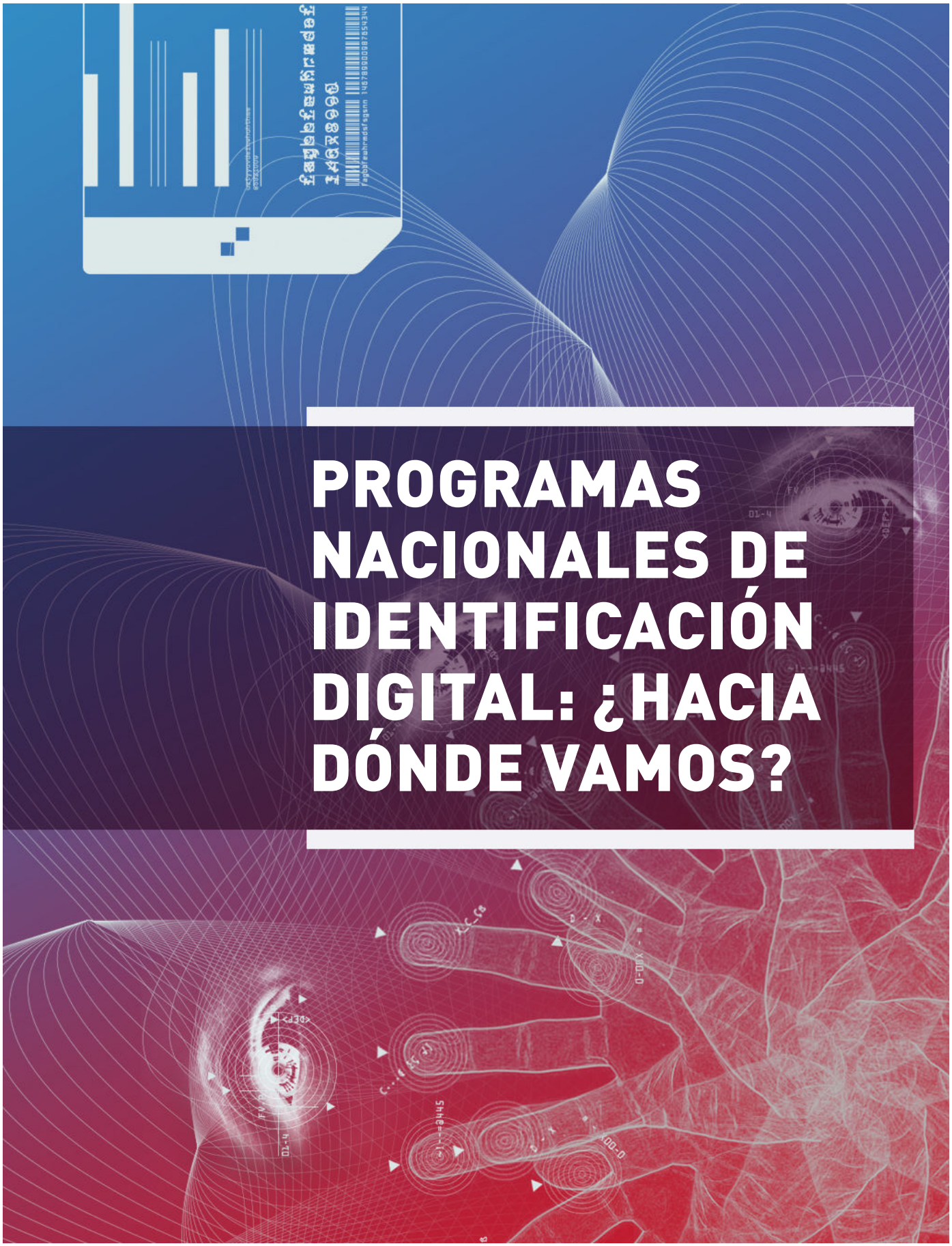

PROGRAMAS NACIONALES DE IDENTIFICACIÓN DIGITAL: ¿HACIA DÓNDE VAMOS?

accessnow

Access Now defiende y extiende los derechos digitales de los usuarios en riesgo alrededor del mundo. Mediante la combinación de apoyo técnico directo, campañas globales, el análisis integral de políticas públicas, el financiamiento a grupos locales emergentes, intervenciones jurídicas y eventos como RightsCon, luchamos por los derechos humanos en la era digital.

Programas nacionales de identificación digital: ¿Hacia dónde vamos?

ARTÍCULO DE POLÍTICAS PÚBLICAS DE ACCESS NOW |

Publicado en inglés en mayo 2018. Traducción de marzo de 2021.

ÍNDICE

I. RESUMEN EJECUTIVO **2**

II. PREOCUPACIONES EN CUANTO AL DEBATE SOBRE LOS PROGRAMAS NACIONALES DE IDENTIFICACIÓN DIGITAL **5**

Casos prácticos 7

Estonia 8

Túnez 10

India 13

III. DEFINICIONES: TÉRMINOS PARA EL DEBATE SOBRE LOS PROGRAMAS NACIONALES DE IDENTIFICACIÓN DIGITAL **18**

IV. RECOMENDACIONES PARA LA ADOPCIÓN DE POLÍTICAS PÚBLICAS **20**

Gobernanza 21

Protección de la privacidad y los datos personales 24

Ciberseguridad 27

V. USO DE DATOS BIOMÉTRICOS EN LOS SISTEMAS DE IDENTIFICACIÓN: CONSIDERACIONES ESPECIALES **31**

VI. CONCLUSIÓN **33**

I. RESUMEN EJECUTIVO

La identificación digital cobra cada vez más importancia en las discusiones sobre políticas públicas de una gran cantidad de países, y cada día son más los gobiernos que proponen o implementan programas nacionales de esta naturaleza, así como las instituciones multilaterales que realizan inversiones en estos proyectos. Los gobiernos administran o coordinan este tipo de programas con el objetivo de proporcionar una identificación digital única a los residentes (o solo a los ciudadanos, en algunos casos) de su país. A su vez, muchos de estos proyectos tienen el objetivo de recopilar, almacenar y utilizar los datos biométricos de los individuos como el medio principal para establecer y autenticar su identidad.

Quienes defienden los programas centralizados de identificación nacional, en particular, aquellos que promueven la vinculación biométrica, argumentan que las estrategias de este tipo suponen ciertos beneficios, ya que permiten ejecutar servicios gubernamentales, programas contra la pobreza y esquemas de bienestar social de forma más precisa y eficiente. A su vez, sostienen que ayudan a reducir la corrupción y aumentar la inclusión y que colaboran con los intereses de seguridad nacional. La respuesta de quienes lo critican destaca que los esquemas nacionales de identificación digital no necesariamente garantizan una distribución más efectiva de los beneficios, una mejor prestación de servicios ni avances en la gobernanza y que, por el contrario, suponen riesgos críticos, por ejemplo, para el modo en que se diseñan y controlan los programas, la exclusión social, la protección de la privacidad y los datos personales y la ciberseguridad.

Dado que Access Now es una organización comprometida a defender y extender los derechos digitales de los usuarios en riesgo, cualquier iniciativa diseñada para implementar legalmente un programa nacional y centralizado de identificación digital genera gran preocupación. Estos programas suponen grandes riesgos para los derechos humanos, ya que, específicamente, pueden debilitar el **derecho a la privacidad** y las **libertades de movimiento y de expresión**, entre otros derechos protegidos. Además, dado que, normalmente, implican la creación de valiosas bases de datos personales sensibles susceptibles de filtraciones por parte de agentes maliciosos o abusos de las autoridades públicas, también suponen riesgos para la ciberseguridad y la protección de la información. Los programas centralizados de este tipo tienen el potencial de convertir la identidad digital en un medio invasivo de identificación, seguimiento o control, en especial, si dichas identidades contienen información biométrica y son obligatorias.

Este es el contexto que despierta nuestro escepticismo en cuanto a la implementación universal de los programas nacionales de identificación digital a pesar de los beneficios que destacan sus defensores. Desde nuestra perspectiva, no es conveniente que los formuladores de políticas públicas promuevan la idea de que la identidad y las libertades civiles son necesidades que se deben equilibrar entre sí; la identidad se debe garantizar junto con la protección de nuestros derechos humanos, no a cambio de estos. Si no contamos con salvaguardas adecuadas y estrictas para proteger los derechos humanos, los programas nacionales de identificación pueden ser contraproducentes para el bienestar de las personas, violar derechos humanos protegidos a nivel internacional y debilitar nuestra seguridad informática. Por eso, es indispensable que se adopten salvaguardas (legales, tecnológicas y de esquemas de gobernanza) de manera integral y que la implementación de una no afecte la adopción de las demás. **Si no se incluyen las salvaguardas necesarias de forma integral en los programas nacionales de identificación, recomendamos que estos esquemas se suspendan y se reestructuren, o que se reconsidere si es necesario.**

En este artículo preliminar, se examinan los programas nacionales de identificación digital desde una perspectiva basada en los derechos humanos. Para ello, se analiza el contexto global de estas iniciativas y se recomiendan salvaguardas y políticas públicas a las partes involucradas: funcionarios públicos, legisladores, representantes de instituciones judiciales y de derechos humanos, especialistas en tecnología, representantes de instituciones de desarrollo y miembros del sector privado. Se incluyen los casos de estudio de Estonia, Túnez y la India, así como una sección que define los términos del debate. Por último, en una sección separada, brindamos algunas recomendaciones y consideraciones especiales relacionadas con los sistemas de identificación biométrica, ya sea en el marco de programas gubernamentales o en el sector privado.

A continuación, presentamos un resumen de nuestras recomendaciones y salvaguardas para proteger los derechos digitales; los análisis detallados correspondientes se encuentran en la sección IV. Se dividen en tres pilares:

1. GOBERNANZA

1) Realizar consultas transparentes, inclusivas y abiertas al comienzo de cualquier propuesta de programa de identificación digital
2) Garantizar un alcance definido y estricto para la implementación del programa de identificación digital conforme a la ley vigente
3) Permitir que la inscripción y el uso de la identificación digital sean voluntarios
4) Crear mecanismos independientes y eficientes para presentar reclamos y recibir reparaciones

5) Garantizar la inclusión en las etapas de inscripción e implementación, independientemente de las diferencias de recursos tecnológicos o capacidad estructural

2. PROTECCIÓN DE LA PRIVACIDAD Y LOS DATOS PERSONALES

1) Limitar el propósito para el que se recopilan y se utilizan los datos
2) Implementar medidas adecuadas para evitar el perfilamiento de los usuarios en función de los datos proporcionados voluntariamente
3) Garantizar a los individuos los derechos relacionados con sus datos, como la exactitud, la rectificación y la eliminación
4) Establecer marcos sólidos de protección de datos personales para regular los programas de identificación digital
5) Minimizar la cantidad y los tipos de datos que los gobiernos y proveedores de servicios asociados pueden recopilar
6) Restringir la interceptación y el monitoreo lícitos del uso de la identificación digital y establecer medidas de rendición de cuentas

3. CIBERSEGURIDAD

1) Implementar una infraestructura tecnológica eficiente y segura
2) Garantizar que la recopilación y el almacenamiento de los datos no sean centralizados
3) Separar las funciones de identificación y autenticación y evitar crear registros de transacciones centralizados para la autenticación
4) Establecer principios de "privacidad por diseño" en el programa
5) Garantizar que los programas nacionales de identificación se basen en modelos de comunicación segura, por ejemplo, mediante la encriptación de extremo a extremo del tráfico en la mayor medida posible
6) Brindar transparencia mediante la divulgación de las políticas de ciberseguridad
7) Proporcionar un marco legal y de políticas públicas que fomente la comunicación y la divulgación de las vulnerabilidades
8) Tomar medidas para informar las filtraciones de datos a las partes afectadas

NOTA PARA LOS LECTORES

Sus consultas y aportes acerca de este artículo son bienvenidos. En particular, los invitamos a enviar sus análisis y sugerencias en cuanto a la terminología que utilizamos y nuestras recomendaciones de políticas públicas para los programas nacionales de identificación digital y el uso de datos biométricos en los sectores público y privado.

La versión actual de este artículo incorpora los aportes que recibimos sobre la versión preliminar, que presentamos en marzo de 2018. Agradecemos a la gran cantidad de colaboradores externos y colegas de Access Now que compartieron sus comentarios. Pueden enviar sus consultas o comentarios sobre este artículo a los siguientes miembros del equipo de políticas públicas de Access Now:

Naman M. Aggarwal (naman@accessnow.org)
Verónica Arroyo (veronica@accessnow.org)
Raman Jit Singh Chima (raman@accessnow.org)
identity@accessnow.org

II. PUNTOS PROBLEMÁTICOS DEL DEBATE SOBRE LA IDENTIFICACIÓN DIGITAL NACIONAL

El objetivo principal de este artículo es analizar los programas nacionales de identificación digital, es decir, los esquemas de políticas públicas que los gobiernos coordinan o administran directamente y que tienen el propósito de proporcionar una "identidad digital"[1] a los residentes o ciudadanos de un estado en particular. Estas identidades digitales suelen estar compuestas por datos personales extremadamente sensibles que permiten autenticar o verificar la identidad de una persona. En muchos de los programas actuales o propuestos de este tipo, los gobiernos almacenan este tipo de información en bases de datos centralizadas.[2] Y eso es un error.

Los requisitos de identificación obligatorios perjudican el anonimato y ponen a los usuarios en peligro. Tal como observa David Kaye, Relator Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y expresión, en mayo de 2015, "… la encriptación y el anonimato permiten a los individuos hacer uso de sus derechos a las libertades de opinión y expresión en la era digital y, por ende, se deben proteger estrictamente". En su informe, concluye lo siguiente:

"… Los estados deben abstenerse de obligar a los usuarios a identificarse para acceder a los medios de comunicación digital y servicios en línea, así como de requerir el registro de las tarjetas SIM a los usuarios de dispositivos móviles".[3]

Las bases de datos personales centralizadas son susceptibles de filtraciones por parte de agentes maliciosos y abusos de las autoridades públicas por medio del acceso a datos personales y sistemas de vigilancia o hackeo liderados o patrocinadas por los gobiernos. Kaye destaca que vincular una identidad digital o biométrica a una tarjeta SIM, lo cual se contempla en algunos países, no solo pone en riesgo la seguridad digital, sino que además, puede limitar el derecho de accesibilidad de las personas a través de su capacidad de conectarse a Internet y utilizar la conectividad para obtener información y expresarse libremente. No obstante, a lo largo de los últimos años, varios gobiernos nacionales, así como instituciones multilaterales, han demostrado gran interés en los programas nacionales de identificación digital.

---

[1] Para comprender más a fondo el término "identidad digital", consulte la sección III de este artículo.
[2] En este artículo, se incluyen estudios de caso de gobiernos que administran información personal de forma centralizada. Otros han destacado el hecho de que los sistemas nacionales de identificación pueden evolucionar de diversas maneras. Por ejemplo, Jim Harper, de Cato Institute, indica que un sistema de identificación nacional cuenta con tres elementos: (1) se utiliza para identificar a los individuos, (2) sus elementos clave se aplican de manera uniforme en todo el país, (3) la participación es obligatoria a nivel práctico o legal. *Ver* Jim Harper, Policy Analysis: The New National ID Systems, Cato Institute, 30 de enero de 2018, n.° 831, https://www.cato.org/publications/policy-analysis/new-national-id-systems.
[3] Informe del Relator Especial sobre la promoción y protección de los derechos a las libertades de opinión y expresión, David Kaye, A/HRC/29/32, 22 de mayo de 2015, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

En febrero de 2017, el Grupo del Banco Mundial coordinó la creación y el lanzamiento de los "Principios sobre la Identificación para el Desarrollo Sostenible: hacia la era digital"[4] a través de su programa Identificación para el Desarrollo, comúnmente conocido como "ID4D". Estos diez principios tienen el objetivo de brindar orientación a los gobiernos respecto de la creación y la implementación de los sistemas de identificación. Tanto los principios como el informe anual de ID4D se plantean en el contexto del cumplimiento de los Objetivos de Desarrollo Sostenible de las Naciones Unidas, específicamente la meta 16.9, que establece que "En 2030, se debe proporcionar acceso a una identidad jurídica para todos, en particular, mediante el registro de nacimientos". En el informe, y en las conversaciones subsiguientes relacionadas, los defensores de los programas de identificación digital suelen mezclar el concepto tradicional de identificación legal con el de identificación digital, en especial, cuando intentan persuadir a los legisladores de los países del Sur Global y las economías emergentes para que ignoren los enfoques tradicionales basados documentos físicos.[5] Normalmente, una identificación legal se entiende como un documento legítimo que certifica la identidad de una persona mediante datos básicos (como su nombre y la fecha y lugar de nacimiento). En cambio, la identificación digital puede estar compuesta por información básica sobre una persona y datos de autenticación, incluidos datos biométricos inalterables, como las huellas dactilares o el patrón de iris. Aun así, los gobiernos eligen omitir los pasos principales y básicos de la creación de programas de identificación legal y, en cambio, establecer programas nacionales de identificación digital, los cuales suelen traer aparejados problemas que ponen en riesgo los derechos de los usuarios y la seguridad de sus datos personales.

Otro razonamiento que proponen los defensores de los programas nacionales de identificación digital se basa en la idea de que su uso es necesario, o esencial, para implementar diversas iniciativas internacionales de desarrollo en pro de la inclusión económica, las tecnologías financieras, el desarrollo sustentable y la seguridad nacional.[6] Con este enfoque, se debilita la necesidad de vincular una identidad digital nacional a los datos biométricos del portador de la tarjeta.

Si bien los argumentos a favor de la identificación legal pueden parecer convincentes (dado que puede ser útil para obtener beneficios sociales y realizar actividades cotidianas que requieran verificación de la identidad), aquellos que imponen una identificación digital nacional obligatoria, incluida la vinculación a los datos biométricos, no lo son. Los individuos no deberían estar obligados a poner sus datos biométricos, inalterables y personales en riesgo de invasión a la privacidad solo para "demostrar" su identidad legal, la cual se puede verificar de muchas otras formas. Evitar este riesgo es incluso más importante si consideramos que los programas

---

[4] Banco Mundial, "Diez principios sobre la Identificación para el Desarrollo Sostenible", http://pubdocs.worldbank.org/en/168561509656716894/web-Spanish-ID4D-IdentificationPrinciples.pdf

[5] *Id.*, Identificación para el Desarrollo (ID4D), "Debido al potencial de transformación de las soluciones modernas (los avances en las tecnologías de identificación, tanto digital como biométrica, y los costos cada vez más bajos de la tecnología y la implementación) surge la oportunidad de omitir los enfoques tradicionales basados en los documentos físicos y crear sistemas de identificación sólidos y eficientes a una escala sin precedentes". http://www.worldbank.org/en/programs/id4d#.

[6] *Id.*

nacionales de identificación digital suelen implementarse primero en las comunidades en que las personas tienen menos motivos para confiar en las autoridades públicas, incluidas las comunidades rurales y las marginadas, como las de refugiados y los grupos minoritarios.

Para que la identidad digital fortalezca a las personas en ciertos contextos, el marco tecnológico, legal y político debe basarse en la voluntad y la elección de los usuarios, así como el consentimiento informado, el reconocimiento de varias formas de identificación, la posibilidad del anonimato y el respeto de la privacidad. Enfocarse en un solo sistema de identificación nacional centralizado y administrado directamente impide la formación y el uso competitivo de diversas formas de identificación, una competencia que podría generar eficiencia y empoderamiento para los usuarios. De hecho, algunos sostienen que las políticas gubernamentales deberían enfocarse en fomentar el desarrollo de una variedad de sistemas de identificación y acreditación y que, en lugar de insistir en su propia identificación nacional, los gobiernos deberían aceptar cualquier tarjeta o dispositivo que brinden suficientes pruebas para verificar la información requerida en una transacción determinada.[7]

Además, es importante recordar que, dado el desarrollo tecnológico, no hay motivos para pensar que la mejor solución para verificar la identidad de un individuo son los sistemas nacionales de identificación digital que requieren autenticación basada en datos biométricos. Por ejemplo, algunos académicos proponen el uso de **tecnologías de *blockchain* (cadena de bloques)** para autenticar la identidad de los usuarios. Con este sistema, dado que los datos almacenados en la cadena pública son extremadamente difíciles de cambiar, los usuarios no necesitan proporcionar información biométrica o datos personales de otros tipos para autenticar su identidad. En cambio, este esquema requiere almacenar datos mínimos del usuario en la cadena de bloques, y la identidad se validaría debido a su pertenencia a dicho registro. No obstante, otros académicos han advertido acerca del potencial del blockchain para incumplir las leyes de privacidad de Europa,[8] en particular, el Reglamento General de Protección de Datos (RGDP), que establece que, en una gran cantidad de circunstancias, los individuos deben tener la posibilidad de solicitar que sus datos personales se rectifiquen o se eliminen. También es posible que, aunque los registros de transacciones de algunos sistemas de blockchain no siempre satisfagan los principios de protección de datos,[9] los sistemas de **identidad soberana** basados en blockchain puedan brindar a las entidades mecanismos eficientes de cumplimiento de las leyes de protección de datos dado que dichos mecanismos dejan el control de los datos y el acceso granular a estos en manos de los

[7] National ID Systems, capítulo 21, Cato Handbook for Policymakers (8.° ed., 2017), https://object.cato.org/sites/cato.org/files/serials/files/cato-handbook-policymakers/2017/2/cato-handbook-for-policymakers-8th-edition-21_0.pdf

[8] Blockchain Technology is on a collision course with EU privacy law, 27 de febrero de 2018, https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/

[9] Es importante recordar que los datos de los usuarios se pueden rectificar fácilmente en un sistema de blockchain, pero las transacciones registradas allí no se pueden eliminar. En muchos sistemas de identificación basados en blockchain, la base de datos personales de los usuarios no se almacena en el blockchain, de modo que su nombre, número de seguridad social, fecha de nacimiento, número de licencia de conducir, etc. se almacenan en una "billetera" o sistema similar en manos del usuario. Solo las transacciones se registran en el blockchain, por ejemplo, el hecho de que el Departamento de Vehículos Motorizados emitió la licencia de conducir del usuario, o que una tienda de bebidas alcohólicas solicitó al usuario verificar su mayoría de edad, etc.

usuarios.[10] Así, una gran cantidad de información personal de los titulares ya no necesitaría ser almacenada por entidades que requieran sistemas de autenticación y autorización para interactuar con los usuarios. Los sistemas de identificación soberana también incluyen el consentimiento del titular en su diseño. Esto significa que brindan a los usuarios mucho más control para actualizar, cambiar, agregar o eliminar sus datos personales según su necesidad, de modo que el control queda en sus manos.

Aún queda pendiente comprender qué tan útil puede ser blockchain para la administración de la identificación digital, pero estas discusiones demuestran que hay más de un camino posible y que algunas soluciones pueden ser significativamente menos riesgosas y más efectivas que las que se contemplan hoy.

CASOS PRÁCTICOS

Es fundamental que las partes interesadas no solo consideren los problemas y las preocupaciones generales que surgen de los enfoques centralizados y basados en la vinculación biométrica en cuanto a la identificación digital nacional, sino que también aprendan de los intentos de desarrollo e implementación de programas de este tipo en otras jurisdicciones.

A lo largo de los años, diversos países han considerado, analizado, probado y excluido distintos programas nacionales de identificación digital centralizados. Australia fue probablemente uno de los primeros países en proponer un sistema de este tipo con la iniciativa Australia Card. Esta propuesta no llegó a implementarse y se descartó. Reino Unido también consideró aplicar un esquema de identificación nacional, pero luego lo canceló.[11] Algunos países como Bélgica han utilizado programas de identificación nacional con datos no biométricos, y otros, como Portugal, han implementado sistemas de tarjetas de ciudadanía basados en datos biométricos en los que dichos datos se almacenan en la tarjeta de cada individuo.[12] En Asia, según los informes de la Asociación de Taiwán para los Derechos Humanos, Taiwán ha analizado la posibilidad de utilizar una identificación electrónica (eID) desde 1999. Ahora, en medio de preocupaciones de la sociedad civil en cuanto a la privacidad y la vigilancia, este país está considerando implementar un sistema de e-ID. Esta identificación combinaría varias identificaciones de Taiwán basadas en documentos físicos, como el seguro de salud y la licencia de conducir, en un e-ID único.

---

[10] "La identidad soberana establece la idea de que las personas y las empresas pueden almacenar sus propios datos de identificación en sus propios dispositivos y proporcionarlos de forma eficiente a quienes necesitan validarlos, pero sin necesidad de confiar en un repositorio central de datos de identidad. Es un método digital para hacer lo que hacemos hoy con trozos de papel"; https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/

[11] Success Story: Dismantling UK's Biometric ID Database, Electronic Frontier Foundation, https://www.eff.org/pages/success-story-dismantling-uk%E2%80%99s-biometric-id-database

[12] Identification for Development (ID4D) Integration Approach, página 104, http://pubdocs.worldbank.org/en/205641443451046211/ID4D-IntegrationAproachStudyComplete.pdf

Tanto a un nivel práctico como conceptual, muchos programas nacionales de identificación digital generan cada vez más preocupaciones en cuanto a la privacidad, la protección de datos, la gobernanza y la ciberseguridad. También generan reservas en cuanto al diseño del esquema y la inclusión (o la exclusión) de personas de los servicios del gobierno. Presentamos tres casos de estudio que consideramos particularmente relevantes en este debate global: Estonia, Túnez y la India.

Estonia

Estonia se considera un país pionero en la gobernanza digital. Tras adquirir su independencia en 1991, este país, como un verdadero *millennial*, ha aprovechado la tecnología en todos los aspectos de la gobernanza. Este es el concepto detrás del término "e-Estonia". Estonia fue la primera nación en llevar a cabo sus elecciones a través de Internet y proporcionar una residencia electrónica. La tarjeta de identificación de Estonia marca otro avance hacia la implementación de un gobierno electrónico.

Esta tarjeta de ID es un documento de identificación obligatorio para los ciudadanos de Estonia. Cumple las funciones de brindar un medio de identificación y establecer la identidad de las personas específicamente en el entorno electrónico, incluso como firma digital.

Conforme al programa de identificación digital de Estonia, el sistema se puede usar de tres maneras:

ID-Card

Esta tarjeta contiene los componentes generales de una identificación legal con foto. Sin embargo, incluye también un chip que almacena archivos y utiliza una encriptación de clave pública de 2048 bits que funciona como prueba definitiva de identificación en el entorno electrónico.[13]

Mobile-ID

El Mobile-ID permite a las personas utilizar sus teléfonos móviles como un medio seguro de identificación digital. Al igual que la ID-card, esta identificación también se puede utilizar para acceder a servicios electrónicos de forma segura y firmar documentos por medios digitales, pero sin la necesidad de un lector de tarjeta. El sistema se basa en una tarjeta SIM de ID móvil que el cliente debe solicitar a su operador de telefonía móvil.[14]

[13] Ver descripción de ID-card de E-Estonia: https://e-estonia.com/solutions/e-identity/id-card.
[14] Ver descripción de Mobile ID de E-Estonia: https://e-estonia.com/solutions/e-identity/mobile-id.

Smart-ID

Smart ID es una solución de identificación mediante una aplicación para dispositivos móviles que, por lo tanto, no requiere una tarjeta SIM en el dispositivo móvil inteligente.[15]

Con la ID-card, cada ciudadano también recibe una dirección de correo electrónico con el dominio @eesti.ee. El gobierno utiliza esta dirección para enviar información importante. A fin de utilizar la dirección de correo electrónico de @eesti.ee, los ciudadanos deben enviarla a sus direcciones de correo electrónico personales.

La ID-card contiene un chip que se utiliza para almacenar datos digitalizados sobre el usuario, como su nombre completo, género y número de identificación nacional. Además, el sistema de identificación utiliza un sistema público de criptografía de claves como mecanismo de autenticación. Las tarjetas de ID-card utilizan un sistema de encriptación de clave pública/privada de código abierto de 2048 bits y contienen dos certificados digitales separados, uno para confirmar la identidad del portador y el otro para permitir que los individuos usen su firma digital.

Las ID-card se usan de forma generalizada en la atención médica, las compras y las bancas electrónicas, la firma de contratos y correos electrónicos encriptados, los boletos de transporte público y mucho más, incluso para votar. En total, el estado de Estonia ofrece 600 servicios electrónicos a sus ciudadanos y 2,400 a las empresas.[16]

En octubre de 2017, las noticias anunciaron que había una falla de seguridad en las claves criptográficas de aproximadamente 750.000 tarjetas de ID nacionales de Estonia. Esta falla podría haber causado que las claves privadas de los usuarios se dedujeran a partir de las claves públicas. La vulnerabilidad, denominada ROCA, se descubrió en una de las bibliotecas de códigos, "Infineon", en el sistema de tarjetas inteligentes. Es importante destacar que, para que un sistema de criptografía de clave funcione, la clave pública se comparte con los demás, pero la clave privada debe permanecer en confidencialidad. Esta falla provocó vulnerabilidades de robo de identidad en las tarjetas de ID-card.

[15] Ver descripción de Smart ID de E-Estonia: https://e-estonia.com/solutions/e-identity/smart-id.
[16] "*Estonia takes the plunge",* The Economist, 28 de junio de 2014, https://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge.

El primer ministro de Estonia, tras reconocer el "riesgo inminente" de ataque, anunció que los certificados de las ID-card afectadas dejarían de ser efectivos el 4 de noviembre de 2017. También se implementaron actualizaciones para los certificados.[17]

Si bien la experiencia de Estonia con un programa de identificación digital es un ejemplo de una de las implementaciones más sofisticadas, demuestra la escala del impacto que pueden tener las vulnerabilidades, incluso cuando la población tiene amplios conocimientos en tecnología. A su vez, es importante destacar que, a pesar de que Estonia tiene una población pequeña y presume su infraestructura de alto nivel de desarrollo, fue necesario tomar medidas significativas para mitigar el riesgo. En los países en vías de desarrollo, con infraestructuras y poblaciones vulnerables, el impacto podría haber sido mucho más grave.

Además, si bien, en este caso particular, los riesgos se consideraron "teóricos", y las autoridades pudieron evitar que se produjeran daños irreparables, si las vulnerabilidades hubiesen escalado, el impacto podría haber sido mucho peor, y el esfuerzo para restablecer la normalidad, más drástico. La respuesta de Estonia frente a esta situación fue rápida. La mayoría de los países en vías de desarrollo no podrían haber respondido con tal fuerza y rapidez debido a múltiples factores, incluidas las carencias de capacidad y la falta de conciencia por parte del público y las agencias de implementación.

El ejemplo de Estonia, que casi resulta en una catástrofe, también es un argumento en contra de los ID digitales basados en datos biométricos. Estonia utiliza la criptografía de claves públicas como atributo de autenticación, lo cual puede representar una alternativa más segura y respetuosa de los derechos en comparación con los datos biométricos.

Túnez

Con el objetivo de crear un proyecto para mejorar la calidad de las operaciones y los servicios administrativos,[18] Túnez diseñó la primera ley[19] para introducir cambios a la tarjeta de identidad nacional actual en julio de 2016. Si bien la tarjeta de ID vigente contiene un número único de identificación y un código de barra, la legislación propuso enmendar la Ley N.° 27 de 1993 acerca de la tarjeta de

[17] Ver actualización aquí: https://www.id.ee/?lang=en&id=38239
[18] "En Tunisie, le projet de modernisation de la carte d'identité nationale inquiète les ONG", Jeune Afrique, 1 de diciembre de 2017, http://www.jeuneafrique.com/495963/societe/en-tunisie-le-projet-de-modernisation-de-la-carte-didentite-nationale-inquiete-les-ong/.
[19] "Basic Draft Law amending and completing Law No. 1993-27 of 22 March 1993 on the National Identity Card", https://www.accessnow.org/cms/assets/uploads/2017/08/Tunisia_CIN_Draft_ENG.pdf [traducción al inglés], http://www.anc.tn/site/servlet/Fichier?code_obj=94673&code_exp=1&langue=1 [original en árabe].

identificación nacional[20] para agregar a la tarjeta un chip electrónico con datos personales sensibles.

Inicialmente, el proyecto atrajo atención positiva por parte de los medios debido al foco posrevolucionario del país en cuanto a la lucha contra la corrupción y el avance de las reformas administrativas. Sin embargo, cuando el borrador se publicó, los principales activistas de redes sociales (tanto de Túnez[21] como del resto del mundo)[22] y los líderes de las autoridades nacionales de protección de datos comenzaron a visibilizar las implicancias de este proyecto de ley para la privacidad, que se analizan a continuación.

El Ministerio del Interior presentó ante el Consejo Ministerial un proyecto de ley para enmendar la legislación actual sobre las tarjetas de identidad nacionales. El Consejo aprobó el borrador y lo envió a la Asamblea de Representantes de la Gente (ARP, Assembly of Representatives of the People) el 27 de junio de 2016. Luego, este proyecto se asignó a la Comisión Legislativa de Derechos y Libertades para su revisión y aplicación de enmiendas.

El borrador inicial incluía disposiciones que representaban un gran riesgo para la privacidad, la ciberseguridad y protección de los datos personales de los tunecinos. Utilizaba un lenguaje vago y ambiguo y no incluía salvaguardas esenciales para la privacidad. Por ejemplo, el Artículo 2 bis del proyecto inicial establecía lo siguiente: "[La parte encriptada del chip incluirá] los datos administrativos relacionados con la digitalización y el registro de la tarjeta". En ninguna parte del proyecto se definían los términos "digitalización", "registro" ni, el más importante, "datos administrativos". Este hecho dejaba la puerta abierta para que se incluyera todo tipo de información personal en el chip.

El proyecto de ley inicial también generaba serias preocupaciones en cuanto a la seguridad de los datos personales, ya que almacenaba datos personales sensibles de los ciudadanos de Túnez, como datos biométricos (p. ej., huella dactilar), la dirección y la fecha de nacimiento, en una base de datos única, lo que creaba un punto único de fallo (*single point of failure*) en caso de robo o hackeo de datos. A su vez, no indicaba qué tipo de datos se almacenarían, quién tendría acceso a ellos o qué medidas se tomarían para garantizar su seguridad. Y lo que es peor, el proyecto de ley no otorgaba a los tunecinos acceso a los datos sobre sí mismos que se almacenarían en la tarjeta (y establecía una sentencia de cinco años de prisión para

[20] "Loi n° 93-27 du 22 mars 1993 relative à la carte d'identité nationale": http://www.legislation.tn/sites/default/files/journal-officiel/1993/1993F/Jo02493.pdf.
[21] Access Now, "Tunisia: Statement on Proposed ID Card", https://www.accessnow.org/tunisia-statement-proposed-national-id-card/.
[22] "Experts Cast Doubt on Tunisia's Biometric Identitifcation Bill", Global Voices, 30 de noviembre de 2016, https://advox.globalvoices.org/2016/11/30/experts-cast-doubt-on-tunisias-biometric-identification-bill/.

quien intentara acceder a dichos datos). No obstante, sí concedía acceso pleno a los perfiles de datos exhaustivos de millones de ciudadanos a la policía, las agencias de seguridad nacionales y los agentes administrativos.

Casi un año después, el 7 de julio de 2017, la Comisión de Derechos y Libertades completó su revisión. El proyecto de ley iba a debatirse en la sesión plenaria el 18 o 19 de julio de 2017.[23] Sin embargo, debido a otros compromisos legislativos, el debate se pospuso y el proyecto se envió nuevamente a la Comisión de Derechos y Libertades. Permaneció allí hasta conseguir un nuevo lugar en la agenda del plenario el 9 de enero de 2018.

El 4 de enero de 2018, Chawki Gaddes, director de la autoridad nacional de protección de datos (INPDP), dio un discurso frente a la Comisión de Derechos y Libertades a fin de debatir los riesgos que suponía el proyecto de ley para la privacidad de los datos personales y aclaró que el problema no radicaba en el carácter biométrico de los datos en sí, sino en la alarmante ausencia de protecciones y garantías para la privacidad y los datos personales de los ciudadanos.

Un día después, el Ministro del Interior, Lotfi Brahem, habló frente a la misma comisión para debatir la aprobación de dicho proyecto. Afirmó que "nadie podría hackear los datos personales de ningún individuo y que el Ministerio del Interior cuenta con medidas de protección estrictas" y agregó que los tunecinos debían "confiar en ello".[24] El testimonio del ministro no logró convencer a los legisladores, quienes aplicaron varias enmiendas para garantizar la seguridad de los datos personales de todos los tunecinos un día antes de que se programara el análisis del proyecto en el plenario. Dichas enmiendas abolieron la creación de una base de datos nacional. A lo largo del debate, muchos insistieron en el hecho de que, si bien incluir las huellas dactilares en la tarjeta podría ser útil para fines de verificación, almacenar esta información en una base de datos nacional puede implicar riesgos para la seguridad digital.

El 9 de enero de 2018, el día en que el proyecto estaba programado para discutirse en el plenario, el Ministerio del Interior lo retiró de la agenda de la Asamblea de Representantes de la Gente (ARP). Si bien esto significa que el proyecto fue rechazado en el contexto legislativo por ahora, muchos temen que el gobierno vuelva a intentar aprobarlo, ya sea a través de un decreto ejecutivo para cambiar

[23] La finalización de la revisión y publicación de los detalles y el informe de la reunión de la Comisión de Derechos y Libertades se completaron el 18 de julio de 2017. Ver el informe (árabe) aquí: http://www.arp.tn/site/servlet/Fichier?code_obj=99034&code_exp=1&langue=1.
[24] "Lotfi Brahem : Le système de ministère de l'Intérieur ne peut être piraté, Kapitalis", 6 de enero de 2018, http://kapitalis.com/tunisie/2018/01/06/lotfi-brahem-le-systeme-du-ministere-de-linterieur-ne-peut-etre-pirate/.

ciertas "especificaciones técnicas" o mediante otro proyecto de ley que se presente ante la ARP con una composición política diferente después de las próximas elecciones legislativas.

Es importante destacar que el proyecto de ley que enmendaba la ley de tarjeta de identidad en Túnez se retiró una vez que se adoptaron enmiendas para proteger los derechos fundamentales de los ciudadanos a la privacidad. Estas medidas eliminaban completamente la necesidad de mantener la base de datos; por ejemplo, tras las revisiones del proyecto de ley, las autoridades solo podrían tomar huellas dactilares con el fin de incluir esta información en el chip, pero luego debían destruirla. Básicamente, esto garantizaba que las huellas dactilares funcionen únicamente como herramienta de autenticación. Si bien las organizaciones de derechos humanos celebraron la victoria, son conscientes de la intención del Ministerio de avanzar en este proceso y permanecen atentas al cumplimiento de Túnez de los derechos humanos en cualquier programa de identificación que se proponga.

India

El programa nacional de India para el desarrollo de una identificación única (UID), conocido como "Aadhaar" (un término en hindi que se traduce vagamente como "base"), se estableció en 2008. Consiste en asignar un número único de 12 dígitos a todos los residentes de la India, el cual se encuentra vinculado a los datos biométricos y demográficos de cada persona. Con más de mil millones de suscripciones declaradas en la India, se considera el sistema nacional de identificación con vinculación biométrica más grande el mundo.

Este no fue el primer proyecto nacional de identificación que emprendió el Gobierno de la India. El primer programa a gran escala fue una iniciativa explícitamente basada en la seguridad nacional y diseñada para emitir tarjetas de identificación que se lanzó poco tiempo después de la conclusión del conflicto de Kargil; tenía el objetivo de que todos los residentes de la India se inscribieran en el Registro Nacional Popular, el cual distinguiría entre los ciudadanos y los no ciudadanos. En 2008, la nueva administración comenzó a desarrollar una iniciativa de identificación única que tenía el propósito de crear una base de datos maestra para hacer un seguimiento de los programas de bienestar social a fin de eliminar los "beneficios fantasmas" duplicados.[25]

Cuando se implementó, las autoridades establecieron que la identificación única de Aadhaar sería voluntaria y que ayudaría al gobierno indio a lograr dos objetivos

[25] "Aadhaar shows India's governance is susceptible to poorly tested ideas pushed by powerful people", Scroll.in, 27 de diciembre de 2016, https://scroll.in/article/825103/aadhaar-shows-indias-governance-is-susceptible-to-poorly-tested-ideas-pushed-by-powerful-people

paralelos: (1) cerrar las brechas de los sistemas de beneficios sociales mediante una mejor orientación y (2) aumentar la eficiencia del sistema de beneficios sociales mediante implementaciones tecnológicas.

La administración del programa de identificación Aadhaar se encuentra a cargo de un ente gubernamental (y ahora reglamentario) llamado Autoridad de Identificación Única de la India (UIDAI, Unique Identity Authority of India). La inscripción de los residentes en el esquema (incluida la recopilación de los datos biométricos) se ha realizado a través de agencias seleccionadas por la UIDAI, que incluyen una amplia variedad de proveedores privados y agencias del sector público. La idea principal de Aadhaar es llevar a cabo la autenticación adecuada de la identidad mediante solicitudes que envíen las agencias a la base de datos central de Aadhaar: el Repositorio Central de Datos de Identidad (CIDR, Central Identities Data Repository). Para solicitar la autenticación, las agencias deben enviar la información de Aadhaar junto con los datos biométricos o demográficos del autenticado. El CIDR tiene toda la información de los individuos registrados bajo el programa Aadhaar. Procesa cada solicitud y proporciona una respuesta positiva o negativa junto con otros datos a la agencia solicitante. En el caso de la autenticación "conozca a su cliente" o KYC (*know your customer*, en inglés) del programa Aadhaar, el CIDR responde con "datos de e-KYC" (verificación electrónica de KYC), que incluyen la información demográfica y la fotografía del autenticado. Esta autenticación solo puede realizarse mediante datos biométricos o a través de una contraseña única que se genera y se envía al número de teléfono móvil registrado de la persona autenticada .

A lo largo de los años de operación, el sistema Aadhaar se ha vinculado de forma cada vez más explícita a las iniciativas de participación cívica basadas en medios tecnológicos y a la prestación de servicios digitales del Gobierno de la India. El programa Aadhaar se considera un pilar fundamental del programa gubernamental “Digital India” diseñado para respaldar los servicios que se prestan de forma electrónica a los ciudadanos. Como resultado, Aadhaar se ha vinculado a una amplia variedad de servicios, desde servicios de Internet y bancas electrónicas hasta viajes internacionales y el registro de matrimonios. El uso de Aadhaar por parte de las firmas privadas de tecnología para la prestación de servicios digitales al consumidor final también ha crecido, y hay informes que indican que Facebook ha probado nuevas maneras de acceder a su plataforma que podrían requerir el uso de Aadhaar.[26] Todos estos servicios están diseñados para funcionar con un sistema de autenticación como se indica anteriormente.

[26] "Want to open a Facebook account? Keep your Aadhaar card by your side", Economic Times, 27 de diciembre de 2017, https://economictimes.indiatimes.com/tech/internet/want-to-open-a-facebook-account-keep-your-aadhaar-card-by-your-side/articleshow/62267904.cms.

El uso de Aadhaar ha causado controversias y desafíos importantes en la India. Para empezar, el sistema ha enfrentado una serie de problemas que se pueden dividir en las siguientes categorías: (1) problemas de implementación, (2) problemas de privacidad, (3) problemas de seguridad y (4) problemas de vigilancia.

Problemas de implementación

De acuerdo con sus defensores, Aadhaar se diseñó principalmente para mejorar la prestación de servicios sociales en la India. Sin embargo, la variedad de problemas tecnológicos y de infraestructura que ha enfrentado, como problemas de conectividad, errores de hardware y duplicación, han obstaculizado la aplicación efectiva de Aadhaar con este fin.

Los casos de trabajadores y personas mayores con problemas para acceder al sistema porque sus huellas digitales no funcionan en los mecanismos de autenticación son importantes para ilustrar la brecha entre el concepto de Aadhaar y su realidad. Economistas importantes, como John Dreze y Reetika Khera, han escrito numerosos artículos acerca de la exclusión de ciudadanos de la asignación de beneficios sociales debido a la implementación de Aadhaar.[27] A su vez, académicos y grupos de interés público han indicado que el requisito de registro y autenticación en Aadhaar para una cantidad cada vez mayor de esquemas de bienestar social y derechos gubernamentales ha provocado un daño y un nivel de exclusión considerables para la población más pobre de India. Esto es especialmente cierto si consideramos la exclusión que provoca Aadhaar en el sistema público de distribución (PDS) de granos, la cual genera hambruna y restricciones para la seguridad social, en particular para las personas mayores y las discapacitadas.[28]

También han surgido inquietudes en cuanto a la narrativa de que Aadhaar ayudó a proporcionar identificaciones a quienes no las tenían, dado que los datos de las solicitudes que revela la Ley de Derecho a la Información demuestran que solo el 0.3% de los 840 millones de residentes de la India que obtuvieron la identificación de Aadhaar eligieron la opción de "primera identificación" disponible para quienes no tenían pruebas previas de identidad. La gran mayoría parece haber

[27] "Aadhaar or else", The Indian Express, 21 de noviembre de 2017, http://indianexpress.com/article/opinion/columns/aadhaar-biometric-authentication-abba-public-distribution-system-pds-jharkhand-4946834/.
[28] "Testimonies Reveal How Aadhaar Has Brought Pain, Exclusion to Poor", thewire.in, 15 de marzo de 2018, https://thewire.in/government/aadhaar-right-to-food-pain-exclusion.

obtenido la inscripción en Aadhaar con sus documentos autenticados existentes de verificación de identidad y domicilio.[29]

Problemas de privacidad y derechos básicos

El marco regulatorio de privacidad de la India, o la falta de este, ha sido uno de los puntos más conflictivos del discurso en torno a Aadhaar. Muchos individuos y organizaciones activos en la comunidad de los derechos digitales de la India han expresado en repetidas ocasiones sus preocupaciones en cuanto al hecho de que el programa Aadhaar no es coherente con los principios de privacidad, que se deberían cumplir de forma inherente.

Actualmente, la Corte Suprema de la India enfrenta una serie de desafíos en torno al programa Aadhaar. Una magistratura constitucional de la Corte Suprema[30] está llevando a cabo audiencias para determinar la legalidad del programa. Uno de los pilares clave de los desafíos que impone el esquema de Aadhaar es la abolición del derecho fundamental a la privacidad.

La Corte Suprema de la India, en su juicio trascendental del caso *Puttaswamy* v. *Union of India* en 2017,[31] afirmó que cada indio tiene el derecho fundamental a la privacidad conforme a la Constitución de la India. Sin embargo, el impacto de esta disposición en el destino de los problemas del programa Aadhaar aún no es certero. El argumento principal en cuanto a la privacidad es la naturaleza semicoercitiva con la que el estado recopila los datos biométricos y crea una base de datos centralizada. Si bien el esquema de Aadhaar se considera como voluntario, con el tiempo, el gobierno ha hecho que el programa sea necesario para llevar a cabo una serie de funciones básicas en la sociedad, como presentar declaraciones fiscales, obtener asignaciones alimenticias o incluso utilizar una cuenta bancaria y realizar una variedad de actividades del sector privado, como

[29] "Very few Indians didn't have ID proof before Aadhaar", Hindustan Times, 13 de junio de 2015, https://www.hindustantimes.com/india/very-few-indians-didn-t-have-id-proof-before-aadhaar/story-0v4U95UH57i0Q0snYE1EeN.html (Trasfondo: "Las personas pueden inscribirse en Aadhaar de dos maneras. Pueden presentar documentos autenticados para establecer su identidad y lugar de residencia. Entre estos, se incluye una variedad de pruebas de identidad que las personas ya tienen, como tarjetas de votante, pasaportes, tarjetas alimentarias, licencias de conducir y tarjetas PAN. La segunda opción consiste en utilizar el sistema de "primera identificación", en el cual un portador de un número de Aadhaar autentica las credenciales de un solicitante. Esto significa que una persona puede obtener una tarjeta de Aadhaar sin poseer ningún otro documento").

[30] Una magistratura constitucional de la Corte Suprema de la India está compuesta por cinco o más jueces designados específicamente para analizar únicamente casos sobre la interpretación de cuestiones legales sustanciales en relación con la Constitución de la India.

[31] Ver el juicio aquí: http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

activar tarjetas SIM de telecomunicación.[32] En consecuencia, hoy Aadhaar es obligatorio para el público indio. Actualmente, se discute si obligar a las personas a brindar sus datos biométricos para obtener servicios es un incumplimiento del derecho fundamental a la privacidad y una violación de los estándares de necesidad y proporcionalidad que determinan las excepciones del derecho a la privacidad.

Durante las audiencias finales del caso contra Aadhaar ante una magistratura constitucional de la Corte Suprema a fines de abril y principios de mayo, la corte aclaró que el gobierno utilizaba un mandato aprobado el 6 de febrero del año anterior por la misma corte como "herramienta" para implementar el uso de Aadhaar en las tarjetas SIM de telecomunicaciones. La Corte Suprema luego indicó que no había emitido ningún mandato de vinculación obligatoria de Aadhaar y las tarjetas SIM.

El Gobierno de India, por su parte, ha tomado medidas para formular un marco legal para la protección de datos en este país. Supuestamente, este esquema debería abordar las cuestiones acerca de la privacidad y el uso de Aadhaar, entre otros asuntos relacionados. A fin de crear este marco con aportes de expertos y consultas a las partes interesadas, el Ministerio de Electrónica y Tecnologías de Información de India creó un comité bajo el liderazgo del anterior jefe de la Corte Suprema B. N. Srikrishna.[33] Este comité tiene la tarea de elaborar un informe y un proyecto de ley acerca de la protección de datos, y se espera que publique sus recomendaciones a mediados de 2018. El gobierno anterior de la UPA (United Progressive Alliance) había establecido un comité de expertos bajo el mando de la Comisión de Planificación, liderada por el anterior jefe de la Corte Suprema de Delhi, A. P. Shah, que publicó un informe centrado en 9 puntos[34] y llevó a cabo una iniciativa departamental para desarrollar un proyecto legislativo interministerial y proponer un proyecto de ley de privacidad entre 2011 y 2015.[35]

---

[32] Ver el informe aquí: "Didn't order Aadhaar-SIM link: Supreme Court", The Hindu Businessline, 26 de abril de 2018, https://www.thehindubusinessline.com/news/didnt-order-aadhaar-sim-link-supreme-court/article23680780.ece

[33] Ver el artículo aquí: http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited

[34] Ver el informe aquí: http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

[35] "High Level Summary and Critique to the Leaked Right Privacy Bill 2011", Centre for Internet and Society India, https://cis-india.org/internet-governance/high-level-summary-and-critique-to-the-leaked-right-to-privacy-bill-2011; "Comments on the Privacy Bill, 2011", Apar Gupta, https://iltb.net/comments-on-the-privacy-bill-2011-8b916ca96a81.

Problemas de seguridad

La seguridad de los datos que almacena el programa Aadhaar sigue siendo un problema desconcertante. Los informes repetidos de filtraciones de datos y exposición de datos personales,[36] así como los reiterados ataques a los datos biométricos y accesos a la base de datos por parte de personas no autorizadas,[37] no solo demuestran la deficiencia de las protecciones provistas por la ley, sino también las fallas de la arquitectura y las salvaguardas técnicas de Aadhaar.

El uso de datos biométricos como mecanismo de autenticación conlleva un riesgo significativo para la seguridad. Dada la naturaleza única y singular de la información biométrica, las filtraciones de datos de este tipo pueden ser irreversibles. A diferencia de un sistema que depende de una contraseña, en el sistema Aadhaar, si se comprometen los datos biométricos, tal vez sea imposible recuperar una identidad completamente.[38]

Si bien la encriptación puede mejorar la seguridad de una base de datos central, algunos expertos, como Bruce Schneier consideran que dichos sistemas son vulnerables a filtraciones causadas por ataques a las computadoras que utilizan esos datos.[39] Incluso si la encriptación no es descifrada, corre riesgo de ser evadida. Los informes de noticias sobre filtraciones de datos por parte de agencias de recolección y los ataques reiterados para eludir la autenticación son más indicadores de las vulnerabilidades no resueltas. Otro motivo de preocupación que destaca Troy Hunt es la centralización de los datos, un medio inherentemente inseguro para el almacenamiento de información.[40] Una base de datos central crea un punto de falla único. Aunque se empleen los mejores mecanismos para asegurar la base de datos, en materia de ciberseguridad, este método es el equivalente poner todos los huevos en una sola canasta. Los

[36] "In Supreme Court, Centre admits Aadhaar data leak, critics cite 'civil liberties'", The Indian Express, 4 May 2017, http://indianexpress.com/article/india/govt-admits-aadhaar-data-leak-critics-cite-civil-liberties-4639819/; "#AadhaarLeaks: A list of Aadhaar data leaks", medianama.com, 24 April 2017, https://www.medianama.com/2017/04/223-aadhaar-leaks-database/

[37] "Aadhaar data hack: IIT Kharagpur graduate arrested, earns Rs 40 lakh a year at Ola", Financial Express, 5 August 2017, http://www.financialexpress.com/india-news/aadhaar-data-hack-iit-kharagpur-graduate-arrested-earns-rs-40-lakh-a-year-at-ola/793999/; "Aadhaar's Security Questioned Again: Are Indians At Risk Of Identity Theft? ", Bloomberquint, 9 January 2018, https://www.bloombergquint.com/law-and-policy/2018/01/04/aadhaars-security-questioned-again-are-indians-at-risk-of-identity-theft

[38] "India's National ID Program May Be Turning The Country Into A Surveillance State", Buzzfeed India, 4 April 2017, https://www.buzzfeed.com/pranavdixit/one-id-to-rule-them-all-controversy-plagues-indias-aadhaar?utm_term=.nupprgWOk#.ga7mlQ0qz

[39] Ibíd.

[40] Ibíd.

investigadores de seguridad también han destacado las fallas en la cultura de la ciberseguridad de la Autoridad de Identificación Única de la India: no cuenta con un programa público de divulgación de fallas[41] y además, contiene legislación subordinada que define su marco de ciberseguridad como clasificado y rechaza las solicitudes de divulgación conforme a la Ley de Derecho a la Información.[42]

Problemas de vigilancia

Los mecanismos de autenticación del sistema Aadhaar conllevan a la creación de registros de autenticación. Cada vez que se usa Aadhaar para verificar la identidad de una persona, se registran los metadatos de dicha operación. Los expertos han destacado que, a gran escala y a lo largo del tiempo, esta práctica podría ser una herramienta de perfilamiento y vigilancia generalizados.[43]

Además del almacenamiento de datos, los estándares que se aplican para compartir estos datos con las agencias de implementación, entre otras, representan otro motivo de preocupación. La legislación proporciona un amplio estándar de "seguridad nacional" que se debe considerar al evaluar las solicitudes de datos y que, en general, utiliza un proceso legal que es más débil que el de la ley india en cuanto a la interceptación de datos de telecomunicación.[44] A su vez, es importante destacar que actualmente, solo la rama ejecutiva del gobierno se encuentra a cargo de evaluar dichas solicitudes, de modo que no hay ningún tipo de supervisión sobre el proceso. También vale la pena mencionar a modo ilustrativo que, recientemente, el gobierno de Uttar Pradesh procesó y aceptó 10.000 solicitudes de vigilancia telefónica en dos días.[45]

---

[41] "A billion users, but no bug reporting policy", Srinivas Kodali, 5 de diciembre de 2017, https://medium.com/karana/a-billion-users-but-no-bug-reporting-policy-20ce35122795

[42] "Under the right to information law, Aadhaar data breaches will remain a state secret", scroll.in, 5 de marzo de 2017, https://scroll.in/article/830589/under-the-right-to-information-law-aadhaar-data-breaches-will-remain-a-state-secret

[43] "Metadata = Surveillance", Bruce Schneier, 13 de marzo de 2014, https://www.schneier.com/blog/archives/2014/03/metadata_survei.html

[44] Conforme a la Ley de Telégrafo de India (sección 5, regla 419A de las Reglas de Telégrafo) y una disposición análoga de la Ley de Tecnologías de Información (Sección 69), la interceptación de las comunicaciones solo se debe autorizar en circunstancias ordinarias por el funcionario a cargo del departamento doméstico del Gobierno de la India o algún nivel del gobierno estatal de algún parea específica sujeta a cumplir las precondiciones de "emergencia pública o peligro inminente para el orden público". En comparación, la Ley de Aadhaar permite que se conceda acceso a la información de este programa a un área de nivel más bajo (una secretaría conjunta) con el motivo de proteger la "seguridad nacional", un término que no cuenta con una definición legal en la India.

[45] Yogi Government Trawled 10,000 Phone Records to Catch 'Potato Dumping' Protestors, thewire.in, 14 de enero de 2018, https://thewire.in/213729/adityanath-phone-tapping-uttar-pradesh/

III. TÉRMINOS DEL DEBATE SOBRE LA IDENTIFICACIÓN DIGITAL NACIONAL: DEFINICIONES

Con el objetivo de brindar asistencia a las partes interesadas a la hora de resolver los problemas que identificamos, desarrollamos un glosario breve de los términos utilizados en el debate. Esperamos que esta recopilación ayude a crear una base de información compartida que permita comprender las decisiones respecto de la legislación o las políticas en esta área. Nuestras recomendaciones de políticas para los programas de identificación se detallan en la siguiente sección. Recuerden que pueden enviar sus comentarios, tanto acerca de estos términos como de las recomendaciones que se indican a continuación.

Autenticación La autenticación establece que un individuo que intenta acceder a un servicio digital cuenta con uno o más autenticadores válidos asociados con su identidad digital.[46] Para que una autenticación sea exitosa, el solicitante debe demostrar la posesión y el control del autenticador mediante un protocolo de autenticación seguro.[47]

Autenticador Un autenticador es cualquier tipo de información que se puede utilizar para verificar la identidad de una persona. El paradigma clásico de los sistemas de autenticación identifica tres factores como los pilares de este proceso: (1) algo que el individuo sabe (p. ej., una contraseña), (2) algo que el individuo posee (p. ej., una tarjeta de ID o una clave criptográfica) o (3) una característica del individuo (p. ej., una huella dactilar o cualquier otro dato biométrico).[48]

Datos biométricos Los datos biométricos son características que representan atributos personales únicos que se pueden utilizar para verificar la identidad de una persona presente físicamente en el punto de verificación. Estas características pueden ser físicas o de comportamiento. Incluyen atributos faciales, las huellas dactilares, el patrón del iris, la impresión vocal, la forma de caminar y muchas otras.[49] En el contexto de los programas de identificación nacional que se incluyen en este artículo, los datos biométricos se usan con frecuencia como autenticadores para verificar la identidad del usuario o el portador del documento de autenticación. Los datos biométricos se pueden plasmar en el medio de identificación digital correspondiente o se pueden utilizar de otras maneras, por ejemplo, en puntos de datos específicos o en fórmulas para el reconocimiento de la forma de caminar.

---

[46] Instituto Nacional de Estándares y Tecnología, publicación especial 800-63, "Digital Identity Guidelines", https://pages.nist.gov/800-63-3/, pág. iv.
[47] *Id*. pág. vii.
[48] *Id.*, pág. 12.
[49] NIST Digital Identity Guidelines, pág. 13-4.

Identidad digital	Si bien no hay una definición estándar de la identidad digital, generalmente, hace referencia a la representación en línea de un individuo.[50] Se entiende que contiene componentes idénticos para la identificación y la autenticación.[51] Cuando estas funciones se ejecutan de manera digital, se considera que la identidad es digital. Existen varios modelos de identificación digital, como (1) la identificación digital que se utiliza exclusivamente en un servicio particular[52] o (2) la identificación que es común para varios servicios y funciona como la identificación central del individuo en el ecosistema digital.
Identificación	La identificación es el proceso mediante el cual se establece información sobre un individuo mediante un atributo o conjunto de atributos que describen exclusivamente a dicho sujeto en un contexto determinado.[53] En la actualidad, este proceso implica examinar documentos primarios, como pasaportes y certificados de nacimiento, consultar fuentes alternativas de datos para corroborar la identidad que se declara y, potencialmente, recopilar datos biométricos del individuo.[54]
Datos personales	En la mayoría de los contextos, el término "datos personales" hace referencia simplemente a información acerca de un individuo". La prueba principal para que un dato se considere como personal es el atributo de "identificabilidad". Muchas jurisdicciones clasifican los datos como personales si un individuo se puede identificar razonablemente a partir de esta información.[55]
Datos personales sensibles	Algunos datos personales se consideran más sensibles y reveladores que otros. Estos se conocen como datos personales sensibles. Cualquier procesamiento no autorizado de este tipo de datos es una violación y una interferencia con los derechos de los usuarios; a su vez, dichos datos se consideran como un asunto de interés primordial en cuanto a la privacidad y la intimidad. Muchas jurisdicciones[56] han establecido que estos datos incluyen, por ejemplo, información sobre la salud, la información genética, los datos biométricos y la información sobre las creencias religiosas, la etnia o el origen étnico y la

[50] NIST Digital Identity Guidelines
[51] Omidyar Network-Hyperion, "Digital Identity, Issue Analysis report", http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Omidyar-Network-Digital-Identity-Issue-Analysis-Executive-Summary-v1_2-1.pdf
[52] NIST Digital Identity Guidelines
[53] *Id.*, page 47.
[54] Omidyar Network-Hyperion, "Digital Identity, Issue Analysis report", http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Omidyar-Network-Digital-Identity-Issue-Analysis-Executive-Summary-v1_2-1.pdf, pág. 8-9.
[55] Artículo 4(1), GDPR de la UE; Sección 2(1) de la Ley de Protección de Datos Personales de 2012, Singapur; Sección 2, Ley de Protección de la Información y de Documentos Electrónicos, Canadá; Sección 1, Ley de Protección de la Información Personal, Sudáfrica.
[56] Artículo 9, GDPR de la UE; Sección 6, Ley de Privacidad, Australia; Sección 26, Ley de Protección de la Información Personal, Sudáfrica.

orientación sexual. Cuando se combinan datos no sensibles entre sí a lo largo del tiempo, estos también pueden representar datos sensibles, dado que la esencia de los datos derivados tendría las mismas características de los datos sensibles.

Verificación La verificación es el proceso de garantizar la posesión y el control de uno o varios autenticadores por parte de un solicitante en relación con una tarjeta de identificación mediante un protocolo de autenticación. Para ello, es posible que un verificador (en los programas de identificación nacional, suele ser un agente estatal) también necesite validar las credenciales que vinculan al autenticador con el identificador del suscriptor a fin de comprobar su estado.[57]

IV. RECOMENDACIONES PARA LAS POLÍTICAS PÚBLICAS

Nuestras recomendaciones clave se derivan de nuestras experiencias en las distintas jurisdicciones en que se implementaron o se considera implementar programas de identificación digital. Tal como lo destacamos anteriormente, estas recomendaciones se basan en tres pilares:

1. **GOBERNANZA**
2. **PROTECCIÓN DE LA PRIVACIDAD Y LOS DATOS PERSONALES**
3. **CIBERSEGURIDAD**

A continuación de estas recomendaciones, se incluye una sección separada en la que presentamos nuestros lineamientos propuestos para los sistemas de identificación, ya sean públicos o privados.

GOBERNANZA

Quienes promueven la implementación de programas de identificación digital, como lo mencionamos más arriba, con frecuencia basan su postura en la facilidad de gobernanza o en la seguridad nacional.[58] La aplicación de programas de identificación digital se basa en la provisión de servicios, como los beneficios sociales, de forma más eficiente y precisa, y en la reducción de la corrupción mediante el uso de tecnologías que permitan una identificación precisa y una autenticación segura. Sin embargo, estos mismos programas pueden convertirse en impedimentos para la gobernanza y perjudicar la prestación de servicios de bienestar social, así como la inclusión adecuada de los ciudadanos. En la India, varios académicos y analistas han destacado que el desarrollo de dichos

[57] Id., pág. 56.
[58] Banco Mundial, Informe de Desarrollo Mundial de 2016, "Digital Dividends", pág. 147, http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf.

programas, en realidad, fomenta la exclusión de ciudadanos de los servicios sociales y públicos en varios casos.[59]

A FIN DE ABORDAR ESTOS PROBLEMAS, RECOMENDAMOS A LOS LEGISLADORES LO SIGUIENTE:

1. Realizar consultas transparentes, inclusivas y abiertas al comienzo de cualquier propuesta de programa de identificación digital

Los gobiernos y responsables de la toma de decisiones deben garantizar que las consultas relacionadas con los programas de identificación digital se realicen de manera abierta, transparente e inclusiva. Esto significa que se deben realizar consultas públicas y mesas redondas de expertos, publicar artículos sobre estos análisis, recibir comentarios de todas las partes interesadas (con fechas límite razonables) y brindar respuestas a dichos aportes. En todas las etapas, se debe asegurar la participación significativa de los distintos grupos de la sociedad civil, y todas las reuniones de los responsables de la toma de decisiones con representantes de la industria, ONG y grupos de consumidores se deben realizar de forma pública y con registros de fácil acceso. El proceso debe acompañarse con un nivel máximo de transparencia respecto de todos los actos de *lobby*. A su vez, se debe asignar la relevancia adecuada a los aportes de la sociedad civil a fin de rectificar el inevitable desequilibrio de la cantidad de voces en comparación con la industria. [60]

Un caso práctico interesante sobre la participación ciudadana efectiva respecto de los

[59] "Reetika Khera, Impact of Aadhaar on Welfare Programmes", Economic and Political Weekly, Vol. 52, Edición N.° 50, 16 de diciembre de 2017, http://www.epw.in/journal/2017/50/special-articles/impact-aadhaar-welfare-programmes.html

[60] A modo de ejemplo de modelos de temas relacionados, las negociaciones del Reglamento General de Protección de Datos se llevaron a cabo conforme al proceso legislativo de la UE. Este proceso es relativamente transparente y, por lo general, ha garantizado la publicación de las propuestas de proyectos de ley, así como las opiniones, los informes, las enmiendas y las opiniones legales relacionadas de todas las instituciones de la UE en cuanto a todas las legislaciones discutidas. Para obtener más información, ver "La creación de un marco para la protección de datos: Una guía para los legisladores sobre qué hacer y qué no", Access Now, https://www.accessnow.org/cms/assets/uploads/2018/04/manual-de-proteccion-de-datos.pdf

programas de identificación surge en Columbia Británica.[61] El plan de participación ciudadana del gobierno provincial de Columbia Británica para el paquete de la BC Services Card constaba de los siguientes elementos:

1. Creación de un *informe oficial* sobre las iniciativas de servicios digitales planificadas en torno a esta plataforma de identificación y solicitud de comentarios
2. *Convocación de expertos*, en particular, a aquellos de la comunidad de derechos humanos y a los comisionados provinciales en materia de privacidad
3. Un *panel de ciudadanos* seleccionados aleatoriamente para fomentar la participación civil a la hora de determinar las decisiones de políticas clave futuras
4. Una *encuesta* en línea disponible durante un mes para cualquier ciudadano de la provincia que desee dar su opinión

2. Garantizar un alcance definido y restringido para la implementación del programa de identificación digital conforme a la ley vigente

Los responsables de la toma de decisiones deben definir de manera clara y explícita el propósito de cualquier programa de identificación digital. A su vez, el gobierno debe explicar claramente el alcance de la implementación y el uso de tal proyecto ante el público.

3. Permitir que la inscripción y el uso de la identificación digital sean voluntarios

La inscripción en un programa de identificación digital debe ser opcional. Si bien el gobierno puede tener un propósito legítimo para solicitar una identificación digital cuando los individuos acceden a servicios gubernamentales (atención

[61] Kaliya Hamlin, "BC'S Citizen Engagement: A Model for Future Programmes", re:ID, primavera de 2014, edición 37, disponible en https://identitywoman.net/bc-identity-citizen-consultation-results/

médica, educación), el uso de dicho sistema no debe ser obligatorio para recibir estos servicios. No contar con una identidad digital no debe impedir que una persona reciba los servicios básicos que el gobierno tiene la obligación de proporcionar. Los funcionarios públicos y los responsables de la creación de políticas deben operar de un modo que refleje la comprensión de las distintas formas de identidad.

Los programas de identificación digital deben respetar la voluntad y la elección de los usuarios. Por lo tanto, los gobiernos no deben establecer que un tipo de identidad sea obligatorio. Este principio se debe aplicar a las acciones estatales, ya sean explícitas (p. ej., cuando el gobierno establece que es obligatorio poseer una forma particular de identificación digital mediante una ley o un mandato) o coercitivas (cuando se requiere una identificación digital nacional para acceder a servicios proporcionados por otras agencias públicas o cuando se ejerce presión sobre distintas plataformas o empresas privadas para que soliciten el uso obligatorio de dichas identificaciones).

4. Crear mecanismos independientes y eficientes para presentar reclamos y recibir reparaciones

Los individuos deben contar con mecanismos adecuados para recibir reparaciones en casos de abuso o mal uso de sus datos personales o filtraciones de datos. Con este propósito, las autoridades públicas deben llevar registros detallados de los accesos a datos conservados por parte de los funcionarios públicos, así como crear registros detallados de los objetivos de dichos accesos.

5. Garantizar la inclusión en las etapas de inscripción e implementación,

Los usuarios no deben experimentar ninguna forma de discriminación en el proceso de inscripción. Las prohibiciones técnicas o las diferencias de infraestructura no deben impedir ni prohibir que los usuarios accedan a servicios durante la implementación. Esto significa que se

independientemente de las diferencias de recursos tecnológicos o capacidad estructural

deben crear sistemas eficientes que solo conserven una cantidad mínima de datos sobre las personas y que puedan brindar alternativas cuando haya problemas.

Los programas de identificación digital administrados o coordinados por agencias públicas se deben crear bajo la premisa de que la falta de acceso a Internet puede exacerbar la exclusión de los ciudadanos, en especial, cuando su capacidad de acceder a los servicios del gobierno, asignaciones legales o transacciones se encuentre vinculada a un ecosistema de identificación que requiera conectividad constante para llevar a cabo autenticaciones periódicas.

Si no se toman estas medidas, los programas de identificación digital pueden frustrar sus propios objetivos, incluido el cumplimiento del Objetivo de Desarrollo Sustentable N.° 16, que se basa en la inclusividad y el acceso a la justicia, las instituciones y los servicios básicos. Un programa nacional de identificación digital poco eficiente puede provocar que cientos de personas no tengan acceso a servicios básicos porque no poseen la identificación digital que requieren las agencias gubernamentales o porque su identificación digital se encuentra "incompleta" dado que no se pudieron cargar sus huellas dactilares en la base de datos nacional a causa de una conexión a Internet deficiente.

PROTECCIÓN DE LA PRIVACIDAD Y

Los programas nacionales de identificación digital almacenan una gran cantidad de datos, tanto en la etapa de inscripción como durante la autenticación periódica de las transacciones, lo cual genera grandes preocupaciones para la protección de la privacidad y los datos personales.

LOS DATOS PERSONALES

Dado que la administración de estos programas se encuentra en manos de los gobiernos, existe un nivel de confianza y autoridad inherentes por parte del público en cuanto a la recopilación de estos datos. Esto puede conllevar a un uso generalizado de los sistemas de identificación digital y poner en riesgo la información que los individuos proporcionan a dichos programas. A su vez, la mera escala de estos programas requiere salvaguardas eficientes.

PARA PROTEGER LA PRIVACIDAD Y LOS DATOS PERSONALES, RECOMENDAMOS LO SIGUIENTE:

1. Limitar el propósito para el que se recopilan y se utilizan los datos e implementar medidas adecuadas para evitar el perfilamiento de usuarios en función de los datos proporcionados voluntariamente

De conformidad con el principio internacional de derechos humanos de necesidad,[62] los gobiernos deben limitar los datos obtenidos de los individuos a aquellos que son estricta y demostrablemente necesarios para lograr un fin legítimo. Dicho objetivo debe definirse de manera clara y publicarse. A su vez, los responsables de la toma de decisiones deben aplicar medidas legales y de seguridad para prevenir el perfilamiento de usuarios.

2. Garantizar a los individuos los derechos relacionados con sus datos, como la exactitud, la rectificación y la eliminación

Para que un mecanismo de identificación digital empodere a los individuos, se debe crear un marco que se centre en el usuario y que fomente la transparencia. Las personas deben tener acceso a los datos recopilados a través de su identificación digital o relacionados con esta y deben contar con la posibilidad y el derecho legal de corregir fácilmente cualquier error. Todos los participantes de un programa de identificación digital deben gozar de los siguientes derechos, como mínimo:

- *Consentimiento informado y bases sólidas para el procesamiento:* Los usuarios deben informar su consentimiento para la recopilación de sus datos a fin de que se

[62] *Id.*, Principio 3, https://necessaryandproportionate.org/principles#principle3.

utilicen en el programa de identificación digital. A su vez, deben tener el derecho de anular dicho consentimiento en cualquier momento.

- *Exactitud:* Los datos personales deben ser precisos y se deben actualizar siempre que sea necesario. Los usuarios deben tener el derecho de acceder a su información personal, así como rectificarla y eliminarla. A su vez, los individuos deben tener el derecho de acceder a información sobre el uso de sus datos personales con propósitos definidos y deben poder objetar cualquier procesamiento que no sea estrictamente necesario.

- *Limitación de la retención:* Los datos personales procesados con cualquier fin no deben retenerse por más tiempo del necesario para el objetivo en cuestión.

- *Integridad y confidencialidad:* Los datos personales deben procesarse de un modo que garantice la máxima seguridad de los datos, incluida la protección contra los procesamientos ilícitos o no autorizados y contra la pérdida, la destrucción o los daños accidentales, a través de medidas técnicas u organizacionales adecuadas.

3. Establecer marcos sólidos de protección de datos personales para regular los programas de identificación digital

Los programas nacionales de identificación digital deben estar sujetos a marcos de protección de datos personales y a cualquier regulación específica que se aplique a dichos planes si proporciona mecanismos complementarios más eficientes para los usuarios. A su vez, los gobiernos deben garantizar que estos programas cuenten con la supervisión de alguna autoridad de protección de datos personales o algún comisionado independiente de protección de la privacidad.

	Los actores estatales deben estar obligados a monitorear e implementar medidas estrictas para proteger los datos personales de los usuarios que procesan los agentes del sector privado involucrados en la operación de los programas nacionales de identificación digital o que presten servicios que requieran la autenticación a través de dichos mecanismos digitales. Los agentes estatales deben diseñar e implementar regulaciones para garantizar que estos terceros no creen bases de datos centralizadas paralelas a partir de los indicadores de la identidad digital nacional de las personas.
4. Minimizar la cantidad y los tipos de datos que los gobiernos y proveedores de servicios asociados pueden recopilar	Los programas nacionales de identificación digital deben limitar la cantidad de información personal que recopilan a lo que es estrictamente necesario en función del propósito en cuestión. Esto incluye la recopilación de datos que realizan directamente las distintas agencias gubernamentales, así como la que llevan a cabo los proveedores de servicios o terceros con autorización para utilizar dichos ecosistemas de identificación digital.

5. Restringir la interceptación y el monitoreo lícitos del uso de la identificación digital y establecer medidas de control

El acceso a los datos almacenados por cualquier programa nacional de identificación digital conforme a mandatos legales o de otros agentes estatales debe encontrarse sujeto a los estándares legales internacionales relevantes, en particular, los principios de "Necesidad y Proporcionalidad"[63] si no se aplican salvaguardas domésticos de mayor jerarquía establecidos por la ley. Los datos biométricos, así como cualquier otro tipo de dato sensible, como la información que solicitan los sistemas de autenticación o identificación, deben reconocerse como "información protegida". A su vez, se deben implementar marcos o regulaciones legales que establezcan medidas de control del acceso, por ejemplo, requiriendo que el emisor de la identificación digital lleve un registro de los accesos a cada identificación que los usuarios puedan consultar en cualquier momento. El registro de accesos debe contener la siguiente información: quién accedió a los datos, cuándo, dónde y con qué fin.

CIBERSEGURIDAD

Un marco regulatorio efectivo para un programa de identificación digital debe contar con el respaldo de una tecnología y un marco de ciberseguridad igual de eficaces. La recopilación de grandes cantidades de datos personales relacionados con la identidad (incluidos los datos biométricos), con frecuencia, constituyen blancos tentadores para accesos ilegítimos e invasiones a la privacidad por parte de criminales y otros agentes maliciosos. Los demás desafíos relacionados con la seguridad de la comunicación de los datos durante la autenticación se deben abordar mediante mecanismos adecuados de encriptación.

NUESTRAS RECOMENDACIONES PARA LOS LEGISLADORES:

[63] Principios de Necesidad y Proporcionalidad, https://necessaryandproportionate.org/es/principios/ .

1. Implementar una infraestructura tecnológica eficiente y segura

A fin de establecer un marco efectivo para los programas de identidad digital a nivel nacional, se requiere una infraestructura tecnológica robusta. Esto es fundamental debido a los siguientes factores:

- Estos programas dependen estrictamente de las tecnologías de comunicación para llevar a cabo todas sus funciones.
- Los programas de identificación digital constituyen la base de muchas acciones de bienestar social en numerosas jurisdicciones. Las fallas de infraestructura pueden provocar graves adversidades en la vida de los beneficiarios.
- Estos marcos de identidad procesan información personal extremadamente crítica. Por eso, es fundamental que se proporcionen medidas de protección adecuadas para dichos datos.

En este contexto, es crítico contar con una infraestructura tecnológica sólida. A su vez, es importante comprobar la eficacia de estas estructuras mediante el uso de diversas herramientas de prueba de estrés y penetración.

2. Garantizar que la recopilación y el almacenamiento de los datos no sean centralizados

La recopilación y el almacenamiento centralizados de los datos para los programas nacionales de identificación digital (en particular, aquellos que involucran datos biométricos) suponen grandes peligros y no se deben promover. Nuestras recomendaciones son las siguientes:

- **Arquitectura de almacenamiento descentralizada:** La arquitectura de estos sistemas es clave, y los modelos basados en proveedores de identificación federada, proveedores de identificación digital de

administración centralizada, proveedores de servicios de credenciales de administración centralizada o proveedores de identificación personal brindan un mayor nivel de protección para los derechos de los usuarios.[64]

- **Identificaciones múltiples:** Utilizar un modelo basado en varias formas de identificación es una alternativa efectiva, dado que brinda opciones y practicidad. Los beneficios de los sistemas de identidad digital no centralizados se deben reconocer y promover.

3. Separar las funciones de identificación y autenticación y evitar crear registros centralizados de transacciones para la autenticación

En algunos modelos nacionales de identificación digital, la agencia central actúa como núcleo para la identificación y la autenticación.

La conjunción de estas dos funciones crea un cuello de botella para la implementación que aumenta los riesgos para la ciberseguridad. El eslabón más débil en el sistema de identificación podría aprovecharse para exponer los datos de identificación o de autenticación. A fin de evitar este riesgo, se deben separar las funciones de identificación y autenticación, como lo hace UK.Gov Verify (en que el autenticador y el identificador son agencias separadas), o se debe utilizar un mecanismo como el de SecureKey Concierge[65] en Canadá (donde el servicio de conserjería solo funciona como un mecanismo para conectar al proveedor del servicio con la agencia de identificación, sin intercambiar datos personales entre las dos agencias).

[64] Omidyar Network-Hyperion, "Digital Identity, Issue Analysis report", http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Omidyar-Network-Digital-Identity-Issue-Analysis-Executive-Summary-v1_2-1.pdf, Definiciones disponibles en páginas 12a 15.
[65] https://securekeyconcierge.com/about/

	La mayoría de las agencias de autenticación crean un registro de transacciones de las solicitudes de autenticación que se enviaron para cada usuario. Si bien estos registros no siempre captan datos por sí mismos, guardan metadatos sobre la transacción en que se originó la solicitud de autenticación. Mediante modelos de administración centralizada, como lo indicamos anteriormente, la necesidad de crear este tipo de registros se puede minimizar significativamente. Como mínimo, estos registros de transacciones se pueden separar de los núcleos en los que se administra la información sobre la identidad. A su vez, los registros de transacciones se encuentran separados de los registros de acceso, que son controlados por el usuario.
4. Establecer principios de "privacidad por diseño" en el programa	Cualquier programa nacional de identificación digital debe considerar la privacidad desde el origen de su diseño. Prevenir es más fácil que curar, en especial, cuando se trata de arquitecturas de sistemas. Por lo tanto, es clave que la privacidad se incorpore desde la base (trabajando en conjunto con autoridades de protección de datos, expertos legales no gubernamentales y la sociedad civil) del diseño administrativo, legislativo y técnico de dichos programas y tanto desde el comienzo como a lo largo del ciclo de vida y la implementación de la iniciativa.
5. Garantizar que los programas nacionales de identificación se basen en modelos de comunicación segura, por ejemplo, mediante el cifrado de extremo a extremo del tráfico en la mayor medida posible	Tal como lo analizamos anteriormente, estas redes de programas almacenan información extremadamente crítica. Por eso, tomar medidas de protección adecuadas para proteger las actividades de comunicación, como las solicitudes y respuestas de autenticación, es fundamental para brindar seguridad. La comunicación encriptada de extremo a extremo a través de los sistemas de identificación digital es clave para garantizar la

	seguridad digital y se debe implementar en la mayor medida posible.
6. Brindar transparencia mediante la divulgación de las políticas de ciberseguridad	Se deben tomar medidas para garantizar la divulgación de las políticas de ciberseguridad y los principios desarrollados a fin de proteger la infraestructura de la identificación digital. Dada la importancia para el público y la escala de estos proyectos, las divulgaciones deben considerarse como un derecho de los ciudadanos. A su vez, las prácticas de este tipo fomentan la revisión de las políticas por parte de expertos y otras partes interesadas, lo cual permite comunicar distintos aspectos al gobierno, realizar consultas abiertas sobre los problemas y desarrollar políticas de ciberseguridad más sólidas, así como un ecosistema más seguro.
7. Proporcionar un marco legal y de políticas públicas que fomente la comunicación y la divulgación de las vulnerabilidades	Cualquier iniciativa en favor de un programa de identificación digital orientado a mejorar la seguridad debe fomentar la participación de investigadores de este campo y proporcionar un marco adecuado que respalde la participación de la comunidad. En dicho marco, la autoridad relevante debe interactuar con los investigadores y promover la divulgación de las vulnerabilidades. A su vez, las autoridades gubernamentales no deben intentar intimidar o criminalizar, ya sea de forma directa o indirecta, los esfuerzos de los investigadores de seguridad independientes que busquen exponer las vulnerabilidades potenciales o los abusos que se hayan detectado en los programas de identificación digital.
8. Tomar medidas para informar las filtraciones de datos a las partes afectadas	Aun con los sistemas más sólidos implementados, se pueden producir filtraciones de datos. En este contexto, se deben tomar medidas para informar tales problemas a los usuarios. Dado que los sistemas de identificación administran datos personales y

sensibles, además de implementar mecanismos robustos de prevención para la filtración de datos, es necesario aplicar sistemas complementarios para notificar a los usuarios afectados acerca de los incidentes que ocurran. A su vez, las notificaciones a los usuarios sobre las filtraciones de datos y el impacto potencial en sus datos se deben tratar como requisitos legales. Es importante que no se utilicen fundamentos basados en la seguridad nacional para mantener esta información en confidencialidad.

V. USO DE DATOS BIOMÉTRICOS EN SISTEMAS DE IDENTIFICACIÓN: CONSIDERACIONES ESPECIALES

Los identificadores biométricos se han vuelto cada vez más populares en los sectores público y privado como medio para identificar a los individuos, y proporcionan una alternativa para la autenticación de los usuarios.

En general, los identificadores biométricos incluyen las huellas dactilares, el ADN, las firmas y los patrones de iris y retina. Sin embargo, en ocasiones, también se usan otros, como los patrones venosos, la geometría facial o incluso los patrones de voz. Al igual que los demás métodos de autenticación, los datos biométricos son vulnerables a los hackeos, pero, a diferencia de las contraseñas, estos indicadores no se pueden restablecer cada vez que sea necesario. Esto implica un gran riesgo a la seguridad, dado que es cada vez más difícil resarcir las filtraciones o los hackeos de datos biométricos y restablecer la seguridad de los sistemas basados en este tipo de información.

La recolección y el uso de datos biométricos suponen altos riesgos para los individuos. Debido al potencial de explotación de esta información, desalentamos su uso en los programas de identificación digital. En su manual de políticas de 2017, Cato Institute también se manifiesta en contra del uso de los datos biométricos en los sistemas nacionales de identificación digital.[66] El

[66] Cato Handbook For Policymakers, 8.° edición (2017) https://www.cato.org/cato-handbook-policymakers/cato-handbook-policy-makers-8th-edition-2017/national-id-systems

almacenamiento y el uso de datos biométricos se deben limitar estrictamente, incluso cuando tengan el propósito de aumentar la conveniencia o mejorar la seguridad.

RECOMENDACIONES PARA EL USO DE DATOS BIOMÉTRICOS EN LAS INICIATIVAS DE IDENTIFICACIÓN DIGITAL EN LOS SECTORES PÚBLICO Y PRIVADO

1. Evitar la creación de bases de datos centralizadas con los datos biométricos de los individuos	Dada la sensibilidad de los datos biométricos y el hecho de que la posibilidad de "restablecimiento" es limitada cuando resultan comprometidos, recomendamos garantizar que dicha información se almacene de forma descentralizada. Una base de datos centralizada es más vulnerable porque crea un punto único de fallo.
2. Garantizar que la provisión de identificadores biométricos sea voluntaria y habilitada por el usuario, no una medida (de seguridad) predeterminada	El registro de identificadores biométricos por parte de los individuos no debe ser obligatorio. Esta opción debe ser voluntaria y no debe representar una condición para la prestación de servicios.
3. Minimizar la recopilación y la transferencia de datos	Los creadores de iniciativas de identificación digital deben minimizar la recopilación y la transferencia de datos asociados con identificadores biométricos. Esto permite reducir los riesgos y los daños si los datos resultan comprometidos. Recomendamos que, en general, los desarrolladores implementen sistemas de autenticación en el dispositivo que utilicen los identificadores biométricos como contraseñas, en lugar de emplear sistemas centralizados de almacenamiento/autenticación en nube.
4. Garantizar que los dispositivos que detectan los datos biométricos de los usuarios sean seguros y no almacenen los datos biométricos reales	Si se opta por recolectar y procesar datos biométricos en un programa de identificación digital, recomendamos que dichos datos biométricos en bruto no se almacenen en el sistema. Esto es posible mediante sistemas que utilizan técnicas de "transformación de características" (*feature transformation*) o funciones unidireccionales. Mediante **estas, los datos biométricos se transforman en nuevos datos que se almacenan en el sistema eliminando la necesidad de conservar la información biométrica real de los usuarios.**

En el proceso de autenticación, los datos biométricos recopilados en tiempo real se someten al mismo proceso de transformación y la información transformada es la que se analiza para establecer o no la coincidencia. Esto permite garantizar el mayor nivel de seguridad posible para los usuarios y el ecosistema en general.

5. Desarrollar procedimientos legales y estándares basados en evidencia para los datos biométricos que protejan los derechos humanos y el debido proceso

Al procesar datos biométricos con fines probatorios, debemos garantizar que los procedimientos sean adecuados y respetuosos de los derechos humanos. Para ello, recomendamos lo siguiente:

- Cuando se usen datos biométricos en la identificación criminal, la evidencia física debe retenerse y utilizarse como la fuente de identificación principal. Se debe minimizar el uso obligatorio de datos biométricos de dispositivos de los consumidores por parte de las fuerzas de seguridad.
- La información biométrica recopilada por agentes privados se debe reconocer como "información protegida" y debe estar sujeta a los estándares legales requeridos para dichos datos en función de los principios de "Necesidad y Proporcionalidad".

VI. CONCLUSIÓN

Los programas nacionales que crean identificaciones digitales deben, desde el comienzo de su desarrollo, procurar proteger los derechos humanos de los individuos participantes. Los programas con diseños deficientes, en especial, aquellos que vinculan los datos biométricos con sistemas centralizados de autenticación y almacenamiento de datos, tienen altas probabilidades de violar estos derechos. Estos sistemas centralizados, que, con frecuencia, operan con un enfoque negligente basado en la recopilación o la vinculación generalizadas, introducen riesgos innecesarios con escasas evidencias de beneficios para la sociedad. Estos programas ponen en riesgo los intereses de las mismas personas que los funcionarios públicos y responsables de la toma de decisiones manifiestan querer proteger. Cualquier programa de identificación digital que suponga un riesgo para los derechos humanos es inaceptable.

Los programas de identificación digital deben incluir, tanto en su diseño como su implementación, suficientes salvaguardas y mecanismos para respetar y proteger los derechos humanos de los usuarios. Los incumplimientos en cuanto a la creación o la contemplación de estas medidas de protección deben provocar la cancelación de la implementación de estos programas y deben requerir medidas significativas de restructuración para proteger los derechos humanos de los usuarios. En nuestras recomendaciones, instamos a los responsables de la toma de decisiones para que tomen medidas en cuanto a la gobernanza, la protección de la privacidad y los datos

personales y la ciberseguridad. Es indispensable que las salvaguardas (legales, tecnológicas y de esquemas gubernamentales) se adopten de manera integral y que la implementación de una no afecte la adopción de las demás.

Nuestro enfoque surge de nuestras experiencias de participación en el desarrollo y la implementación de distintos programas nacionales de identificación digital en todo el mundo. El ejemplo de la India que analizamos en este artículo ilustra la variedad de problemas asociados a los programas de identificación digital que se deben abordar para lograr los objetivos deseados y proteger los derechos humanos. En el ejemplo de Túnez, vimos cómo la sociedad civil puede tomar medidas para evitar los peligros de la creación de este tipo de programas sin considerar todas las implicancias, tanto para los derechos humanos como la seguridad. La experiencia de Estonia muestra que, incluso con la implementación más sofisticada, un programa nacional de identificación digital tiene riesgos significativos y que el uso de sistemas públicos de criptografía de clave puede ser más seguro que los datos biométricos. El desarrollo de tecnologías como el *blockchain* demuestra que hay alternativas a la tendencia actual en favor de los sistemas nacionales de identificación digital centralizados y basados en la vinculación de datos biométricos, aunque todavía hay dudas respecto de cuál es el mejor camino a seguir.

Esperamos que los lectores de este artículo preliminar nos envíen sus comentarios y aportes. Los especialistas en tecnología y líderes involucrados en programas gubernamentales de identificación deben ejercer un alto nivel de liderazgo y demostrar públicamente su responsabilidad frente a la protección de nuestro derecho fundamental a la privacidad. Es mejor reconocer los problemas en las etapas iniciales a fin de interactuar con las partes interesadas, crear un marco significativo e implementar un curso de acción que priorice explícitamente la protección de la privacidad a nivel legal y administrativo.

Para obtener más información, pueden comunicarse con:
Naman M. Aggarwal (naman@accessnow.org)
Verónica Arroyo (veronica@accessnow.org)
Raman Jit Singh Chima (raman@accessnow.org)
identity@accessnow.org