcic.

ostensibly, the Integrated Security Service (ECU 911) emergency platform.[37] It has also recently developed a system to enable remote voting.

[37] Danilo Corral-De-Witt *et al.,* (2018). From E-911 to NG-911: Overview and Challenges in Ecuador. See: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1629&context=electricalengineeringfacpub.

Analysis I: Trends on Adoption of Digital ID Systems

1. Preference for Centralized ID Databases

Among the analyzed LAC countries, there seems to be an evident division between countries maintaining centralized digital ID systems managed by a single entity and countries where ID systems are decentralized. In the first group are Colombia and Ecuador, whereas Bolivia and Brazil are in the latter group. It is important to note that Brazil is a federal and constitutional republic, which explains the multiplicity of registries and entities that provide identity services.

We note that centralized registration systems have facilitated a swifter adoption and implementation of digital ID and biometric technologies into identification systems, as evidenced in Colombia and Ecuador. Different organizations have highlighted the serious risks involved in creating and maintaining centralized databases.[38] Generally, the adoption of centralized databases processing biometric data by government agencies for service provision poses a significant risk to the protection of the right to privacy. Centralized ID databases create a single point of failure for large amounts of individuals' personal and sensitive personal information. Contextually, government agencies in LAC region have been subjected to ransomware attacks, resulting in systems and services being shutdown to prevent further website and database intrusions.[39]

Further, centralized databases limit individuals' control and ownership of their personal and sensitive data and grant unlimited access and control to the managing authority. In Ecuador, there is a lack of clarity regarding the legal framework that supports the development of digital ID systems, especially in the case of the Civil Registry. Further,

[38] Privacy International (2021). Digital National ID systems: Ways, shapes and forms. See: https://privacyinternational.org/long-read/4656/digital-national-id-systems-ways-shapes-and-forms.
[39] Security Week (2022). Ransomware Attacks Target Government Agencies in Latin America. See: https://www.securityweek.com/ransomware-attacks-target-government-agencies-latin-america/.

despite the enactment of the Personal Data Protection Organic Law on May 26, 2021, this has not yet been enforced.[40] Additionally, the ECU 911 system has facial recognition capabilities that enable the government to track individuals' phones, which poses very serious risks to the right of privacy.[41]

On the other hand, the second group of countries have different identification registration processes and different entities charged with their maintenance. While decentralized databases generally prioritize empowering users to maintain ownership and control over their identity data, with a reduced risk of data breaches, they make it difficult to establish a unified and interconnected identity infrastructure (or interoperability challenge). Despite this, there are initiatives aimed at centralizing the databases for countries in the second group. In 2017, Brazil approved a new system to unify all its identity registrations into a single database.[42]

This leads to the conclusion that there is a trend to favor the centralized digital ID model in the LAC region compared to other options such as the decentralized, federated, or open market models.[43]

2. Increased Processing of Biometric Data Without Sufficient Human Rights Safeguards

The number of private sector companies that develop biometric technologies and the number of States that have implemented these technologies has grown exponentially.[44] As

[40] DLA Piper (2023). Data Protection Laws of the World: Ecuador. See: https://www.dlapiperdataprotection.com/index.html?t=law&c=EC#:~:text=Since%20May%2026%2C%202021%2C%20Ecuador,well%20as%20its%20corresponding%20protection.

[41] The Verge (2019). The NYT investigates China's surveillance-state exports. See: https://www.theverge.com/2019/4/29/18522248/china-surveillance-state-exporting-ecuador-senain-ecu-911-privacy-facial-recognition-tracking.

[42] Data Privacy BR (2022). Between visibility and exclusion: Mapping the risks associated with the National Civil Identification System and the usage of its database by the GOV.BR platform. See: https://www.dataprivacybr.org/wp-content/uploads/2022/11/Policy-paper-Data-Privacy-Brazil-Research-BETWEEN-VISIBILITY-AND-EXCLUSION.pdf.

[43] World Bank (2023). Types of ID systems. See: https://id4d.worldbank.org/guide/types-id-systems.

[44] Asociación por los Derechos Civiles (2019). Tu yo digital – Descubriendo las narrativas sobre identidad y biometría en América Latina (Page 6). See: https://adc.org.ar/informes/tu-yo-digital-descubriendo-las-narrativas-sobre-identidad-y-biometria-en-america-latina/.

stated by *La Asociación por los Derechos Civiles* (ADC) in the report, *Your Digital Self – Uncovering the Narratives on Identity and Biometrics in Latin America,* several LAC countries have built with relative success "narratives linked to the need for biometric technology for the infallible recognition of people's identity"[45] permitting the collection and processing of biometric data in foundational and functional ID systems under broad arguments and without pre-established limits to its use. This is consistent in both unitary and federal countries in the LAC region.

As magnified above, all analyzed countries, through the managing government entities, are collecting and processing biometric data in one or multiple digital ID databases without conducting prior human rights impact assessment to identify and measure the effect of this collection on individuals' human rights. This situation has permitted the implementation of biometric identification and authentication systems with fingerprint and facial recognition capabilities, exponentially increasing the dangers associated to state surveillance, in addition to security breaches. The researchers were unable to locate any publicly available human rights impact assessment studies or reports for the implemented digital ID systems in all focus countries.

The collection of biometric data in countries such as Brazil and Colombia is undertaken without proper legal basis. Despite both countries having enacted data protection laws, the collection of biometrics has not been expressly and precisely outlined by law, thus defying the principle of legality.[46] Without clear parameters on biometric data collection, their uses and delimitations, the states in question have the leeway to use this data for multiple purposes.[47]

Bruno Bioni *et al.,* in a 2022 report examining Brazil's *Identificação Civil Nacional* (National Civil Identification System or ICN), demonstrated that a tension exists between the ICN and Brazil's data protection law. The report flagged that the ICN's architecture "[is] a largescale

[45] *Ibid.*
[46] *Ibid.*
[47] Data Privacy BR (2022). Between visibility and exclusion: Mapping the risks associated with the National Civil Identification System and the usage of its database by the GOV.BR platform. See: https://www.dataprivacybr.org/wp-content/uploads/2022/11/Policy-paper-Data-Privacy-Brazil-Research-BETWEEN-VISIBILITY-AND-EXCLUSION.pdf.

personal database, composed of the fusion of other databases, with a centralized structure, [that] presents risks in terms of data protection and privacy, such as possibilities of abusive secondary use of data, insecurity of data, and government surveillance."[48]

Different organizations have stated many times the serious risks involved in creating and maintaining centralized databases.[49] Contrary to this, all countries analyzed in this report maintain one or several databases of this type, many of which contain biometric data.

However, the trend in the region seems to be aimed at deepening of these practices, which includes creation of functional digital identity systems that incorporate biometric data, even when the traditional systems on which they are based had not previously incorporated such information. This means that generally the adoption of any digital identity system would be a potential enabler for the proliferation of biometric technologies, some of them in especially critical areas such as public safety, access to social security services, and immigration control.

This leads to the conclusion that there is an emerging increase in the collection and processing of biometric data, guided by narratives presenting the inclusion of biometric data as necessary for the implementation of digital ID systems, without sufficient human rights safeguards.

3. Common Suppliers for Surveillance Technologies and Digital ID/Biometric Technologies

Reports by Access Now, an international digital rights non-profit organization, [50] and AlSur, a consortium of civil society and academia organizations in Latin America,[51] lead to the

[48] Bruno Bioni *et al.,* (2022). The digitization of the Brazilian national identity system: A descriptive and qualitative analysis of its information architecture. See: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/9383EF02D1892A5581D93F40348ABD16/S2632324922000141a.pdf/the-digitization-of-the-brazilian-national-identity-system-a-descriptive-and-qualitative-analysis-of-its-information-architecture.pdf.
[49] *Ibid, n, 36.*
[50] Access Now (2021). Surveillance Tech in Latin America: Made Abroad, Deployed at Home. See: https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf.
[51] AlSur (2021). Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa. See: https://www.alsur.lat/sites/default/files/2021-11/ALSUR_Reconocimiento_facial_en_Latam_ES.pdf.

conclusion that the technology market supplying governments with surveillance tools is dominated by few large providers, namely, AnyVision, Hikvision, Dahua, Cellebrite, Huawei, ZTE, NEC, IDEMIA, and VERINT, among others.

This report aligns with the statements of ITS Rios in its report *Good ID in Latin America: Strengthening appropriate uses of Digital Identity in the region*[52] that there is no basic difference between digital ID systems and a state surveillance system. This report notes that some of the listed suppliers of digital ID products and systems and biometric ID technologies are the same companies that provide states with surveillance technologies. Specifically, the French company IDEMIA (formerly OT-Morpho) provides or has provided digital ID services to Colombia.[53]

According to the referenced reports, the companies offering surveillance and biometric technologies show a lack of appreciation for the consequences their utilization will have on target populations in the LAC region. Furthermore, they generally display disinterest in establishing transparent standards, accountability mechanisms, and safeguards for human rights within their industry. This suggests that many surveillance technology providers do not adhere to the UN Guiding Principles on Business and Human Rights, particularly regarding their commitment to respect human rights, implement due diligence processes to identify and prevent significant harm to human rights, and openly disclosing information on their compliance with existing laws.[54]

[52] ITS Río (2020). Good ID in Latin America: Strengthening appropriate uses of Digital Identity in the region (Page 11). See: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf.
[53] Fundación Karisma (2021). The facial recognition system of the National Registry. See: https://digitalid.karisma.org.co/2021/07/01/sistema-reconocimiento-facial-registraduria/.
[54] Access Now (2023). Vigilancia biométrica remota en América Latina: ¿las empresas están respetando los derechos humanos? See: https://www.accessnow.org/wp-content/uploads/2023/04/ESPANOL-Analysis-Remote-biometric-surveillance-LATAM.pdf.

Analysis II: Risks of Digital ID to Human Rights

This section details the core risks of foundational or functional digital ID systems to human rights. This material is not exhaustive.

1. Ambiguity in Digital ID Concept Preventing Purpose and Scope Delimitations

There is no universally agreed definition of the 'digital ID' concept. International organizations such as the World Bank, the International Telecommunication Union (ITU), and the Organisation for Economic Co-operation and Development (OECD) have proposed definitions that are similar but that suffer from a core problem: they do not make it possible to delimit the purpose and scope of these systems.

While this ambiguity facilitates flexibility in public and private service delivery and encourages innovation, we note that it can also create inconsistent implementation practices, leading to fragmented and inefficient digital ID ecosystems. Further, the failure to adopt a universally agreed concept prevents the development of harmonized and standardized privacy and security standards, leading to variations in the level of privacy protection in LAC countries.

We express concern that this ambiguity has enabled LAC countries to continuously expand the legal remit of their digital ID databases beyond identification to encompass any purposes identified as a state need, including migration control, and the delivery of social security programs. Even when the use of certain terminology is agreed by consensus, if the limits on digital ID systems are not clearly and expressly provided, this prevents stakeholders, such as CSOs, charged with ensuring transparency, accountability, and the protection of individuals' rights from assessing the level of threats and risks to human rights against pre-set limits.

2. Poor Transparency and Limited Public Participation

Except in the case of Brazil, where the adoption of its new digital ID system has been carried out through a legal reform, the other three countries analyzed in this report have not effected digital ID changes to their identification processes and systems through a bill or other regulations that facilitate broad and participative discussion processes.[55]

In effect, this means that digitalized ID systems in some LAC countries have been implemented without transparency and public participation. For example, the government of Colombia implemented facial recognition technologies into the National Registry of Civil Status in 2018 but failed to publicize this measure.[56] This and other cases have gradually eroded the public's trust in the government regarding the use of these technologies.

Besides the lack of specific regulation on digital ID, not all analyzed countries have laws and regulations establishing specific limits to the adoption and use of these systems. For example, Bolivia does not currently have a law on protection of personal data, whereas other countries are facing implementation challenges.[57]

[55] Asociación por los Derechos Civiles (2019). Tu yo digital – Descubriendo las narrativas sobre identidad y biometría en América Latina (Page 28). See: https://adc.org.ar/informes/tu-yo-digital-descubriendo-las-narrativas-sobre-identidad-y-biometria-en-america-latina/.
[56] Fundación Karisma (2021). The facial recognition system of the National Registry. See: https://digitalid.karisma.org.co/2021/07/01/sistema-reconocimiento-facial-registraduria/.
[57] Fundación Internet Bolivia (2021). Conectados y protegidos: Estado del acceso a Internet y la protección de datos personales, tendencias y desafíos en América Latina (Pages 27-35). See: https://internetbolivia.org/file/2021/11/ib_conectados.pdf.

Conclusion and Recommendations

This report reveals that digital ID systems are used for both functional and foundational purposes in four LAC countries examined in this report, and all four countries are collecting and processing biometric data for varying purposes. Notably, some digital ID systems are in an initial stage, while others have already enabled the provision of government services. These ID systems are mainly centralized, and the researchers were unable to locate any publicly available human rights impact assessment studies or reports for the implemented digital ID systems in all focus countries. This leads to the conclusion that most LAC countries have not internalized human rights risks and provided mitigation measures to address the same.

Based on this, the report proposes the following recommendations to governments and civil society actors in four LAC countries.

Recommendations

This section presents a set of recommendations addressed to States and civil society organizations.

To States and National Governments

We urge States and national governments in LAC region to:

- **Conduct human rights impact assessments (HRIAs) prior to implementing digital ID systems and monitor their implementation to respond to human rights impacts:** HRIAs should comply with internationally recognized principles of legality, necessity, and proportionality. Where digital ID systems have already been implemented, we urge governments to publicly audit their digital ID systems and processes to assess and address the human rights impact.
- **Develop mechanisms of accountability and participation of multiple stakeholders prior to and during the implementation of digital ID systems and**

processes: Adopt a participatory approach to the implementation of digital ID systems by involving and engaging stakeholders in the design and implementation and ensuring that the public's input is incorporated into the final product. Guided by the transparency principle under international law, states should provide the public with sufficient notice on the intended adoption of a digital ID system, or any upgrades to the existing ID system, in a manner that allows meaningful engagement and debate.

- **Develop and/or adapt personal data protection legislation in accordance with human rights standards:** LAC states should enact or amend their data protection laws, clearly defining the rules and adopt differentiated safeguards for the proper collection and processing of sensitive data, particularly biometric data. Further, all authorities or entities charged with managing or implementing digital ID systems must adhere to national data protection laws or international data protection principles, prior to data processing, including conducting data protection impact assessments.
- **Establish sufficient safeguards in relation to the protection of data collected and stored in databases:** operationalize data protection authorities to enable the implementation of data protection safeguards and oversee entities processing data in digital ID systems. Specifically, personal data should be protected by reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure of data.
- **Amend identity laws to make the collection of biometric data optional:** states should delink individuals' access to public and private services from the mandatory provision of biometric data.

To Civil Society Organizations

We urge CSOs in the LAC region to:

- **Conduct further and deeper research on digital ID in the broader LAC region:** to identify uses and trends that this report has not managed to cover, given its

exploratory nature, including case studies to identify good practices with a human rights approach. We recommend the following topics as useful starting points:

- ❖ Comparison between digital ID systems developed in unitary and federal countries and how these differences impact human rights.
- ❖ Governmental narratives regarding the need to implement digital ID systems and how these have been received and addressed (when it has occurred) by the private sector or civil society.
- ❖ Financing of digital ID systems to identify which international organizations have been operating in the region and why they seek to promote these systems.

- **Pursue advocacy campaigns and undertake strategic litigation contesting digital ID systems that adversely impact human rights:** undertake advocacy and strategic litigation to challenge digital ID systems that do not comply with human rights principles on legality, necessity, proportionality, due process, control mechanisms and right to appeal, active transparency, prior impact assessment, democratic debate for its adoption, and guarantees for international cooperation.[58]

[58] Canales, María Paz; Lara, J. Carlos (2018). Propuesta de estándares legales para la vigilancia en Chile (2018). See: https://www.derechosdigitales.org/wp-content/uploads/propuesta-estandares-legales-vigilancia-chile.pdf.

Annex 1: Ecuador Case Study

Introduction

Studies around the world have concluded that the development of public policies and the deployment of digital identity systems can create serious human rights risks and deepen existing gaps, reinforcing or creating new types of discrimination.[59] In the same vein, international organizations have expressed concern about the use of intrusive technologies such as biometrics and facial recognition, which are often used in these systems, and have called for re-evaluating their adoption taking into account the international human rights law principles of necessity and proportionality.[60]

Within the framework of the Greater Internet Freedom (GIF) project, Derechos Digitales carried out exploratory research in 2023 to understand the level of adoption of digital identity systems in Latin America and the Caribbean, as well as to identify regional trends and problems. One of the results of this research was recognizing the need for case studies to analyze, in greater depth and detail, the processes for implementing technologies associated with digital identity and evaluating the scenario of risks and threats to personal rights, as well as potential advocacy and strategic litigation strategies.

Case Study Rationale

The country selected for exploration in this case study is the Republic of Ecuador, which was informed by various reasons. To begin with, there is sparse local research on digital identity systems that adopts a human rights focus. Finally, given that Ecuador shares common characteristics with its neighbors, such as Colombia, the results can serve as a guide for a detailed, future exploration of the digital ID systems in these countries, and beyond in the region.

[59] Refer to the bibliography section for more details.

[60] For example, the report "Standards for a Free, Open and Inclusive Internet" from 2017 by the Office of the Special Rapporteur for Freedom of Expression of the OAS (Organization of American States); Resolution No. 48/31 of 2021 of the Human Rights Council; and Resolution 77/211 of 2022 of the United Nations General Assembly.

During the drafting of this case study, a significant event occurred in Ecuador: on May 17, 2023, President Guillermo Lasso dissolved the National Assembly and called for General Elections, employing a constitutional mechanism known as “cross-party deadlock”. This action, which was the response to a process opened by the Assembly to impeach him, worsened the social and political crisis that Ecuador has been experiencing since the beginning of his government’s tenure in 2021[61]. This political situation significantly affected the dynamics of the interviews conducted for this case study, and in turn, raised queries about the need to pursue the research.

Before the events of May 17, this case study sought to reveal the level of local development of the three most common digital identity systems in the region, namely (a) foundational digital identity systems; (b) digital identity systems based on the mandatory registration of mobile lines or devices; and (c) functional digital identity systems used in specific domains. Regarding the findings, it was intended to analyze the scenario of risks and threats to rights, considering various elements such as the operational framework of the identified systems and the norms that typically pose limits on their development, such as personal data protection regulations.

However, after the Assembly was dissolved, a comprehensive review of the document was made, and the interview questions were adjusted to contextualize the findings, emphasizing elements that could be more relevant to the current situation in the country. Thus, although the first section, which describes the situation of digital identification systems, follows the pattern of the regional report, the sections on trends and issues have been adapted so that the information aligns with this new scenario.

How do the changes made appear? Prior to the review, ECU 911, the Integrated Security Service emergency platform, had been identified as the most important analysis vector since it is the largest state surveillance platform in the country, and it is unknown whether it interoperates with the Civil Registry's digital identity system. Similarly, the analysis of the electronic voting system had originally been shelved due to its minimal relationship with

[61] La República (2023). Ecuador's President Dissolves National Assembly Amid Impeachment Trial. See: https://www.larepublica.co/globoeconomia/el-presidente-de-e.

digital identity. However, after review, the analysis of ECU 911 has been expanded to address the potential role it could play during the interregnum. Additionally, the analysis of electronic voting was resumed, given its probable use in upcoming elections.

Finally, this case study offers a series of recommendations for the Ecuadorian government and Ecuadorian civil society organizations working on issues related to digital identity.

Methodology

This case study complements the Latin America and the Caribbean regional report "*Digital Identity in Latin America: Current Situation, Trends and Problems"* published under the USAID Greater Internet Freedom (GIF) project implemented by Internews and the GIF consortium. In this case study, we adopt the same exploratory approach, but provide more detailed, granular information within the framework of the analysis model used in the regional research. This approach was selected to ensure that both exploratory reports can be read as a *continuum*, composed of a general description and another more specific and analytical section.

This case study adopts a qualitative approach, consisting of secondary and tertiary desk research and supplemented by semi-structured interviews with key actors of the Ecuadorian digital ecosystem. These interviews permitted the researchers to validate, correct, and expand the information presented.

To analyze collected information we relied on the guide *'¿Qué buscar en los sistemas de Identidad Digital? Una tipología de etapas,'*[62] proposed by the Engine Room (a non-profit organization), and used several concepts located in '*Governing ID: Principles for Evaluation'*[63] developed by the Centre for Internet & Society (a non-profit organization), which outlines parameters for evaluating digital identity systems.

[62] The Engine Room (2019). ¿Qué buscar en los sistemas de Identidad Digital? Una tipología de etapas. See: https://www.theengineroom.org/wp-content/uploads/2019/11/Digital-ID-Typology-Espan%CC%83ol-The-Engine-Room.pdf.

[63] Centre for Internet and Society India (2020). Governing ID: Principles for Evaluation. See: https://digitalid.design/docs/CIS_DigitalID_EvaluationFrameworkDraft02_2020.01.pdf.

Similarly to the regional research, this text uses the definitions of *digital identity*[6] *and digital identity systems* proposed by the World Bank, allowing it to be read as a response to the research carried out by this body.[64] In the same way, we follow the line of thought proposed by the *Instituto de Tecnologia & Sociedade do Rio* (ITS Rios) in their report *'Good ID in Latin America: Strengthening Appropriate Uses of Digital Identity in the Region'*[65], in which they point out that within the concept of digital identity, certain systems identified by other studies as surveillance systems also fall into this category.

The dissolution of the National Assembly on May 17, 2023, has not impacted the methodology of this study; however, it influenced the interview questions and certain data analysis approaches. This is primarily so that the final outcome remains connected to the current situation in Ecuador.

Several rounds of review were carried out by the Derechos Digitales Digital Rights team, and regional experts, including some of the interviewees.

Results: Current Situation of Digital Identity Systems in Ecuador

The regional report documents that four countries under exploration as part of the GIF project have digital identity systems, both foundational and functional.[66] In most cases, the first ones are constituted by digitized databases of authorities responsible for civil records, while the latter include a wide range of systems, ranging from healthcare service provision to immigration control, and are operated by entities with competencies in those areas.

[64] **Digital identity**: A set of electronically captured and stored attributes and/or credentials that uniquely identify a person (free translation). **Digital identity system:** An identification system that uses digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication (free translation). The World Bank (2019). Practitioner's Guide: Glossary. See: https://id4d.worldbank.org/guide/glossary.
[65] ITS Río (2020). Good ID in Latin America: Strengthening appropriate uses of Digital Identity in the region (Page 11). See: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf.
[66] Following the terminology proposed by the World Bank, the main difference between a foundational digital identity system and a functional one is that the latter is generally a mandatory registration that, in addition to identification, can serve other purposes, while the former is created for a single purpose.

Likewise, a tendency to favor the creation of unified records and the mandatory collection of biometric data was identified.

This section presents an overview that identifies the current level of adoption of digital identity systems in Ecuador. This review is preliminary, non-exhaustive, and focusses on the description of three types of systems: a) Foundational digital identity systems; b) Digital identity systems based on mandatory registration of mobile lines or devices for law enforcement purposes; and c) Functional digital identity systems in specific domains, as well as related initiatives.

1. Foundational Digital Identity Systems

The most important digital identity system in Ecuador is the set of digitized personal records created and maintained by the *Dirección General de Registro Civil, Identificación y Cedulación* (DIGERCIC, or the *General Directorate of Civil Registration, Identification, and Identification Card Issuance,* or Civil Registry). At the regulatory level, this system is governed by the provisions *of the Constitutional Law on Management of Identity and Civil Data*, approved in 2016. This law establishes that the registration of persons in the registry is mandatory from birth, at which time biometric data is captured, and which will be updated, as necessary, over time.[67]

This system presents a unique combination of characteristics that may resemble or differ from other practices in the region. For example, Ecuador collects biometric data, such as fingerprint and facial images.[68] Ecuador has used the system to support the provision of online services, procedures, and online payments.[69] However, unlike Colombia, the Civil Registry creates and maintains not only databases of Ecuadorian citizens but also of foreign residents in the country.

[67] Official Registry, Government of Ecuador (2018). Organic Law on Identity and Civil Data Management. See: https://www.registrocivil.gob.ec/wp-content/uploads/downloads/2018/03/ley_organica_de_gestion_de_la_identidad_y_datos_civiles.pdf.
[68] *Ibid.*
[69] Government Portal of Ecuador. Online procedures. See: https://www.gob.ec/dashboard/tramites-en-linea.

It is also worth noting that the Civil Registry has utilized this system to provide identification services. One of these uses is the issuance of electronic signature certificates, an operation that is regulated by the *Law on Electronic Commerce, Signatures and Data Messages* approved in 2002[70]. The other is the direct sale of the service to private entities through the *National Citizen Identification System*, which operates under subscription agreements that do not have a clear legal basis, a practice that has also been identified in Peru's digital identity systems.[71]

2. Digital Identity Systems Based on Registers of Mobile Lines or Devices

In 2009, Resolution 191-07-CONATEL-2009 was approved, which created the *Standard that Regulates the Procedure for Enrolling Subscribers of Advanced Mobile Services (SMA) and Registering Lost, Stolen or Robbed Terminals* (the Standard). This Standard, which has been modified up to two times, orders the creation of two lists, one to allow the operation of devices (positive list) and the other to order their blocking (negative list). This system is managed by the *Telecommunications Regulation and Control Agency* (ARCOTEL) and is updated by telecommunications companies.[72]

The registry in Ecuador shares similar characteristics with its counterparts in the region, such as Bolivia, and Colombia. To begin with, it is mandatory and contains personal data of the owner, IMEI code, mobile number, as well as data associated with the status of the device (lost, stolen, etc.). On the other hand, the Standard states that access to this database is available to *Agencia de Regulacion y Control de las Telecomunicaciones* (*ARCOTEL, or* the Telecommunications Regulatory and Control Agency), but also to any other competent

[70] Ministry of Telecommunications Law on Electronic Commerce, signatures and data messages (2012). See: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Messajes-de-Datos.pdf.

[71] Hiperderecho NGO (2018). How does RENIEC (National Registry of Identification and Civil Status) sell our personal data? See: https://hiperderecho.org/2018/07/como-asi-reniec-vende-nuestros-datos-personales/.

[72] National Telecommunications Council (2019). Resolution 191-07-CONATEL-2009. See: https://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/07/191_07_conatel_20091.pdf.

entity or entity linked to “national security issues”, which is broad and has an undefined scope.[73]

3. Other Digital Identity Systems

Finally, there are other functional systems in specific domains. The most striking is the possible use of identity systems to complement the use of video surveillance cameras, particularly those equipped with facial recognition technologies. As Access Now, an international digital rights non-profit organization, points out in their report, ‘*Surveillance Tech in Latin America: Made Abroad, Deployed at Home,*’[74] these technologies have been deployed in Ecuador since 2002, with the alleged purpose of contributing to public security; many of these are part of the Integrated Security Service ECU 911 (ECU 911).[75]

Although the evidence suggests that the adoption of these systems is extensive, there is no official information available to determine whether these capabilities are used in conjunction with biometric databases, and if so, which entity maintains these databases. The report, ‘*Video Surveillance in Ecuador Violates Citizen Rights*,’ by the organization FUNDAMEDIOS, a regional non-profit organization defending digital rights in the Americas, points out that it is not possible to answer this question because the operational protocols of ECU 911 have been classified as confidential until 2028.[76]

There is also another system, the *Electronic Voting System Abroad,* that is even more obscured, despite its expected use in the general elections scheduled to take place in August 2023. The *Electronic Voting System Abroad* is a non-face-to-face electronic voting mechanism enabled by the National Electoral Council (CNE) to allow Ecuadorians residing abroad to vote.[77] This system validates the voter's identity by two methods, one of which is facial

[73] National Telecommunications Council (2012). Resolution TEL 535-18-CONATEL-2012. See: https://www.gob.ec/sites/default/files/regulations/2018-11/TEL-535-18-CONATEL-2012.pdf.
[74] Access Now (2021). Surveillance Tech in Latin America: Made Abroad, Deployed at Home. See: https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf.
[75] Government Portal of Ecuador (2018). Technological innovations of the ECU 911 for emergency care were presented at Smart City 2018. See: https://www.ecu911.gob.ec/innovaciones-tecnologicas-del-ecu-911-para-la-atencion-de-emergencias-se-presentaron-en-smart-city-2018/.
[76] FUNDAMEDIOS (2021). Video surveillance in Ecuador violates citizens' rights. See: https://www.fundamedios.org.ec/wp-content/uploads/2021/12/Inf.-Videovigilancia.pdf.
[77] National Electoral Board (2023). Telematic voting 2023. See: https://www.voto-telematico.cne.gob.ec/ayuda.

recognition. It is not clear with which database it operates, whether it is the electoral roll of the CNE or through interoperability with the Civil Registry.[78]

Analysis I: Trends in Digital Identity Systems in Ecuador

The regional report identified the following trends: the promotion of centralized digital identity models; the prevalence of narratives emphasizing the absolute necessity of biometric data collection; the widespread absence of inclusive approaches in the development of digital identity systems; and the existence of providers of digital identity products and services who also market surveillance-capable technologies.

This section presents an account of the main trends identified in the digital identity systems mapped in Ecuador. The study commences by examining the foundational trends identified in the regional report to replicate those observed in neighboring countries. However, the primary focus is on highlighting the distinctive characteristics that may be present in Ecuador. In some cases, the information has been refined based on information provided in the interviews. This information is preliminary and not exhaustive.

1. Ecuador Exemplifies Riskiest Digital ID Practices

Ecuador has a centralized database managed by the Civil Registry, and registration is mandatory for all people. The legislation on identification establishes the collection and storage of biometric data from registered individuals, even from birth. It should also be noted that this database documents information on both citizens and foreigners residing in the country, which is not commonly observed in the region. Similarly, the Civil Registry currently offers identity validation services to private individuals under interoperability agreements with questionable legal bases.

Regarding other systems, Ecuador maintains a mandatory registry of mobile lines and devices aimed at preventing theft and use for criminal purposes, since the database is

[78] National Electoral Board (2023). Telematic voting registration manual. See: https://www.voto-telematico.cne.gob.ec/_files/ugd/157be5_e34f007e38294a2d80257c514317ba8c.pdf?index=true.

accessible to any public entity for national security purposes. Further, the ECU 911 currently operates cameras with facial recognition, which gives rise to the well-grounded assumption that biometric facial records exist for this purpose. Lastly, the telematic voting system maintained by the CNE operates using biometric databases, but its legal and technical framework is opaque.

Different official documents such as the National Electronic Government Plan 2018-2021[79], the Digital Ecuador Policy 2019[80] and the recent Digital Transformation Agenda 2022-2025[81] consider the Civil Registry database as an asset available for other uses beyond personal identification.

Cumulatively, this leads to the conclusion that there is a tendency in the country to favor digital ID practices that are particularly risky for human rights protections, which is also documented in the regional report. In sum, these risk practices include:

- the use of centralized databases with a high risk of data breach and security vulnerabilities;
- permitting function creep of the Civil Registry database without proper oversight;
- the failure to provide appropriate legal grounding for sensitive personal data collection.

2. Prevalent Narrative about the Necessity of Biometrics in the Public Sector

The public policies and legislation of Ecuador that have been reviewed for this case study seem to indicate that the public sector considers the use of biometrics in digital identification processes as essential. This narrative runs in the Digital Transformation

[79] Ministry of Telecommunications and Information Society (2018). National Electronic Government Plan 2018- 2021. See: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/09/PNGE_2018_2021sv2.pdf.
[80] Ministry of Telecommunications and Information Society (2018). Digital Ecuador Policy. See: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2019/05/PPT-Estrategia-Ecuador-Digital.pdf.
[81] Ministry of Telecommunications and Information Society (2018). Digital Transformation Agenda 2022-2025. See: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2022/08/Agenda-transformacion-digital-2022-2025.pdf.

Agenda 2022-2025, where digital identity is referenced. This is also present in other integral policy documents, such as a report by the Civil Registry outlining its digital identity vision. The report highlights that biometrics are "part of the process of enrollment and validation of the digital identification service,"[82] although this is not an essential element.

3. No Prioritization of Inclusion for Vulnerable Populations

No evidence has been found that the digital identity systems of Ecuador have been designed with an inclusive approach for vulnerable populations or those at risk of being excluded from the adoption of technologies such as biometrics. Comparatively, in other Latin American countries such as Bolivia[83] and Brazil,[84] there are projects or plans for systems aimed at facilitating access to social aid. Based on the research, the only mention of the concept of "digital inclusion" (which is also more restricted) is in the *Organic Law for Digital Audiovisual Transformation* approved in 2023, but this is still pending proper implementation.[85]

Based on the research findings, and echoing the trend in the region, Ecuador maintains digital identity systems to facilitate access to digital government services, electronic voting, and presumably police control (ECU 911) to a group of the population with privileged conditions. These conditions include good connectivity, digital skills, amongst others.

The Digital Transformation Agenda 2022-2025 does not include objectives or action items with an inclusion focus. On the contrary, in relation to digital identity, it includes actions aimed at improving the effectiveness of police control systems. Illustratively, two of its

[82] General Management of Civil Registry, Identification and Identification Card Issuance (2022). The right to privacy in the digital age/DIGERCIC 05-25-2022. See: https://www.ohchr.org/sites/default/files/documents/issues/digitalage/reportprivindigage2022/submissions/2022-09-06/CFI-RTP-Ecuador.pdf.

[83] Venturini, Jamila; Díaz, Marianne (2021). Social identification and protection systems in Venezuela and Bolivia: surveillance, gender and human rights (Pages 29-42). See: https://www.derechosdigitales.org/wp-content/uploads/sistemas-de-Identificacion_ES.pdf.

[84] ITS Río (2020). Good ID in Latin America: Strengthening appropriate uses of Digital Identity in the region (Pages 49-50). See: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf.

[85] Official Registry, Government of Ecuador (2023). Organic Law for Digital Audiovisual Transformation. See: https://www.go Gobiernoelectronico.gob.ec/wp-content/uploads/2023/02/7e52b3d7-0ba5-4c58-a474-00e19fcbe127.pdf.

objectives of the Security and Digital Trust axis include the "acquisition of equipment and licensing for facial, fingerprint and vehicle recognition, on mobile devices" and the "development of police intervention applications with cameras and crime recording, with infrastructure."[86]

4. Common Providers of Digital Identity and Surveillance Technologies

Like other Latin American countries such as Colombia[87], Ecuador has a common supplier of digital identity technologies and technologies with surveillance capabilities, namely IDEMIA (formerly OT-Morpho). Historically, the Civil Registry relied on a technology corporation, the International Business Machines Corporation's (IBM), support for the digitization of its identity system.[88] However, since 2019, IDEMIA, a multinational provider of identity technologies, has been responsible for maintaining the system for issuing biometric passports and identity cards.[89] In 2022, IDEMIA responded to a report by Access Now[90] noting that they "do not commercialize surveillance technologies."[91]

However, it should be noted that there is also a relatively large ecosystem of technology providers with surveillance capabilities that maintain the robust video surveillance camera system installed in the country, especially those operating under the umbrella of the ECU 911, which was a project financed and developed by two Chinese companies: China National Electronics Import & Export Corporation (CEIEC), a defense electronics company, and

[86] Ministry of Telecommunications and Information Society (2018). Digital Transformation Agenda 2022-2025. See: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2022/08/Agenda-transformacion-digital-2022-2025.pdf.
[87] Karisma Foundation (2021). The facial recognition system of the National Registry. See: https://digitalid.karisma.org.co/2021/07/01/sistema-reconocimiento-facial-registraduria/.
[88] Civil Registry, Identification and Identification Card Issuance. Historical review. See: https://www.registrocivil.gob.ec/resena-historica/.
[89] Civil Registry, Identification and Identification Card Issuance (2019). Civil Registry awarded a contract for a new system for issuing biometric passports and identity cards. See: https://www.registrocivil.gob.ec/registro-civil-adjudico-contrato-para-nuevo-sistema-de-emision-de-pasaportes-biometricos-y-cedulas-de-identidad/.
[90] Access Now (2021). Surveillance Tech in Latin America: Made Abroad, Deployed at Home. See: https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf.
[91] Business and Human Rights Resource Centre (2022). Response from IDEMIA to allegations about the sale of surveillance technology in Latin America. See: https://www.business-humanrights.org/en/latest-news/response-from-idemia-to-allegations-about-sale-of-surveillance-technology-in-latin-america/.

Huawei Technologies Company Limited, a Chinese multinational technology corporation.[92] It is unclear whether the ECU 911 and the digital identity system are interoperable.

In Access Now's report, '*Surveillance Tech in Latin America: Made Abroad, Deployed at Home,*' that was answered by IDEMIA, it is mentioned that several companies participate in the Ecuadorian market for video surveillance systems. These include Axis (Switzerland), Hikvision (China), Intelligent Security Systems (Russia), Pelco Corporations (United States), Tiandy and ZKTeco (China) and VERINT (Israel and the United States)[93]. Likewise, in FUNDAMEDIOS' report, '*Video surveillance in Ecuador violates citizen rights'* it is pointed out that the technologies used to implement ECU 911 are unique in the market, so its maintenance would be restricted to the original suppliers.[94]

Analysis II: Problems of Digital Identity Systems in Ecuador

The regional report identified the following problems: the proliferation of surveillance technologies due to the intensive use of biometrics; the lack of transparency in the development of policies and the deployment of digital identity systems; the absence of concrete limits on the present and future evolution of these systems; and the real or potential cases of human rights impacts such as privacy, data protection and discrimination in access to public services.

This section presents an account of the main challenges identified in the digital identity systems mapped in Ecuador. In some cases, direct mention has been made of information provided in interviews. This list is preliminary and not exhaustive.

[92] New York Times (2019). Made in China and exported to Ecuador: the state surveillance apparatus. See: https://www.nytimes.com/en/2019/04/24/espanol/america-latina/ecuador-vigilancia-seguridad-china.html.
[93] Access Now (2021). Surveillance Tech in Latin America: Made Abroad, Deployed at Home. See: https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf.
[94] FUNDAMEDIOS (2021). Video surveillance in Ecuador violates citizens' rights. See: https://www.fundamedios.org.ec/wp-content/uploads/2021/12/Inf.-Videovigilancia.pdf.

1. Digital Identity Systems are Extremely Risky for Human Rights

All digital identity systems identified in Ecuador replicate the riskiest practices for human rights, especially for privacy and the protection of personal data. In the case of the system maintained by the Civil Registry, these risks include the possibility of unauthorized access, security breaches, and leaks that expose the information of Ecuadorian citizens and foreign residents. This risk is not a potential, as it has already been realized on several occasions, the most notable being a massive data leak in 2019, which the government has failed to explain.[95]

In the case of mandatory registrations of mobile lines and devices, in addition to the previous risks, there is the risk of function creep, i.e., uses that are different from the purpose claimed by ARCOTEL, namely, to prevent the theft and use of lines for criminal purposes. This risk is exacerbated by the fact that the rules that regulate this system indicate that, in addition to ARCOTEL, other entities related to "national security" may also gain access. The inclusion of the 'national security' category is broad, and exposes data collected in this system to monitoring and surveillance efforts, without due process or the possibility of subsequent oversight.

Regarding the alleged digital identity system that could be used in conjunction with the ECU 911 video surveillance systems, the possibility of technological failures (such as false positives), must be added to the risks already mentioned, which would violate rights such as due process, non-discrimination and guarantees such as the presumption of innocence.

Finally, regarding the Telematic Voting System used abroad, although little is known about its operation, it is foreseeable that the database it operates on would present a similar level of risk as that of the Civil Registry. Risks also extend to other rights, such as the right to vote,

[95] El Comercio Newspaper (2019). How was the security breach that affected the data of 20 million Ecuadorians discovered? See: https://www.elcomercio.com/tendencias/tecnologia/hackeo-etico-filtracion-datos-ecuatorianos.html.

since a compromise of this system could lead to a breach of voting secrecy and even alter the results of election results, with an impact on democratic processes generally.

2. Failure to Enact Legal Frameworks that Impose Legislative Limits

As FUNDAMEDIOS points out in the conclusions of its report on video surveillance systems, especially ECU 911, Ecuador does not have specific legislation that establishes limits on the use of surveillance systems. Based on this, the legal safeguards that would ordinarily be imposed over these systems, including those designed to protect the right to privacy enshrined in the Constitution of Ecuador, will inevitably not be imposed.[96] This situation extends to the use of biometric technologies implemented in the digital identity system used by the Civil Registry, which has been developed without a specific law determining its scope. This also applies to the telematic voting system of the CNE.

Positively, on May 10, 2021, the National Assembly of Ecuador approved the Organic Law on Personal Data Protection. The existence of standards of this type imposes limits on the adoption of technologies that process personal data, such as biometrics and facial recognition. However, the interviews yielded conflicting views. One group pointed out that the approval of the norm and the entry into force of the sanctioning regime will effectively impose limits on the processing of data by public entities. On the other hand, another group of interviewees pointed out that the failure to establish a data protection authority, the election of its executive management, and the absence of subsidiary regulation is delaying the implementation of the law.

Another rule that could impose limits on public entities in the specific field of digital identity is the Organic Law for Digital Audiovisual Transformation that was approved in March 2023. This law creates the “Digital Identity Framework” and defines its scope. Some of the interviewees consider that this framework proposes a change in competences at the level of identity policy creation, between the Civil Registry and the digital transformation

[96] FUNDAMEDIOS (2021). Video surveillance in Ecuador violates citizens' rights. See: https://www.fundamedios.org.ec/wp-content/uploads/2021/12/Inf.-Videovigilancia.pdf.

authority, which is the Ministry of Telecommunications and Information Society. In any case, this law is still new, and the country's political crisis suggests delays in its implementation.

While the scenario of risks and threats to the rights created by digital identity systems in Ecuador could be limited through public interest litigation, taking advantage of the fact that the Constitution protects the right to privacy, no such actions have been found during this investigation. This is despite serious complaints from civil society protesting the use of ECU 911 for illegal surveillance and political espionage.[97] This situation has been described in a 2022 report sent to the Human Rights Council, through the Universal Periodic Review mechanisms.[98]

3. Potential and Real Human Rights Impacts

The combination of risks and threats posed by the preceding issues paint a complicated landscape, which is further exacerbated by the political and social crisis that Ecuador has been experiencing in recent years, leading to the recent dissolution of the National Assembly and the call for General Elections. Thus, besides privacy, the protection of personal data, due process and the presumption of innocence, there exists the possibility of violations of rights such as freedom of expression, peaceful assembly, the secrecy of voting, among others.

As discussed above, there are multiple precedents of illegal uses of surveillance technologies that may be facilitated by digital identity systems, specifically in the case of ECU 911, which is the most developed video surveillance system in the country. The most recent case was reported in 2022 by local human rights organizations, which suggests that

[97] El Comercio Newspaper (2019). Lenin Moreno says the ECU 911 was used 'perversely' for espionage. See: https://www.elcomercio.com/actualidad/seguridad/lenin-moreno-ecu-911-espionaje.html.
[98] FUNDAMEDIOS (2022). Report on the violation of citizens' rights through video surveillance in Ecuador, and recommendations to the Ecuadorian Government, with an eye on announcements of mass implementation of facial recognition technology. See: https://www.fundamedios.org.ec/wp-content/uploads/2022/04/1-EPU-Ecuador-Videovigilancia-1.docx-1.pdf.

the worsening situation in the country could lead to the use of these surveillance capabilities illegally by the current government or subsequent attempts.[99]

Regarding the virtual electronic voting system provided by CNE, there are additional concerns. While this report has not been able to find sufficient information to fully understand the functioning and scope of this system that is underpinned by a biometric database, it is important to emphasize the problems identified in other electronic voting systems in the region and the world.[100] The widespread perception of interviewees about the poor technical capacity of those responsible for deploying technologies in the Ecuadorian public sector, together with data breaches such as those of 2019, that corroborate this perception, suggest that these problems could also arise in this country.

4. Other Issues Relating to the Current Situation in the Country

The current crisis in Ecuador risks exacerbating these the problems of digital identity systems that Ecuador shares with most of the countries analyzed in the regional report.

The most obvious assumption is the possibility that current digital identity systems could be weaponized against political and social leaders who express opposition against the decision taken by H.E. President Lasso, especially through the interoperability of the Civil Registry and ECU 911 databases (*if this is not already happening*). Given that there are already precedents for illegitimate use, and that rules affecting other related rights have recently been adopted,[101] the risk level is high. While the interviewees consider this unlikely, most recognize that the installed surveillance capabilities will not prevent them from being used in this way in the future.

[99] LaLibre.Net (2022). Civil society organizations reject attempts to silence and criminalize social movements in the context of protest in Ecuador and demand respect for human rights. See: https://lalibre.net/comunicado-paroec/.
[100] Díaz, Valentín (2022). Electronic Voting and Public Policy Considerations in Latin America. See: https://www.derechosdigitales.org/wp-content/uploads/VotoElectronico-mapalatino.pdf.
[101] Derechos Digitales (2023). Ecuador: many changes, but little to celebrate. See: https://www.derechosdigitales.org/20752/ecuador-muchos-cambios-poco-que-celebrar/.

Another scenario of interest is the behavior of the Telematic Voting System implemented by the CNE for voters abroad, which was already used in the sectional elections of February 2023[102] for the first time and will be used again in the general elections in August 2023. To a lesser extent, smart city implementation plans can also be highlighted. In the latter case, precedent has been set that different deployments of video surveillance cameras have been financed within the framework of local strategies for this type of policies.[103]

Finally, it is worth noting that the dissolution of the National Assembly momentarily suspends relevant initiatives for this study. Perhaps the most notable one was a digital rights bill, which addressed different issues, including digital identity. Based on a human rights perspective, the initiative proposed substantial changes to various practices related to identification and video surveillance in Ecuador. This Bill would have been another tool to limit the adoption of digital identity systems, adding to the laws on data protection and digital transformation.[104]

Conclusion and Recommendations

This case study provides an in-depth exploration of Ecuador's digital identity systems, modelled on the Latin America regional report produced by Derechos Digitales, "*Digital Identity in Latin America: Current Situation, Trends and Problems*". Ecuador's current political situation impacts the implementation of laws that would introduce legislative limits on the use of personal data in digital identity systems. This situation further entrenches the possibility that current digital identity systems could be weaponized against political and social leaders who express opposition.

The case study notes that Ecuador exemplifies the riskiest digital identity practices, such as the adoption of centralized databases that are at a higher risk of security vulnerabilities and

[102] El Universo Newspaper. Elections 2023: Registration for telematic voting abroad will be available until February 5. See: https://www.eluniverso.com/noticias/politica/elecciones-2023-inscripcion-para-voto-telematico-en-el-exterior-estara-disposable-hasta-el-5-de-febrero-nota/.

[103] Biometric Update (2019). Quito to launch facial recognition for public surveillance under smart city project. See: https://www.biometricupdate.com/201908/quito-to-launch-facial-recognition-for-public-surveillance-under-smart-city-project.

[104] National Assembly of Ecuador (2023). Draft Organic Law on Digital Rights. See: http://ppless.asambleanacional.gob.ec/alfresco/d/d/workspace/SpacesStore/78c3cfba-956d-4c46-b325-da410bc428d0/pp-der-dig-0026-ortiz-proyecto-de-ley.pdf.

data breaches. Further, the necessity of biometrics in digital identity is a popular narrative advanced by the public sector, including in several foundational policy and strategy documents. The case study also notes that there is no prioritization for the inclusion of vulnerable populations, that risks exacerbating exclusion and discrimination risks.

Based on this, the case study presents a set of recommendations for the Ecuadorian government (at the national and regional levels), and for civil society organizations.

Recommendations

This section presents a set of recommendations addressed to the Ecuadorian government and civil society organizations.

To National and Regional Governments

We urge national and regional governments in Ecuador to:

- Ensure that the development and use of digital identity systems respects the fundamental rights enshrined in the Constitution, especially privacy and the protection of personal data. Specifically, ensure that the legislative frameworks that enable these technologies comply with the principles of international law on legality, necessity, and proportionality, restricted by the purpose limitation, and subjected to public participation.
- Implement the laws on personal data protection and digital and audiovisual transformation that delimit the development and use of digital identity systems.
- Cease developing or using digital identity systems where there is an imminent risk of causing serious harm to people's rights or where such harm has already occurred, whenever feasible and without disrupting the provision of essential services that rely on the technologies in question.
- Promote the creation of multistakeholder discussion fora, inclusive of civil society, to ensure continuity or discuss new developments of digital identity systems. Specifically, these fora should allow for a review of existing systems and those being considered for implementation in different sectors (such as trade, health, migration control, etc.).

To Civil Society

We urge civil society in Ecuador to:

- Deepen the study of the most relevant vectors of interest, both in the current situation and looking towards the future. This includes:
    - Examining and clarifying the operation of the CNE system for virtual electronic voting for citizens abroad, due to its implications for the elections that will take place in August 2023.
    - Examining the potential for the ECU 911 platform to become a mass surveillance tool and its interoperability with the Civil Registry' database, and the risks for activists and political and social leaders.
- Promote awareness-raising actions among the population and other civil society organizations working on human rights issues, regarding the risks associated with digital identity systems. This includes:
    - Advocating for the implementation of the laws and standards on personal data protection and digital and audiovisual transformation.
- Explore the possibility of initiating advocacy and strategic litigation actions that directly target digital identity systems like the Civil Registry. This could include focusing on the validation services it offers, or its potential interoperability with the ECU 911 platform, and the potential for illegal surveillance.

Reference List

Access Now (2018). National Digital Identity Programmes: What's next?

Access Now (2021). Surveillance Tech in Latin America: Made Abroad, Deployed at Home.

Africa Digital Rights Hub (2022). Data Protection Code of Practice for Digital Identity Schemes in Africa.

Africa Digital Rights Hub (2022). The inclusiveness or exclusiveness of National IDs in West Africa: Countries of focus: Côte d'Ivoire, Ghana and Nigeria.

AlSur (2018). Business and Human Rights: Regional Report on Technology, Big Data and Cyber Surveillance.

AlSur (2021). Facial recognition in Latin America: trends in the implementation of a perverse technology.

Association for Civil Rights (2015). If we know each other better, we take better care of ourselves: Report on biometrics policies in Argentina.

Association for Civil Rights (2016). The Personal Data Protection System in Latin America: Opportunities and Challenges for Human Rights.

Association for Civil Rights (2017). Quantifying Identities in Latin America.

Association for Civil Rights (2017). Challenges for biometrics in the protection of personal data – Reflections on the SIBIOS case.

Association for Civil Rights (2017). The Identity We Cannot Change: How Biometrics Affects Our Human Rights.

Association for Civil Rights (2019). Your Digital Self: Discovering the Narratives of Identity and Biometrics in Latin America.

Association for Civil Rights (2021). Surveillance Technologies in Argentina.

Canales, María Paz; Lara, J. Carlos (2018). Proposal of legal standards for surveillance in Chile (2018).

Center for Human Rights and Global Justice (2022). Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID.

Centre for Internet and Society India (2020). Governing ID: Principles for Evaluation.

CETyS (2021). Video surveillance with facial recognition, artificial intelligence and human rights: neither apocalypse nor utopia.

Data Privacy Brasil (2022). Between visibility and exclusion: Mapping the risks associated with the National Civil Identification System and the usage of its database by the GOV.BR platform.

Data Privacy Brazil and TEDIC (2023). Technology and Human Rights in the Tri-Border: An Exploratory Study of the Intelligent Muralha Security Programs (Brazil) and the Automated Migratory Facial Recognition System (Paraguay).

Díaz, Marianne (2017). Data Retention and Registration of Mobile Phones: Chile in the Latin American Context.

Díaz, Marianne (2018). The body as data.

Figueroa, Javiera; Venegas, Catalina (2020). Narratives on the use of the digital footprint in public health.

Garay, Vladimir (2019). Evil eye: facial recognition in Latin America.

Hiperderecho (2018). Biometric Identity in Peru: State of the matter.

Hiperderecho (2020). Digital Identity in Peru: Deciphering the Leviathan

InternetLab (2015). State Surveillance of Communications in Brazil and the Protection of Fundamental Rights.

IPANDETEC (2021). Digital Masks: Digital Identity in Central America.

ITS Rio (2020). Good ID in Latin America: Strengthening appropriate uses of Digital Identity in the region.

Karisma Foundation (2019). Biometrics in the Colombian State: When and how has its use been justified?

Karisma Foundation (2022). ID Colombia: Digital Identity and Human Rights.

KICTANet (2022). Policy brief Data Protection and Digital Identity in Kenya.

Library of the National Congress of Chile (2022). Digital Identity: Concepts and Legislation.

McKinsey Global Institute (2019). Digital identification: A key to inclusive growth.

OCDE (2023). Draft Recommendation on the Governance of Digital Identity.

Paradigm Initiative (2021). COVID-19 and Digital Rights: A Compendium on Health Surveillance Stories in Africa.

Paradigm Initiative (2021). Deploying Digital Identity Systems: Human Rights Implications and Lived experiences in Kenya.

Paradigm Initiative (2022). Internet freedoms in Chad and DRC: Better understanding the notion of digital identity.

TEDIC (2017). The lack of protection of personal data and gender inequality, risks to the freedoms of people on the Internet.

TEDIC (2018). The continued alienation of our rights. Identity Systems: Biometrics and Unregulated Surveillance Cameras in Paraguay.

The Engine Room (2019). What to Look for in Digital Identity Systems? A typology of stages.

The Engine Room (2020). Understanding the Effects of Digital Identification on Everyday Life: A Multinational Study.

The Engine Room (2022). A Digital ID Handbook: Strategies for Navigating Electronic Identification Systems.

Venturini, Jamila; Díaz, Marianne (2021). Social identification and protection systems in Venezuela and Bolivia: surveillance, gender and human rights

World Bank (2016). Digital identity: towards shared principles for public and private sector cooperation.

World Bank (2017). Principles on Identification for Sustainable Development: Toward the Digital Age.

World Bank (2018). ID Enabling Environment Assessment (IDEEA): Guidance Note.

World Bank (2019). Digital ID and the Data Protection Challenge: Practitioner's Note.

World Bank (2019). ID Enrollment Strategies: Practical Lessons from Around the Globe.

World Bank (2019). ID4D Practitioner’s Guide.

World Bank (2022). Engaging Civil Society Organizations (CSOs) for Successful ID Systems: Guidance Note.

World Bank (2022). ID4D Global Dataset.