Identidad digital: conceptos y legislación

Autores

Christine Weidenslaufer
cweidenslaufer@bcn.cl

Raimundo Roberts
rroberts@bcn.cl

Equipo de trabajo:
Paola Truffello

Nº SUP: 135618

Resumen

Varios países del mundo están implementando sistemas de identificación digital.

El proceso implica la adopción de normas legales y reglamentarias, así como la implementación de sistemas tecnológicos que entreguen seguridad informática y protección a la identidad digital de las personas. Desde un punto de vista jurídico, el derecho a la identidad es considerado un derecho de la personalidad, y, el derecho al reconocimiento de la personalidad jurídica es reconocido como un derecho humano por el derecho internacional.

El ejercicio de este derecho se garantiza mediante la ejecución de medidas destinadas a la obtención de una identificación reconocida por un Estado, traducida en un documento que certifique la identidad (por ej. La cédula de identidad chilena es un medio identificatorio).

Por tanto, identidad e identificación son conceptos diferentes que, en el ámbito digital, requieren de sistemas tecnológicos que otorguen el mismo nivel de seguridad online que en el mundo físico. Mientras la identidad física incluye atributos inherentes a la persona (nombre, edad, huella digital, fecha de nacimiento), la identidad digital se construye con más datos, como los acumulados (datos médicos, gustos, datos de comportamiento) y atribuidos (número de teléfono, correo electrónico o número de identificación nacional).

El Estado puede participar en la creación de un sistema de identificación digital a través de tres modelos: uno centralizado, donde se encarga de la creación del instrumento y su administración; uno descentralizado, donde privados elaboran el instrumento y otros se encargan de la verificación, y un tercero, similar al anterior, donde el Estado actúa de verificador (intermediario) entre quien elabora la identificación digital y quien verifica.
Chile está desarrollando un sistema de identificación digital (Clave Única), que permite el acceso de la mayoría de los servicios del Estado. Su regulación, dado que se trata de un proceso en desarrollo, se basa en normativa reglamentaria y decretos.
En la experiencia comparada la construcción de mecanismos de identificación digital y su regulación varían. La **Unión Europea**, desde 2014, cuenta con el eIDAS, Reglamento europeo de identificación digital, el cual está pronto a ser reemplazado por una versión más amplia, que principalmente mejora el uso transfronterizo de los elementos de identificación digital que están desarrollando sus estados miembros. En particular, los siguientes países cuentan con legislación específica en la materia:
En **España**, la identidad digital se establece a través de métodos de identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física y se traduce en la solicitud del interesado de un certificado que la acredite.

Agradecemos la edición técnica de este informe de la abogada especialista en transformación digital, Carla Illanes.

Estonia cuenta con un sistema público que provee de identidad digital a casi toda su población, que incluye, entre los atributos para la identificación personal, elementos que permiten la identificación digital.
India, país que cuenta actualmente con el sistema más extendido de identificación electrónica con más de 1.300 millones de personas, exige enrolarse en un sistema de identificación electrónica para la entrega de beneficios públicos.

I. Introducción

El siguiente documento analiza el concepto "identidad digital" (en adelante, ID), los avances de su regulación en Chile y la legislación extranjera sobre la materia. Cabe destacar que la mayor parte de la regulación sobre identidad digital se basa actualmente en reglamentos y normas técnicas, tanto en la Unión Europea, cuyos avances están siendo analizados por otras organizaciones internacionales, así como Chile. Ello se debe en parte porque se trata de la implementación de sistemas tecnológicos que evolucionan contantemente.

Para la elaboración de este informe se revisaron las normativas relevantes en una decena de países, además de la propia de la Unión Europea (UE). Se seleccionaron finalmente los casos de siete naciones más la UE. Se utilizaron también como fuentes revistas científicas y jurídicas, y convenios internacionales. Finalmente, cabe mencionar que, en la mayoría de los países revisados, no existiría legislación específica sobre ID.

Las traducciones son propias.

II. Personalidad, identidad e identificación

La civilística clásica, según señala Gonzalo Figueroa (1998)[1], ha definido los llamados "atributos de la personalidad" como características de las personas, que comprenden el nombre, capacidad de goce, estado civil, nacionalidad, domicilio, y algunos también agregan el patrimonio. Estas características son consideradas insuficientes por el autor, quien afirma que "una persona no es ni un nombre, ni un estado civil, ni un domicilio, si bien puede "tener" esos atributos" (Figueroa 1998:22).

A partir de mediados del siglo XX, precisa Figueroa, la civilística agregó a los "atributos" tradicionales los llamados "derechos de la personalidad", que consideran: el derecho a la vida, a la integridad física y psíquica, al honor, a la libertad, a la actividad vital y al trabajo, a la privacidad o intimidad y el **derecho a la identidad personal**, entre otros.

El **derecho al reconocimiento de la personalidad** se encuentra reconocido en instrumentos internacionales de derechos humanos. La Declaración Universal de los Derechos Humanos2 (1948) dispone en su artículo 6 que "todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica".

[1] Figueroa Y., Gonzalo. Derechos de la personalidad en general. Concepción tradicional- Revista de Derecho de la Universidad Católica de Valparaíso XIX, Valparaíso, Chile, 1998).
[2] Declaración Universal de Derechos Humanos, Naciones Unidas. Disponible en: https://www.un.org/es/about-us/universal-declaration-of-human-rights (octubre, 2022).

Del mismo modo lo hace el artículo 16 del Pacto Internacional de Derechos Civiles y Políticos[3] y el artículo 3 de la Convención Americana sobre Derechos Humanos (Pacto San José de Costa Rica)[4]. La Corte Interamericana de Derechos Humanos (CIDH)[5] ha señalado que el derecho al reconocimiento de la personalidad jurídica implica la capacidad de ser titular de derechos (capacidad de goce) y de deberes.

En nuestro país, de acuerdo con Álvarez y Rueda (2022)[6], si bien "[l]a actual Constitución de la República de Chile no cuenta con una norma expresa que contemple el derecho a la identidad […], su existencia se comprende y emana de la dignidad humana, consagrada en su art. 1º, correspondiendo a los denominados en doctrina como derechos constitucionales implícitos". Por tanto, la identidad surge como un atributo del hecho de ser persona.

Por su parte, el Código Civil[7] (CC) chileno regula parte de esta materia en su Libro I (entre los art. 54 a 97) donde define a las personas naturales, su nacimiento y muerte, así como a algunos atributos de la personalidad, como el domicilio (Figueroa, 1998:21).

Con relación a la identificación de las personas, corresponde al Servicio de Registro Civil e Identificación establecer y registrar la **identidad civil** de las personas y otorgar los documentos oficiales que acreditan la identidad" (art. 4, N° 4, Ley Orgánica del Servicio de Registro Civil e Identificación[8].

El principal documento de acreditación de identidad es la cédula de identidad, cuyas características están descritas en la Resolución Exenta N° 861 del Ministerio de Justicia[9], y que pueden agruparse en dos áreas:

- Elementos de seguridad de la tarjeta física.
- Datos del titular inherentes (como la fotografía, huella digital, firma, sexo, fecha de nacimiento) y atribuidos (número de RUT, nombre y apellidos, entre otros).

El objeto de este documento (que además cuenta con un sistema electrónico de almacenamiento de datos, así como con un código QR) es verificar, tanto en el país como en el extranjero, la identidad de una persona registrada en Chile. Sin embargo, este documento no es actualmente efectivo en el mundo

[3] Pacto Internacional de Derechos Civiles y Políticos: Disponible en: https://bcn.cl/2ho0j (octubre, 2022).
[4] Convención Americana sobre Derechos Humanos, denominada "Pacto San José de Costa Rica". Disponible en: https://bcn.cl/2j3zn (octubre, 2022).
[5] En sentencia en caso Bámaca Velásquez Vs. Guatemala de 25 de noviembre de 2000. Disponible en: https://www.corteidh.or.cr/docs/casos/articulos/Seriec_70_esp.pdf (octubre, 2022).
[6] Álvarez, Rommy y Rueda, Natalia. "Right to Identity, Filiation and Surnames. Perspective from the Rights of Children and Women in the Chilean and Colombian Legal Systems". *Ius et Praxis* [online]. 2022, vol.28, n.2, pp.124-144. Disponible en: http://bcn.cl/38sp8 (octubre, 2022).
[7] El DFL N° 1 de 2000 del Ministerio de Justicia fija el texto refundido, coordinado y sistematizado del Código Civil. Disponible en: https://bcn.cl/2f6t3 (octubre, 2022).
[8] Ley N° 19.477, LOC del Servicio de Registro Civil e Identificación de Chile. Disponible en: https://bcn.cl/2l8lb (octubre, 2022).
[9] Resolución Exenta N° 861, de 02-Sep-2013, Ministerio de Justicia; Servicio de Registro Civil e Identificación, Señala características y fija menciones de la Cédula de Identidad Electrónica que emita el Servicio de Registro Civil E Identificación" (modificada por la Res. Ex. N°166, de 2014). Disponible en: https://bcn.cl/2x3ac (octubre, 2022).

digital, por lo que Chile (con experiencias como el desarrollo de la Clave Única[10]), así como gran parte del mundo, está asumiendo el desafío de desarrollar un sistema de identificación digital que permita el cumplimiento de los derechos humanos en los espacios virtuales.

III. Identidad digital e Internet

Según un informe de la Biblioteca del Congreso Nacional[11], Internet ha sido declarado por la Asamblea de las Naciones Unidas como un derecho humano inalienable, considerando a Internet como "un instrumento insustituible en la realización de una serie de derechos humanos y en la lucha contra la desigualdad". Este derecho ha sido reconocido por varios países a distintos niveles: México y Grecia lo han integrado en sus constituciones; Francia y Costa Rica han reconocido por jurisprudencia el acceso a Internet; Finlandia y Suiza han reconocido el acceso a Internet como un servicio universal.

La principal razón para este reconocimiento, en cualquiera de sus formas, es la ventaja que supone para los ciudadanos el acceso a la información digital de la red, relacionado directamente con la libertad de expresión y el artículo 19 de la Declaración Universal de Derechos Humanos[12], así como con los reportes del Relator Especial sobre la promoción y la protección del derecho a la libertad de opinión y de expresión de 2011[13].

Dicha Relatoría aprobó en 2017[14] una serie de estándares para una Internet libre, abierta e incluyente, los cuales se resumen en: garantizar una red libre y abierta principalmente en términos técnicos; garantizar el acceso, no sólo en infraestructura sino también en información para las personas, incluyendo la alfabetización digital y pluralidad lingüística; garantizar una gobernanza multisectorial, que respete la Internet como un espacio público; y garantizar la igualdad y no discriminación, promoviendo el acceso de grupos vulnerables de la población (este informe complementa el presentado en 2013 por la misma organización[15]).

Dadas las características rectoras de Internet (pública, abierta, multigobernada) y de la WWW, el uso de una identificación digital (ya sea de carácter fundacional, funcional o transaccional) debe centrarse en el respeto a los principios rectores antes mencionados.

1. Implicancias e impacto de la identidad digital

[10] "¿Qué es la Clave Única y para qué sirve?", Gobierno de Chile. Disponible en: http://bcn.cl/38skg (octubre, 2022).
[11] Informe BCN "Garantía de acceso a Internet en la legislación extranjera", elaborado por James Wilkins, diciembre de 2017. Disponible en: http://bcn.cl/29ft8 (octubre, 2022).
[12] Artículo 19, DUDH: "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión". Resolución 217 A (III) del 10 de diciembre de 1948, de la Asamblea General de las Naciones Unidas. Disponible en: https://dudh.es/19/ (octubre, 2022).
[13] Informes del Relator Especial sobre la promoción y la protección del derecho a la libertad de opinión y de expresión, en especial el y A/HRC/17/27 y el A/66/290. Oficina del Alto Comisionado de DDHH de las Naciones Unidas. Disponible en: http://bcn.cl/29fta (octubre, 2022).
[14] "Estándares para una Internet libre, abierta e incluyente", Comisión Interamericana de Derechos Humanos, OEA (2016). Disponible en: http://bcn.cl/29ftd (octubre, 2022).
[15] "Libertad de Expresión e Internet", Comisión Interamericana de Derechos Humanos, OEA (2013). Disponible en: http://bcn.cl/29fte (octubre, 2022).

De acuerdo con el Foro Económico Mundial (WEF, por sus siglas en inglés), "si se diseñan correctamente, las identidades digitales pueden proporcionar a los países un valor económico equivalente al 13% de su PIB" y, al mismo tiempo, ahorrar millones de horas de trabajo gubernamental y reducir costos para las empresas[16]. Sin embargo, la implementación técnica y regulatoria de sistemas de identidad digital comprende esfuerzos en múltiples niveles, enmarcados además dentro de los planes de gobierno electrónico de los países.

Según el Índice de Gobierno Digital de la OECD (2019)[17], la mayor parte de los países de la organización tienen mecanismos de identificación en línea, "con un 85% de países que poseen sistemas de identidad única y un 15% que prevén la posibilidad de que los individuos creen y gestionen diferentes identidades digitales para los servicios". Aunque el informe señala que "en 64% de los países, el sistema implantado es equivalente a los documentos de identidad nacionales físicos, con una autenticación más rudimentaria en el 21%", aun no logran un impacto significativo por la poca oferta de servicios existentes: sólo el 58% de los países tienen al menos la mitad de los servicios accesibles a través de estos sistemas.

En el mismo sentido, un informe del grupo de trabajo *(Digital Government Exchange (DGX) Digital Identity Working Group (DIWG))*, formado por ocho países en 2020, destacó la relevancia del acceso a servicios digitales para el manejo de la respuesta de cada país a la pandemia de COVID-19. En el futuro, las iniciativas de ID también podrían permitir la emisión de un certificado de vacunación contra el COVID-19 sólido, mutuamente reconocido e interoperable para permitir un mayor movimiento internacional, incluso para el comercio y los viajes. La ID también podría permitir la interoperabilidad internacional de las "cartera de datos" o "billeteras digitales" (*data wallet*), para que las personas puedan usar sus diversos atributos de identidad y credenciales a través de las fronteras, como su licencia de conducir digital, su nivel de educación y calificaciones y su información de salud[18].

En Chile, como se verá más adelante, más de 14 millones de personas tienen la **"Clave Única", sistema de identificación digital**[19] reconocido como firma digital simple a través de distintos actos administrativos, de los cuales más del 70% están disponibles digitalmente, y con la que se han realizado más de 44 millones de acceso válidos cada mes durante el primer semestre de 2022[20].

2. Qué es una identidad digital

Una identidad digital es, según el Foro Económico Mundial, un conjunto de atributos que se pueden agrupar en tres áreas[21]:

[16] "Digital Identity", World Economic Forum, 2022. Disponible en: http://bcn.cl/38skj (octubre, 2022).
[17] "Digital Government Index, 2019 results" octubre de 2020, OECD. P. 29. Disponible en: http://bcn.cl/38skl (octubre, 2022).
[18] Aldane, Jack. "Canada to launch public consultation on digital ID framework for federal public services". Global government forum. 17 agosto, 2022. Disponible en: http://bcn.cl/38spj (octubre, 2022).
[19] "Más de 13 millones de personas ya cuentan con su ClaveÚnica y 9 de cada 10 trámites se realizan por Internet", agosto de 2021, noticias, Gobierno de Chile. Disponible en: http://bcn.cl/38spq (octubre, 2022).
[20] "Cantidad de login OK con ClaveÚnica" último registro, junio de 2022. Datos.gob, Gobierno de Chile. Disponible en: Disponible en: http://bcn.cl/38spr (octubre, 2022).
[21] "A Blueprint for Digital Identity", The Role of Financial Institutions in Building Digital Identity. World Economic Forum, 2016. P. 41. Disponible en: http://bcn.cl/38spt (octubre, 2022).

- los inherentes, como el nombre, la edad, la huella digital o la fecha de nacimiento;
- los acumulados, como los datos médicos, gustos o datos de comportamiento (como los recolectados por los teléfonos celulares);
- y los atribuidos, como el número de teléfono, el correo electrónico o el número de identificación nacional.

Por otra parte, cuando se habla de ID existen dos dimensiones: la oficial, o de registro legal que está a cargo de las autoridades, y la personal, es decir, aquélla que depende del conocimiento de la red, así como de los riesgos que ésta conlleva, en una relación análoga a las relaciones personales[22].

En el caso de la **identidad digital como registro oficial**, se trata de la afirmación verificable y sin ambigüedades de la identidad de una persona. En términos técnicos, ésta ha sido definida por la Unión Internacional de Telecomunicaciones[23] (ITU, por sus siglas en inglés) como

> La representación de una entidad bajo la forma de uno o varios atributos que permiten distinguir suficientemente a la entidad o entidades dentro del contexto. A los efectos de la gestión de la identidad (IdM, sigla de "*Identification Management*"), se entiende que este término constituye una identidad contextual (subconjunto de atributos), es decir que la diversidad de atributos está limitada por un marco con fronteras definidas (el contexto) en el cual existe e interactúa la entidad.

En este marco, la ITU define que la **identificación digital** es la "representación digital de la información conocida acerca de un particular, un grupo o una organización concretos".

Pensado en la creación de entidades nacionales de registro digital, la ITU realizó un análisis en profundidad del alcance de la identificación digital, definiendo al menos tres categorías[24]:

- Fundacional, es decir, aquella referida a la identificación de una persona según documentos como el acta de nacimiento o el número de seguridad social;
- Funcional, destinada a asegurar la fiabilidad de los actores dentro de áreas como el transporte o la salud, y
- Transaccional, dedicada a la fiabilidad de transacciones comerciales.

Una vez definida la identidad en términos formales, ésta debe asociarse a mecanismos de gestión y comprobación que sean seguros y eficientes. Tanto en el mundo físico como en el digital, hoy en día se

[22] Giones-Vallls, Serrat-Brustenga, "La gestión de la identidad digital: una nueva habilidad informacional y digital", BiD: textos universitaris de biblioteconomia i documentació, n.24, juny 2010. Disponible en: http://dx.doi.org/10.1344/105.000001545 (octubre, 2022).
[23] Definición de Identidad (6.40) e Identidad digital (6.29), "Seguridad en el ciberespacio – Gestión de identidades. Términos y definiciones de referencia para la gestión de la identidad", SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD, ITU - Recomendación UIT-T X.1252. Disponible en: https://www.itu.int/rec/T-REC-X.1252-202104-I/es (octubre, 2022).
[24] International Telecommunication Union, ITU "Digital Identity Roadmap Guide". Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO) ITU, 2018. Disponible en: http://bcn.cl/29ft7 (octubre, 2022).

requieren sofisticados sistemas de comprobación que se ayudan de la tecnología para evitar falsificaciones.

En este marco, cabe mencionar dentro de las definiciones de identidad digital el concepto de **identidad digital soberana**: se trata de utilizar los datos personales digitales de la misma forma que hoy se utiliza el carné físico, en que éstos están concentrados en una tarjeta, y que no estén almacenados y gestionados por un tercero, sea público o privado[25].

3. Modelos de implementación de una identidad digital

Para su implementación, la ITU, en 2018 describió tres modelos de gobernanza para la creación de un Marco de Identidad Digital Nacional[26], donde:

a) El gobierno está directamente involucrado como Proveedor de Identidad. En este caso, el sistema público (además de su rol regulador) actúa como proveedor de identidad (*identity providers*), siendo responsable de todo el proceso, tanto en la entrega de credenciales como en la verificación de identidad. Es, además, un modelo centralizado en su gestión. Estonia es un caso exitoso de este modelo, donde incluso se ha extendido al sector privado.

b) El gobierno actúa sólo como Regulador y no participa como Proveedor de Identidad. En este modelo, el gobierno externaliza la entrega de credenciales y la verificación de identidad, e incorpora regulación específica para quienes entregarán las credenciales (los Proveedores de Identidad). Según señala el informe de la ITU, este modelo suele ser menos centralizado que el anterior, dado que se suele incorporar varios Proveedores de Identidad y no hay un registro único de datos.

c) El gobierno actúa como Regulador y también como Centro de intercambio de información entre Proveedores. Este modelo es similar al anterior, pues externaliza la provisión de credenciales, pero el gobierno toma el rol de intermediario entre los Proveedores de Identidad y los Proveedores de Servicios: un agente público es el encargado de dirigir la consulta desde el usuario al proveedor de identidad, actuando como *broker* o certificador. Según la ITU, este modelo ofrece la ventaja para las personas que el ente público queda en medio de quien pregunta y quien contesta: así ni el Proveedor de Servicios ni el Proveedor de Identidad pueden tener datos del otro, favoreciendo la privacidad del usuario. El ejemplo citado por la fuente es el modelo británico *GOV.UK Verify*[27].

Cada país puede establecer distintos objetivos para la creación de una ID que incluya una o todas las categorías anteriores. Igualmente, las razones que impulsan estos objetivos pueden ser diversas, desde mejorar la eficiencia de los servicios públicos hasta mantener un mayor control de la población. Así, según el estudio, los objetivos para implementar nuevos o mejores sistemas de identificación electrónica varían:

---

[25] "A gentle introduction to self-sovereign identity", Bits on blocks, mayo 2017. Disponible en: http://bcn.cl/38sq0 (octubre, 2022).
[26] Ibid.
[27] "Guidance, GOV.UK Verify (Updated 28 April 2022)", UK Government. Disponible en: http://bcn.cl/38sq1 (octubre, 2022).

- Reino Unido: el objetivo principal fue aumentar el acceso de los ciudadanos a servicios públicos, así como mejorar su eficiencia y eficacia[28].
- India: eliminar las duplicidades de identidad en los servicios públicos, así como incluir a más personas en el sistema, ya que muchos habitantes (especialmente de estratos socioeconómicos pobres) no pueden acceder a servicios por no contar con una identificación fiable[29].
- Estonia: siendo una de las naciones más avanzadas en el desarrollo de un gobierno digital, el objetivo es avanzar en la sociedad digital con sistemas de identificación eficientes en el mundo físico y en el mundo digital[30].

IV. Chile: identidad digital y Clave Única

Nuestro país cuenta con un sistema de identificación a cargo del Servicio de Registro Civil e Identificación[31], así como con un sistema de identificación digital llamado "Clave Única" (CU), a cargo de la Dirección de Gobierno Digital del Ministerio Secretaría General de la Presidencia de la República[32].

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) presentó en 2019 un completo informe sobre "Identidad Digital en Chile", comparando la situación del país con trece naciones miembros y no miembros. En él se propone, además de marcos de acción para el fortalecimiento de una ID, la priorización de la Clave Única para dotar a la ciudadanía de un control sobre sus datos, así como de un sistema que permita acceder no sólo a servicios públicos sino también privados.

Según la OCDE, Chile ya cuenta con un servicio eficiente y maduro de identificación personal (a través del carné de identidad entregado por el Servicio de Registro Civil e Identificación), el cual permite luego obtener la Clave Única. Sin embargo, entre las recomendaciones generales está el integrar ambos sistemas a la hora de obtener credenciales de identificación, simplificando su proceso de obtención para las personas[33], así como tender a la convergencia y no competencia con otros servicios de identificación digital existentes en el país.

También sugiere estudiar sistemas de validación de datos "sin contacto" desde el carné de identidad (como los que han implementado España, Uruguay o Italia), lo que permiten interactuar con tecnologías NFC (*Near Field Communication* o Comunicación por Campos Cercanos, en español[34]) que están integradas en los teléfonos celulares de uso común. Esto permitiría disminuir costos en dispositivos exclusivos para validación.

---

[28] "Digital Identity Roadmap Guide". ITU, pp. 55.
[29] ITU, Op. cit., pp. 47.
[30] ITU, Op. cit., pp. 45.
[31] Numeral 4, art. 4° sobre funciones del Servicio, Ley 19.477 que "aprueba ley orgánica del Servicio de Registro Civil e Identificación", Ley Chile, Biblioteca del Congreso Nacional. Disponible en: https://bcn.cl/2l8lb (octubre, 2022).
[32] Art. 3° Ley 18.993 que crea Ministerio Secretaría General de la Presidencia de la República. Disponible en: https://bcn.cl/2ramg (octubre, 2022).
[33] "Digital Government in Chile – Digital Identity", OECD Digital Government Studies, OECD. P. 9 (2019). Disponible en: https://doi.org/10.1787/9ecba35e-en (octubre, 2022).
[34] "¿Qué es el NFC en un celular y para qué sirve?", blog Movistar, marzo 2022. Disponible en: http://bcn.cl/38sq4 (octubre, 2022).

El informe, de casi un centenar de páginas, contextualiza los avances en esta materia y orienta sobre las medidas a seguir. Entre otras, propone:

- Fortalecer el apoyo político y financiero a la División de Gobierno Digital y al Servicio de Registro Civil, para convertir la Clave Única en un servicio respetado y confiable por la ciudadanía.
- Potenciar una política pública para la ID que considere la adopción de este mecanismo por parte de los servicios públicos, modernizando tecnologías, capacitando y difundiendo su uso.
- Integrar la ID en la Política y la Estrategia Nacional de Seguridad Digital.
- Mejorar la gobernanza de la ID, fortaleciendo la relación entre el Registro Civil y la División de Gobierno Digital, con un monitoreo constante del Comité de Modernización del Estado y la posible inclusión de un responsable de alto nivel que esté atento a una buena integración entre quien provee la identidad (Servicio de Registro Civil) y quien es responsable del éxito de la agenda de transformación digital (División de Gobierno Digital). Para la OCDE, esta división de responsabilidades es un eslabón débil dentro de la gobernanza actual.
- Establecer un sistema de ID que permita también que la ciudadanía acceda de forma segura a servicios privados. De hecho, destaca que los desarrollos en identidad digital existentes permitirían ampliarlos al sector privado en vez de ver la opción de crear otro sistema para generar identidades[35].
- La organización sugiere, además, que el país necesita establecer un sistema de gobernanza para la futura relación entre el sector público y el privado en la entrega de un sistema de ID efectivo.

En relación con esta última recomendación, la OCDE señala que debería darse más apoyo político y financiero a las entidades encargadas de la ID (Servicio de Registro Civil y la División de Gobierno Digital), de modo que la Clave Única sea, para los privados, un servicio tan confiable y respetado como lo es para los ciudadanos. Para ello, la OCDE sugiere que la inversión debiera incluir un aumento en la capacidad de gestión para coordinar y estimular la adopción, así como invertir en documentación técnica y en mejorar la incorporación dentro del aparato público, así como capacidades sobre cómo determinar los beneficios para explican el retorno de la inversión.

Para la OCDE, Chile debe seguir trabajando en fortalecer la ID por medio de la Clave Única, de manera que, en el futuro, ésta cuente con más funcionalidades a disposición de las personas, tales como una billetera digital, entre otros.

En términos legales, la Clave Única no está contenida en una ley, por lo que Chile en rigor no cuenta con una legislación que homologue los sistemas físicos de identidad (como el carné de identidad o el pasaporte) a sistemas digitales.

Sin embargo, la CU es el sistema de identificación que el Gobierno está implementando como ID y que, al mes de agosto de 2021, ya era usado por más de 13 millones de personas[36]. Este sistema es reconocido como firma digital simple o como mecanismo de autenticación a través de distintos actos

[35] OECD. P. 9 (2019).
[36] "Más de 13 millones de personas ya cuentan con su ClaveÚnica y 9 de cada 10 trámites se realizan por Internet", agosto de 2021, noticias, Gobierno de Chile. Disponible en: http://bcn.cl/38spq (octubre, 2022).

administrativos[37] y se ha convertido en la práctica en el instrumento oficial de identificación para trámites digitales. Según el Gobierno, la Clave Única "es una iniciativa que busca proveer a los ciudadanos de una Identidad Electrónica Única (RUN y contraseña) para la realización de trámites en línea del Estado"[38], de los cuales más del 70% están disponibles digitalmente.

Las principales referencias normativas de la CU (llamada en sus inicios "clave Internet" para usuarios del Servicio de Registro Civil) son la "Circular N°1, de 18 de junio de 2010, de la Dirección Nacional de SRCeI a los Directores Regionales de dicha institución", en que se instruye a las oficinas sobre el proceso de enrolamiento; y el "Instructivo Presidencial N° 002, de 17 de agosto de 2012, que imparte instrucciones sobre simplificación y eliminación de trámites", la cual insta a su uso para validación de trámites electrónicos (ya como Clave Única) y establece que la Unidad de Modernización del Estado y Gobierno Digital sería la encargada de coordinar, entregar asistencia técnica y acompañar la implementación de los procesos de eliminación o simplificación de trámites públicos pudiendo utilizar la CU como instrumento.

Con todo, la Clave Única es actualmente el instrumento nacional de identificación digital más avanzado y extendido en Chile, y está en tramitación la Norma Técnica de Autenticación que establecería la CU como el mecanismo oficial de autenticación para acceder a servicios digitales del Estado[39], según lo dispuesto en la Ley N° 21.180 de Transformación Digital del Estado.

V. Regulación e implementación de la identidad digital en la experiencia extranjera

Los resultados de la investigación en la que se basa este informe muestran que la regulación de identidad digital (en Chile y otros países) se encuentra contenida principalmente en reglamentos y decretos, los que promueven y soportan los distintos desarrollos tecnológicos que están dando forma a los instrumentos de ID. En este sentido, se describen a continuación el reglamento de sistemas de identificación electrónica de la Unión Europea, así como los avances de Canadá y Chile en identificación electrónica.

En 2020, ocho países (Australia, Canadá, Finlandia, Israel, Nueva Zelanda, Singapur, Países Bajos y Reino Unido), presidido por la Agencia de Transformación Digital de Australia y con el Banco Mundial como observador, formaron un grupo de trabajo *(Digital Government Exchange (DGX) Digital Identity Working Group (DIWG)*), en pos de la identificación digital[40].

[37] Resolución N° 138 exenta, "Aprueba instructivo del Sistema de tramitación electrónica de los derechos de propiedad industrial cuyo registro es administrado por el Instituto Nacional de Propiedad Industrial", Ministerio de Economía, mayo de 2022. Disponible en: https://bcn.cl/38sjw (octubre, 2022).
[38] "¿Qué es la Clave Única"? Preguntas frecuentes, Clave Única, Gobierno de Chile. Disponible en: https://claveunica.gob.cl/preguntas-frecuentes (octubre, 2022).
[39] "Informe tercera consulta pública Ley N° 21.180, de Transformación Digital del Estado: Norma Técnica de Autenticación", Dirección de Gobierno Digital, febrero, 2022. Disponible en: http://bcn.cl/38sq6 (octubre, 2022).
[40] Aldane, Jack, "Canada to launch public consultation on digital ID framework for federal public services". Global government forum. 17 agosto, 2022. Disponible en: http://bcn.cl/38spj (octubre, 2022).

El grupo redactó un conjunto de principios para apoyar el desarrollo de sistemas e infraestructura de identificación digital interoperables y mutuamente reconocidos, y tiene como objetivo mejorar los acuerdos comerciales en busca de la recuperación económica posterior a COVID[41].

Sin embargo, los países señalados han adoptado diferentes enfoques sobre cómo implementar sus sistemas de ID. Por ejemplo, el programa *One Login* del Reino Unido, permitirá a los usuarios crear una cuenta del gobierno para acceder a los servicios en línea o a través de una aplicación. El programa representaría un cambio en el enfoque del gobierno, cuyo esfuerzo anterior (*GOV.UK Verify*) consistía en una plataforma web que permitía a las personas registrarse para probar su identidad y cuya prueba era luego aceptada por los departamentos y agencias gubernamentales para acceder a los servicios. El sistema estaba destinado a brindar seguridad a las personas para que se registraran en servicios tales como beneficios estatales, pero sufrió una baja aceptación[42].

Fuera de Estonia, las diferentes naciones europeas se encuentran en diferentes etapas de desarrollo[43]:

- El programa de identidades digitales del gobierno alemán ahora permite que los ciudadanos alemanes puedan guardar su prueba de ID, de su tarjeta de identificación alemana, directamente en su teléfono inteligente.

- La agencia del gobierno francés, *Agence Nationale des Titres Sécurisés* (Agencia Nacional para Documentos Seguros), seleccionó a la firma de identificación digital IDEMIA para trabajar en su programa nacional de identificación digital, *France Identité Numérique*.

Los planes nacionales en los países europeos también se acoplarán al marco de identidad digital para ciudadanos de la Comisión Europea, y el gobierno alemán afirma que “nuestro objetivo es utilizar soluciones de identificación interoperables de los estados miembros de la UE para establecer una alternativa europea a los servicios de identificación privados no europeos”[44].

Por otra parte, la estrategia digital del gobierno de Canadá incluye un esfuerzo continuo para introducir identidades digitales seguras para los ciudadanos[45]. En agosto de 2022, Canadá lanzó el programa *Digital Ambition 2022,* cuyas metas de modernización digital contenidas contemplan una consulta pública sobre un futuro marco del uso de ID en los servicios públicos federales[46]. El objetivo del gobierno canadiense es desarrollar un sistema de credenciales digitales para todas las provincias de ese país, así como armonizar sus sistemas de ID con otras naciones.

El gobierno federal de EE. UU. tiene un programa para un servicio de verificación de ID en tiempo real[47]. En junio de 2021 se ingresó al Congreso de ese país el proyecto de ley *H.R.4258 - Improving Digital*

[41] “Digital Identity in response to COVID-19. DGX Digital Identity Working Group”, Digital Transformation Agency, Australia 2022. Disponible en: http://bcn.cl/38sqb (octubre, 2022).
[42] Digital Transformation Agency, Australia 2022.
[43] Digital Transformation Agency, Australia 2022.
[44] Digital Transformation Agency, Australia 2022.
[45] Digital Transformation Agency, Australia 2022.
[46] Digital Ambition, Government of Canada. Disponible en: http://bcn.cl/38sqc (octubre, 2022).
[47] Digital Transformation Agency, Australia 2022.

Identity Act of 2021, cuyo objeto es desarrollar un sistema de identificación digital de nivel supraestatal. En junio de este año fue visto por el Comité de Supervisión y Reforma, pero aún no ha sido votado en primer trámite[48]. Con el mismo nombre, se ingresó en julio de 2022, pero en el Senado, un proyecto de ley de similares características[49].

El sistema australiano de ID fue lanzado en 2015 como parte de una política gubernamental. Su implementación estuvo a cargo de la Agencia de Transformación Digital de ese país, hasta mayo de 2021, momento en que pasó a manos de agencia de servicios sociales de ese país, *Services Australia*. Según información del Parlamento australiano, el sistema ha recibido críticas técnicas, así como oposición política, dado lo cual el borrador del proyecto que circuló durante 2021 aún no ha sido ingresado a trámite[50]. Actualmente, el proyecto de ley está a la espera de ser presentado al Parlamento luego de un proceso de consulta desarrollado en octubre de 2021[51].

Sin embargo, el sistema está en funcionamiento con cerca de 80 servicios públicos accesibles vía ID. El sistema es voluntario, incluye parámetros biométricos de identificación, y cuenta con un proveedor público (llamado *MyGovID*[52]) y otro privado (*Digital iD*, operada por Australia Post)[53].

Por último, el desarrollo de un sistema de ID está contenido en la Estrategia para un Servicio Público Digital del gobierno de Nueva Zelanda, con legislación planeada para crear un marco de confianza de servicios digitales después de que los ministros aprobaran la inversión en el sistema en junio de 2021[54].

A continuación, se describen los avances regulatorios y legislativos de la Unión Europea, España, Estonia e India, por cuanto estos países cuentan con normas legales que asocian la identidad física con la identidad digital.

1. Unión Europea (UE)

En 2014, el Parlamento Europeo aprobó el Reglamento (UE) N° 910/2014[55] (obligatorio para todos los Estados miembros), que normaliza y regula los distintos sistemas de identificación electrónica usados en los países de la UE, también conocido como Reglamento eIDAS de 2014. Luego de un período de implementación, este reglamento obliga a que los sistemas de identificación electrónica implementados por los miembros de la Unión sean reconocidos en el resto de los países[56].

---

[48] H.R. 4258 - Improving Digital Identity Act of 2021, Congress of United States of America. Disponible en: http://bcn.cl/38sxj (octubre, 2022).
[49] S. 4528 - Improving Digital Identity Act of 2022, Congress of United States of America. Disponible en: http://bcn.cl/38sxm (octubre, 2022).
[50] Hamilton, P. "Digital Identity system", mayo 2022, Parliament of Australia. Disponible en: http://bcn.cl/38sxo (octubre, 2022).
[51] Consultation, Digital Identity, Australian government. Disponible en: http://bcn.cl/38sxt (octubre, 2022).
[52] myGovID, Australian Government. Disponible en: https://www.mygovid.gov.au/ (octubre, 2022).
[53] The System. Digital Identity, Australian Government. Disponible en: http://bcn.cl/38sxw (octubre, 2022).
[54] Digital Transformation Agency, Australia 2022.
[55] REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. Disponible en: http://bcn.cl/29ftf (octubre, 2022).
[56] Identificación electrónica, Mercado único digital. Com. Europea. Disponible en: http://bcn.cl/29ftg (octubre, 2022).

Actualmente se está discutiendo una modificación al reglamento citado (a la fecha de cierre de este informe, en primera lectura de Parlamento Europeo desde finales de 2021[57]), propuesta por la Comisión Europea[58] y que debería haber estado en pleno funcionamiento en septiembre de 2022.

El nuevo reglamento permitirá el uso transfronterizo (dentro de la Unión) de sistemas de identidad digital con la misma validez que los sistemas de identidad físicos. Entre otros avances, se espera que el nuevo reglamento permita que al menos el 80% de los ciudadanos de la UE puedan utilizar una identidad digital al año 2030, algo que a la fecha sólo un 59% de los residentes puede hacer de forma segura.

Una de las claves para la implementación de la ID es el desarrollo de "Servicios electrónicos de confianza", que son sistemas de emisión o de validación de certificados o firmas electrónicas. Éstos deben estar autorizados por el Estado[59] al que pertenecen. En general, se trata de empresas de servicios que entregan certificados electrónicos de firma o de sello electrónico, entregan sellos electrónicos de tiempo, así como servicios de validación y conservación de firmas y sellos electrónicos.

Además, el nuevo reglamento destaca por el control de datos por parte de los usuarios. Tal como señala la web de la UE, la "identidad digital europea les permitirán elegir qué aspectos de su identidad, datos y certificados comparten con terceros y mantenerse al corriente de lo que con ellos se haga. Este control por los usuarios garantiza que solo se comparta aquella información que realmente deba compartirse"[60].

Según la OCDE[61], tanto la "Red de gobierno electrónico de América Latina y el Caribe" (Red GEALC[62]) como el Foro de Cooperación Económica Asia Pacífico (APEC[63]) están considerando desarrollar un sistema de ID similar al que está implementando la Unión Europea mediante el reglamento eIDAS[64].

a) Estonia

Estonia tiene un modelo de gobernanza en que es el Estado quien provee la ID, iniciado en 2002, y que actualmente abarca a casi toda la población, de aproximadamente 1,3 millones de personas.

---

[57] Proceso de tramitación del Documento "52021PC0281": Procedure 2021/0136/COD COM (2021) 281: Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea". Eur-Lex, Unión Europea. Disponible en: http://bcn.cl/38sy0 (octubre, 2022).

[58] "La Comisión propone una identidad digital segura y de confianza para todos los europeos", comunicado de prensa, Comisión Europea, junio, 2021. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/IP_21_2663 (octubre, 2022).

[59] A modo de ejemplo, se puede consultar el sitio "Prestadores de servicios electrónicos de confianza", de la Secretaría de Estado para el Avance Digital del gobierno Español. Disponible en: http://bcn.cl/29fth (octubre, 2022).

[60] Comisión Europea, 2021, Op. cit.

[61] OECD (2019), P. 16, Op. cit.

[62] Red de gobierno electrónico de América Latina y el Caribe. Disponible en: https://www.redgealc.org/ (octubre, 2022).

[63] Foro de Cooperación Económica Asia Pacífico. Disponible en: https://www.apec.org/ (octubre, 2022).

[64] Presentación de C. Gómez, "eIDAS – Construyendo el futuro digital", Red GEALC – BID Taller Alianza del Pacífico y Mercosur de firma e identidad digital transfronteriza, abril, 2020. Disponible en: http://bcn.cl/38sy6 (octubre, 2022).

El sistema estonio de identidad e identidad digital están bajo el marco legal de la "Ley de Documentos de Identidad"[65] de 2018 (originalmente de 1999) y la "Ley de Identificación Electrónica y Servicios de Confianza para Transacciones Electrónicas" de 2016[66]. Ambas normas han sido modificadas para incluir el reglamento eIDAS ya mencionado.

Cabe destacar que en lo relativo a la identificación digital, la primera ley citada establece, en el numeral 3 del artículo 9°, los datos personales que pueden ingresarse en un documento de identidad, entre los cuales está una modificación posterior que integra datos electrónicos de identificación: nombre; fecha y lugar de nacimiento; código de identificación personal; foto o imagen facial; sexo; ciudadanía; imágenes de huellas dactilares; firma o imagen de firma; imágenes de iris; color de cabello; y otros datos personales si así lo prescribe un tratado, ley u otra legislación de aplicación general establecida sobre la base de los mismos.

Los numerales 4 y 5 de este artículo establecen que:

> (4) Los datos especificados en el inciso (3) de esta sección también pueden ingresarse digitalmente en un documento.
>
> (5) Se podrá ingresar información que permita la identificación de una persona digitalmente, incluyendo una clave criptográfica que permita la identificación digital y el respectivo certificado, e información que permita la firma digital, incluyendo una clave criptográfica que permita la firma digital y el respectivo certificado, y otros datos digitales en un documento. La lista de información prevista en este inciso será establecida por reglamento del ministro responsable del área".

Dado que el inciso (3) es el "código de identificación personal", se utiliza éste para incluir dentro de los datos personales del documento de identidad aquellos datos digitales de identificación. Igualmente, esta ley también regula el tratamiento de datos biométricos, fotografías y certificados que deban ser ingresados en el documento de identidad.

Por su parte, la Ley de Identificación Electrónica y Servicios de Confianza para Transacciones Electrónicas integra al ordenamiento jurídico estonio el Reglamento de la Unión Europea mencionado anteriormente.

b) España

Los artículos 6 y 7 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza[67] (que deroga el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma

[65] "Isikut tõendavate dokumentide seadus" Vastu võetud 15.02.1999 - RT I 1999, 25, 365 jõustumine 01.01.2000. Disponible (en inglés) en: http://bcn.cl/38sy9 (octubre, 2022).
[66] Ley de Identificación Electrónica y Servicios de Confianza para Transacciones Electrónicas. Disponible (en inglés) en: http://bcn.cl/38sya (octubre, 2022).
[67] Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Disponible en: https://www.boe.es/eli/es/l/2020/11/11/6/con (octubre, 2022).

electrónica[68]) tiene por objeto adaptar la legislación de ese país al eIDAS y, entre otras modificaciones, establece que la firma electrónica será sólo para personas naturales.

En lo relativo a la ID señala, en su artículo 6, que:

> 1. La **identidad del titular en los certificados cualificados** se consignará de la siguiente forma:
>
> a) En el supuesto de certificados de firma electrónica y de autenticación de sitio web expedidos a personas físicas, por su nombre y apellidos y su número de Documento Nacional de Identidad, número de identidad de extranjero o número de identificación fiscal, o a través de un pseudónimo que conste como tal de manera inequívoca. Los números anteriores podrán sustituirse por otro código o número identificativo únicamente en caso de que el titular carezca de todos ellos por causa lícita, siempre que le identifique de forma unívoca y permanente en el tiempo.
>
> b) En el supuesto de certificados de sello electrónico y de autenticación de sitio web expedidos a personas jurídicas, por su denominación o razón social y su número de identificación fiscal. En defecto de éste, deberá indicarse otro código identificativo que le identifique de forma unívoca y permanente en el tiempo, tal como se recoja en los registros oficiales.
>
> 2. Si los certificados admiten una relación de representación incluirán la identidad de la persona física o jurídica representada en las formas previstas en el apartado anterior, así como una indicación del documento, público si resulta exigible, que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales.

Por su parte, el artículo 7, numerales 1 a 3, describen la comprobación de identidad de la siguiente manera:

> Artículo 7. Comprobación de la identidad y otras circunstancias de los solicitantes de un certificado cualificado.
>
> 1. La identificación de la persona física que solicite un certificado cualificado exigirá su personación ante los encargados de verificarla y se acreditará mediante el Documento Nacional de Identidad, pasaporte u otros medios admitidos en Derecho. Podrá prescindirse de la personación de la persona física que solicite un certificado cualificado si su firma en la solicitud de expedición de un certificado cualificado ha sido legitimada en presencia notarial.
>
> 2. Reglamentariamente, mediante Orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, se determinarán otras condiciones y requisitos técnicos de **verificación de la identidad a distancia** y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación como videoconferencia o vídeo-identificación que aporten una seguridad equivalente en términos de

[68] Real Decreto 1553/2005, de 23 de diciembre. Disponible en: http://bcn.cl/38syf (octubre, 2022).

> fiabilidad a la presencia física según su evaluación por un organismo de evaluación de la conformidad. La determinación de dichas condiciones y requisitos técnicos se realizará a partir de los estándares que, en su caso, hayan sido determinados a nivel comunitario.
>
> Serán considerados métodos de identificación reconocidos a escala nacional, a los efectos de lo previsto en el presente apartado, aquellos que aporten una seguridad equivalente en términos de fiabilidad a la presencia física y cuya equivalencia en el nivel de seguridad sea certificada por un organismo de evaluación de la conformidad, de acuerdo con lo previsto en la normativa en materia de servicios electrónicos de confianza.
>
> 3. La forma en que se ha procedido a identificar a la persona física solicitante podrá constar en el certificado. En otro caso, los prestadores de servicios de confianza deberán colaborar entre sí para determinar cuándo se produjo la última personación.

Según lo señalado, para la obtención de un certificado que acredite identidad digital, quien lo solicite debe presentarse personalmente o vía solicitud autorizada notarialmente.

2. India

Otro país que ha integrado en su legislación la identidad digital es India. "Aadhaar" es tanto el nombre del sistema electrónico como de la Ley, de 2016, de "Entrega selectiva de subsidios, beneficios y servicios, financieros o de otro tipo[69]".

En lo técnico, el Aadhaar[70] es un documento de identidad digital autentificable en línea, que consiste esencialmente en un número aleatorio de 12 dígitos generado tras la "deduplicación" (revisión y eliminación de datos informáticos repetidos de una base de datos) de datos biométricos (huella dactilar e iris) de quienes voluntariamente soliciten enrolarse.

Tal como señala el título de la Ley, la ventaja para quienes soliciten este documento es la entrega de beneficios, así como la obtención vía web de servicios estatales.

Según el citado informe de la ITU, el primer número UID se emitió el 29 de septiembre de 2010, y a 2020 se habían emitido números Aadhaar al 90% de los residentes de la India, más de 1.300 millones de personas. Con ello, es actualmente el sistema de autentificación digital más extendido del mundo.

En lo regulatorio, la Ley Aadhaar (que es en sí una modificación de la *National Identification Authority of India Act, 2010*[71]) instruye a la Autoridad de Identificación Única de la India para la administración y entrega del documento de identificación (que es esencialmente un carné de identidad) solicitando los siguientes datos:

---

[69] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, India Government. Disponible en: http://bcn.cl/38syg (octubre, 2022).
[70] "Unique Identification Authority of India", Gobierno de India. Disponible en: https://uidai.gov.in/en/ (octubre, 2022).
[71] "The Aadhaar Bill, 2016 - What's New?", The Internet Society, India. Disponible en: http://bcn.cl/38syp)octubre, 2022).

a) Información biométrica: la fotografía, la huella dactilar, el escáner de iris o cualquier otro atributo biológico de una persona que se especifique en la normativa (art. 2; letra g, Ley Aadhaar).

b) Información demográfica: información relativa al nombre, la fecha de fecha de nacimiento, dirección y otros datos pertinentes de una persona, según se especifique para la expedición de un número Aadhaar, pero no incluye la raza, la religión, la casta, la tribu, el origen étnico, la lengua, los registros de derechos, los ingresos o el historial médico (art. 2; letra k, Ley Aadhaar).

Sobre el uso de datos personales, el art. 32 señala:

> 32. (1) La Autoridad mantendrá los registros de autenticación de la manera y durante el período que se especifique en los reglamentos.
>
> (2) Todo titular de un número Aadhaar tendrá derecho a obtener su registro de autenticación de la manera que se especifique en los reglamentos.
>
> (3) La Autoridad no podrá, ni por sí misma ni a través de ninguna entidad bajo su control, recoger, conservar o mantener ninguna información sobre el propósito de la autenticación.