Informe regional

Identidad digital en América Latina: situación actual, tendencias y problemas

Mayor libertad en Internet

Derechos Digitales.

Junio de 2023

Agradecimientos

Quisiéramos expresar nuestro agradecimiento a Derechos Digitales (DD) y a los investigadores de DD, Carlos Guerrero y Paloma Lara Castro, que llevaron a cabo esta investigación y son los autores de este informe.

Derechos Digitales es una organización independiente, sin fines de lucro y de alcance en toda América Latina que se fundó en 2005, y cuya meta principal es el desarrollo, la defensa y la promoción de los derechos humanos en el entorno digital. El trabajo de la organización se enfoca en tres ejes fundamentales:

- Libertad de expresión.
- Privacidad y datos personales.
- Derechos de autor y acceso al conocimiento.

Asimismo, queremos darles las gracias a todas las comunidades y personas que han compartido su tiempo, experiencias y perspectivas con nosotros con tanta generosidad, y contribuyeron al proceso de investigación. En concreto, nos gustaría dar las gracias a las siguientes personas que participaron en las entrevistas y/o aportaron sus comentarios sobre las distintas versiones del informe: Daniel Vizuete (CTS-Lab de FLACSO); Diego Álvarez (Niubox Legal); Rafael Bonifaz (DD); y Ricardo Chica Reino (Fundación Ciudadanía y Desarrollo).

Este informe se publica en el marco del proyecto Greater Internet Freedom (GIF, Mayor libertad en Internet) de USAID, que ejecuta Internews y el consorcio GIF.

Este reporte ha sido posible gracias al generoso apoyo del pueblo estadounidense mediante la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID). El contenido es responsabilidad de DD y no refleja necesariamente las opiniones de USAID ni del Gobierno de los Estados Unidos.

Tabla de contenido

Resumen ejecutivo

El enfoque de este informe es la región de América Latina y el Caribe (ALC) y forma parte de una investigación multirregional, cuya finalidad es identificar y comparar el estado de las amenazas, el uso y las repercusiones de la biometría y la identidad digital en África, los Balcanes, Asia Central, América Latina y el Caribe, y el Sur y Sudeste Asiático.

El informe ofrece un resumen general del nivel y la naturaleza de la adopción de la identidad digital (ID) en cuatro países de ALC: Bolivia, Brasil, Colombia y Ecuador, enfocándose en tres tipos de sistemas de identidad digital digitalizados. Incluyen: (a) sistemas de identidad digital fundacionales; (b) sistemas de identidad digital basados en el registro obligatorio de líneas o equipos móviles con fines policiales; y (c) sistemas de identidad digital funcionales utilizados en ámbitos específicos, como la salud y la seguridad social.

Nos alineamos con la declaración hecha por el *Instituto de Tecnologia & Sociedade do Rio* (ITS Rios) en el reporte titulado *"Buena identidad digital en América Latina: Fortalecer los usos adecuados de la Identidad Digital en la región"*[1] al declarar que no existe una diferencia básica entre los sistemas de identidad digital (ID) y los sistemas de vigilancia estatal. Si bien estos dos sistemas apuntan a distintos objetivos teóricos, en la práctica pueden solaparse, lo cual resulta en preocupaciones en materia de derechos humanos, particularmente sobre la protección del derecho a la intimidad.

La preocupación más notable que se indica en este reporte es la posibilidad de que los sistemas de identificación digital se integren en una infraestructura de vigilancia estatal más extensa, resultando así en la consolidación de datos personales y el aumento del potencial de vigilancia. Como se describe más adelante, es posible acceder a las bases de datos de documentos de identidad digitales mediante un extenso rango de entidades estatales y privadas, lo que causa preocupación sobre el alcance, las salvaguardias y la transparencia de estos intercambios.

[1] ITS Río (2020). Buena identidad digital en América Latina: Fortalecer los usos adecuados de la Identidad Digital en la región (Página 11). Consultar: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf.

A continuación se resumen detalladamente los hallazgos clave y se analizan en profundidad en el reporte.

Hallazgos clave

Este reporte describe los siguientes hallazgos:

- **Hallazgo 1:** los cuatro países de ALC investigados han implementado sistemas de identificación digital y desplegado tecnologías biométricas con fines fundacionales y/o funcionales.
- **Hallazgo 2:** la mayoría de los países de ALC prefiere modelos de identificación digital centralizados, en vez de sistemas de identificación digital descentralizados, federados o de mercado abierto.
- **Hallazgo 3:** los cuatro países de ALC investigados están recopilando y procesando datos biométricos en una o varias bases de datos de identificación digital sin una evaluación previa de los derechos humanos.
- **Hallazgo 4:** ciertos proveedores de tecnologías de vigilancia para los gobiernos de ALC son similares a los proveedores de tecnologías de identificación digital y biométricas.
- **Hallazgo 5:** la evidente ambigüedad en el concepto de "documento de identidad digital" ha permitido a los países de ALC expandir continuamente el ámbito legal de sus bases de datos de documentos de identidad digitales más allá de la identificación para abarcar cualquier fin marcado como necesidad estatal, incluido el control de la migración y la prestación de programas de seguridad social. Al no imponer límites a la finalidad y el alcance de los sistemas de identificación digital, es más difícil para las partes interesadas -como las OSC responsables de garantizar la transparencia, la rendición de cuentas y la protección de los derechos de las personas- evaluar el nivel de amenazas y riesgos para los derechos humanos en relación con los límites preestablecidos.

Recomendaciones

Se urge a los Estados y gobiernos nacionales de la región de ALC a:

- Realizar evaluaciones del impacto en los derechos humanos (EIDH) antes de la implementación de sistemas de identificación digital y monitorear su aplicación para responder a las repercusiones sobre los derechos humanos;
- Desarrollar mecanismos de rendición de cuentas y participación de varias partes interesadas antes y durante la implementación de sistemas y procesos de identificación digital;
- Modificar las leyes de identidad para que la recopilación de datos biométricos sea opcional y desvincular el acceso de las personas a los servicios públicos y privados de la provisión obligatoria de datos biométricos.

Se urge a las organizaciones de la sociedad civil de la región de ALC a:

- Realizar una investigación más extensa y profunda sobre el DNI digital en la región de ALC;
- Realizar campañas de defensa y emprender litigios estratégicos contra los sistemas de identificación digital que afectan a los derechos humanos.

Este documento facilita un resumen general del DNI digital en cuatro países de América Latina que se han sometido a investigación con la esperanza adicional de que estos hallazgos sirvan de inspiración para los gobiernos y la sociedad civil para coordinarse en favor de sistemas de DNI digital que respeten los derechos.

Introducción

La tendencia mundial de implementar sistemas de identidad digital (ID) se ha consolidado en las últimas décadas bajo argumentos tecnosolucionistas que aportan tecnologías como "soluciones" a distintos problemas sociales, que suelen encubrirse como parte de los esfuerzos de digitalización y transformación digital. El sector público ha adoptado los sistemas de identidad digital, lo cual ha permitido su integración en la digitalización de servicios vitales, como la salud, el pago de impuestos y la seguridad social.

El argumento de los Estados es que la tecnología actual hace que sea posible desarrollar sistemas más fiables, resistentes y sostenibles en comparación con los sistemas tradicionales basados en papel. En la región de América Latina, los estados han integrado la identificación digital en sus sistemas de identificación con distintas finalidades, que incluyen agilizar el tiempo para facilitar servicios por medio de la identificación única de las personas. Particularmente, muchos países de América Latina cuentan con registros o bases de datos de identificación centralizados que capturan y procesan datos relativos a la identidad de las personas y que, en muchos casos, condicionan su acceso a beneficios sociales.

Ciertos gobiernos de América Latina han expresado su interés en proporcionar identidad legal a través de sistemas de identificación digitalizados al verse guiados por la Meta 16.9 de los Objetivos de Desarrollo Sostenible (ODS), que alienta a los Estados a "proporcionar acceso a una identidad jurídica para todos, en particular mediante el registro de nacimientos"[2]. Todavía se cuenta con el apoyo de organizaciones internacionales de desarrollo e instituciones financieras, como el Banco Mundial[3] para estos esfuerzos, y estas partes apoyan y, en ciertos casos, han colaborado activamente en el desarrollo de sistemas de identificación digital.

Bajo el artículo 6 de la Declaración Universal de Derechos Humanos (DUDH) y del artículo 16 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP), el derecho a ser

[2] ONU. Objetivos de Desarrollo Sostenible, Objetivo 16, Meta 16.9. Consultar: https://sdgs.un.org/goals/goal16.
[3] Algunos ejemplos incluyen el proyecto ID4D del Banco Mundial. Consultar: https://id4d.worldbank.org/about-us

reconocido como persona ante la ley es un derecho inalienable y universal.[4] A pesar de ello, reiteramos que el derecho a la identidad no equivale a que la identificación sea un requisito obligatorio.[5] Conjuntamente, si bien las tecnologías de identidad y biométricas son capaces de simplificar los procesos y agilizar la prestación de servicios públicos y privados, vale la pena destacar que el requisito de tener una identidad legal no está supeditado a la implementación de sistemas de identificación digital. Asimismo, no existe un sistema único y estandarizado aplicable para todos los países y contextos, por lo cual cada país debe analizar sus propias necesidades y finalidades internas antes de implementar sistemas de identificación digital.

De forma crítica, los sistemas de identificación digital se promueven como ser beneficiosos para los países en desarrollo cuyos sistemas de identificación son débiles o ineficaces. No obstante, estas declaraciones extensas y con enfoque en la tecnología no fomentan soluciones simultáneas que aborden las grandes disparidades en el acceso a Internet y a las Tecnologías de la Información y la Comunicación (TIC) entre distintas generaciones, ubicaciones geográficas, estatus socioeconómico y género. Estas disparidades destacan las desigualdades existentes, las cuales deben abordarse tomando medidas alternativas de política pública. [6]

Este reporte nota que los sistemas de identificación digital han ido mucho más allá del ámbito de la identificación, lo cual ha genera repercusiones potenciales sobre los derechos humanos asociados a la vigilancia estatal y a la profundización de situaciones de discriminación preexistentes. Una organización internacional de derechos digitales sin fines de lucro, Access Now, y 73 firmantes instaron, mediante una carta abierta, al Banco Mundial y a otras organizaciones internacionales a “tomar medidas inmediatas para cesar

---

[4] OACDH. DUDH. Consultar: 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. OACDH. ICCPR - Resolución 2200A (XXI) de la Asamblea General. Consultar: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

[5] ITS Río (2020). Buena identidad digital en América Latina:

Fortalecer los usos adecuados de la Identidad Digital en la región. Consultar: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf.

[6] Barbosa, A. Carvalho, C. Machado, C. Costa, J (2020). Buena identidad digital en América Latina:

Fortalecer los usos adecuados de la Identidad Digital en la región. Consultar: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf

las actividades que fomentan modelos perjudiciales de sistemas de identificación digital (ID digital)". [7]

Esto subraya la urgencia de tomar medidas inmediatas contra los riesgos para los derechos humanos que plantean los sistemas de identidad digital, que incluyen:[8]

Extensa justificación y marcos jurídicos insuficientes: La incorporación de tecnologías digitales y biométricas se justifica en términos generales como beneficiosa sin evidencia que se considere suficiente y convincente, y sin un marco jurídico global acompañante.

Participación deficiente de las partes interesadas: Los sistemas de identificación digital se despliegan de forma excluyente, sin la participación de las varias partes interesadas.

Implementación de sistemas de identificación digital sin las salvaguardias correspondientes: Los Estados de la región de América Latina han empleado distintas tecnologías, incluyendo tecnologías biométricas, que tienen capacidad para procesar datos personales, aunque con medidas de seguridad y protección de datos que se consideran inadecuadas, transparencia limitada y salvaguardias deficientes de los derechos humanos, como evaluaciones previas de los derechos humanos y mecanismos de supervisión independientes.

Falta de mitigación y tratamiento de los riesgos para los derechos humanos que plantean los sistemas de identificación digital: Esto se demostró en los casos de Aadhaar en India; Huduma Namba en Kenia; y el Sistema Patria en Venezuela. Como Derechos Digitales ha mencionado en investigaciones anteriores,[9] el uso de sistemas de identificación digital, particularmente aquellos que integran tecnologías biométricas, para el acceso a recursos básicos no solamente afecta el derecho a la privacidad, sino que a su vez lesiona directamente el derecho a la integridad, la autonomía y la dignidad. Los sistemas de identificación digital pueden fomentar, reforzar o profundizar situaciones de

[7] Access Now (2022). Carta abierta: El Banco Mundial y sus donantes deben proteger los derechos humanos en los sistemas de identificación digital Consultar: https://www.accessnow.org/press-release/carta-abierta-el-banco-mundial-sistemas-de-identificacion-digital/.

[8] Centro de Derechos Humanos y Justicia Global, Facultad de Derecho de la Universidad de Nueva York (2022). ¿Camino al infierno? Manual básico sobre el papel del Banco Mundial y las redes mundiales en la promoción de la identificación digital. Consultar: 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. Consultar: https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf *y* https://www.derechosdigitales.org/wp-content/uploads/sistemas-de-Identificacion_ES.pdf.

discriminación y exclusión de grupos vulnerables e históricamente excluidos, y esto es particularmente cierto en el contexto de los programas de protección social. Esta situación es más notable en el contexto de la salud, en el cual los riesgos empeoran para las poblaciones vulnerables y marginadas, como las mujeres, las personas con discapacidades, los ancianos y la comunidad LGBTIQ+.

El derecho a la intimidad en la era digital ha pasado a ser una puerta de acceso a la protección de muchos otros derechos.[10] La Resolución 68/167 de 2014 de la ONU relativa al derecho a la privacidad en la era digital detalla que el derecho a la privacidad requiere una protección firme como "una condición previa necesaria para la protección de valores como la libertad, la dignidad y la igualdad frente a la intrusión gubernamental", y "un ingrediente esencial para las sociedades democráticas….". Los sistemas de identificación digital posan una amenaza para el derecho a la intimidad a pesar de esta puerta de acceso, lo cual repercute en la protección y el cumplimiento de otros derechos humanos.

Instructivamente, la recopilación de datos jamás ocurre en un entorno neutral y es necesario que se enmarque en el ámbito operativo de un país, en particular en su entorno social. El procesamiento de datos sensibles posa riesgos para las comunidades en situación de vulnerabilidad. A modo de ejemplo, se puede decir que es posible que las mujeres, y particularmente las lesbianas, gays, bisexuales, intersexuales y transexuales (LGBTQI+), sean víctimas de estigmatización, marginación y violencia tras la exposición de información privada relativa a su historial sexual y reproductiva, su sexualidad y/o su identidad.

Se ha expresado la preocupación que sienten las organizaciones y mecanismos de derechos humanos por el aumento en el uso de tecnologías que no satisfacen la prueba tripartita de legalidad, necesidad y proporcionalidad, ni la limitación de finalidad de las leyes de protección de datos.[11] Una de las preocupaciones principales que plantean los agentes del espacio de la identificación digital es el "acercamiento de la misión", que conlleva

[10] ONU. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, David Kaye, A/HRC/29/32 (2015) y la ONU. Resolución 68/167 de la Asamblea General, A/HRC/13/37 y resolución 20/8 del Consejo de Derechos Humanos). Consultar https://undocs.org/A/HRC/29/32.

[11] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2014). El derecho a la privacidad en la era digital, A/HRC/27/37 Consultar: https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

implicaciones de vigilancia.[12] Los estados de América Latina han ido más allá del propósito original de los sistemas de identificación digital, algo que plantea dudas sobre su diferenciación de los sistemas de vigilancia.

Dado el contexto histórico de la vigilancia en la región de América Latina y la falta de mecanismos de supervisión independientes debido a las vulnerabilidades institucionales, esta situación es particularmente alarmante. En ciertos casos, los Estados que implementan sistemas de identificación digital no tienen leyes de protección de datos personales que puedan regular exhaustivamente la recopilación y el tratamiento de datos, lo cual incluye el intercambio de datos entre entidades públicas y público-privadas. Esto es capaz de afectar a ciertos grupos, como los defensores de los derechos humanos, los activistas y los periodistas.

Los actores se cuestionan la pertinencia y la necesidad de los sistemas de identificación digital y la adopción de tecnologías biométricas. En este reporte, se destaca que ciertas tecnologías biométricas que se están desplegando en los sistemas de identificación digital son similares a aquellas que se utilizan en los sistemas de vigilancia estatal. Con base en esto, parece que es probable que los problemas y riesgos específicos de los sistemas de vigilancia surjan en los sistemas de identificación digital, y que estos riesgos se intensifiquen debido al contexto histórico de vigilancia estatal continua en la región de América Latina. La Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACDH) destacó el potencial de vigilancia masiva latente en los sistemas de identificación digital y las bases de datos biométricos en los siguientes términos:

> *"En varios países, los sistemas de identidad están vinculados a un extenso almacenamiento central de datos personales, que incluye información biométrica como huellas digitales, geometría facial, escáneres de iris y ADN. Asimismo, las bases de datos suelen estar interconectadas y disponibles para que sean consultadas por otras agencias. Consecuentemente, es cada vez más fácil identificar a las personas dondequiera que se encuentren".*[13]

[12] Omidyar Network (2019). Cinco decisiones sorprendentemente consecuentes que toman los gobiernos sobre la identidad digital. Consultar: https://omidyar.com/five-surprisingly-consequential-decisions-governments-make-about-digital-identity/.

[13] ACNUDH (2022). El derecho a la privacidad en la era digital Consultar: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F51%2F17&Language=E&DeviceType=Desktop&LangRequested=False.

Los actores han solicitado una serie de soluciones para los desafíos de una industria de la vigilancia en expansión, desde la revisión de los procesos de adopción y gobernanza hasta el establecimiento de suspensiones sobre el uso de tecnologías biométricas.[14] Si bien el llamamiento del Alto Comisionado de las Naciones Unidas para los Derechos Humanos a favor de una suspensión sobre la producción y venta de sistemas de vigilancia no se enfocaba en los sistemas de identificación digital, apoyamos el argumento del ACNUDH expuesto anteriormente para expandir este llamamiento para abarcar los sistemas de identificación digital, en reconocimiento de los riesgos para los derechos humanos latentes en estos sistemas.[15]

[14] Noticias ONU (2021). Se requieren medidas urgentes contra los riesgos de la inteligencia artificial para los derechos humanos. Consultar: https://news.un.org/en/story/2021/09/1099972.
[15] *Ibid.*

Metodología

Tabla 1. *Tema y pregunta de investigación (por DD)*

Tema de investigación	Estudio exploratorio: El Nivel de Adopción y Uso de Sistemas de Identidad Digital y Biometría en América Latina y el Caribe (ALC)
Preguntas relativas a la investigación	a. ¿Qué sistemas de identificación digital se han adoptado en Bolivia, Brasil, Colombia y Chile? b. ¿Cuáles son las tendencias emergentes en el desarrollo y adopción de sistemas de identidad digital y biometría en la región de América Latina y el Caribe? c. ¿Qué riesgos plantean los sistemas de identidad digital para los derechos humanos?

Este reporte consolida la información en la región de América Latina y el Caribe y aporta un análisis exploratorio relativo al estado actual de los sistemas de identificación digital y los riesgos particulares para los derechos humanos latentes en estos sistemas. Este reporte adoptó un enfoque cualitativo restringido a una revisión documental de fuentes secundarias y terciarias dado su carácter exploratorio, en especial documentos que fueron preparados por organizaciones de la sociedad civil, el sector privado y organizaciones internacionales.[16] Esta metodología de investigación sirve para explorar temas complejos y matizados en una región con diferentes niveles de implementación de la identificación digital con finalidades funcionales y fundacionales.[17]

Para el estudio, los investigadores seleccionaron cuatro países con base en las iniciativas de digitalización a nivel gubernamental, las consideraciones sobre la brecha digital y la cantidad de información sobre la implementación de sistemas de identidad digital que se encuentra disponible.

Nos basamos en la guía *"¿Qué buscar en los sistemas de Identidad Digital? Una tipología de etapas,"*[18] para analizar la información recopilada, la cual fue propuesta por la Sala de

[16] Puede consultarse la lista completa en el Documento de revisión bibliográfica.
[17] La diferencia principal entre un sistema de identidad digital fundacional y uno funcional es que el primero generalmente es un registro obligatorio que, no solo sirve como identificación, sino que también tiene otros fines, mientras que el segundo se crea con un único propósito, todo esto siguiendo la terminología propuesta por el Banco Mundial.
[18] The Engine Room (La sala de máquinas) (2019). ¿Qué buscar en los sistemas de Identidad Digital? Una tipología de etapas. Consultar: https://www.theengineroom.org/wp-content/uploads/2019/11/Digital-ID-Typology-Espan%CC%83ol-The-Engine-Room.pdf.

Máquinas (una organización sin fines de lucro), y se emplearon varios conceptos localizados en '*Governing ID: Principles for Evaluation*'[19] desarrollado por el Centre for Internet & Society (organización sin fines de lucro), que detalla parámetros para analizar los sistemas de identidad digital. Miembros de otras organizaciones aliadas y expertos de la región han revisado el texto final de este reporte para corregir errores e incoherencias. Este reporte es el resultado de todos esos esfuerzos.

Limitaciones de la investigación

Los temas que se detallan abajo fueron limitantes para este reporte de investigación:

- **Supuestos en las fuentes**: este reporte se basa en material de acceso público, y los estudios e reportes revisados contienen los supuestos de los respectivos autores tanto en sus capacidades individuales como profesionales.

Glosario de términos

Biometría	Este documento se basa en la definición de biometría del Banco Mundial que detalla "el uso de rasgos faciales, patrones de iris o huellas digitales capturados electrónicamente para autenticar la identidad de una persona".[20]
Identidad digital (ID):	Este documento se basa en la definición de identidad digital del Banco Mundial como "un conjunto de atributos y/o credenciales recopilados y almacenados electrónicamente que identifican de forma única a una persona".[21]

[19] Centre for Internet and Society India (Centro de Internet y Sociedad de la India) (2020). Regir la identidad digital: Principios de evaluación. Consultar: https://digitalid.design/docs/CIS_DigitalID_EvaluationFrameworkDraft02_2020.01.pdf.
[20] Grupo del Banco Mundial, 'Brief on Digital Identity,' (reporte sobre identidad digital) https://thedocs.worldbank.org/en/doc/413731434485267151-0190022015/render/BriefonDigitalIdentity.pdf, consultado el 24 de abril de 2023.
[21] Identidad digital: Consultar: https://id4d.worldbank.org/guide/glossary

Sistema de identificación digital	Este documento se basa en la definición de sistemas de identidad digital del Banco Mundial, que indica que son "un sistema de identificación que emplea tecnología digital durante todo el ciclo de vida de la identidad, incluso para la recopilación, validación, almacenamiento y transferencia de datos; la gestión de credenciales; y la verificación de la identidad y la autenticación".[22]

[22] Sistema de identidad digital: Un sistema de identificación que emplea la tecnología digital a lo largo de todo el ciclo de vida de la identidad, incluso para la recopilación, validación, almacenamiento y transferencia de datos; la gestión de credenciales; y la verificación de la identidad y la autenticación (traducción libre). Consultar: https://id4d.worldbank.org/guide/glossary

Resultados: situación actual de los sistemas de identificación digital en América Latina y el Caribe

En esta sección, se describe un resumen general de tres sistemas de identificación digital en cuatro países de América Latina y el Caribe: Bolivia, Brasil, Colombia y Ecuador. Los tres sistemas de identificación digital son: (a) Sistemas de identificación digital fundacionales; (b) Sistemas de identificación digital creados mediante el registro obligatorio de líneas móviles o equipos digitales; y (c) Sistemas de identificación digital funcionales utilizados para fines específicos, como la salud, la seguridad social y el control de la migración.

1. Bolivia

En la República de Bolivia, los dos principales sistemas de identificación digital que capturan los datos de identidad digital de las personas son: el *Servicio General de Identificación Personal* (SEGIP) y el *Servicio de Registro Civil* (SERECI).[23] El Ministerio de Gobierno supervisa al SEGIP y se encarga de expedir los documentos de identidad, mientras que el Tribunal Supremo Electoral administra el SERECI.[24] Las características de estos sistemas incluyen: registro obligatorio, recopilación de datos biométricos y, en el caso del SEGIP, disponibilidad de una versión digital del documento de identidad mediante una aplicación móvil.[25]

El *Registro de Propiedad de Equipos Terminales Móviles y Registro de Titulares de Cuenta* se creó en 2009 mediante el Decreto Supremo n.º 0353. Este registro incluye, sin limitarse a, los datos del titular de la cuenta, el código IMEI y el número de móvil. Las características de este sistema incluyen: el registro obligatorio, la prevención del robo de móviles y la accesibilidad de la base de datos a entidades públicas y privadas.

[23] Venturini, Jamila; Díaz, Marianne (2021). Sistemas de protección social e identificación en Venezuela y Bolivia: vigilancia, género y derechos humanos (Páginas 26 a 28). Consultar: https://www.derechosdigitales.org/wp-content/uploads/sistemas-de-Identificacion_ES.pdf.

[24] ACNUR, OEA, CLARCIEV (2020). Estudio regional sobre inscripción tardía de nacimientos, otorgamiento de documentos de nacionalidad y apatridia. Consultar: https://www.refworld.org.es/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=61a9765b4.

[25] Diario La Razón (2023). Segip activa 'Mi Identidad' para portar el carnet de identidad y la licencia de forma digital. Consultar: 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/.

Asimismo, hay varios sistemas de identificación digital funcionales en ámbitos específicos, particularmente para la seguridad social. Hay bases de datos digitalizadas para la transferencia monetaria de ayudas económicas, el cual incluye el *Bono Juana Azurduy,* y planes de pensiones como *Renta Dignidad*. Registrarse en estas bases de datos es voluntario y son accesibles tanto para las entidades públicas como para las privadas.[26]

2. Brasil

En la *República Federativa do Brasil* (República Federativa de Brasil o Brasil), los datos de identidad digital de las personas se capturan mediante tres registros de identificación digital principales que incluyen: el *Sistema Nacional de Informações de Registro Civil* (Sistema Nacional de *Información* de Registro Civil o SIRC) mantenido por el *Instituto Nacional do Seguro* Social (Instituto Nacional de Seguridad Social o INSS), los Mandatos Electivos - Tribunal *Superior Electoral mantenido por el Tribunal Superior Eleitoral* (TSE) y la *Receita Federal do* Brasil (RFB) mantenido por la *Receita federal do* Brasil (Secretaría de Ingresos Federales de Brasil).[27] Estos sistemas tienen ciertas características, tales como que el registro en los sistemas SIRC y TSE es obligatorio, que el TSE siempre recopila datos biométricos y los tres aportan una tarjeta física o digital que puede utilizarse como documento de identidad.[28]

La creación de un nuevo sistema de identificación digital denominado *Identificación Civil Nacional* (ICN) se aprobó en 2017 bajo la Ley n.º 13.444, que declara la implementación de una base de datos compuesta por distintos registros como el SIRC, TSE, entre otros, y la emisión de un nuevo documento de identidad. Una de las finalidades inmediatas de este sistema es ofrecer acceso a los servicios gubernamentales mediante a través el Portal del Gobierno de Brasil, *Gov.br.*[29]

---

[26] Venturini, Jamila; Díaz, Marianne (2021). Sistemas de protección social e identificación en Venezuela y Bolivia: vigilancia, género y derechos humanos (Páginas 26 a 42). Consultar: https://www.derechosdigitales.org/wp-content/uploads/sistemas-de-Identificacion_ES.pdf.

[27] Banco Mundial (2021). Proceso de inscripción y elegibilidad del Auxílio Emergencial de Brasil: Trato de datos y uso de registros administrativos. Consultar: https://documents1.worldbank.org/curated/en/099255012142136232/pdf/P1748360d7131402e086730fbce1d687fa1.pdf.

[28] BR sobre privacidad de datos (2022). Entre la visibilidad y la exclusión: Descifrar los riesgos asociados al Sistema Nacional de Identificación Civil y el aprovechamiento de su base de datos por la plataforma GOV.BR. Consultar: https://www.dataprivacybr.org/wp-content/uploads/2022/11/Policy-paper-Data-Privacy-Brazil-Research-BETWEEN-VISIBILITY-AND-EXCLUSION.pdf

[29] *Ibid*.

Por último, hay varios sistemas funcionales, de los cuales el más pertinente es el que se utiliza para fines de seguridad social. El *Cadastro Único* (CadÚnico) es una base de datos que mantiene el gobierno federal de Brasil y que los gobiernos de cada estado gestionan, a partir de la cual se identifican los beneficiarios de ayudas económicas como *Bolsa Família*, *ID Jovem*, *Carteira do Idoso*, entre otras. Registrarse en estas bases de datos se hace de forma voluntaria y las entidades públicas tienen acceso a la base de datos.[30]

3. Colombia

En la República de Colombia (Colombia), la *Registraduría Nacional del Estado Civil* (RNEC) mantiene el sistema de identificación digital más importante que captura los datos de identificación digital de las personas (el registro único de identificación), que se encarga de gestionar y organizar el registro civil y la identificación de las personas.[31] Ciertas características de este sistema incluyen: el registro obligatorio, la recopilación de datos biométricos y la disponibilidad de una versión digital del documento de identidad mediante una aplicación móvil.[32]

El Decreto n.º 1630 obligó, en 2011, a registrar por primera vez todos los equipos móviles adquiridos, mediante lo cual se creó el registro de Identidad Internacional de Equipos Móviles (IMEI). Entre otras cosas, esta base de datos está compuesta por los datos del titular del equipo, el código IMEI y el número de móvil. Las características de este sistema incluyen: el registro obligatorio, la prevención del robo de móviles y la accesibilidad de la base de datos a entidades públicas.[33]

Por último, hay varios sistemas funcionales, de los cuales el más notable es el que se utiliza para fines de control de la migración. El Ministerio de Relaciones Exteriores a través de la

[30] ITS Río (2020). Buena identidad digital en América Latina: Fortalecer los usos adecuados de la Identidad Digital en la región (Páginas 49 a 50). Consultar: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf

[31] Registraduría Nacional del Estado Civil, Corporación Opción Legal y ACNUR (2013). Fortalecer el Registro Civil Nacional para ayudar a las poblaciones desplazadas o en riesgo de desplazamiento. Consultar: https://www.acnur.org/fileadmin/Documentos/Publicaciones/2013/9159.pdf?file=fileadmin/Documentos/Publicaciones/2013/9159.

[32] Fundación Karisma (2021). El sistema de reconocimiento facial del Registro Nacional. Consultar: https://digitalid.karisma.org.co/2021/07/01/sistema-reconocimiento-facial-registraduria/.

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

Unidad Administrativa Especial Migración Colombia mantiene la base de datos denominada *Registro Único de Migrantes Venezolanos* (RUMV). La finalidad del RUMV es identificar a los migrantes venezolanos en Colombia y determinar su situación migratoria.[34] El registro en esta base de datos es obligatorio y recopila datos biométricos.[35]

4. Ecuador

En la República del Ecuador (Ecuador), el gobierno ha desarrollado varios sistemas de identificación digital. La *Dirección General de Registro Civil, Identificación y Cedulación* (DIGERCIC) gestiona el sistema de identificación básico de Ecuador. El sistema de identificación fundacional consiste de tres bases de datos: nacimientos y defunciones, registro civil e identificación. Estas bases de datos centralizadas contienen datos biométricos y se utilizan para facilitar distintos servicios de identificación tanto en el sector público como en el privado.[36]

Conjuntamente, el gobierno ha implementado sistemas de identificación funcional con fines policiales. Los ejemplos incluyen el Registro de Dispositivos Móviles Perdidos, Robados o Hurtados y, ostensiblemente, la plataforma de emergencias del Servicio Integrado de Seguridad (ECU 911).[37] Además, recientemente ha desarrollado un sistema que permite votar a distancia.

---

[34] Paula Rossiasco y Patricia de Narváez (2023). Adaptar las políticas públicas en respuesta a una afluencia sin precedentes de refugiados y migrantes: estudio de caso de Colombia relativo a la migración desde Venezuela - Documento de referencia para el reporte sobre el Desarrollo Mundial 2023: Migrantes, refugiados y sociedades. Consultar: 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. Consultar: https://digitalid.karisma.org.co/2021/07/01/sistema-multibiometrico-etpmv/.

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

[37] Danilo Corral-De-Witt *y otros,* (2018). Del E-911 al NG-911: Panorama y retos en Ecuador. Consultar: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1629&context=electricalengineeringfacpub.

Análisis I: Tendencias en la adopción de sistemas de identificación digital

1. Preferencia por las bases de datos de identificación centralizadas

Parece existir una división clara entre los países de ALC analizados que mantienen sistemas de identificación digital centralizados y que son gestionados por una única entidad y los países en los que los sistemas de identificación están descentralizados. Colombia y Ecuador son parte del primer grupo, mientras que Bolivia y Brasil son parte del segundo. Vale la pena destacar que Brasil es una república federal y constitucional, lo cual explica la multiplicidad de registros y entidades que prestan servicios de identidad.

Como se ha demostrado en los casos de Colombia y Ecuador, hemos notado que los sistemas de registro centralizados han facilitado una adopción e implementación más rápida de la identificación digital y las tecnologías biométricas en los sistemas de identificación. Distintas organizaciones han destacado los graves riesgos que entraña la creación y el mantenimiento de bases de datos centralizadas.[38] A modo general, la adopción de bases de datos centralizadas que procesan datos biométricos por parte de los organismos gubernamentales para prestar servicios plantea un gran riesgo para la protección del derecho a la intimidad. Para grandes cantidades de información personal y sensible de las personas, las bases de datos de identificación centralizadas crean un único punto de fallo. En este contexto, los organismos públicos de la región de América Latina han estado sujetos a ataques de ransomware, lo cual han causado el cierre de sistemas y servicios para evitar nuevas intrusiones en sitios web y bases de datos.[39]

Adicionalmente, las bases de datos centralizadas limitan el control y la propiedad de las personas a nivel individual sobre sus datos personales y sensibles y aportan acceso y

[38] Privacy International (2021). Sistemas de identificación nacional digital: Maneras, formas y formularios. Consultar: https://privacyinternational.org/long-read/4656/digital-national-id-systems-ways-shapes-and-forms.

[39] Semana de la seguridad (2022). Ataques de ransomware contra agencias gubernamentales en América Latina. Consultar: https://www.securityweek.com/ransomware-attacks-target-government-agencies-latin-america/.

control ilimitados a la autoridad de gestión. No hay claridad sobre el marco legal que sustenta el desarrollo de sistemas de identificación digital en Ecuador, en particular en el caso del Registro Civil. Asimismo, a pesar de que la Ley Orgánica de Protección de Datos de Carácter Personal se promulgó el 26 de mayo de 2021, todavía no ha entrado en vigor.[40] Conjuntamente, el sistema ECU 911 tiene características de reconocimiento facial mediante las cuales el gobierno puede rastrear los teléfonos de las personas, lo que plantea riesgos muy graves para el derecho a la privacidad.[41]

Por otra parte, el segundo grupo de países tiene distintos procesos de registro de identificaciones y hay distintas entidades encargadas de su mantenimiento. Si bien generalmente las bases de datos descentralizadas dan prioridad a que los usuarios mantengan la propiedad y el control sobre sus datos de identidad mediante un riesgo reducido de filtración de datos, hacen que sea más difícil establecer una infraestructura de identidad unificada e interconectada (o un desafió de la interoperabilidad). A pesar de esto, hay iniciativas que se enfocan en centralizar las bases de datos de los países del segundo grupo. Brasil aprobó un nuevo sistema en 2017, con el fin de unificar todos sus registros de identidad en una base de datos única.[42]

La conclusión es que existe una tendencia a favorecer el modelo de identificación digital centralizado en la región de América Latina contra otras opciones como los modelos descentralizado, federado o de mercado abierto.[43]

[40] DLA Piper (2023). Leyes de protección de datos del mundo: Ecuador. Consultar: 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). El NYT investiga las exportaciones del Estado de vigilancia de China. Consultar: https://www.theverge.com/2019/4/29/18522248/china-surveillance-state-exporting-ecuador-senain-ecu-911-privacy-facial-recognition-tracking.

[42] BR sobre privacidad de datos (2022). Entre la visibilidad y la exclusión: Descifrar los riesgos asociados al Sistema Nacional de Identificación Civil y el aprovechamiento de su base de datos por la plataforma GOV.BR. Consultar: https://www.dataprivacybr.org/wp-content/uploads/2022/11/Policy-paper-Data-Privacy-Brazil-Research-BETWEEN-VISIBILITY-AND-EXCLUSION.pdf.

[43] Banco Mundial (2023). Tipos de sistemas de identificación. Consultar: https://id4d.worldbank.org/guide/types-id-systems.

2. Aumento del tratamiento de datos biométricos sin suficientes garantías de derechos humanos

La cantidad de empresas del sector privado que desarrollan tecnologías biométricas y la cantidad de Estados que han implementado estas tecnologías ha aumentado exponencialmente.[44] Tal como indica *La Asociación por los Derechos Civiles* (ADC) en el reporte, *Tu Yo Digital - Revelación de las Narrativas sobre Identidad y Biometría en América Latina,* varios países de América Latina han desarrollado relativamente exitosamente "narrativas vinculadas a la necesidad de la tecnología biométrica para el reconocimiento infalible de la identidad de las personas"[45] lo cual permite la recopilación y procesamiento de datos biométricos en sistemas de identificación fundacional y funcional bajo argumentos extensos y sin límites preestablecidos para su uso. Esto es coherente tanto en los países unitarios como en los federales de la región de ALC.

Todos los países analizados están recopilando y procesando datos biométricos en una o varias bases de datos de identificación digital sin llevar a cabo una evaluación previa de las repercusiones sobre los derechos humanos para identificar y medir el efecto de esta recopilación sobre los derechos humanos de las personas, lo cual se hace mediante entidades gubernamentales gestoras, como se ha detallado arriba. Esta situación ha hecho posible que se implementen sistemas de identificación y autenticación biométricos con capacidad de reconocimiento facial y de huellas digitales, aumentado exponencialmente de esta manera los peligros asociados a la vigilancia estatal, además de las brechas de seguridad. Los investigadores no fueron capaces de localizar ningún estudio ni reporte público de evaluación de las repercusiones sobre los derechos humanos de los sistemas de identificación digital implementados en todos los países estudiados.

La recopilación de datos biométricos en países como Brasil y Colombia se lleva a cabo sin una base jurídica adecuada. La recopilación de datos biométricos no ha sido delimitada de forma expresa y precisa por la ley a pesar de que ambos países han promulgado leyes de

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

protección de datos, lo cual desafía el principio de legalidad.[46] Los Estados en cuestión tienen margen para utilizar datos con múltiples fines, al no tener parámetros claros sobre la recopilación de datos biométricos, sus usos y delimitaciones.[47]

En un informe de 2022 en el que examinaban la *Identificação Civil Nacional* (ICN) de Brasil, Bruno Bioni y otros demostraron que existe una tensión entre la ICN y la ley de protección de datos de Brasil. El reporte indicaba que la arquitectura del ICN "[es] una base de datos personales a gran escala, que consiste de la fusión de otras bases de datos, con una estructura centralizada, [que] presenta riesgos en términos de protección de datos y privacidad, como posibilidades de uso secundario abusivo de los datos, inseguridad de los mismos y vigilancia gubernamental".[48]

Distintas organizaciones han destacado varias veces los graves riesgos relativos a la creación y el mantenimiento de bases de datos centralizadas.[49] Por otro lado, todos los países analizados en este reporte mantienen una o varias bases de datos de este tipo, muchas de las cuales contienen datos biométricos.

No obstante, la tendencia en la región parece apuntar a la profundización de estas prácticas, lo que incluye la creación de sistemas de identidad digital funcionales que incorporan datos biométricos, incluso cuando los sistemas tradicionales en los que se basan no habían incorporado tales datos en el pasado. Esto quiere decir que, generalmente, la adopción de cualquier sistema de identidad digital sería un posible facilitador de la proliferación de tecnologías biométricas, algunas de las cuales están en ámbitos particularmente críticos como la seguridad pública, el acceso a los servicios de la seguridad social y el control de la inmigración.

---

[46] *Ibid.*

[47] BR sobre privacidad de datos (2022). Entre la visibilidad y la exclusión: Descifrar los riesgos asociados al Sistema Nacional de Identificación Civil y el aprovechamiento de su base de datos por la plataforma GOV.BR. Consultar: https://www.dataprivacybr.org/wp-content/uploads/2022/11/Policy-paper-Data-Privacy-Brazil-Research-BETWEEN-VISIBILITY-AND-EXCLUSION.pdf.

[48] Bruno Bioni y otros, (2022). The digitization of the Brazilian national identity system: A descriptive and qualitative analysis of its information architecture. (La digitalización del sistema brasileño de identidad nacional: un análisis descriptivo y cualitativo de su arquitectura de la información.) Consultar: 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.*

La conclusión es que la recopilación y el tratamiento de datos biométricos está aumentando, guiado por narrativas que presentan la inclusión de datos biométricos como necesaria para la implementación de sistemas de identificación digital, sin suficientes salvaguardias de los derechos humanos.

3. Proveedores comunes de tecnologías de vigilancia e identificación digital/biométrica

Mediante los reportes de Access Now, una organización internacional de derechos digitales sin fines de lucro, [50] y AlSur, un consorcio de organizaciones de la sociedad civil y académicas de América Latina,[51] es posible concluir que el mercado tecnológico que facilita herramientas de vigilancia a los gobiernos está dominado por unos pocos grandes proveedores, tales como AnyVision, Hikvision, Dahua, Cellebrite, Huawei, ZTE, NEC, IDEMIA y VERINT, entre otros.

Este reporte se alinea con las declaraciones hechas por ITS Ríos en su reporte titulado Buena identidad digital en América Latina: *Fortalecer los usos adecuados de la Identidad Digital en la región*[52] el cual detalla que no existe una diferencia básica entre los sistemas de identificación digital y un sistema de vigilancia estatal. Este reporte destaca que algunos de los proveedores de productos y sistemas de identificación digital y tecnologías de identificación biométrica que se mencionan en la lista son las mismas empresas que aportan tecnologías de vigilancia a los Estados. Particularmente, la empresa francesa IDEMIA (antes conocida como OT-Morpho) presta o ha prestado servicios de identificación digital a Colombia.[53]

[50] Access Now (2021). Tecnología de vigilancia en América Latina: Hecho en el extranjero, desplegado a nivel nacional. Consultar: 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. Consultar: https://www.alsur.lat/sites/default/files/2021-11/ALSUR_Reconocimiento_facial_en_Latam_ES.pdf.
[52] ITS Río (2020). Buena identidad digital en América Latina: Fortalecer los usos adecuados de la Identidad Digital en la región (Página 11). Consultar: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf.
[53] Fundación Karisma (2021). El sistema de reconocimiento facial del Registro Nacional. Consultar: https://digitalid.karisma.org.co/2021/07/01/sistema-reconocimiento-facial-registraduria/.

Las empresas que ofrecen tecnologías biométricas y de vigilancia muestran una falta de aprecio por las repercusiones de su uso para las poblaciones objetivo de la región de ALC, de acuerdo con los reportes citados. Conjuntamente, suelen mostrar desinterés por establecer normas que sean transparentes, mecanismos de rendición de cuentas y salvaguardias de los derechos humanos dentro de su industria. Es claro que muchos proveedores de tecnología de vigilancia no siguen los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos, particularmente aquello relativo a su compromiso de respetar los derechos humanos, aplicar procesos de diligencia debida para identificar y prevenir daños importantes a los derechos humanos y divulgar abiertamente información sobre el cumplimiento de las leyes vigentes.[54]

[54] Access Now (2023). Vigilancia biométrica remota en América Latina: ¿las empresas están respetando los derechos humanos? Consultar: https://www.accessnow.org/wp-content/uploads/2023/04/ESPANOL-Analysis-Remote-biometric-surveillance-LATAM.pdf.

Análisis II: Riesgos de la identificación digital para los derechos humanos

En esta sección, se detallan los riesgos principales de los sistemas de identificación digital fundacionales o funcionales para los derechos humanos. Este material no es exhaustivo.

1. La ambigüedad del concepto de identificación digital impide delimitar la finalidad y el ámbito de aplicación

No hay una definición del concepto de "identificación digital" que se acepte a nivel universal. Organizaciones internacionales como el Banco Mundial, el Sindicato Internacional de Telecomunicaciones (UIT) y la Organización de Cooperación y Desarrollo Económicos (OCDE) han propuesto definiciones similares, pero que tienen un problema básico: no permiten delimitar la finalidad y el alcance de estos sistemas.

Si bien esta ambigüedad aporta flexibilidad en la prestación de servicios públicos y privados y promueve la innovación, hemos notado que también es capaz de desarrollar prácticas de aplicación incoherentes, lo cual resulta en ecosistemas de identificación digital fragmentados e ineficaces. También, la falta de adopción de un concepto universalmente acordado impide el desarrollo de normas de privacidad y seguridad armonizadas y estandarizadas, obteniendo de esta manera diferencias en el nivel de protección de la privacidad en los países de América Latina.

Algo que nos preocupa es que esta ambigüedad haya permitido a los países de ALC expandir de forma continua el ámbito legal de sus bases de datos de identificación digital más allá de la identificación para que cubra cualquier propósito identificado como una necesidad del Estado, lo cual incluye el control de la migración y el ofrecimiento de programas de seguridad social. Si los límites de los sistemas de identificación digital no se establecen de forma clara y expresa, es más difícil para las partes interesadas (como las OSC encargadas de garantizar la transparencia, la rendición de cuentas y la protección de los derechos de las personas) evaluar el nivel de amenazas y riesgos para los derechos humanos en relación

con los límites preestablecidos, incluso cuando el uso de cierta terminología se acuerda por consenso.

2. Transparencia y participación pública deficientes

Los tres países analizados en este reporte -salvo en el caso de Brasil, donde la adopción de su nuevo sistema de identificación digital se ha llevado a cabo a través de una reforma legal- no han modificado sus procesos y sistemas de identificación digital mediante un proyecto de ley u otra normativa que facilite procesos de debate extensos y participativos.[55]

Esto significa efectivamente que los sistemas de identificación digitalizados de algunos países de América Latina se han implementado sin transparencia ni participación pública. A modo de ejemplo, el gobierno de Colombia implementó tecnologías de reconocimiento facial en la Registraduría Nacional del Estado Civil en 2018, pero esta medida no fue dada a conocer al público.[56] La confianza del público en el gobierno en lo que respecta al uso de estas tecnologías se ha visto afectada gradualmente por este y otros casos.

Además de la falta de regulación específica sobre la identificación digital, no todos los países analizados cuentan con leyes y reglamentos que establezcan límites específicos a la adopción y uso de estos sistemas. Por ejemplo, en Bolivia no hay una ley de protección de datos personales en la actualidad, mientras que otros países se enfrentan a problemas de aplicación.[57]

[55] Asociación por los Derechos Civiles (2019). Tu yo digital - Descubriendo las narrativas sobre identidad y biometría en América Latina (Página 28). Consultar: https://adc.org.ar/informes/tu-yo-digital-descubriendo-las-narrativas-sobre-identidad-y-biometria-en-america-latina/.

[56] Fundación Karisma (2021). El sistema de reconocimiento facial del Registro Nacional. Consultar: 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 (Páginas 27 a 35). Consultar: https://internetbolivia.org/file/2021/11/ib_conectados.pdf.

Comentarios y recomendaciones

Este reporte divulga que los sistemas de identificación digital se utilizan con fines tanto funcionales como fundacionales en cuatro países de América Latina que se analizaron en este reporte, y los cuatro países recopilan y procesan datos biométricos con distintas finalidades. En particular, algunos sistemas de identificación digital se encuentran en una fase inicial, mientras que otros ya han admitido que se presten servicios gubernamentales. Principalmente, estos sistemas de identificación son centralizados, y los investigadores no fueron capaces de localizar ningún estudio ni reporte de evaluación de repercusiones sobre los derechos humanos disponible públicamente para los sistemas de identificación digital implementados en todos los países del estudio. Con base a esto, la conclusión es que la mayoría de los países de América Latina no han internalizado los riesgos relativos a los derechos humanos ni aportado medidas de mitigación para abordarlos.

Sobre esta base, se proponen las siguientes recomendaciones a los gobiernos y a los agentes de la sociedad civil de cuatro países de América Latina el reporte.

Recomendaciones

En esta sección, se detalla una serie de recomendaciones enfocadas a los Estados y a las organizaciones de la sociedad civil.

A los Estados y Gobiernos nacionales

Alentamos encarecidamente a los Estados y gobiernos nacionales de la región de América Latina y el Caribe a:

- **Realizar evaluaciones de impactos sobre los derechos humanos (EIDH) antes de implementar sistemas de identificación digital y supervisar su aplicación para responder a las repercusiones sobre los derechos humanos:** Las EIDH deben satisfacer los principios internacionalmente reconocidos de legalidad, necesidad y proporcionalidad. Una vez que se hayan implementado sistemas de identificación digital, alentamos a los gobiernos a que auditen públicamente sus

sistemas y procesos de identificación digital para evaluar y abordar las repercusiones sobre los derechos humanos.

- **Desarrollar mecanismos de rendición de cuentas y participación de varias partes interesadas antes y durante la implementación de sistemas y procesos de identificación digital:** Adoptar un enfoque participativo para la implementación de sistemas de identificación digital que implique y comprometa a las partes interesadas en el diseño y la implementación, al garantizar que los aportes del público se incorporen al producto final. Los Estados deben informar al público con suficiente antelación sobre la adopción prevista de un sistema de identificación digital, o sobre cualquier actualización del sistema de identificación existente, de manera que permita un compromiso y un debate significativos, todo esto al estar guiados por el principio de transparencia del derecho internacional.
- **Desarrollar y/o adaptar la legislación de protección de datos personales de acuerdo con las normas de derechos humanos:** Los Estados de América Latina y el Caribe deben promulgar o modificar sus leyes de protección de datos, de forma que se definan claramente las normas y se adopten salvaguardias diferenciadas para la recopilación y el tratamiento adecuado de datos sensibles, particularmente los biométricos. Conjuntamente, es necesario que todas las autoridades o entidades encargadas de gestionar o implementar sistemas de identificación digital satisfagan las leyes nacionales de protección de datos o los principios internacionales de protección de datos, antes de proceder al tratamiento de los datos, lo cual incluye la realización de evaluaciones de repercusiones sobre la protección de datos.
- **Establecer salvaguardias en relación con la protección de los datos recopilados y almacenados en bases de datos que sean suficientes:** para esto, se debe hacer que las autoridades de protección de datos sean operativas para poder permitir la aplicación de salvaguardias de protección de datos y supervisar a las entidades que procesan datos en sistemas de identificación digital. Específicamente, se deben proteger los datos personales con salvaguardias de seguridad razonables contra riesgos como la pérdida o el acceso no autorizado, la destrucción, el uso, la modificación o la divulgación de datos.

- **Modificar las leyes de identidad para que la recopilación de datos biométricos sea opcional:** los Estados deben desvincular el acceso de las personas a los servicios públicos y privados de la obligatoriedad de facilitar datos biométricos.

A las Organizaciones de la Sociedad Civil

Solicitamos con ánimo a las OSC de la región de América Latina y el Caribe a:

- **Llevar a cabo una investigación más extensa y profunda relativa a la identificación digital en la región de ALC en general:** para identificar usos y tendencias que este reporte no haya podido cubrir, dado su carácter exploratorio, incluyendo estudios de casos para identificar prácticas recomendadas que se enfoquen en los derechos humanos. Como puntos de partida útiles, recomendamos los siguientes temas:
    - ❖ Comparación entre los sistemas de identificación digital desarrollados en países unitarios y federales y cómo estas diferencias afectan los derechos humanos.
    - ❖ Narrativas gubernamentales relativas a la necesidad de implementar sistemas de identificación digital y cómo el sector privado o la sociedad civil los han recibido y abordado (cuando se ha dado el caso).
    - ❖ Financiación de sistemas de identificación digital para identificar qué organizaciones internacionales han estado operando en la región y por qué pretenden fomentar estos sistemas.
- **Realizar campañas de promoción y emprender litigios estratégicos para impugnar los sistemas de identificación digital que sean perjudiciales para los derechos humanos:** emprender campañas de fomento y litigios estratégicos para impugnar los sistemas de identificación digital que no satisfagan los principios de derechos humanos en materia de legalidad, necesidad, proporcionalidad, garantías procesales, mecanismos de control y derecho de recurso, transparencia activa,

evaluación previa de las repercusiones, debate democrático para su adopción y garantías de cooperación internacional.[58]

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

Anexo 1: Caso práctico del Ecuador

Introducción

Estudios en todo el mundo han concluido que el desarrollo de políticas públicas y el despliegue de sistemas de identificaciones digitales pueden crear graves problemas de derechos humanos y profundizar vacíos existentes, reforzando o creando nuevos tipos de discriminación.[59] En el mismo sentido, las organizaciones internacionales han manifestado su preocupación sobre el uso de tecnologías intrusivas, como la biometría y el reconocimiento facial, que se utilizan con frecuencia estos sistemas, y han abogado por reevaluar su adopción, tomando en cuenta los principios de necesidad y proporcionalidad de las normas internacionales de derechos humanos.[60]

En el marco del proyecto Greater Internet Freedom (GIF), Derechos Digitales llevó a cabo en 2023 una investigación exploratoria para entender el nivel de adopción de sistemas de identificación digital en América Latina y el Caribe, al igual que para identificar tendencias y problemas regionales. Uno de los resultados de esta investigación fue reconocer la necesidad de casos prácticos para analizar, en mayor profundidad y detalle, los procesos para implementar tecnologías asociadas a la identificación digital y evaluar el escenario de riesgos y amenazas a los derechos personales, al igual que potenciales estrategias de defensa y de litigación.

Lógica del caso práctico

El país seleccionado para este estudio es la República del Ecuador, lo cual fue decidido por varias razones. Para empezar, es escasa la investigación local sobre sistemas de identificación digital que adopte un enfoque de derechos humanos. Por último, dado que Ecuador comparte características comunes con sus vecinos, como Colombia, los resultados pueden servir de guía para una investigación detallada del futuro de los sistemas de identificación digitales de estos países, y más allá de la región.

[59] Por favor refiérase a la sección de bibliografía para ver más detalles.

[60] Por ejemplo, el informe "Estándares para una Internet libre, abierta e incluyente" de 2017 de la Relatoría Especial para la Libertad de Expresión de la OEA (Organización de Estados Americanos); Resolución N.º 48/31 de 2021 del Consejo de Derechos Humanos; y la Resolución 77/211 de 2022 de la Asamblea General de las Naciones Unidas.

Durante la preparación de este caso práctico, ocurrió un evento significativo en Ecuador: el 17 de mayo de 2023, el presidente Guillermo Lasso disolvió la Asamblea Nacional y convocó elecciones generales mediante un mecanismo constitucional conocido como "muerte cruzada." Esta acción, que fue la respuesta a un proceso iniciado por la Asamblea para destituirlo, empeoró la crisis social y política en la que ha estado inmersa el Ecuador desde el comienzo de su administración en 2021.[61] Esta situación política afectó de manera importante la dinámica de las entrevistas realizadas para este caso práctico, y a su vez, planteó interrogantes acerca de la necesidad de proseguir la investigación.

Previo a los eventos del 17 de mayo, este caso práctico trataba de revelar el nivel de desarrollo local de los tres sistemas de identificación digital más comunes en la región, a saber (a) sistemas fundacionales de identificación digital; (b) sistemas de identificación digitales basados en el registro obligatorio de líneas o dispositivos móviles; y (c) sistemas funcionales de identificación digital utilizados en dominios específicos. En relación con los hallazgos, se intentó analizar el escenario de riesgos y amenazas a los derechos, considerando varios elementos como el marco operativo de los sistemas identificados y las normas que generalmente imponen límites a su desarrollo, como los reglamentos de protección de datos personales.

Sin embargo, después de la disolución de la Asamblea, se llevó a cabo una revisión exhaustiva del documento y se ajustaron las preguntas del cuestionario para contextualizar los hallazgos, haciendo énfasis en elementos que podrían ser más relevantes en vista de la situación actual del país. Así, aunque la primera sección, que describe la situación de los sistemas de identificación digitales, sigue el patrón del informe regional, las secciones sobre tendencias y problemas han sido adaptadas de manera que la información esté en línea con este nuevo escenario.

¿Cómo aparecen los cambios realizados? Antes de la revisión, se había identificado la plataforma de emergencia ECU 911, Servicio Integrado de Seguridad, como el vector de análisis más importante, ya que es la mayor plataforma de vigilancia estatal en el país, y se desconoce si esta opera con el sistema de identificación digital del Registro Civil. De manera

[61] La República (2023). El presidente del Ecuador disuelve la Asamblea Nacional en medio de un proceso de destitución. Véase: https://www.larepublica.co/globoeconomia/el-presidente-de-e.

similar, el análisis del sistema de votación telemática había sido inicialmente pospuesto debido a su mínima relación con la identificación digital. Sin embargo, después de su revisión, el análisis de la plataforma ECU 911 ha sido ampliado para abordar el potencial papel que podría jugar durante el interregno. Además, se reanudó el análisis del voto telemático en vista de su probable utilización en las próximas elecciones.

Finalmente, este caso práctico ofrece una serie de recomendaciones para el gobierno ecuatoriano y las organizaciones de la sociedad civil de ese país que trabajan en los problemas relacionados con la identificación digital.

Metodología

Este caso práctico complementa el informe regional de América Latina y el Caribe "*identificación digital en América Latina: situación actual, tendencias y problemas*", publicado en el marco del proyecto Greater Internet Freedom (GIF) de USAID implementando por Internews y el consorcio GIF. En este estudio práctico, adoptamos el mismo enfoque exploratorio pero proporcionamos información más detallada, granular, dentro del marco del modelo de análisis utilizado en la investigación regional. Este enfoque fue seleccionado para garantizar que ambos informes exploratorios puedan leerse como un continuo compuesto de una descripción general y otra sección más específica y analítica.

Este caso práctico adopta un enfoque cualitativo que consiste en investigación secundaria y terciaria complementada con entrevistas con actores clave del ecosistema digital ecuatoriano. Estas entrevistas permitieron a los investigadores validar, corregir, y ampliar la información presentada.

Para analizar la información recolectada, consultamos la guía *"Qué buscar en los sistemas de identificación digital? Una tipología de etapas,"*[62] propuesta por Engine Room (una organización sin fines de lucro), y utilizamos varios conceptos ubicados en "*Governing ID: Principles for Evaluation"*[63] [La identidad que gobierna: principios para su evaluación] desarrollados por el

[62] The Engine Room (2019). ¿Qué buscar en los sistemas de identificación digital? Una tipología de etapas. Véase: 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). La identidad que gobierna: principios para su evaluación. Véase: https://digitalid.design/docs/CIS_DigitalID_EvaluationFrameworkDraft02_2020.01.pdf.

Centre for Internet & Society (organización sin fines de lucro), que resume parámetros para la evaluación de sistemas de identificación digital.

De forma similar a la investigación regional, este texto utiliza las definiciones de *identidad digital*[6] *y sistemas de identificación digital* propuestos por el Banco Mundial, lo que permite que pueda leerse como una respuesta a la investigación realizada por este ente.[64] De la misma forma, seguimos la línea de pensamiento propuesta por el *Instituto de Tecnologia & Sociedade do Río* (ITS Rios) en su informe "*Buena identificación en América Latina: Fortaleciendo los usos adecuados de identificación digital en la región*"[65] en el que indican que, dentro del concepto de identificación digital, también entran dentro de esta categoría ciertos sistemas identificados por otros estudios como sistemas de vigilancia.

La disolución de la Asamblea Nacional el 17 de mayo de 2023 no ha afectado la metodología de este estudio; sin embargo, sí influyó en las preguntas de las entrevistas y ciertos enfoques de análisis de datos. Esto es así primordialmente de manera que el resultado final siga conectado con la situación actual en Ecuador.

El equipo de derechos digitales de Derechos Digitales y los expertos regionales, incluidos algunos de los entrevistados, realizaron varias rondas de revisión.

Resultados: Situación actual de los sistemas de identificación digital en Ecuador

El informe regional documenta que cuatro países bajo exploración como parte del proyecto GIF tienen sistemas de identificación digital, tanto fundacionales como funcionales.[66] En la mayoría de los casos, los primeros están constituidos por bases de datos digitalizados de las

[64] I**dentidad digital**: Un juego de atributos o credenciales capturados y almacenados electrónicamente que identifican de forma única a una persona (traducción libre). **Sistemas de identificación digital:** Un sistema de identificación que utiliza tecnología digital a través del ciclo de vida identitario, incluidos captura, validación, almacenamiento y transferencia de datos, gestión de credenciales, y verificación y autenticación de identidad digital (traducción libre). Banco Mundial (2019) Guía para profesionales: Glosario Véase: https://id4d.worldbank.org/guide/glossary.

[65] ITS Río (2020). Buena identificación en América Latina: fortaleciendo los usos apropiados de la identificación digital en la región (página 11). Véase: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf.

[66] En consonancia con la terminología propuesta por el Banco Mundial, la principal diferencia entre un sistema de identificación digital fundacional y uno funcional es que este último es normalmente un registro obligatorio que, además de la identificación, puede servir otros fines, mientras que el primero está creado con un solo propósito.

autoridades responsables de los registros civiles, mientras que los segundos incluyen un amplio rango de sistemas que abarcan desde la prestación de servicios sanitarios hasta el control de la inmigración, y son operados por entidades con competencias en esas áreas. Similarmente, se identificó una tendencia a favor de la creación de registros unificados y la recolección obligatoria de datos biométricos.

Esta sección presenta una perspectiva general que identifica el nivel actual de adopción de sistemas de identificación digital en Ecuador. Esta revisión es preliminar, no exhaustiva, y se centra en la descripción de tres tipos de sistemas: a) sistemas de identificación digital fundacional; b) sistemas de identificación digital basados en el registro obligatorio de líneas o dispositivos móviles con fines policiales; y c) sistemas de identificación digital en dominios específicos, al igual que iniciativas relacionadas.

1. Sistemas de identificación digital fundacionales

El sistema de identificación digital más importante en Ecuador es el conjunto de registros personales digitalizados creados y mantenidos por la Dirección General de Registro Civil, Identificación y Cedulación (DIGERCIC). A nivel de reglamentación, este sistema se rige por las disposiciones de la Ley Orgánica de Gestión de Identidad y Datos Civiles aprobada en 2016. Esta ley establece que la inscripción de personas en el registro es obligatoria desde el nacimiento, momento en el cual se capturan datos biométricos que serán actualizados según sea necesario a través del tiempo.[67]

Este sistema presenta una combinación única de características que puede parecerse o diferir de otras prácticas de la región. Por ejemplo, Ecuador recolecta datos biométricos, como huellas digitales e imágenes faciales.[68] Ecuador ha utilizado el sistema para apoyar la prestación de servicios en línea, procedimientos, y pagos en línea.[69] Sin embargo, a diferencia de Colombia, el Registro Civil crea y mantiene no solo bases de datos de ciudadanos ecuatorianos, sino también de residentes extranjeros en el país.

---

[67] Registro Oficial del Ecuador (2018). Ley Orgánica de Gestión de Identidad y Datos Civiles. Véase: 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] Portal del Gobierno del Ecuador. Procedimientos en línea. Véase: https://www.gob.ec/dashboard/tramites-en-linea.

También es interesante anotar que el Registro Civil ha utilizado este sistema para proveer servicios de identificación. Uno de estos usos es la emisión de certificados de firma electrónica, una operación regulada por la Ley de Comercio Electrónico, Firmas y Mensajes de Datos aprobada en 2002.[70] La otra es la venta directa del servicio a entidades privadas a través del Sistema Nacional de Identificación Ciudadana, que funciona bajo contratos de subscripción que no tienen un fundamento legal claro, una práctica que también ha sido identificada en los sistemas de identificación digital del Perú.[71]

2. Sistemas de identificación digital basados en registros de líneas o dispositivos móviles.

En 2009 fue aprobada la Resolución 191-07-CONATEL-2009, la cual creó la Norma que rige el procedimiento para inscribir suscriptores de Servicios Móviles Avanzados (SMA) y el registro de terminales perdidos, robados o hurtados (la Norma) Esta Norma, que ha sido modificada hasta dos veces, ordena la creación de dos listas, una para permitir la operación de dispositivos (lista positiva) y otra para ordenar su bloqueo (lista negativa). El sistema es gestionado por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) y es actualizado por las empresas de telecomunicaciones.[72]

El registro en Ecuador comparte características similares con sus contrapartes en la región, como Bolivia y Colombia. Para comenzar, es obligatorio y contiene datos personales del propietario, código IMEI, número móvil, al igual que datos asociados con el estatus del dispositivo (perdido, robado, etc.). Por otro lado, la Norma establece que el acceso a esta base de datos está disponible para la *Agencia de Regulación y Control de las Telecomunicaciones* (*ARCOTEL,* y también para cualquier otra entidad competente ligada a "asuntos de seguridad nacional", lo cual es amplio y tiene un alcance no definido.[73]

[70] Ley del Ministerio de Telecomunicaciones sobre Comercio Electrónico, Firmas y Mensajes de Datos (2012). Véase: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Messajes-de-Datos.pdf.
[71] ONG Hiperderecho (2018). ¿Cómo vende nuestros datos personales el RENIEC (Registro de Identificación y Estado Civil? Véase: https://hiperderecho.org/2018/07/como-asi-reniec-vende-nuestros-datos-personales/.
[72] Consejo Nacional de Telecomunicaciones (2019). Resolución 191-07-CONATEL-2009. Véase: https://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/07/191_07_conatel_20091.pdf.
[73] Consejo Nacional de Telecomunicaciones (2012). Resolución TEL 535-18-CONATEL-2012. Véase: https://www.gob.ec/sites/default/files/regulations/2018-11/TEL-535-18-CONATEL-2012.pdf.

3. Otros sistemas de identificación digital

Finalmente, existen otros sistemas funcionales en dominios específicos. Lo más llamativo es el posible uso de sistemas de identificación para complementar el uso de cámaras de videovigilancia, especialmente las que están equipadas con tecnologías de reconocimiento facial. Como lo indica la organización internacional de derechos digitales sin fines de lucro Access Now en su informe "*Tecnología de vigilancia en América Latina: fabricada en el extranjero, desplegada en casa,*" [74] estas tecnologías han sido desplegadas en el Ecuador desde 2002 con el supuesto fin de contribuir a la seguridad pública; muchas de estas tecnologías forman parte del Servicio Integrado de Seguridad ECU 911 (ECU 911).[75]

Aunque la evidencia sugiere que la adopción de estos sistemas es extensa, no hay información oficial disponible para determinar si estas capacidades son utilizadas en conjunto con bases de datos biométricas, y si es así, cuál entidad mantiene estas bases de datos. El informe "La videovigilancia en Ecuador viola los derechos ciudadanos" de la organización FUNDAMEDIOS, una organización regional sin fines de lucro que defiende los derechos digitales en las Américas señala que no es posible responder esta pregunta porque los protocolos operativos de la plataforma ECU 911 han sido clasificados como confidenciales hasta el 2028.[76]

Existe también otro sistema, el Sistema de Votación Telemática en el Exterior, que es aún más opaco, a pesar de que se espera que sea utilizado en las elecciones generales pautadas para agosto de 2023. El Sistema de Votación Telemática en el Exterior es un mecanismo de votación telemática no presencial habilitado por el Consejo Nacional Electoral (CNE) para permitir votar a los ecuatorianos que residen en el exterior.[77] Este sistema valida la identidad de los votantes mediante dos métodos, uno de los cuales es el reconocimiento

[74] Access Now (2021). Tecnología de vigilancia en América Latina: fabricada en el extranjero, desplegada en casa. Véase: https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf.
[75] Portal del Gobierno del Ecuador (2018). Las innovaciones tecnológicas de la plataforma ECU 911 para la atención de emergencia fueron presentadas en Smart City 2018. Véase: https://www.ecu911.gob.ec/innovaciones-tecnologicas-del-ecu-911-para-la-atencion-de-emergencias-se-presentaron-en-smart-city-2018/.
[76] FUNDAMEDIOS (2021). La videovigilancia en Ecuador viola los derechos ciudadanos. Véase: https://www.fundamedios.org.ec/wp-content/uploads/2021/12/Inf.-Videovigilancia.pdf.
[77] Junta Nacional Electoral (2023). Votación telemática 2023. Véase: https://www.voto-telematico.cne.gob.ec/ayuda.

facial. No está claro qué base de datos opera, si es el registro electoral del CNE o a través de interoperabilidad con el Registro Civil.[78]

Análisis I: Tendencias de los sistemas de identificación digital en Ecuador

El informe regional identificó las siguientes tendencias: la promoción de modelos centralizados de identificación digital; la prevalencia de narrativas que enfatizan la absoluta necesidad de la recolección de datos biométricos; la ausencia generalizada de enfoques incluyentes en el desarrollo de sistemas de identificación digital; y la existencia de proveedores de productos y servicios de identificación digital que también venden tecnologías con capacidad de vigilancia.

Esta sección presenta un recuento de las principales tendencias identificadas en los sistemas de identificación digital representados en el Ecuador. El estudio comienza con el análisis de las tendencias fundacionales identificadas en el informe regional para replicar los observados en los países vecinos. Sin embargo, el foco principal yace en resaltar las características distintivas que puedan estar presentes en el Ecuador. En algunos casos, la información ha sido refinada con base en información obtenida en las entrevistas. Esta información es preliminar y no es exhaustiva.

1. Ecuador ejemplifica las prácticas de identificación digital más riesgosas

Ecuador tiene una base de datos centralizada gestionada por el Registro Civil, y la inscripción es obligatoria para todas las personas. La legislación de identificación establece la recolección y el almacenamiento de datos biométricos de las personas inscritas, incluso desde el nacimiento. Debe hacerse notar que esta base de datos documenta información tanto de los ciudadanos como de los extranjeros residentes en el país, lo cual no es una práctica común en la región. De manera similar, el Registro Civil actualmente ofrece

[78] Junta Nacional Electoral (2023). Manual de inscripción para la votación telemática. Véase: https://www.voto-telematico.cne.gob.ec/_files/ugd/157be5_e34f007e38294a2d80257c514317ba8c.pdf?index=true.

servicios de validación de identidad a particulares bajo contratos de interoperabilidad bajo bases legales cuestionables.

Con respecto a otros sistemas, Ecuador mantiene un registro obligatorio de líneas y dispositivos móviles con el fin de prevenir el robo y su uso con fines criminales, ya que la base de datos es accesible a cualquier entidad pública para fines de seguridad nacional. Adicionalmente, el ECU 911 actualmente opera cámaras de reconocimiento facial, lo que da lugar a la bien fundada suposición de que existen registros faciales biométricos para este fin. Por último, el sistema de votación telemática que tiene el CNE opera mediante la utilización de bases de datos biométricos, pero su marco legal y técnico es opaco.

Diferentes documentos oficiales como el Plan Nacional de Gobierno Electrónico 2018-2021,[79] la Política Ecuador Digital 2019[80] y la reciente Agenda de Transformación Digital 2022-2025[81] consideran que la base de datos del Registro Civil es un activo disponible para otros usos más allá de la identificación personal.

Acumulativamente, esto lleva a la conclusión de que existe una tendencia en el país a favorecer prácticas de identificación digital que son especialmente riesgosas para la protección de los derechos humanos, lo cual también está documentado en el informe regional. En resumen, estas prácticas riesgosas incluyen:

- el uso de bases de datos centralizadas con un alto riesgo de violación de datos y vulneraciones de la seguridad;
- permitir el deslizamiento de funciones de la base de datos del Registro Civil sin la supervisión adecuada;
- la falta de provisión de fundamento legal adecuado para la recolección de datos personales sensibles.

[79] Ministerio de Telecomunicaciones y de la Sociedad de la Información (2018). Plan Nacional de Gobierno Electrónico 2018-2021 Véase: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/09/PNGE_2018_2021sv2.pdf.

[80] Ministerio de Telecomunicaciones y de la Sociedad de la Información (2018). Política Ecuador Digital. Véase: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2019/05/PPT-Estrategia-Ecuador-Digital.pdf.

[81] Ministerio de Telecomunicaciones y de la Sociedad de la Información (2018). Agenda de Transformación Digital 2022-2025. Véase: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2022/08/Agenda-transformacion-digital-2022-2025.pdf.

2. Narrativa prevalente sobre la necesidad de la biometría en el sector público

Las políticas públicas y la legislación del Ecuador que han sido revisadas en este caso práctico parecen indicar que el sector público considera esencial el uso de la biometría en los procesos de identificación digital. Esta narrativa está presente en la Agenda de Transformación Digital 2022-2025, en la que se hace referencia a la identificación digital. Esto también está presente en otros documentos de política integral, como el informe del Registro Civil que esboza su visión de la identificación digital. El informe resalta que la biometría es "parte del proceso de inscripción y validación del servicio de identificación digital,"[82] aunque no es un elemento esencial.

3. Falta de priorización de la inclusión de poblaciones vulnerables

No se ha encontrado evidencia de que los sistemas de identificación digital del Ecuador hayan sido diseñados con un enfoque incluyente de las poblaciones vulnerables o en riesgo de ser excluidos de la adopción de tecnologías como la biometría. En comparación, en otros países latinoamericanos como Bolivia[83] y Brasil,[84] existen proyectos o planes de sistemas que tienen como fin facilitar el acceso a la ayuda social. Según la investigación, la única mención del concepto de "inclusión digital" (el cual también es más restringido) aparece en la Ley Orgánica de Transformación Digital y Audiovisual aprobada en 2023, pero su adecuada implementación aún está pendiente.[85]

Con base en los hallazgos en la investigación, y haciendo eco de la tendencia en la región, el Ecuador mantiene sistemas de identificación digital para facilitar el acceso a servicios

[82] Dirección General del Registro Civil, Identificación y Cedulación (2022). El derecho a la privacidad en la era digital/DIGERCIC 25-05-2022. Véase: 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). Sistemas de identificación y protección social en Venezuela y Bolivia: vigilancia, género y derechos humanos (páginas 29-42). Véase: https://www.derechosdigitales.org/wp-content/uploads/sistemas-de-Identificacion_ES.pdf.

[84] ITS Río (2020). Buena identificación en América Latina: fortaleciendo los usos apropiados de la identificación digital en la región (página 49-50). Véase: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf.

[85] Registro Oficial del Ecuador (2023). Ley Orgánica de Transformación Digital y Audiovisual. Véase: https://www.go Gobiernoelectronico.gob.ec/wp-content/uploads/2023/02/7e52b3d7-0ba5-4c58-a474-00e19fcbe127.pdf.

gubernamentales digitales, el voto telemático, y presumiblemente control policial (ECU 911) a un grupo de la población con condiciones de privilegio. Estas condiciones incluyen buena conectividad, destrezas digitales, entre otras.

La Agenda de Transformación Digital 2022-2025 no incluye objetivos o puntos de acción con un foco incluyente. Al contrario, en relación con la identificación digital, incluye acciones dirigidas a mejorar la efectividad de los sistemas de control policial. Como ilustración, dos de los objetivos del eje de Seguridad y Confianza Digital incluyen la "adquisición de equipos y licencias para el reconocimiento facial, dactilar y de vehículos, en dispositivos móviles" y el "desarrollo de aplicaciones de intervención policial con cámaras y grabación de delitos, con infraestructura"[86]

4. Proveedores comunes de tecnologías de identificación digital y de vigilancia

Como otros países latinoamericanos como Colombia[87], Ecuador tiene un proveedor común de tecnologías de identificación digital y tecnologías con capacidad de vigilancia, a saber, IDEMIA (anteriormente OT-Morpho). Históricamente, el Registro Civil ha dependido del apoyo de una corporación tecnológica, *International Business Machines Corporation* (IBM), para la digitalización de su sistema de identificación.[88] Sin embargo, desde 2019, IDEMIA, un proveedor multinacional de tecnologías de identificación, ha sido responsable de mantener el sistema de emisión de pasaportes biométricos y tarjetas de identificación.[89] En 2022, IDEMIA respondió a un informe de Access Now[90] haciendo notar que ellos "no comercializan tecnologías de vigilancia."[91]

---

[86] Ministerio de Telecomunicaciones y de la Sociedad de la Información (2018). Agenda de Transformación Digital 2022-2025. Véase: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2022/08/Agenda-transformacion-digital-2022-2025.pdf.

[87] Karisma Foundation (2021). El sistema de reconocimiento facial del Registro Nacional. Véase: https://digitalid.karisma.org.co/2021/07/01/sistema-reconocimiento-facial-registraduria/.

[88] Registro Civil, Identificación y Cedulación. Revisión histórica. Véase: https://www.registrocivil.gob.ec/resena-historica/.

[89] Registro Civil, Identificación y Cedulación (2019). El Registro Civil otorgó un contrato para un nuevo sistema de emisión de pasaportes biométricos y cédulas. Véase: 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). Tecnología de vigilancia en América Latina: fabricada en el extranjero, desplegada en casa. Véase: https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf.

[91] Centro de Recursos Empresariales y de Derechos Humanos (2022). Respuesta de IDEMIA a acusaciones acerca de la venta de tecnología de vigilancia en América Latina. Véase:

Sin embargo, debe tenerse en cuenta que también existe un amplio ecosistema de proveedores de tecnología con capacidades de vigilancia que mantienen el robusto sistema de cámaras de videovigilancia instalado en el país, especialmente los que operan bajo el ECU 911, que fue un proyecto financiado y desarrollado por dos empresas chinas. La Corporación Nacional China de Importación y Exportación de Sistemas Electrónicos (CEIEC), una empresa de sistemas electrónicos de defensa, y *Huawei Technologies Company Limited*, una corporación multinacional china de tecnología.[92] No está claro si la plataforma ECU 911 y el sistema de identificación digital pueden interoperar.

En el informe de Access Now, "Tecnología de vigilancia de América Latina: fabricado en el extranjero, desplegado en casa," que fue respondido por IDEMIA, se menciona que varias empresas participan en el mercado ecuatoriano en cuanto a sistemas de videovigilancia. Estas incluyen Axis (Suiza), Hikvision (China), Intelligent Security Systems (Rusia), Pelco Corporations (Estados Unidos), Tiandy y ZKTeco (China) y VERINT (Israel y Estados Unidos).[93] De la misma manera, en el informe de FUNDAMEDIOS, "La videovigilancia en el Ecuador viola los derechos de los ciudadanos", se menciona que las tecnologías utilizadas para implementar la plataforma ECU 911 son únicas en el mercado, de manera que su mantenimiento estaría restringido a los proveedores originales.[94]

Análisis II: Problemas de los sistemas de identificación digital en el Ecuador

El informe regional identificó los siguientes problemas: la proliferación de tecnologías de vigilancia debido al uso intensivo de la biometría; la falta de transparencia en el desarrollo de políticas y el despliegue de sistemas de identificación digital; la ausencia de límites concretos a la evolución presente y futura de estos sistemas; y los casos reales o potenciales

https://www.business-humanrights.org/en/latest-news/response-from-idemia-to-allegations-about-sale-of-surveillance-technology-in-latin-america/.

[92] New York Times (2019). Fabricado en China y exportado al Ecuador: el aparato de vigilancia del estado. Véase: https://www.nytimes.com/en/2019/04/24/espanol/america-latina/ecuador-vigilancia-seguridad-china.html.

[93] Access Now (2021). Tecnología de vigilancia en América Latina: fabricada en el extranjero, desplegada en casa. Véase: https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf.

[94] FUNDAMEDIOS (2021). La videovigilancia en Ecuador viola los derechos ciudadanos. Véase: https://www.fundamedios.org.ec/wp-content/uploads/2021/12/Inf.-Videovigilancia.pdf.

de efectos sobre derechos humanos tales como la privacidad, la protección de datos y la discriminación en el acceso a los servicios públicos.

Esta sección presenta un recuento de los principales retos encontrados en los sistemas de identificación digital representados en el Ecuador. En algunos casos, se ha mencionado directamente información obtenida en entrevistas. Esta lista es preliminar y no es exhaustiva.

1. Los sistemas de identificación digital son extremadamente peligrosos para los derechos humanos

Todos los sistemas de identificación digital identificados en el Ecuador replican las prácticas más riesgosas para los derechos humanos, especialmente la privacidad y la protección de datos personales. En el caso del sistema mantenido por el Registro Civil, estos riesgos incluyen la posibilidad de acceso no autorizado, violaciones de seguridad, y fugas que expongan la información de ciudadanos ecuatorianos y residentes extranjeros. Este riesgo no es potencial, porque ya se ha concretado en varias ocasiones, siendo la más llamativa de estas una fuga masiva de datos en 2019 que el gobierno no ha explicado.[95]

En el caso de los registros obligatorios de líneas y dispositivos móviles, además de los anteriores riesgos, existe el riesgo del deslizamiento de funciones, es decir, usos que son distintos del fin declarado por ARCOTEL, es decir, prevenir el robo y el uso de líneas con fines delictivos. Este riesgo se ve exacerbado por el hecho de que las normas que regulan este sistema indican que, además de ARCOTEL, otras entidades relacionadas con la "seguridad nacional" también pueden obtener acceso. La inclusión de la categoría de "seguridad nacional" es amplia, y expone los datos recolectados en este sistema a esfuerzos de monitoreo y vigilancia, sin el debido proceso o la posibilidad de supervisión posterior.

Con respecto al supuesto sistema de identificación digital que podría ser utilizado en conjunto con los sistemas de videovigilancia de la plataforma ECU 911, la posibilidad de fallas tecnológicas (como falsos positivos), debe añadirse a los riesgos ya mencionados, que

[95] Diario El Comercio (2019). ¿Cómo se descubrió la violación de seguridad que afectó los datos de 20 millones de ecuatorianos? Véase: https://www.elcomercio.com/tendencias/tecnologia/hackeo-etico-filtracion-datos-ecuatorianos.html.

violarían derechos como el debido proceso, la no discriminación, y garantías como la presunción de inocencia.

Finalmente, con respecto al sistema de voto telemático utilizado en el exterior, aunque se sabe poco de su operación, es predecible que la base de datos sobre el que opera presenta un nivel de riesgo similar al del Registro Civil. Los riesgos también se extienden a otros derechos, como el derecho al voto, ya que si este sistema se ve comprometido podría llevar a una violación del secreto del voto e inclusive alterar los resultados de las elecciones, con un impacto en los procesos democráticos en general.

2. Falta de sancionar marcos legales que impongan límites legales

Como lo indica FUNDAMEDIOS en las conclusiones de su informe sobre sistemas de videovigilancia, especialmente ECU 911, Ecuador no tiene legislación específica que establezca límites al uso de los sistemas de vigilancia. Según esto, inevitablemente se dejarían de imponer las normales salvaguardas legales sobre estos sistemas, incluidas las que están diseñadas para proteger el derecho a la privacidad consagrados en la Constitución del Ecuador.[96] Esta situación se extiende al uso de tecnologías biométricas implementadas en el sistema de identificación digital utilizado por el Registro Civil, que ha sido desarrollado sin una ley específica que defina su alcance. Esto también aplica al sistema de votación telemática del CNE.

De forma positiva, el 10 de mayo de 2021 la Asamblea Nacional del Ecuador aprobó la Ley Orgánica de Protección de Datos Personales. La existencia de normas de este tipo impone límites a la adopción de tecnologías que procesan datos personales, como la biometría y el reconocimiento facial. Sin embargo, las entrevistas resultaron en visiones conflictivas. Un grupo señaló que la aprobación de la norma y la entrada en vigor del régimen sancionador impondrá límites efectivos al procesamiento de datos por las entidades públicas. Por otro lado, otro grupo de entrevistados señaló que al no establecer una autoridad de protección

[96] FUNDAMEDIOS (2021). La videovigilancia en Ecuador viola los derechos ciudadanos. Véase: https://www.fundamedios.org.ec/wp-content/uploads/2021/12/Inf.-Videovigilancia.pdf.

de datos, la elección de su gestión ejecutiva, y la ausencia de reglamentación subsidiaria, están demorando la implementación de la ley.

Otra norma que podría imponer límites a las entidades públicas en el área específica de identificación digital es la Ley Orgánica de Transformación Digital aprobada en marzo de 2023. Esta ley crea el "Marco de Identificación Digital" y define su alcance. Algunos de los entrevistados consideran que este marco propone un cambio de competencias a nivel de la creación de políticas de identificación entre el Registro Civil y la autoridad de transformación digital, que es el Ministerio de Telecomunicaciones y de la Sociedad de la Información. En cualquier caso, esta ley aún es nueva, y la crisis política del país sugiere demoras en su implementación.

A pesar de que el escenario de riesgos y amenazas a los derechos creado por los sistemas de identificación digital en el Ecuador podría limitarse a través de litigios de interés público, aprovechando el hecho de que la Constitución protege el derecho a la privacidad, no se han encontrado acciones de este tipo durante esta investigación. Esto, a pesar de graves quejas de la sociedad civil que protestan el uso de la plataforma ECU 911 para la vigilancia ilegal y el espionaje político.[97] Esta situación ha sido descrita en un informe de 2022 enviado al Consejo de Derechos Humanos a través de los mecanismos del Examen Periódico Universal.[98]

3. Efectos potenciales y reales sobre los derechos humanos

La combinación de riesgos y amenazas planteados por los asuntos que anteceden pinta un paisaje complicado, reforzado además por la crisis política y social que ha venido experimentando el Ecuador en los últimos años y que llevó a la reciente disolución de la Asamblea Nacional y la convocatoria de elecciones generales. Así, además de la privacidad,

[97] Diario El Comercio (2019). Lenín Moreno dice que el ECU 911 fue utilizado "de manera perversa" para el espionaje. Véase: https://www.elcomercio.com/actualidad/seguridad/lenin-moreno-ecu-911-espionaje.html.

[98] FUNDAMEDIOS (2022). Informe sobre la violación de los derechos ciudadanos a través de la videovigilancia en el Ecuador, y recomendaciones al gobierno ecuatoriano en relación con anuncios de la implementación masiva de tecnología de reconocimiento facial. Véase: https://www.fundamedios.org.ec/wp-content/uploads/2022/04/1-EPU-Ecuador-Videovigilancia-1.docx-1.pdf.

la protección de datos personales, el debido proceso y la presunción de inocencia, existe la posibilidad de violaciones de derechos como la libertad de expresión, de reunión pacífica, el secreto del voto, entre otros.

Como se indica anteriormente, existen múltiples precedentes de usos ilícitos de tecnologías de vigilancia que los sistemas de identificación digital pueden facilitar, específicamente en el caso de la plataforma ECU 911, que es el sistema de videovigilancia más desarrollado del país. El caso más reciente fue reportado en 2022 por organizaciones locales de derechos humanos, lo que sugiere que el empeoramiento de la situación en el país podría llevar al uso de estas capacidades de vigilancia de forma ilícita por el gobierno actual o intentos posteriores.[99]

Con respecto al sistema de votación telemática virtual proporcionado por el CNE, existen otras inquietudes. A pesar de que este informe no ha podido encontrar información suficiente para entender totalmente el funcionamiento y el alcance de este sistema que está apuntalado por una base de datos biométrica, es importante resaltar los problemas identificados en los sistemas de votación telemática de la región y del mundo.[100] La extendida percepción de los entrevistados acerca de la mala capacidad técnica de los responsables de desplegar tecnologías en el sector público ecuatoriano, junto con las violaciones de derechos como las del 2019, que corroboran esta percepción, sugieren que estos problemas también podrían surgir en este país.

4. Otros asuntos relativos a la situación actual del país

La crisis actual del Ecuador presenta el riesgo de exacerbar estos problemas de los sistemas de identificación digital que el Ecuador comparte con la mayoría de los países analizados en el informe regional.

El supuesto más obvio es la posibilidad de que los sistemas de identificación digital actuales podrían ser utilizados como armas contra los líderes políticos y sociales que expresen oposición contra una decisión tomada por S.E. el presidente Lasso, especialmente a través

[99] LaLibre.Net (2022). Las organizaciones de la sociedad civil rechazan los intentos de silenciar y criminalizar los movimientos sociales en el contexto de protesta en el Ecuador y exigen que se respeten los derechos humanos. Véase: https://lalibre.net/comunicado-paroec/.
[100] Díaz, Valentín (2022). Voto telemático y consideraciones de políticas públicas en América Latina Véase: https://www.derechosdigitales.org/wp-content/uploads/VotoElectronico-mapalatino.pdf.

de la interoperabilidad de las bases de datos del Registro Civil y de la plataforma ECU 911 *(si es que esto no está ocurriendo ya)*. Dado que ya existen precedentes para su uso ilegítimo, y de que recientemente se han adoptado normas que afectan otros derechos relacionados,[101] el nivel de riesgo es alto. A pesar de que los entrevistados consideran esto poco probable, la mayoría reconoce que dichas normas no prevendrían que las capacidades de vigilancia instaladas puedan ser utilizadas de esta forma en el futuro.

Otro escenario de interés es el comportamiento del Sistema de voto telemático implementado por el CNE para los votantes en el exterior, que ya fue utilizado en las elecciones seccionales de febrero de 2023[102] por primera vez y que serán utilizadas de nuevo en las elecciones generales de agosto de 2023. En menor medida, también se pueden resaltar los planes de implementación de la ciudad inteligente. En este último caso, se ha sentado el precedente de que diferentes despliegues de cámaras de videovigilancia han sido financiados dentro del marco de estrategias locales para este tipo de políticas.[103]

Finalmente, es de hacer notar que por el momento la disolución de la Asamblea Nacional suspende las iniciativas relevantes de este estudio. Tal vez la más destacada era un proyecto de ley de derechos digitales que abordaba diversos problemas, incluida la identificación digital. Fundamentada en una perspectiva de derechos humanos, la iniciativa proponía cambios sustanciales a varias prácticas relacionadas con la identificación y la videovigilancia en el Ecuador. Este proyecto de ley habría sido otra herramienta para limitar la adopción de sistemas de identificación digital, como un refuerzo a las leyes de protección de datos y transformación digital.[104]

Conclusiones y recomendaciones

[101] Derechos Digitales (2023). Ecuador, muchos cambios pero poco que celebrar. Véase: https://www.derechosdigitales.org/20752/ecuador-muchos-cambios-poco-que-celebrar/.
[102] Diario El Universo. Elecciones de 2023: la inscripción para la votación telemática en el exterior estará disponible hasta el 5 de febrero. Véase: https://www.eluniverso.com/noticias/politica/elecciones-2023-inscripcion-para-voto-telematico-en-el-exterior-estara-disposable-hasta-el-5-de-febrero-nota/.
[103] Actualización biométrica (2019). Quito lanzó el reconocimiento facial para la vigilancia pública dentro del proyecto de ciudad inteligente. Véase: https://www.biometricupdate.com/201908/quito-to-launch-facial-recognition-for-public-surveillance-under-smart-city-project.
[104] Asamblea Nacional del Ecuador (2023). Proyecto de Ley Orgánica de Derechos Digitales. Véase: http://ppless.asambleanacional.gob.ec/alfresco/d/d/workspace/SpacesStore/78c3cfba-956d-4c46-b325-da410bc428d0/pp-der-dig-0026-ortiz-proyecto-de-ley.pdf.

Este caso práctico proporciona una exploración en profundidad de los sistemas de identificación digital en el Ecuador utilizando como modelo el informe regional sobre América Latina producido por Derechos Digitales "*La identidad digital en América Latina: situación actual, tendencias y problemas".* La situación política actual del Ecuador afecta la implementación de leyes que introducirían límites legislativos al uso de datos personales en los sistemas de identificación digital. Esta situación refuerza la posibilidad de que los sistemas de identificación digital actuales podrían ser utilizados como armas contra los líderes políticos y sociales que expresen oposición.

El caso práctico señala que el Ecuador ejemplifica las prácticas más riesgosas de identificación digital, como la adopción de bases de datos centralizadas que tienen mayor riesgo de vulneraciones de seguridad y fugas de datos. Además, la necesidad de la biometría en la identificación digital es una narrativa popular promovida por el sector público, incluida en varias normas fundacionales y documentos de estrategias. El caso práctico también señala que no existe priorización para la inclusión de poblaciones vulnerables, lo que presenta el riesgo de que empeoren los riesgos de exclusión y discriminación.

Basado en lo anterior, el caso práctico presenta un conjunto de recomendaciones al gobierno ecuatoriano (a los niveles nacional y regional) y a las organizaciones de la sociedad civil.

Recomendaciones

Esta sección presenta un conjunto de recomendaciones dirigidas al gobierno ecuatoriano y a las organizaciones de la sociedad civil.

Al gobierno nacional y los gobiernos regionales

Instamos al gobierno tanto a nivel nacional como regional del Ecuador a que:

- Garantice que el desarrollo y el uso de sistemas de identificación digital respete los derechos fundamentales consagrados en la constitución, especialmente la privacidad y la protección de datos personales. Específicamente, que garantice que los marcos legislativos que permiten estas tecnologías cumplan con los principios del derecho internacional de legalidad, necesidad, y proporcionalidad, y que estén restringidos a través de la limitación de sus fines, y sujetos a la participación pública.

- Implemente las leyes de protección de datos personales y transformación digital y audiovisual que delimiten el desarrollo y la utilización de los sistemas de identificación digital.
- Detenga el desarrollo o la utilización de sistemas de identificación digital donde haya un riesgo inminente de producir daños graves a los derechos de las personas o en los que ya hayan ocurrido dichos daños, donde sea factible, sin perturbar la prestación de servicios esenciales que dependen de las tecnologías en cuestión.
- Promueva la creación de foros de discusión con las múltiples partes interesadas, incluida la sociedad civil, para garantizar la continuidad o discutir nuevos desarrollos de sistemas de identificación digital Específicamente, estos foros deberían permitir una revisión de los sistemas existentes y de los que se esté considerando implementar en diferentes sectores (como el comercio, la salud, control de migraciones, etc).

A la sociedad civil

Instamos a la sociedad civil del Ecuador a que:

- Profundice el estudio de los vectores de interés más importantes tanto en la situación actual y de cara al futuro. Esto incluye:
    - El examen y clarificación de la operación del sistema de votación telemático virtual del CNE para los ciudadanos en el exterior debido a sus implicaciones para las elecciones que tendrán lugar en agosto de 2023.
    - Examine el potencial de la plataforma ECU 911 de convertirse en una herramienta de vigilancia masiva y su interoperabilidad con la base de datos del Registro Civil, y los riesgos para activistas y líderes políticos y sociales.
- Promueva acciones para incrementar la concienciación entre la población y otras organizaciones de la sociedad civil que trabajan en asuntos de derechos humanos con respecto a los riesgos de los sistemas de identificación digital. Esto incluye:
    - Abogar por la implementación de leyes y normas de protección de datos personales y de transformación digital y audiovisual.

- Explorar la posibilidad de iniciar acciones de defensa y litigación estratégica que tengan como objetivo directo los sistemas de identificación digital como el Registro Civil. Esto podría incluir concentrase en los servicios de validación que ofrece, o la interoperabilidad potencial con la plataforma ECU 911, y el potencial para la vigilancia ilegal.

Lista de referencias

Access Now (2018). National Digital Identity Programmes: ¿Qué viene después?

Access Now (2021). Tecnología de vigilancia en América Latina: Hecho en el extranjero, desplegado a nivel nacional.

Centro de Derechos Digitales de África (2022). Data Protection Code of Practice for Digital Identity Schemes in Africa. (Programas nacionales de identidad digital:
Código de buenas prácticas de protección de datos para los sistemas de identidad digital en África.)

Centro de Derechos Digitales de África (2022). The inclusiveness or exclusiveness of National IDs in West Africa: Countries of focus: Côte d'Ivoire, Ghana and Nigeria. (Inclusividad o exclusividad de los documentos nacionales de identidad en África Occidental: países de interés: Costa de Marfil, Ghana y Nigeria.)

AlSur (2018). Empresas y derechos humanos: informe regional sobre Tecnología, Big Data y Cibervigilancia.

AlSur (2021). Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa.

Asociación para los Derechos Civiles (2015). Si nos conocemos más, nos cuidamos mejor: Report on biometric policies in Argentina. (Reporte sobre políticas biométricas en Argentina.)

Asociación para los Derechos Civiles (2016). El Sistema de Protección de Datos Personales en América Latina: Oportunidades y desafíos para los derechos humanos.

Asociación por los Derechos Civiles (2017). Cuantificando identidades en América Latina.

Asociación por los Derechos Civiles (2017). Desafíos de la biometría para la protección de los datos personales – Reflexiones sobre el caso SIBIOS.

Asociación por los Derechos Civiles (2017). La identidad que no podemos cambiar: Cómo la biometría afecta nuestros derechos humanos.

Asociación por los Derechos Civiles (2019). Tu yo digital – Descubriendo las narrativas sobre identidad y biometría en América Latina.

Asociación para los Derechos Civiles (2021). Tecnologías de Vigilancia en Argentina.

Biblioteca del Congreso Nacional de Chile (2022). Identidad digital: conceptos y legislación.

Canales, María Paz; Lara, J. Carlos (2018). Propuesta de estándares legales para la vigilancia en Chile (2018).

Center for Human Rights and Global Justice (Centro de Derechos Humanos y Justicia Global) (2022). Paving a Digital

Centre for Internet and Society India (Pavimentar un centro digital de internet y sociedad de la India) (2020). ID del gobierno: Principios de evaluación.

CETyS (2021). Videovigilancia con reconocimiento facial, inteligencia artificial y derechos humanos: ni apocalipsis ni utopía.

Data Privacy Brasil (2022). Entre la visibilidad y la exclusión: Descifrar los riesgos asociados al Sistema Nacional de Identificación Civil y el aprovechamiento de su base de datos por la plataforma GOV.BR.

Data Privacy Brasil y TEDIC (2023). Tecnología y Derechos Humanos en la Triple Frontera: un estudio exploratorio de los programas de seguridad Muralha Inteligente (Brasil) y el Sistema Automatizado Migratorio de Reconocimiento Facial (Paraguay).

Díaz, Marianne (2017). Data Retention and Registration of Mobile Phones: Chile in the Latin American Context. (Conservación de datos y registro de teléfonos móviles: Chile en el contexto latinoamericano.)

Díaz, Marianne (2018). El cuerpo como dato.

Figueroa, Javiera; Venegas, Catalina (2020). Narrativas en torno al uso de la huella digital en la salud pública.

Fundación Karisma (2019). Biometría en el Estado colombiano ¿Cuándo y cómo se ha justificado su uso?

Fundación Karisma (2022). ID de Colombia: Identidad digital y Derechos Humanos.

Garay, Vladimir (2019). Mal de ojo: reconocimiento facial en América Latina.

Hiperderecho (2018). Identidad Biométrica en Perú: Estado de la cuestión.

Hiperderecho (2020). Identidad Digital en Perú: Descifrando al Leviatán.

InternetLab (2015). State Surveillance of Communications in Brazil and the Protection of Fundamental Rights. (La vigilancia estatal de las comunicaciones en Brasil y la protección de los derechos fundamentales.)

IPANDETEC (2021). Caretas Digitales: Digital Identity in Central America. (Identidad digital en Centroamérica.)

ITS Río (2020). Buena identidad digital en América Latina: Fortalecer los usos adecuados de la Identidad Digital en la región

KICTANet (2022). Policy brief Data Protection and Digital Identity in Kenya. (Protección de datos e identidad digital en Kenia.)

Instituto Global McKinsey (2019). Digital identification: A key to inclusive growth. (Identificación digital: una clave para el crecimiento integrador.)

OCDE (2023). Draft Recommendation on the Governance of Digital Identity. (Proyecto de Recomendación sobre la Gobernanza de la Identidad Digital.)

Paradigm Initiative (Iniciativa Paradigma) (2021). COVID-19 and Digital Rights: A Compendium on Health Surveillance Stories in Africa. (COVID-19 y derechos digitales: compendio de historias de vigilancia de la salud en África.)

Paradigm Initiative (Iniciativa Paradigma) (2021). Implementación de sistemas de identidad digital: Human Rights Implications and Lived experiences in Kenya. (Implicaciones para los derechos humanos y experiencias vividas en Kenia.)

Paradigm Initiative (Iniciativa Paradigma) (2022). Internet freedoms in Chad and DRC: Better understanding the notion of digital identity. (Libertades en Internet en Chad y la RDC: comprender mejor la noción de identidad digital.)

Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID. (¿Camino al infierno? Manual básico sobre el papel del Banco Mundial y las redes mundiales en la promoción de la identificación digital.)

TEDIC (2017). La desprotección de los datos personales y la desigualdad de género, riesgos a las libertades de las personas en Internet.

TEDIC (2018). La enajenación continua de nuestros derechos. Sistemas de identidad: Biometría y cámaras de vigilancia no reguladas en Paraguay.

The Engine Room (La sala de máquinas) (2019). ¿Qué buscar en los sistemas de Identidad Digital? Una tipología de etapas.

The Engine Room (La sala de máquinas) (2020). Comprendiendo los Efectos de la Identificación Digital en la Vida Cotidiana: Un estudio multinacional.

The Engine Room (La sala de máquinas) (2022). A Digital ID Handbook: Strategies for Navigating Electronic Identification Systems. (Manual de identificación digital: estrategias para navegar por los sistemas de identificación electrónica.)

Venturini, Jamila; Díaz, Marianne (2021). Sistemas de identificación y protección social en Venezuela y Bolivia: vigilancia, género y derechos humanos

Banco Mundial (2016). Digital identity: towards shared principles for public and private sector cooperation. (Identidad digital: hacia principios compartidos para la cooperación entre los sectores público y privado.)

Banco Mundial (2017). Principles on Identification for Sustainable Development: Toward the Digital Age. (Principios de identificación para el desarrollo sostenible: Hacia la era digital.)

Banco Mundial (2018). ID Enabling Environment Assessment (IDEEA): Guidance Note. (Evaluación del entorno favorable a la ID (IDEEA): Nota de orientación.)

Banco Mundial (2019). Digital ID and the Data Protection Challenge: Practitioner's Note). (El DNI digital y el reto de la protección de datos: Nota del practicante.)

Banco Mundial (2019). ID Enrollment Strategies: Practical Lessons from Around the Globe. (Estrategias de inscripción en el ID: lecciones prácticas de todo el mundo.)

Banco Mundial (2019). Guía para del practicante de ID4D.

Banco Mundial (2022). Engaging Civil Society Organizations (CSOs) for Successful ID Systems: Guidance Note. (Implicar a las organizaciones de la sociedad civil (OSC) en el éxito de los sistemas de identificación: nota de orientación.)

Banco Mundial (2022). ID4D Global Dataset.