DERECHOS DIGITALES
América Latina

IDENTIDAD DIGITAL EN AMÉRICA LATINA:

Situación actual, tendencias y problemáticas

Esta publicación fue realizada por Derechos Digitales, organización independiente y sin fines de lucro, fundada en el año 2005, cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en los entornos digitales en América Latina.

Texto por Carlos Guerrero y Paloma Lara Castro
Supervisión por Michel Roberto de Souza

SEPTIEMBRE 2023

ÍNDICE

RESUMEN EJECUTIVO

El enfoque de este informe es la región de América Latina (AL) 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 12 países de AL: Argentina, Bolivia, Chile, Brasil, Colombia, Costa Rica, El Salvador, México, Paraguay, Perú, Venezuela 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 bases 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.

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 doce países de AL 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 AL opta por modelos de identificación digital centralizados, en vez de sistemas de identificación digital descentralizados, federados o de mercado abierto.
- **Hallazgo 3:** los doce países de AL 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 AL son similares a los proveedores de tecnologías de identificación digital y biométricas.

---

(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.

- **Hallazgo 5:** la evidente ambigüedad en el concepto de "documento de identidad digital" ha facilitado a los países de AL 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 al 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 AL 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 legislaciones 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 AL a:

- Realizar una investigación más extensa y profunda sobre identidad digital en la región de América Latina;
- 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 de la situación sobre identificación digital en 12 países de América Latina que han sido investigados, con la esperanza adicional de que estos hallazgos sirvan de inspiración para los Estados y la sociedad civil para generar acciones en pos de sistemas de identificación digital que respeten los derechos fundamentales.

I. INTRODUCCIÓN

En las últimas décadas, se ha ido consolidando la tendencia mundial de acelerar los procesos de implementación de sistemas de identidad digital, digitalización y transformación digital bajo argumentos tecnosolucionistas que presentan a las tecnologías como "soluciones" a diversas problemáticas sociales que van mucho más allá de la esfera de la identificación, generando potenciales afectaciones a derechos humanos asociadas a la vigilancia estatal y a la profundización de situaciones de discriminación pre existentes. Esto ha enfatizado la urgencia de actuar frente a las problemáticas que estos procesos suponen para el ejercicio de derechos humanos.

Desde el sector público, estos procesos se han manifestado especialmente a través de la digitalización de los servicios públicos —como la asistencia sanitaria, el pago de impuestos y la seguridad social— bajo justificaciones amplias, sin suficiente evidencia que respalde los beneficios invocados, falta de involucramiento de múltiples partes interesadas, muchas veces sin mayores preocupaciones con la seguridad de los datos y sin realización de evaluaciones de impacto en derechos humanos. Para su implementación, los estados han desplegado todo tipo de tecnologías, que se caracterizan por ser esencialmente tecnologías de tratamiento de datos, principalmente datos personales, bajo diferentes niveles de debate público, transparencia y generalmente sin las suficientes salvaguardas de derechos humanos.

Un habilitador crítico en estos procesos ha sido el uso de los sistemas de identificación. En muchos países, estos están compuestos por uno o varios registros centralizados que recopilan y procesan datos asociados a la identidad, y que —en muchos casos— condicionan al acceso a beneficios sociales, atentando contra un derecho humano y universal. A pesar de experiencias en otras regiones que demuestran el riesgo de vigilancia, estatal y privada, que generan estos programas mediante el acceso a la base de datos, los estados de la región latinoamericana han incrementado su aplicación, como se verá en los siguientes apartados. Esto resulta especialmente preocupante considerando los antecedentes históricos de vigilancia en la región, así como la falta de mecanismos de supervisión independiente en contextos de marcada debilidad institucional. Sumado que, en algunos casos, los estados que implementan estos sistemas no cuentan con leyes de protección de datos personales para gobernar la recolección y procesamiento de datos, incluyendo el intercambio entre entidades públicas y privadas.

En el marco de adopción de los ODS, y en relación al objetivo 16,9 de "proveer identidad legal para todos", algunos gobiernos han expresado su interés porque la provisión de la identidad legal se realice a través de la digitalización de los sistemas de identificación. Sobre el punto, es importante señalar, en primer término, que la identidad es un derecho que debería ser garantizado a todas las personas. No obstante, esto no significa que la identificación deba ser obligatoria.[2] A su vez, si bien en algunos casos las tecnologías pueden aportar a simplificar ciertos procesos, la obligación de proveer una identidad legal no está condicionada a la implementación de sistemas digitales de identificación. En tercer lugar, no existe un sistema único que sea aplicable a todos los países, necesidades, objetivos y contextos.

Uno de los principales argumentos esbozados por los estados es que la tecnología actual permite desarrollar sistemas más confiables, resilientes y sostenibles que los tradicionales

(2) ITS Río (2020). Good ID in Latin America: strenghening appropriate uses of Digital Identity in the region. Disponible en: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf

basados en papel, a pesar de que generalmente la implementación de estos sistemas no va acompañado de un marco normativo claro y un marco de supervisión sólido para controlar la recopilación, el almacenamiento, el intercambio y el acceso y protección de la información, que incluya mecanismos de supervisión independiente y derechos a recursos efectivos. Pero la recopilación de datos nunca tiene lugar en un entorno neutro respecto a problemáticas sociales, por lo que la filtración de datos —especialmente los sensibles— plantea riesgos a comunidades en situación de vulnerabilidad. Por ejemplo, las mujeres y, en particular, las personas lesbianas, gays, bisexuales, intersexuales y transexuales (LGBTQI+) pueden sufrir estigmatización, marginación y violencia tras la exposición de información privada relacionada con su historia sexual y reproductiva, sexualidad y/o identidad de género.

También se ha argumentado que adoptar estos sistemas sería beneficioso para países en desarrollo con sistemas de identificación precarios o ineficaces. No obstante, dichas afirmaciones generales y tecnosolucionistas evitan contemplar las significativas brechas digitales generacionales, geográficas, socioeconómicas y a nivel de género en relación al acceso a internet y a las TIC, lo cual refleja desigualdades preexistentes que necesitan ser abordadas mediante otras acciones de política pública. Adicionalmente, esta visión podría ser muy problemática, en tanto podría generar un descuido del papel fundamental que desempeña la documentación básica.[3]

Organismos como el Banco Mundial[4] han apoyado la idea de adoptar sistemas de identificación digitalizados, también llamados *sistemas de identidad digital,* y en algunos casos han colaborado activamente en su desarrollo. Sin embargo, durante estos procesos han quedado en evidencia no solo los problemas que estos sistemas pueden causar, sino los impactos negativos en materia de derechos humanos que ya ocurren en los países en donde se han implementado, como se verá más adelante.[5]

De hecho, mediante una carta abierta, Derechos Digitales junto con otras organizaciones ha instado al Banco Mundial y a otras organizaciones internacionales a tomar medidas inmediatas para poner fin a las actividades que promueven modelos dañinos de identificación digital, en base a la creciente evidencia recopilada por organizaciones de la sociedad civil e investigadores y expertos independientes que establece que los sistemas de identificación digital a menudo tienen un impacto perjudicial en los derechos humanos.[6]

---

(3) Barbosa, A. Carvalho, C. Machado, C. Costa, J. Good ID in Latin America: strenghening appropriate uses of Digital Identity in the region. Disponible en: https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf

(4) Por ejemplo, el proyecto ID4D del Banco Mundial, ver: https://id4d.worldbank.org/about-us

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

(6) Veáse: Carta abierta: El Banco Mundial y sus donantes deben proteger los derechos humanos en los sistemas de identificación digital. https://www.accessnow.org/press-release/carta-abierta-el-banco-mundial-sistemas-de-identificacion-digital/

Al respecto, es importante resaltar que, en la era digital, el derecho a la privacidad se ha convertido en una puerta de acceso a la protección de una serie de derechos.[7] Así lo han entendido diversos organismos de derechos humanos. Por ejemplo, mediante la Resolución 68/167 de 2014 de las Naciones Unidas sobre el derecho a la privacidad en la era digital, se ha afirmado que el derecho a la intimidad requiere una sólida protección como "una condición previa necesaria para la protección de valores fundamentales, como la libertad, la dignidad, la igualdad y la libertad frente a la intrusión gubernamental" y "un ingrediente esencial para las sociedades democráticas…" En ese sentido, organismos y mecanismos de derechos humanos han expresado su preocupación por el creciente uso de tecnologías que no cumplen con las normas de legalidad, necesidad y proporcionalidad reconocidas internacionalmente,[8] ante las graves violaciones de derechos humanos sufridas por las personas, especialmente defensores de derechos humanos, activistas y periodistas, además del reforzamiento de situaciones de discriminación y exclusión de grupos en situación de vulnerabilidad.

A propósito de lo anterior, diferentes reportes de organizaciones de derechos humanos han documentado cómo la adopción de sistemas de identidad digital ha puesto en grave riesgo el derecho la privacidad y derechos conexos, y ha propiciado o profundizado la discriminación en el acceso a servicios sociales, incluida la salud, especialmente entre poblaciones en situación de vulnerabilidad, como las mujeres, personas con discapacidad, adultos mayores y la comunidad LGBTIQ+. Los casos de Aadhaar en la India, Huduma Namba en Kenia y el Sistema Patria en Venezuela son algunos ejemplos. Tal como hemos señalado en investigaciones anteriores,[9] la utilización de estos sistemas, especialmente aquellos que requieren el reconocimiento biométrico, para el acceso a recursos básicos no solo afecta el derecho a la privacidad, sino que perjudica directamente el derecho a la integridad, a la autonomía y a la dignidad. A su vez, las iniciativas de digitalización en el contexto de programas de protección social traen consigo riesgos significativos en términos de discriminación hacia grupos históricamente excluidos.

Actualmente existe un importante acervo de artículos, campañas y reportes que analizan estas amenazas y revelan cómo estas parecen concentrarse en los países en desarrollo, profundizando desigualdades preexistentes y debilitando el acceso a derechos fundamentales. Estos trabajos han aportado cuestiones relevantes para cuestionar la conveniencia de los sistemas de identidad digital y han sustentado diferentes pedidos, que van desde la revisión de los procesos de adopción y gobernanza hasta el establecimiento de moratorias a su uso. Al respecto, es necesario referir que dicho pedido es congruente con las recomendaciones de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos sobre la necesidad de controlar la producción y venta de sistemas de vigilancia que

(7) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, ¶16, A/HRC/29/32 (May 22, 2015); General Assembly resolution 68/167, A/HRC/13/37 and Human Rights Council resolution 20/8). https://undocs.org/A/HRC/29/32

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

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

no respeten los derechos humanos, así como de exigir una moratoria para aquellos que no cumplan los criterios básicos.[10]

A pesar de que muchos de estos documentos no tenían como objeto de estudio la identidad digital, el hecho de que las tecnologías utilizadas por estos sistemas suelan ser las mismas que se utilizan en los denominados sistemas de vigilancia estatal implica que ciertas problemáticas y riesgos, especialmente aquellas relacionadas con las vulneraciones de derechos asociadas a prácticas de vigilancia estatal, son comunes. Este es el caso de muchos reportes producidos en América Latina, en donde dichas prácticas han crecido sostenidamente, profundizándose con el auge de la industria de la vigilancia y han asumido diferentes formas, algunas de las cuales se apoyan en sistemas de identidad digital.

En este contexto, este reporte busca consolidar los datos relativos a nuestra región y ofrecer un análisis exploratorio que refleje no solo el estado actual de la implementación de los sistemas de identidad digital y las tendencias existentes, sino también qué riesgos específicos de vulneración de derechos humanos enfrentamos y podríamos enfrentar en el futuro. También, cómo estos sistemas se relacionan con temas de actualidad, como la comercialización de tecnologías de vigilancia, los mandatos de retención obligatoria de datos y la transformación digital del sector público.

Si bien el objetivo principal de este documento es ofrecer información actualizada que sirva de base para futuras investigaciones, esperamos que estos hallazgos incentiven también la coordinación de la sociedad civil para la realización de acciones de incidencia y litigio estratégico a nivel local y regional.

II. METODOLOGÍA

Dada la naturaleza exploratoria de este reporte, se utilizaron fuentes secundarias y terciarias, principalmente documentos producidos por organizaciones de la sociedad civil, el sector privado y organismos internacionales. En ese sentido, nos gustaría destacar el abundante material producido de manera consistente sobre este tema por parte de organizaciones de derechos humanos como Access Now, la Asociación por los Derechos Civiles (ADC), Data Privacy Brasil, Fundación Karisma, Hiperderecho, Internet Bolivia, ITS Rio y TEDIC.

En cuanto al marco metodológico, para el análisis de la información recopilada utilizamos como referencia el texto *¿Qué buscar en los sistemas de Identidad Digital? Una tipología de etapas*[11] de la organización *The Engine Room*, que propone una guía para recolectar y procesar la información sobre este tema. También utilizamos varios conceptos del texto *Governing ID: Principles for Evaluation*[12] de la organización CIS India, que arroja claridad sobre parámetros que deben orientar el buen uso de la identidad digital.

---

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

(11) The Engine Room (2019). ¿Qué buscar en los sistemas de Identidad 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

(12) Centre for Internet and Society India (2020). Governing ID: Principles for Evaluation. Véase: https://digitalid.design/docs/CIS_DigitalID_EvaluationFrameworkDraft02_2020.01.pdf

Considerando que no existe hasta el momento un consenso general respecto a definiciones en esta materia, en todo el documento se ha optado por utilizar las definiciones de *identidad digital*[13] y *sistemas de identidad digital*[14] que propone el Banco Mundial, para establecer un lenguaje común. Así mismo, es importante remarcar que concordamos con lo señalado por ITS Rio en su reporte *Good ID in Latin America: Strengthening appropriate uses of Digital Identity in the región*,[15] en que no hay una diferencia esencial entre los sistemas de identidad digital y ciertos sistemas de vigilancia y, por ello, ambos son considerados como sistemas de identidad digital.

En cuanto a los países analizados, estos se han elegido bajo dos criterios. Primero, bajo el objetivo de alcanzar cierta representación geográfica y, segundo, en base a la cantidad de información disponible sobre la implementación de sistemas de identidad digital. En la mayoría de los casos, se ha optado por dar mayor relevancia a sistemas de identidad digital fundacionales y a sistemas funcionales[16] creados para ámbitos específicos, como el acceso a la seguridad social, salud y control migratorio, especialmente cuando ya han sido identificados por otras organizaciones.

El texto final de este reporte ha pasado por varias rondas de revisión por parte de Derechos Digitales, así como de miembros de otras organizaciones aliadas y expertas y expertos de la región, con el fin de corregir errores e inconsistencias. El resultado final es la suma de todos estos esfuerzos.

III. SITUACIÓN ACTUAL DE LOS SISTEMAS DE IDENTIDAD DIGITAL EN AMÉRICA LATINA

En esta sección se presenta un panorama general que identifica el nivel de adopción actual de sistemas de identidad digital en diferentes países de América Latina. Esta revisión es preliminar, no exhaustiva y ha priorizado la descripción de tres tipos de sistemas: 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 en ámbitos específicos, como el acceso a la seguridad social, salud y control migratorio e iniciativas relacionadas. En la siguiente sección se analizarán las tendencias y problemáticas comunes que presentan estos sistemas.

---

(13) Identidad digital: Un conjunto de atributos y/o credenciales capturados y almacenados electrónicamente que identifican de manera única a una persona (traducción libre). Véase: https://id4d.worldbank.org/guide/glossary

(14) Sistema de identidad digital: Un sistema de identificación que utiliza tecnología digital durante todo el ciclo de vida de la identidad, incluso para la captura, validación, almacenamiento y transferencia de datos; gestión de credenciales; y verificación de identidad y autenticación (traducción libre). Véase: https://id4d.worldbank.org/guide/glossary

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

(16) Siguiendo la terminología propuesta por el Banco Mundial, la principal diferencia entre un sistema de identidad digital fundacional y uno funcional, es que el primero suele ser siempre un registro obligatorio que, además de la identificación, puede servir a otros fines, mientras que el segundo se crea con único propósito.

1. Argentina

Dos de los sistemas de identidad digital más importantes que ha sido implementados son el *Sistema de Identidad Digital* (SID), que ofrece acceso a servicios gubernamentales[17] y el *Sistema Federal de Identificación Biométrica para la Seguridad* (SIBIOS), cuyo fin alegado es contribuir a la seguridad pública,[18] ambos alimentados por el conjunto de registros personales digitalizados que mantiene el *Registro Nacional de Personas* (RENAPER). Algunas características de estos sistemas son que el registro es obligatorio y que recolecta datos biométricos.

En 2019, el RENAPER firmó un convenio de cooperación con el Ministerio de Seguridad de Buenos Aires, a fin de que se utilice la base de datos para el Sistema de Reconocimiento Facial de Prófugos (SRFP). Para ello, se estableció que el RENAPER otorgaría, a requerimiento, las fotografías de las personas que figuran en el sistema de Consulta Nacional de Rebeldía y Captura (CONARC) del Registro Nacional de Reincidencia, sobre las cuales se realizará el reconocimiento facial, generando alertas de detención.[19] Al respecto, el Jefe de Gobierno de la Ciudad Autónoma de Buenos Aires indicó que fueron implementadas 300 cámaras de videovigilancia con el Sistema de Reconocimiento Facial de Prófugos sobre la base de datos del CONARC, que en 2019 contaba con más de 46.000 registros.[20]

En 2020, tras una acción de amparo colectiva presentada por el Observatorio de Derecho Informático Argentino (O.D.I.A.),[21] mediante el cual se puso en discusión la constitucionalidad y convencionalidad de las normas que implementaron el sistema de reconocimiento facial en la CABA, se declaró la inconstitucionalidad del uso del sistema de reconocimiento facial por no haberse dado cumplimiento a los recursos legales de protección de los derechos personalísimos de la ciudadanía.[22] Entre varias cuestiones, el fallo nota que el sistema se usó de manera ilegal para buscar a más de 15 mil personas que no estaban en la lista de prófugos del CONARC.

---

(17) Portal del Gobierno de Argentina. Sistema de identidad digital. Véase: https://www.argentina.gob.ar/interior/renaper/sid-sistema-de-identidad-digital

(18) ADC (2015). Si nos conocemos más, nos cuidamos mejor: Informe sobre políticas de biometría en la Argentina (Páginas 17-20). Véase: https://adc.org.ar/wp-content/uploads/2019/06/005-si-nos-conocemos-mas-nos-cuidamos-mejor-05-2015.pdf

(19) Portal del Gobierno de Argentina. Nuevo sistema para identificar prófugos con orden de captura a partir de la base de datos de Renaper. Veáse: https://www.argentina.gob.ar/noticias/nuevo-sistema-para-identificar-profugos-con-orden-de-captura-partir-de-la-base-de-datos-de

(20) Portal del Gobierno de la Ciudad Autónoma de Buenos Aires. Rodríguez Larreta presentó el Sistema de Reconocimiento Facial de Prófugos. Veáse: https://buenosaires.gob.ar/jefedegobierno/noticias/horacio-rodriguez-larreta-presento-el-nuevo-sistema-de-reconocimiento-facial#:~:text=Rodr%C3%ADguez%20Larreta%20present%C3%B3%20el%20Sistema%20de%20Reconocimiento%20Facial,ubicadas%20en%20distintas%20calles%20y%20estaciones%20de%20subte

(21) Veáse: https://amicus.odia.legal/accion.pdf

(22) CELS. Declaran inconstitucional el uso del sistema de reconocimiento facial en caba. Véase: https://www.cels.org.ar/web/2022/09/una-jueza-declaro-inconstitucional-el-uso-del-sistema-de-reconocimiento-facial-en-caba/#:~:text=07%20Sep%202022-,Declaran%20inconstitucional%20el%20uso%20del%20sistema%20de%20reconocimiento%20facial%20en,de%20la%20denuncia%20del%20CELS.

También existe un sistema creado en 2016 a partir de la Resolución N° 8507/2016 ENACOM que crea el *Registro de Identidad de Titulares del Servicio de Comunicaciones Móviles*, compuesto por los datos del titular, número de móvil, entre otros. Algunas características de este sistema son que el registro es obligatorio, que su propósito invocado es prevenir el robo de móviles y su uso con fines delictivos, y que la base de datos es accesible para entidades públicas.[23]

2. Bolivia

Dos de los sistemas de identidad digital más importantes que han sido implementados son el conjunto de registros personales digitalizados que mantienen el *Servicio General de Identificación Personal* (SEGIP) y el *Servicio de Registro Civil* (SERECI).[24] Algunas características de estos sistemas son que el registro es obligatorio, que recolectan datos biométricos y, en el caso específico del SEGIP, que actualmente ofrece una versión digital del documento de identidad mediante el uso de aplicaciones móviles.[25]

También existe un sistema creado en 2009, a partir del Decreto Supremo N° 0353 que crea el *Registro de Propiedad de Equipos Terminales Móviles* y *Registro de Titulares de Cuentas*, compuesto por los datos del titular, código IMEI, número de móvil, entre otros. Algunas características de este sistema son que el registro es obligatorio, que su propósito alegado es prevenir el robo de móviles y su uso con fines delictivos, y que la base de datos es accesible para entidades públicas y privadas.

Finalmente, existen varios sistemas funcionales en ámbitos específicos. Algunos de los casos más relevantes se dan en el ámbito de la seguridad social y consisten en el mantenimiento de bases de datos digitalizadas condicionada para la transferencia monetaria de asistencia económicas, como el *Bono Juana Azurduy*, y previsionales, como *Renta Dignidad*. El registro en estas bases de datos es voluntario y son accesibles para entidades públicas y privadas.[26]

3. Brasil

Tres de los sistemas de identidad digital más importantes son el conjunto de registros personales digitalizados que mantienen el *Sistema Nacional de Informações de Registro Civil* (SIRC), el *Tribunal Superior Eleitoral* (TSE) y la *Secretaria da Receita Federal do Brasil* (RFB). Algunas características de estos sistemas son que el registro en los dos primeros es obligatorio, que el

---

(23) Portal del Gobierno de Argentina. Registro de celulares. Véase: https://www.argentina.gob.ar/justicia/derechofacil/leysimple/registro-de-celulares

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

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

(26) 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

segundo siempre recolecta datos biométricos y que todos otorgan una tarjeta física o digital que puede ser utilizada como documento de identidad.[27]

En 2017 se aprobó la creación de un nuevo sistema de identidad digital denominado *Identificação Civil Nacional* (ICN) a partir de la Ley N° 13.444, que establece la creación de una base de datos compuesta por diferentes registros como los del SIRC, TSE, entre otros, y la expedición de un nuevo documento de identidad. Uno de los objetivos inmediatos de este sistema es ofrecer acceso a servicios gubernamentales a través del Portal del Gobierno de Brasil *Gov.br*.[28]

Finalmente, existen varios sistemas funcionales en ámbitos específicos. Uno de los casos más relevantes se da en el campo de la seguridad social y consiste en una base de datos denominada *Cadastro Único* (CadÚnico), mantenida por el gobierno federal de Brasil y gestionada por los gobiernos de cada estado, a partir del cual se identifica a beneficiarios de asistencias económicas como *Bolsa Família, ID Jovem, Carteira do Idoso*, entre otros. El registro en estas bases de datos es voluntario y es accesible para entidades públicas.[29]

4. Chile

El sistema de identidad digital más importante es el conjunto de registros personales digitalizados que mantiene el *Servicio de Registro Civil e Identificación* (SRCeI). Algunas características de este sistema son que el registro es obligatorio y que recolecta datos biométricos.

Un estudio de 2019 de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre el desarrollo de la identidad digital en Chile encontró que la experiencia de uso de la plataforma Clave Única, creada por el SRCeI y gestionada en coordinación con la *Dirección de Gobierno Digital del Ministerio Secretaría General de la Presidencia de la República*, debía ser la base para crear un sistema de identidad digital más avanzado. Algunas recomendaciones fueron fortalecer la plataforma, integrarla en diferentes políticas sectoriales y mejorar su modelo de gobernanza para su adopción en el sector privado.[30] Sin embargo, el sistema de Clave Única fue objeto de un acceso masivo no autorizado, dato que fue muy criticado por la sociedad civil.[31]

Finalmente, existen varios sistemas funcionales en ámbitos específicos. Uno de los casos más relevantes se da en los servicios de salud y consiste en la validación obligatoria biométrica de

---

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

(28) Ibidem.

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

(30) Biblioteca del Congreso Nacional de Chile (2022). Identidad digital: conceptos y legislación. Véase: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/33658/2/Identidad_Digital_BCN_2022.pdf

(31) J. Carlos Lara. Arrestos más, arrestos menos. Disponible en: https://www.derechosdigitales.org/14943/arrestos-mas-arrestos-menos/

identidad a través de la huella dactilar de los afiliados al *Fondo Nacional de Salud* (FONASA) para la compra de bonos electrónicos, que permiten subsidiar las atenciones. El registro en estas bases de datos es obligatorio para la compra de los bonos, aunque existen alternativas en caso no se pueda realizar la validación biométrica.[32]

5. Colombia

El sistema de identidad digital más importante es el conjunto de registros personales digitalizados que mantiene la *Registraduría Nacional del Estado Civil*. Algunas características de este sistema son que el registro es obligatorio, que recolecta datos biométricos y que actualmente ofrece una versión digital del documento de identidad mediante el uso de aplicaciones móviles.[33]

También existe un sistema creado en 2011, a partir del Decreto N° 1630 que establece un registro de los equipos móviles adquiridos por primera vez en una base de datos compuesta por los datos del titular, código IMEI, número de móvil, entre otros. Algunas características de este sistema son que el registro es obligatorio, que su propósito alegado es prevenir el robo de móviles y su uso con fines delictivos, y que la base de datos es accesible para entidades públicas.[34]

Finalmente, existen varios sistemas funcionales en ámbitos específicos. Uno de los casos más relevantes se da en el ámbito del control migratorio y consiste en la base de datos *Registro Único de Migrantes Venezolanos* (RUMV) que mantiene el *Ministerio de Relaciones Exteriores a través de la Unidad Administrativa Especial de Migración Colombia*, con el objetivo de identificar a los migrantes venezolanos en el país y determinar su estado migratorio. El registro en esta base de datos es obligatorio y recolecta datos biométricos.[35]

6. Costa Rica

El sistema de identidad digital más importante es el conjunto de registros personales digitalizados que mantiene la *Dirección General de Registro Civil del Tribunal Supremo de Elecciones* (TSE). Algunas características de este sistema son que el registro es obligatorio y que recolecta datos biométricos.[36]

También existe un sistema creado en 2014 a partir de una obligación genérica presente en el *Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones* de

---

(32) Figueroa, Javiera; Venegas, Catalina (2020). Narrativas en torno al uso de la huella digital en la salud pública. Véase: https://www.derechosdigitales.org/wp-content/uploads/huelladigital-saludpulbica-1.pdf

(33) Fundación Karisma (2021). El sistema de reconocimiento facial de la Registraduría Nacional. Véase: https://digitalid.karisma.org.co/2021/07/01/sistema-reconocimiento-facial-registraduria/

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

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

(36) IPANDETEC (2021). Caretas Digitales: Digital Identity in Central America (Página 9). Véase: https://www.ipandetec.org/wp-content/uploads/2021/05/IPNDTC_CARDIG2021_ingles.pdf

mantener un registro de líneas móviles denominado *Registro Prepago*, compuesto por los datos del titular, número de móvil, entre otros. Algunas características de este sistema son que el registro es obligatorio, que su propósito es prevenir el uso de las líneas con fines delictivos y que la base de datos es accesible para entidades públicas.[37]

Finalmente, existen varios sistemas funcionales en ámbitos específicos. Uno de los casos más relevantes se da en los servicios de salud y consiste en el *Expediente Digital Único de Salud* que mantiene la *Caja Costarricense de Seguro Social*, a partir del cual se puede consultar, a través de una aplicación móvil, las citas médicas, los medicamentos prescritos, el historial de diagnósticos y datos sobre pensiones. El registro en esta base de datos y el uso de la aplicación es voluntario.[38]

7. El Salvador

El sistema de identidad digital más importante es el conjunto de registros personales digitalizados que mantiene el *Registro Nacional de Personas Naturales* (RNPN). Algunas características de este sistema son que el registro es obligatorio y que recolecta datos biométricos.

En 2020, la *Secretaría de Innovación de la Presidencia* presentó la Agenda Digital 2020-2030, que incluye como uno de sus ejes a la identidad digital. El objetivo principal alegado de dicho eje es crear un ecosistema de "soluciones" para la gestión de datos personales, el intercambio seguro de información y la integración de servicios digitales, para lo cual se implementará una única identidad nacional. Algunas acciones incluyen el fortalecimiento del RNPN, el reemplazo de sistemas de identidad funcionales por un solo sistema de identidad fundacional y la simplificación de procesos poniendo al ciudadano en el centro.[39]

Finalmente, existen varios sistemas funcionales en ámbitos específicos. Uno de los casos más relevantes se da en los servicios gubernamentales y consiste en la plataforma *Simple SV,* mantenida por la *Secretaría de Innovación de la Presidencia*, a partir de la cual se ofrece acceso a servicios como consultas, trámites y pagos en una forma similar a *Clave Única* en Chile. El registro en esta base de datos es voluntario.[40]

8. México

Tres de los sistemas de identidad digital más importantes son el conjunto de registros personales digitalizados que mantienen el *Registro Nacional de Población e Identificación Personal* (RENAPO), el *Instituto Nacional Electoral* (INE) y el *Sistema de Administración Tributaria* (SAT). Algunas características de estos sistemas son que el registro es obligatorio, que el segundo

---

(37) Portal de SUTEL. ¿Qué debo saber sobre el registro del servicio prepago? Véase: https://registroprepago.sutel.go.cr/preguntasFrecuentes.action

(38) IPANDETEC (2021). Caretas Digitales: Digital Identity in Central America (Páginas 10-11). Véase: https://www.ipandetec.org/wp-content/uploads/2021/05/IPNDTC_CARDIG2021_ingles.pdf

(39) Secretaría de Innovación de la Presidencia. Agenda Digital 2020-2030 (Página 20). Véase: https://www.innovacion.gob.sv/downloads/Agenda%20Digital.pdf

(40) DPL News. Gobierno digitaliza 2,000 trámites en una ventanilla única. Véase: https://dplnews.com/el-salvador-gobierno-digitaliza-2000-tramites-en-una-ventanilla-unica/

siempre recolecta datos biométricos y que todos otorgan una tarjeta física o digital que puede ser utilizada como documento de identidad.[41]

Aunque llegaron a existir hasta dos sistemas creados a partir de la obligación de registrar líneas móviles, denominados *Registro Nacional de Usuarios de Telefonía Móvil* (RENAUT) en 2009 y *Padrón Nacional de Usuarios de Telefonía Móvil* (PANAUT) en 2021, actualmente ambos se encuentran derogados.[42] Algunas características de estos sistemas eran que la inscripción era obligatoria, que su propósito alegado recaía en prevenir el robo de móviles y su uso con fines delictivos, y que las bases de datos eran accesibles para entidades públicas.[43]

Finalmente, existen diferentes iniciativas que buscan la creación de una *Cédula Única de Identidad Digital* (CUID), cuya base de datos consolide las bases de diferentes sistemas y sea administrada por el RENAPO, pero que además incluya datos biométricos, los cuales actualmente no se añaden al documento *Clave Única de Registro de Población* (CURP) que otorga esta entidad. El Banco Mundial ha promovido activamente estas iniciativas, presentando incluso un plan de trabajo y una oferta de préstamo para su ejecución.[44]

9. Paraguay

El sistema de identidad digital más importante es el conjunto de registros personales digitalizados que mantiene el *Registro del Estado Civil*, siendo el registro obligatorio.[45]

Por su parte, el *Ministerio de Tecnologías de la Información y Comunicación* (MITIC) ha creado el Portal del Gobierno de Paraguay, *Gov.py*, a partir de la cual se ofrece acceso a servicios como consultas, trámites y pagos a través de la plataforma *Identidad Electrónica*, que habilita además un repositorio de documentos en la nube denominado *Carpeta Ciudadana*. Algunas características de este sistema son que el registro es voluntario y que la base de datos es accesible para entidades públicas.[46]

Finalmente, existen varios sistemas funcionales en ámbitos específicos. Uno de los casos más relevantes se da en el control migratorio y consiste en el uso del *Sistema Automatizado Migratorio de Reconocimiento Facial* (SMARF) que mantiene el *Ministerio del Interior* a través de la

---

(41) World Bank (2020). Digital Identification Mexico. Véase: https://documents1.worldbank.org/curated/en/099345105252221502/pdf/P16477008a7aa10c30a04b0905975256220.pdf

(42) R3D. Pleno de la SCJN declara inconstitucional al PANAUT. Disponible en: https://r3d.mx/2022/04/25/pleno-de-la-scjn-declara-inconstitucional-al-panaut/

(43) Forbes México. Corte invalida la creación del padrón de usuarios de celulares. Véase: https://www.forbes.com.mx/corte-invalida-la-creacion-del-padron-de-usuarios-de-celulares/

(44) World Bank. Mexico National Digital Identity System to Facilitate Inclusion (P172647). Véase: https://documents1.worldbank.org/curated/en/657131611543704157/pdf/Mexico-National-Digital-Identity-System-to-Facilitate-Inclusion-Project.pdf

(45) Ver: https://registrocivil.gov.py/tramites

(46) Portal del Gobierno de Paraguay. ¿Qué es la Identidad Electrónica? Véase: https://www.paraguay.gov.py/identidad-electronica/informacion

Dirección General de Migraciones, y que operó brevemente en la triple frontera entre Argentina, Brasil y Paraguay, antes de ser trasladado al Aeropuerto Internacional Silvio Pettirossi, en Asunción. La validación biométrica mediante este sistema opera con bases de datos de la Policía Nacional y su uso es voluntario.[47]

10. Perú

El sistema de identidad digital más importante es el conjunto de registros personales digitalizados que crea y mantiene el *Registro Nacional de Identificación y Estado Civil* (RENIEC). Algunas características de este sistema son que el registro es obligatorio y que recolecta datos biométricos.[48]

También existe un sistema establecido en 2017, a partir del Decreto Legislativo N° 1338 que crea el R*egistro Nacional de Equipos Terminales Móviles para la Seguridad* (RENTESEG), compuesto por los datos del titular, código IMEI, código IMSI, número de móvil, entre otros. Algunas características de este sistema son que el registro es obligatorio, que su propósito alegado es el de prevenir el robo de móviles y su uso con fines delictivos, y que la base de datos es accesible para entidades públicas.[49]

Finalmente, existen varios sistemas funcionales en ámbitos específicos. Uno de los casos más relevantes se da en el control migratorio y consiste en el *Registro Central de Extranjería*, base de datos que mantiene el *Ministerio del Interior* a través de la *Superintendencia Nacional de Migraciones*, con el objetivo de identificar a los migrantes venezolanos y otorgarles documentos de identidad. El registro en esta base de datos es obligatorio y recolecta datos biométricos.[50]

11. Venezuela

El sistema de identidad digital más importante es el *Servicio Administrativo de Identificación, Migración y Extranjería* (SAIME), mediante el cual se otorga documentos de identificación a ciudadanos y extranjeros residentes, el cual es alimentado por el conjunto de registros personales digitalizados que mantiene la *Oficina Nacional de Registro Civil del Consejo Nacional Electoral*. Algunas características de este sistema son que el registro es obligatorio y que recolecta datos biométricos.

Finalmente, existen varios sistemas funcionales en ámbitos específicos. Uno de los casos más relevantes se da en la seguridad social y consiste en una base de datos denominada *Plataforma Patria* que, pese a no ser mantenida directamente por el gobierno, es utilizada para la entrega de

(47) 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). Véase: https://www.tedic.org/wp-content/uploads/2023/01/Tecnologia-y-DDHH-en-la-Triple-Frontera-1.pdf

(48) Hiperderecho (2020). Identidad Digital en Perú: Descifrando al Leviatán. Véase: https://hiperderecho.org/wp-content/uploads/2020/11/guerrero_identidad_digital.pdf

(49) Hiperderecho (2019). Registro obligatorio de celulares. Véase: https://hiperderecho.org/2019/05/registro-obligatorio-de-celulares/

(50) Portal del Gobierno del Perú. Captura de datos biométricos para trámites de extranjeros se realiza únicamente de manera presencial. Véase: https://www.gob.pe/institucion/migraciones/noticias/605143-captura-de-datos-biometricos-para-tramites-de-extranjeros-se-realiza-unicamente-de-manera-presencial

bonos y subsidios estatales de alimentación y combustible, muchas veces de manera arbitraria. El registro en esta base de datos es voluntario, pero indispensable para poder acceder a los beneficios antes mencionados.[51]

12. Ecuador

El sistema de identidad digital más importante en Ecuador es el conjunto de registros personales digitalizados que crea y mantiene la *Dirección General de Registro Civil, Identificación y Cedulación* (REGISTRO CIVIL). A nivel normativo, dicho sistema se rige por las disposiciones de la *Ley Orgánica de Gestión de la Identidad y Datos Civiles* aprobada en 2016.[52] Algunas características de este sistema son que el registro es obligatorio desde el nacimiento (incluyendo en sus bases de datos a extranjeros residentes en el territorio, a diferencia de países como Colombia o Perú) y que recolecta datos biométricos, las cuales se utilizan en la provisión de diferentes servicios de identificación, tanto para el sector público como privado.

Además, el Registro Civil ha instrumentalizado este sistema para proveer servicios de identificación. Uno de estos usos es la emisión de certificados de firma electrónica, una operación que se rige por la Ley de Comercio Electrónico, Firmas y Mensajes de Datos aprobada en 2002.[53] El otro es la venta directa de servicios de identificación a entidades privadas, mediante el *Sistema Nacional de Identificación Ciudadana*, que opera bajo la suscripción de convenios que no tienen una base legal clara.[54]

En cuanto a sistemas de identidad digital basados en registros de líneas o equipos móviles, en 2009 se aprobó la Resolución N° 191-07-CONATEL-2009 que creó la *Norma que Regula el Procedimiento para el Empadronamiento de Abonados del Servicio Móvil Avanzado* (SMA) y *Registro de Terminales Perdidos, Robados o Hurtados.* Esta norma, que ha sido modificada hasta en dos ocasiones, ordena la creación de dos listas: una para permitir la operación de equipos (lista positiva) y otra para ordenar su bloqueo (lista negativa). Este sistema es gestionado por la *Agencia de Regulación y Control de las Telecomunicaciones* (ARCOTEL) y es actualizado por las empresas de telecomunicaciones.[55] El registro es obligatorio y contiene datos personales del titular, código IMEI, número de móvil, así como datos asociados al estado del equipo (perdido, hurtado, etc.). Por otro lado, la norma señala que el acceso a dicha base de datos está disponible para ARCOTEL, pero también para cualquier otra entidad competente o vinculada con aspectos

(51) Venturini, Jamila; Díaz, Marianne (2021). Sistemas de identificación y protección social en Venezuela y Bolivia: vigilancia, género y derechos humanos (Páginas 12-15). Véase: https://www.derechosdigitales.org/wp-content/uploads/sistemas-de-Identificacion_ES.pdf

(52) Registro Oficial, Gobierno de Ecuador. Ley Orgánica de Gestión de la 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

(53) Ministerio de Telecomunicaciones. Ley de Comercio Electrónico, firmas y mensajes de datos. Véase: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

(54) En la sección de Anexos se adjunta una copia de modelo de convenio de esta naturaleza.

(55) Consejo Nacional de Telecomunicaciones. Resolución 191-07-CONATEL-2009. Véase: https://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/07/191_07_conatel_20091.pdf

relativos a "temas de seguridad nacional",[56] lo que amplía significativamente el acceso a los datos, sin limitaciones claras de su alcance.

Finalmente, existen otros sistemas funcionales en ámbitos específicos. El que llama más la atención es el posible uso de sistemas de identidad para complementar el uso de cámaras de videovigilancia, especialmente aquellas que poseen tecnologías de reconocimiento facial. Tal como señala *Access Now en su reporte Surveillance Tech In Latin America: Made Abroad, Deployed at Home,*[57] por lo menos desde 2002 se vienen desplegando estas tecnologías en Ecuador con el fin alegado de contribuir a la seguridad pública, siendo muchas de ellas parte del Servicio Integrado de Seguridad ECU 911 (ECU 911).[58] Aunque la evidencia apunta a que la adopción de estos sistemas es extensiva, no existe información oficial que permita comprobar si estas capacidades se utilizan en conjunto con bases de datos biométricas y si fuera así, qué entidad mantiene dichas bases. El reporte *La videovigilancia en Ecuador vulnera derechos ciudadanos* de la organización FUNDAMEDIOS señala que no es posible contestar esta pregunta, dado que los protocolos de actuación de ECU 911 han sido declarados reservados hasta 2028.[59]

Existe también otro sistema sobre el que se sabe incluso menos, pese a que se prevé su uso en las elecciones generales que se llevarán a cabo en agosto de 2023. Se trata del *Sistema de Votación Telemática en el Exterior,* un mecanismo de voto electrónico no presencial habilitado por el Consejo Nacional Electoral (CNE) para permitir el voto de los ecuatorianos residentes en el extranjero.[60] Dicho sistema permite la validación de la identidad del votante mediante dos métodos, siendo uno de ellos el reconocimiento facial. No es claro con qué base de datos opera, si con el padrón electoral del CNE o mediante interoperabilidad con el Registro Civil.[61]

IV. TENDENCIAS EN LA ADOPCIÓN DE SISTEMAS DE IDENTIDAD DIGITAL

En esta sección se presenta un recuento de las principales tendencias identificadas en los procesos de evaluación y adopción de sistemas de identidad digital fundacionales o funcionales en cada país analizado, así como otras iniciativas relacionadas. De la misma forma que la anterior sección, esta lista es preliminar y no es exhaustiva.

---

(56) Consejo Nacional de Telecomunicaciones. Resolución TEL 535-18-CONATEL-2012. Véase: https://www.gob.ec/sites/default/files/regulations/2018-11/TEL-535-18-CONATEL-2012.pdf

(57) Access Now (2021). Surveillance Tech In Latin America: Made Abroad, Deployed at Home. Véase: https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf

(58) Portal del Gobierno de Ecuador. Innovaciones tecnológicas del ECU 911 para la atención de emergencias se presentaron 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/

(59) FUNDAMEDIOS (2021). La videovigilancia en Ecuador vulnera derechos ciudadanos. Véase: https://www.fundamedios.org.ec/wp-content/uploads/2021/12/Inf.-Videovigilancia.pdf

(60) Consejo Nacional Electoral. Voto telemático 2023. Véase: https://www.voto-telematico.cne.gob.ec/ayuda

(61) Consejo Nacional Electoral. Manual de inscripción voto telemático. Véase: https://www.voto-telematico.cne.gob.ec/_files/ugd/157be5_e34f007e38294a2d80257c514317ba8c.pdf?index=true

1. Existe un favorecimiento de registros centralizados vs. múltiples registros
Entre los países analizados parece haber una división evidente entre aquellos que mantienen sistemas de identidad digital a partir de registros personales centralizados a cargo de una sola entidad y aquellos en los que coexisten sistemas con diferentes registros y diferentes entidades a cargo de su mantenimiento. En el primer grupo se encuentran Chile, Colombia, Costa Rica, El Salvador, Paraguay, Perú, Ecuador y Venezuela, mientras que en el segundo están Argentina, Bolivia, Brasil y México. Al respecto, es importante mencionar que salvo Bolivia, el segundo grupo está compuesto por países federales, lo que explica la multiplicidad de registros y entidades que otorgan servicios de identidad.

De lo analizado, se puede observar que contar con registros centralizados ha favorecido a la rapidez del incremento de la implementación de los sistemas de identidad digital. Así, por ejemplo, todos los países del primer grupo, salvo Venezuela, han optado por aplicar una mediación tecnológica para acceder a ciertos servicios gubernamentales, a través de plataformas o portales en línea.

Por otro lado, en el segundo grupo, si bien no ha tenido un avance menor en la adopción de la identidad digital, se observan iniciativas apuntadas a centralizar sus bases de datos. Así, por ejemplo, Brasil ya aprobó en 2017 un nuevo sistema para unificar todos sus registros en una sola base de datos,[62] mientras que un estudio del Banco Mundial ha sugerido lo mismo para México.[63] Esto permite concluir que existe una tendencia a favorecer un modelo de identidad digital centralizado frente a otras opciones como los modelos federados o de mercado abierto.[64]

2. Aumento significativo en la recopilación y tratamiento de datos biométricos para diversos fines que propician la vigilancia
Conforme han señalado organizaciones de la sociedad civil, el número de empresas del sector privado que desarrollan tecnologías con base en datos biométricos, así como el número de los Estados que han implementados dichas tecnologías, ha crecido de manera exponencial,[65] lo cual es concordante con los ejemplos identificados en la sección anterior.

Tal como afirma el reporte *Descubriendo las narrativas sobre identidad y biometría en América Latina* de la organización ADC, varios países de América Latina han construido con relativo éxito "narrativas vinculadas a la necesidad de la tecnología biométrica para el reconocimiento

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

(63) World Bank (2020). Digital Identification Mexico. Véase: https://documents1.worldbank.org/curated/en/099345105252221502/pdf/P16477008a7aa10c30a04b0905975256220.pdf

(64) World Bank. Types of ID systems. Véase: https://id4d.worldbank.org/guide/types-id-systems

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

infalible de la identidad de las personas",[66] estableciendo la recopilación de datos biométricos bajo argumentos amplios y sin límites preestablecidos a su uso. Esto parece consistente con la recolección y uso de estos datos en sistemas de identidad digital fundacionales o funcionales, tanto en países unitarios como federales.

Como se puede observar, todos los países analizados recolectan datos biométricos, en general de manera impositiva, a través de las entidades que mantienen registros personales centralizados, sin existir estudios de impacto de derechos humanos —al menos de manera disponible— que justifiquen su recopilación frente a otras alternativas. A su vez, en algunos casos como el de Paraguay esto se realiza en ausencia de un marco jurídico de protección de datos. En casos como el de Argentina, Brasil y Colombia, si bien existen leyes de protección de datos, la introducción de la biometría no ha sido delineada de manera expresa, precisa y por ley, desafiando de esta forma al principio de legalidad.[67]

Sin parámetros claros sobre dicha recopilación, sus usos y delimitaciones, los estados en cuestión han utilizado dichos datos para diversas finalidades. Por ejemplo, en Argentina se ha habilitado su uso para la seguridad pública, en Chile y Costa Rica para el acceso a servicios de salud, y en Colombia, Paraguay y Perú para el control migratorio.

A su vez, en ciertos casos se han generado normativas para incluir datos biométricos en bases de datos que antes no los contemplaban. Es el caso de Brasil donde, mediante la ley que crea el sistema de Identificação Civil Nacional (ICN) se prevé que la nueva base de datos incluya los datos biométricos que actualmente solo son recolectados por el *Tribunal Superior Eleitoral* (TSE).[68] A su vez, el Banco Mundial ha propuesto que una futura *Cédula Única de Identidad Digital* (CUID) de México contenga datos biométricos que la *Clave Única de Registro de Población* (CURP) actualmente no posee.[69] Esto permite concluir que existe una tendencia a incrementar la recopilación y tratamiento de datos biométricos bajo narrativas que le presentan como necesarios para la implementación de sistemas de identidad digital, sin suficientes salvaguardas de derechos humanos.

3. Se observa poca inclusión social y mayor potencial de discriminación

Pese a que los argumentos en torno a la transformación digital de los sistemas de identificación se basan en una supuesta mejora en la cobertura de los servicios de identidad y la inclusión de

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

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

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

(69) World Bank (2020). Digital Identification Mexico. Véase: https://documents1.worldbank.org/curated/en/099345105252221502/pdf/P16477008a7aa10c30a04b0905975256220.pdf

poblaciones excluidas por los sistemas tradicionales, esto no se observa en la mayoría de los países de la región que han adoptado sistemas de identidad digital. Más aún, si atendemos a los reportes que existen sobre la *Plataforma Patria* de Venezuela, estamos hablando de sistemas cuyo objetivo parece ser la exclusión.[70]

En el mejor de los casos, estos sistemas han facilitado el acceso a servicios gubernamentales en línea a un grupo de la población con varias condiciones de privilegio (buena conectividad, habilidades digitales) como ocurre en Chile, Costa Rica, Ecuador y El Salvador. Se observa entonces que la digitalización no solo es insuficiente para aportar a mejorías en el acceso a servicios básicos, sino que abre espacios para nuevas formas de discriminación. Por ejemplo, en el caso de Venezuela se han implementado sistemas biométricos para controlar la adquisición de productos de primera necesidad, resultando en diversas denuncias de discriminación hacia personas extranjeras y, especialmente, personas transgénero, conforme hemos reportado en investigaciones anteriores.[71] En ese sentido, es importante resaltar que, además de los impactos por discriminación, estas iniciativas implican, a su vez, una vigilancia diferenciada hacia las personas que se encuentran en una situación de vulnerabilidad y que, por lo mismo, dependen de mayor forma del Estado. Otro ejemplo para destacar es el caso de Brasil y su programa de auxilio de emergencia implementada durante la pandemia. Como hemos observado en investigaciones previas, la decisión tuvo como consecuencia un incremento de las dificultades de acceso para las personas que más necesitaban apoyo y que no necesariamente disponían de un número de teléfono, un dispositivo personal conectado desde donde registrarse o incluso un documento válido.[72]

Estas situaciones evidencian que la tecnología no puede ni debe ser presentada como forma de resolver problemas estructurales, como aquellos relacionados al hecho de que algunas poblaciones han sido históricamente excluidas del acceso a derechos. Así pues, se puede afirmar que existe una tendencia a adoptar sistemas que no están siendo efectivos para avanzar en políticas de inclusión.

4. Existen proveedores comunes para tecnologías de identidad digital y de vigilancia
Los reportes *Surveillance Tech In Latin America: Made Abroad, Deployed at Home* de la organización *Access Now*[73] y *Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa*[74] del consorcio AlSur, permiten concluir que el mercado de suministro de tecnologías con capacidades de vigilancia para gobiernos está dominado por algunos grandes proveedores. Por ejemplo, se mencionan empresas como

(70) Transparencia Venezuela (2018). Carnet de la Patria: El apartheid revolucionario. Véase: https://transparenciave.org/wp-content/uploads/2018/03/Carnet-de-la-patria-2018-TV.pdf

(71) https://www.derechosdigitales.org/wp-content/uploads/sistemas-de-Identificacion_ES.pdf

(72) https://www.derechosdigitales.org/wp-content/uploads/sistemas-de-Identificacion_ES.pdf

(73) Access Now (2021). Surveillance Tech In Latin America: Made Abroad, Deployed at Home. Véase: https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf

(74) AlSur (2021). Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa. Véase: https://www.alsur.lat/sites/default/files/2021-11/ALSUR_Reconocimiento_facial_en_Latam_ES.pdf

AnyVision, Hikvision, Dahua, Cellebrite, Huawei, ZTE, NEC, IDEMIA, VERINT, entre otros. Como se ha señalado en la sección de Metodología, no existe una diferencia esencial entre un sistema de identidad digital y un sistema de vigilancia estatal. Por ello, no resulta extraño hallar que, en varios casos, los proveedores de productos de identidad digital son los mismos que los que proveen tecnologías con capacidades de vigilancia. Este el caso de la empresa francesa IDEMIA (ex Morpho), que presta o ha prestado servicios de identidad digital para Argentina[75], Chile[76], Colombia[77], Costa Rica[78] Ecuador[79] y Perú[80]. Algo parecido ocurre con la empresa china ZTE en algunas provincias de Argentina[81] y en Venezuela.[82]

Los reportes antes mencionados señalan que, en muchos casos, las empresas que proveen estas tecnologías no valoran el impacto que su uso tendrá en las poblaciones objetivo y, en general, no parecen interesadas en establecer estándares de transparencia, rendición de cuentas y salvaguardas de derechos humanos para su industria, lo cual sugiere que la mayoría de las empresas proveedoras de tecnologías de vigilancia no cumple con los Principios rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas, especialmente en cuanto al compromiso de respetar los derechos humanos, los procesos de debida diligencia implementados para identificar y prevenir los perjuicios significativos a los derechos humanos y la divulgación abierta de información sobre el cumplimiento actual de las leyes vigentes.[83]

---

(75) Asociación por los Derechos Civiles (2017). La identidad que no podemos cambiar: Cómo la biometría afecta nuestros derechos humanos (Páginas 24-25). Véase: https://adc.org.ar/wp-content/uploads/2019/06/027-A-la-identidad-que-no-podemos-cambiar-04-2017.pdf

(76) World Bank (2016). Digital identity: towards shared principles for public and private sector cooperation (Pagína 36). Véase: https://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf

(77) Fundación Karisma (2021). El sistema de reconocimiento facial de la Registraduría Nacional. Véase: https://digitalid.karisma.org.co/2021/07/01/sistema-reconocimiento-facial-registraduria/

(78) AlSur (2021). Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa (Páginas 16-17). Véase: https://www.alsur.lat/sites/default/files/2021-11/ALSUR_Reconocimiento_facial_en_Latam_ES.pdf

(79) Registro Civil, Identificación y Cedulación (2019). Registro Civil adjudicó contrato para nuevo sistema de emisión de pasaportes biométricos y cédulas de identidad. Véase: https://www.registrocivil.gob.ec/registro-civil-adjudico-contrato-para-nuevo-sistema-de-emision-de-pasaportes-biometricos-y-cedulas-de-identidad/

(80) Hiperderecho (2018). Identidad Biométrica en Perú: Estado de la cuestión (Página 14). Véase: https://hiperderecho.org/wp-content/uploads/2018/06/identidad_biometrica_peru_2018.pdf

(81) Portal Somos Jujuy (2022). Instalaron 600 cámaras de seguridad en puntos estratégicos del Gran Jujuy. Véase: https://www.somosjujuy.com.ar/jujuy/instalaron-600-camaras-seguridad-puntos-estrategicos-gran-jujuy-n65387

(82) Agencia Reuters (2018). Como ZTE ayuda a Venezuela a implementar un control social al estilo chino. Véase: https://www.reuters.com/investigates/special-report/venezuela-zte-es/

(83) https://www.accessnow.org/wp-content/uploads/2023/04/ESPANOL-Analysis-Remote-biometric-surveillance-LATAM.pdf

V. RIESGOS DE LA IDENTIDAD DIGITAL Y SUS SISTEMAS A LOS DERECHOS HUMANOS

En esta sección se presenta un recuento de las principales problemáticas que atraviesan los procesos de adopción de los sistemas de identidad digitales fundacionales o funcionales, así como otras iniciativas relacionadas. De la misma forma que las dos secciones anteriores, esta lista también es preliminar y no es exhaustiva.

1. Ambigüedad en los conceptos alrededor de la identidad digital

Pese a que el concepto de identidad digital lleva varias décadas siendo objeto de diferentes estudios, hoy en día no existe aún un concepto consensuado sobre la *identidad digital* o de sus términos derivados, *sistemas de identidad digital* y *sistemas de identidad digital fundacionales*. Organismos internacionales como el Banco Mundial, la Unión Internacional de Telecomunicaciones (UIT) y la OCDE han propuesto definiciones que son más o menos similares, pero que adolecen de un problema: no permiten delimitar el propósito de dichos sistemas.

Como se puede apreciar en la sección que analiza los sistemas de identidad de los países de la región, la mayoría de estos ha seguido una ruta más o menos similar, empezando por contar con registros personales centralizados, los que luego han digitalizado y sobre los que han construido o implementando tecnologías para propósitos diferentes a los alegados inicialmente. Pese a este origen común, existe una gran diferencia entre la plataforma de trámites Simple SV de El Salvador y el SIBIOS de Argentina. Y la diferencia no es otra que el propósito para el cual han sido creadas.

Aun si se acordara por consenso el uso de cierta terminología, si no son claros los límites que tendrán los sistemas de identidad digital, la ambigüedad se mantendrá dificultando el uso de un lenguaje común entre las partes interesadas, incluida la sociedad civil, especialmente en contextos donde la confianza en las instituciones es baja. Tampoco podrá valorarse el nivel de amenazas y riesgos para los derechos humanos.

2. Proliferación de tecnologías biométricas

Diferentes organizaciones han señalado en múltiples ocasiones los graves riesgos que conlleva la creación y mantenimiento de bases de datos centralizadas.[84] Contrario a ello, todos los países analizados en este reporte mantienen una o varias bases de datos de este tipo, varias de las cuales contienen datos biométricos. Esta situación ha permitido el despliegue de sistemas de validación biométrica con huella dactilar y cámaras con reconocimiento facial, lo que aumenta exponencialmente los peligros asociados a la vigilancia estatal, además de las brechas de seguridad.

Sin embargo, la tendencia en la región parece ser la profundización de estas prácticas, lo que incluye la creación de sistemas de identidad digital fundacionales que incorporan datos biométricos, aun cuando los sistemas tradicionales en los que están basados no hubieran incorporado previamente dicha información. Esto significa que, a nivel general, la adopción de cualquier sistema de identidad digital sería un potencial habilitador para la proliferación de tecnologías biométricas, algunas de ellas en ámbitos especialmente críticos, como la seguridad pública, el acceso a servicios de seguridad social y el control migratorio.

(84) Digital National ID systems: Ways, shapes and forms. Privacy International. Enlace: https://privacyinternational.org/long-read/4656/digital-national-id-systems-ways-shapes-and-forms

Lo anterior no es una amenaza hipotética, sino que ya viene ocurriendo en varios de los países de la región que operan sistemas de identidad digital fundacionales o funcionales en estos ámbitos, o incluso los que mantienen registros obligatorios de líneas y equipos móviles, como es el caso de Argentina, Bolivia, Colombia, Costa Rica, Ecuador y Perú.

3. Falta de transparencia, marcos legales y garantías

Salvo el caso de Brasil y Ecuador, en donde la adopción de su sistema de identidad digital se ha llevado a cabo a través de una reforma legislativa, en los demás países analizados estos cambios no se han tramitado a través de proyectos de ley u otras normas que permitan un proceso de discusión amplio y participativo.[85] Esto ha significado una reducción de la transparencia y, en algunos casos, ha supuesto la interposición de medidas legales por diferentes organizaciones de la sociedad civil para conocer qué tecnologías se están adquiriendo.[86]

En algunos países estos procesos han sido particularmente opacos. Por ejemplo, en Colombia la Registraduría Nacional del Estado Civil implementó tecnologías de reconocimiento facial a partir de 2018 sin dar publicidad a la medida.[87] De manera similar, en Perú el Registro Nacional de Identificación y Estado Civil adoptó esta tecnología sin emitir ninguna norma, ni siquiera de gestión interna, amparándose únicamente en el mandato genérico de una ley de 1995.[88] Estos y otros casos han erosionado paulatinamente la confianza de la sociedad civil en el gobierno a propósito del uso de estas tecnologías.

A la falta de regulación específica en materia de identidad digital se suma el hecho de que no todos los países analizados cuentan con normas que establezcan límites concretos a la adopción y uso de estos sistemas. Por ejemplo, Bolivia, Paraguay y Venezuela no cuentan actualmente con leyes de protección de datos personales, y los demás que sí las tienen presentan diferentes niveles de desfase temporal o dificultades para la aplicación por diferentes motivos.[89]

4. Potenciales y reales afectaciones a los derechos humanos

El conjunto de amenazas y riesgos que suponen las problemáticas antes señaladas proyectan un panorama complejo, en el que pueden producirse diferentes afectaciones a los derechos

---

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

(86) Diario Clarín (2021). Presentan un amparo contra el uso del reconocimiento facial en la Ciudad de Buenos Aires. Véase: https://www.clarin.com/tecnologia/presentan-amparo-uso-reconocimiento-facial-ciudad-buenos-aires_0_hPbmHMTzV.html

(87) Fundación Karisma (2021). El sistema de reconocimiento facial de la Registraduría Nacional. Véase: https://digitalid.karisma.org.co/2021/07/01/sistema-reconocimiento-facial-registraduria/

(88) Hiperderecho (2020). Identidad Digital en Perú: Descifrando al Leviatán. Véase: https://hiperderecho.org/wp-content/uploads/2020/11/guerrero_identidad_digital.pdf

(89) 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 27-35). Véase: https://internetbolivia.org/file/2021/11/ib_conectados.pdf

humanos. Además, es preciso reforzar que estas afectaciones no se restringen exclusivamente a la privacidad y la protección de los datos personales, sino también a un amplio espectro de derechos conectados a los servicios que los sistemas de identidad digital buscan habilitar o restringir.

En México, organizaciones de derechos humanos han reaccionado de manera muy crítica a las iniciativas que buscan crear un sistema de identidad digital que emplee una *Cédula Única de Identidad Digital* (CUID), incluyendo la propuesta de financiamiento del Banco Mundial. Entre los peligros potenciales que se han expresado están la afectación del derecho a la identidad a partir de los fallos del sistema, la afectación a la privacidad y la protección de datos a partir de posibles fugas de información, la discriminación en el acceso a servicios esenciales por no poseer una identidad reconocible y los potenciales usos ilegítimos del sistema en el futuro.[90]

Pero las afectaciones no solo son potenciales. Ya existen casos reales y documentados de afectaciones a propósito de la adopción de sistemas de identidad digital. En 2019, un hombre fue detenido en Argentina por un error en un sistema de reconocimiento facial y pasó 6 días preso antes de que se descubriera el error.[91] En 2020, un estudio a pequeña escala reveló que en Chile se producía la exclusión de ciertas personas de los servicios de salud por no poder pasar un proceso de validación biométrica.[92] En Ecuador se reveló una fuga masiva de datos del Registro Civil en 2019, que hasta el momento no ha sido explicada[93] y que refleja los riesgos sobre la posibilidad de que se produzcan accesos no autorizados, brechas de seguridad y fugas que expongan la información de la ciudadanía. Finalmente, también en 2020, un sistema de identidad digital creado para la entrega de bonos de emergencia en Perú fue vulnerado, registrándose una pérdida aproximada de 250 mil dólares.[94]

Ante situaciones similares, se han interpuesto acciones legales que han impactado sistemas de identidad digital de manera indirecta, específicamente aquellos que alimentan sistemas de vigilancia basados en el uso de cámaras de videovigilancia. Por ejemplo, en 2021, el Tribunal de Justicia de São Paulo bloqueó el uso de reconocimiento facial en una ruta de transporte por

---

(90) Access Now (2021). Carta abierta: La cédula única de identidad digital incluida en la Ley General de Población amenaza los derechos humanos. Véase: https://www.accessnow.org/wp-content/uploads/2021/09/Carta_La_ce%cc%81dula_u%cc%81nica_de_identidad_digital_incluida_en_la_Ley.pdf

(91) Diario Página 12 (2019). Seis días arrestado por un error del sistema de reconocimiento facial. Véase: https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien

(92) Figueroa, Javiera; Venegas, Catalina (2020). Narrativas en torno al uso de la huella digital en la salud pública. Véase: https://www.derechosdigitales.org/wp-content/uploads/huelladigital-saludpulbica-1.pdf

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

(94) Hiperderecho (2020). Lo que nos enseña la suplantación y robo a los beneficiarios del Bono Familiar Universal. Véase: https://hiperderecho.org/2020/06/lo-que-nos-ensena-la-suplantacion-y-robo-a-los-beneficiarios-del-bono-familiar-universal/

parte de la empresa Via Quatro.[95] Más recientemente, en la Ciudad de Buenos Aires, un tribunal local declaró inconstitucional el uso de reconocimiento facial.[96]

VI. CONCLUSIONES

En esta sección, se presentan las conclusiones del reporte, que a su vez justifican un conjunto de recomendaciones para organizaciones de la sociedad civil, las cuales se encuentran en la siguiente sección.

1. Los sistemas de identidad digital se extienden por la región

De un total de 20 países que forman parte de América Latina, 12 de ellos han sido analizados en este reporte y todos presentan diferentes sistemas de identidad digital, tanto fundacionales como funcionales. Algunos de estos sistemas se encuentran en una etapa muy inicial, mientras que otros ya han habilitado la provisión de ciertos servicios gubernamentales e, incluso, se ha producido despliegues de tecnologías con capacidades de vigilancia para la seguridad pública, acceso a la seguridad social, salud y el control migratorio.

2. Registros centralizados, uso de datos biométricos y baja inclusión son las tendencias principales

El análisis permite concluir que existen las siguientes tendencias:

(i) el favorecimiento de modelos de identidad digital centralizados, en vez de ecosistemas de identidad digital federados o de mercado abierto.
(ii) el aumento significativo en la recopilación y tratamiento de datos biométricos para diversos fines que propician la vigilancia bajo la implementación de narrativas de que la inclusión de datos biométricos es imprescindible para la adopción de sistemas de identidad digital fundacionales, pese a la existencia de otras alternativas, algunas de las cuales podrían ser más seguras y respetuosas con los derechos humanos.
(iii) se identifica que, aunque uno de los argumentos centrales para promover sistemas de identidad digital es su capacidad para avanzar agendas de inclusión (económica, social), la mayoría de los sistemas identificados está siendo utilizado en conjunto con tecnologías de vigilancia para actividades policiales o de distinto tipo de control de la población, incluidos los migrantes.
(iv) Finalmente, se ha detectado que algunos proveedores de tecnologías de identidad digital en la región también proveen tecnologías con capacidades de vigilancia.

3. Problemas potenciales y reales en torno a los sistemas de identidad digital

El análisis revela que existen problemas en múltiples ámbitos. Para empezar, los conceptos sobre identidad digital no son claros entre sus múltiples proponentes, lo que crea incertidumbre sobre el alcance de los sistemas de identidad digital. Así pues, dado que existe

(95) Access Now (2021). Victoria de privacidad para 350.000 personas en São Paulo: tribunal bloquea cámaras de reconocimiento facial en el metro. Véase: https://www.accessnow.org/press-release/sao-paulo-tribunal-prohibe-camaras-de-reconocimiento-facial-en-el-metro/

(96) CELS (2022). Declaran inconstitucional el uso del sistema de reconocimiento facial en CABA. Véase: https://www.cels.org.ar/web/2022/09/una-jueza-declaro-inconstitucional-el-uso-del-sistema-de-reconocimiento-facial-en-caba/

una narrativa estatal tendiente a favorecer sistemas construidos en torno a bases de datos centralizadas, que incluyen datos biométricos, estos sistemas habilitan la proliferación de tecnologías con capacidades de vigilancia como el reconocimiento facial.

Sumado a lo anterior, en muchos casos los sistemas de identidad digital han sido desarrollados sin realizar estudios de impacto en derechos humanos, con muy poca transparencia y sin que existan límites específicos a sus objetivos o a la tecnología que utilizan. Finalmente, existen problemas potenciales en países donde se está intentando adoptar estos sistemas, pero también casos reales de afectaciones a diferentes derechos, incluyendo la discriminación en el acceso a servicios públicos y ayudas sociales, entre otros.

VII. RECOMENDACIONES

En esta sección se presenta un conjunto de recomendaciones dirigidas a los Estados y a las organizaciones de la sociedad civil.

1. A los Estados y gobiernos nacionales:

1) **Desarrollar normativas adecuadas que regulen la aprobación y supervisión de las tecnologías con capacidades de vigilancia:** Se deben incluir normas estrictas de transparencia y rendición de cuentas, y lineamientos que refuercen los controles de exportación e importación, previendo herramientas legales para las víctimas.
2) **Realizar evaluaciones de impacto a derechos humanos previo a la implementación de los sistemas de identidad digital y desarrollar mecanismos de control de efectividad:** El análisis debe ser realizado a partir de los principios de legalidad, necesidad y proporcionalidad reconocidos internacionalmente, aplicando una moratoria para aquellos sistemas/tecnologías que no cumplan con criterios básicos. Garantizar la supervisión judicial y el derecho a recursos efectivos.
3) **Desarrollar mecanismos de rendición de cuentas y participación de múltiples partes interesadas en cualquier proceso de digitalización:** Se deben generar mecanismos públicos de aprobación y supervisión de las tecnologías con capacidades de vigilancia. En base al principio de transparencia, se debe comunicar previamente sobre la adopción de cualquier sistema de identificación que permita un debate público y suficiente sobre el tema, además de generar procesos de auditorías que midan su implementación y permitan comunicar resultados a la ciudadanía.
4) **Desarrollar y/o adecuar legislaciones de protección de datos personales acorde a estándares de derechos humanos:** Esto debe operar como un requisito necesario para poder realizar tratamiento de datos. La legislación debe contar con definiciones claras y salvaguardas diferenciadas respecto a datos sensibles como biometría, así como con autoridades públicas independientes encargadas de supervisar el cumplimiento de la legislación y mecanismos efectivos para la ciudadanía sobre sus datos.
5) **Establecer salvaguardas suficientes en relación a la protección de los datos recopilados y almacenados en bases de datos:** Los datos personales deben estar protegidos por salvaguardas de seguridad razonables en contra de riesgos como la pérdida o el acceso no autorizado, la destrucción, el uso, la modificación o la divulgación de los datos.
6) **Prohibición de condicionar el acceso a servicios a entrega de datos:** Esto especialmente en cuanto a datos biométricos. El acceso a derechos no puede estar condicionado a la entrega de datos, mucho menos datos sensibles.

2. A las organizaciones de la sociedad civil

1) **Mayores estudios sobre identidad digital en la región:** Continuación de estudios más profundos que permitan identificar usos y tendencias que este reporte no ha alcanzado

a cubrir, dada su naturaleza exploratoria,[97] incluso con casos de estudio para identificar buenas prácticas con enfoque de derechos humanos.

2) **Acciones de incidencia y litigio estratégico en materia de identidad digital:** identificar oportunidades de incidencia y litigio estratégico que detengan proyectos de adopción o uso de sistemas de identidad digital que no cumplan con principios de derechos humanos: Legalidad, necesidad, idoneidad, proporcionalidad, debido proceso, mecanismos de control y derecho a recurso, transparencia activa, evaluación de impacto previo, debate democrático para su adopción, y garantías para la cooperación internacional.[98]

VIII. BIBLIOGRAFÍA

Access Now (2018). National Digital Identity Programmes: What's next?
Access Now (2021). Surveillance Tech In Latin America: Made Abroad, Deployed at Home.
Africa Digital Rights Hub (2022). Data Protection Code of Practice for Digital Identity Schemes in Africa.
Africa Digital Rights Hub (2022). The inclusiveness or exclusiveness of National IDs in West Africa: Countries of focus: Côte d'Ivoire, Ghana and Nigeria.
AlSur (2018). 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 por los Derechos Civiles (2015). Si nos conocemos más, nos cuidamos mejor: Informe sobre políticas de biometría en la Argentina.
Asociación por 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 por los Derechos Civiles (2021). Tecnologías de Vigilancia en Argentina.

(97) Existen muchas vetas interesantes de investigación, por ejemplo: (I) Comparación entre los sistemas de identidad digital desarrollados en países unitarios y federales y cómo estas diferencias impactan en los derechos humanos que podrían verse afectados; (II) Narrativas en torno a la necesidad de implementar sistemas de identidad digital, desde el gobierno y cómo estas han sido recibidas y contestadas (cuando haya ocurrido) por el sector privado o la sociedad civil; (III) Financiamiento de los sistemas de identidad digital, con el fin de identificar qué organismos internacionales vienen operando en la región y con qué motivo buscan promover estos sistemas.(IV) Proveedores para la región de tecnologías con capacidades de vigilancia, que también comercializan tecnologías que sirvan a los sistemas de identidad digital, con el fin de analizar si sus prácticas en ambos casos cumplen con las obligaciones de las empresas en materia de derechos humanos.

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

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 Global Justice (2022). Paving a Digital
Centre for Internet and Society India (2020). Governing ID: Principles for Evaluation.
CETYS (2021). Videovigilancia con reconocimiento facial, inteligencia artificial y derechos humanos: ni apocalipsis ni utopía.
Data Privacy Brasil (2022). Between visibility and exclusion: mapping the risks associated with the National Civil Identification system and the usage of its database by the gov.br platform.
Data Privacy 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.
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 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.
IPANDETEC (2021). Caretas Digitales: Digital Identity in Central America.
ITS Rio (2020). Good ID in Latin America: Strengthening appropriate uses of Digital Identity in the region.
KICTANet (2022). Policy brief Data Protection and Digital Identity in Kenya.
McKinsey Global Institute (2019). Digital identification: A key to inclusive growth.
OCDE (2023). Draft Recommendation on the Governance of Digital Identity.
Paradigm Initiative (2021). COVID-19 and Digital Rights: A Compendium on Health Surveillance Stories in Africa.
Paradigm Initiative (2021). Deploying Digital Identity Systems: Human Rights Implications and Lived experiences in Kenya.
Paradigm Initiative (2022). Internet freedoms in Chad and DRC: Better understanding the notion of digital identity.
Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID.
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 (2019). ¿Qué buscar en los sistemas de Identidad Digital? Una tipología de etapas.
The Engine Room (2020). Comprendiendo los Efectos de la Identificación Digital en la Vida Cotidiana: Un estudio multinacional.
The Engine Room (2022). A Digital ID Handbook: Strategies for Navigating Electronic Identification Systems.
Venturini, Jamila; Díaz, Marianne (2021). Sistemas de identificación y protección social en Venezuela y Bolivia: vigilancia, género y derechos humanos

World Bank (2016). Digital identity: towards shared principles for public and private sector cooperation.
World Bank (2017). Principles on Identification for Sustainable Development: Toward the Digital Age.
World Bank (2018). ID Enabling Environment Assessment (IDEEA): Guidance Note.
World Bank (2019). Digital ID and the Data Protection Challenge : Practitioner's Note.
World Bank (2019). ID Enrollment Strategies: Practical Lessons from Around the Globe.
World Bank (2019). ID4D Practitioner's Guide.
World Bank (2022). Engaging Civil Society Organizations (CSOS) for Successful ID Systems: Guidance Note.
World Bank (2022). ID4D Global Dataset.

Este informe ha sido posible, en parte, gracias al generoso apoyo del pueblo estadounidense a través de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID). Este informe también ha contado con el apoyo de otros financiadores. El contenido es responsabilidad de Derechos Digitales y no refleja necesariamente las opiniones de USAID, el Gobierno de los Estados Unidos u otros financiadores.