REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 6 NÚM. 1 (2017) • PÁGS. 67-91 • DOI 10.5354/0719-2584.2017.45825
RECIBIDO: 4/5/2017 • APROBADO: 29/5/2017 • PUBLICADO: 30/6/2017

DOCTRINA

La biometría en Chile y sus riesgos

Biometrics in Chile and its risk

Romina Garrido Iglesias y Sebastián Becker Castellaro

Fundación Datos Protegidos, Chile

RESUMEN El presente trabajo realiza una descripción sobre la biometría y cómo funciona al verificar e identificar a las personas. Junto con ello, realiza un análisis sobre la naturaleza jurídica de la biometría a través de pautas de derecho comparado, destacando que se trata de datos sensibles. Debido a lo anterior, se fijan principios para su tratamiento y se exponen los riesgos de la expansión de la biometría para los derechos humanos.

PALABRAS CLAVE Biometría, datos sensibles, protección de datos personales, riesgos, derechos humanos.

ABSTRACT This current paper makes a description about biometrics and how it works to verify and identify people. Besides that, it makes an analysis about the legal nature of biometrics through comparative law standards, highlighting that biometrics are sensitive data. In consequence, it states principles for their treatment and exposes the risks of the expansion of biometrics for human rights.

KEYWORDS Biometrics, sensitive data, data protection, risks, human rights.

Introducción

La forma en que se desenvuelven las personas en nuestra sociedad digital es a través de un permanente intercambio de información sobre sí mismas. Lo anterior implica que existirán datos personales que necesariamente serán conocidos por otros, es decir, empresas, agencias de marketing, organismos públicos y más podrán saber cuál es el aspecto de mi rostro, cuáles son mis preferencias al vestirme e incluso aspectos más sensibles, como de qué etnia provengo, mi posición política o si padezco o no de alguna enfermedad. Sin embargo, la necesidad del flujo libre de datos (*data flow*), sea

para la vida pública o para ejecutar transacciones y obtener productos y servicios, no puede implicar la pérdida de control del titular de los datos sobre su tratamiento ni de su derecho a ser informado sobre sus eventuales usos; existe un reconocimiento en distintos estamentos legales nacionales e internacionales a la autodeterminación informativa sobre los datos personales, que garantiza que los individuos establezcan por sí mismos la divulgación y utilización (o no) de los datos referentes a su persona (Herrán Ortiz, 2003: 14). Para ciertos tipos de datos personales, la normativa de protección de datos ha fijado condiciones más estrictas para su tratamiento, atendido su especial contenido. La necesidad de reconocer y otorgar mayor protección a ciertos datos surge justamente de que, si son incorrectamente manipulados, entrañarían un grave riesgo para los derechos de las personas. Este tipo de datos generalmente corresponde a características especiales de cada individuo que nos distinguen a unos de otros, y cuya vulneración o conocimiento por terceras personas puede causar un daño difícil de reparar, o bien dar lugar a situaciones graves de discriminación, lo que se debe avizorar y prevenir.

En la normativa chilena —y también en derecho comparado— el concepto que define los datos relativos a cualquier información concerniente a personas naturales que permite identificar o hacer identificable su identidad es el de «dato personal».[1] En el caso de que estos datos se refieran a características físicas o morales de una persona, o bien que develen hábitos personales, éstos serán considerados como «datos sensibles».[2]

De este modo, podemos entrar al tema que convoca el presente trabajo: la biometría y sus riesgos. La motivación del mismo es entender cómo la biometría se regula en la normativa chilena, considerando que no existe ninguna mención explícita a ella en la Ley 19.628 sobre Protección a la Vida Privada. Sumado a lo anterior, busca develar los riesgos que implica el uso de la biometría de cara a los derechos humanos de las personas, especialmente la privacidad e igualdad en derechos. El trabajo se divide en cuatro partes: primero se expone brevemente sobre la biometría y sus usos; segundo, se revisa la regulación comparada y se analiza si es posible encuadrar los conceptos doctrinarios y comparados de la biometría en el ordenamiento jurídico chileno; tercero, y teniendo claro lo anterior, se analizan los riesgos a los derechos que puede ocasionar la biometría, para finalmente presentar las conclusiones al respecto.

La biometría y sus usos

La biometría ya ha sido definida y abordada en el paradigma de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), el que propició una reflexión

1. Véase el artículo 2 letra f) de la Ley 19.628 (Ley de Protección a la Vida Privada).
2. Véase el artículo 2 letra g) de la Ley 19.628 (Ley de Protección a la Vida Privada).

en cuanto a su regulación y los derechos de las personas. De esta forma, OCDE ha señalado que la biometría consiste en características únicas y medibles de rasgos en los seres humanos que sirven para automáticamente reconocer o verificar una identidad (OCDE, 2004a: 24). La relevancia de la biometría hoy en día está dada por el gran aumento de sistemas automatizados para identificar a las personas, ya sea por los gobiernos o las empresas privadas. En la misma línea, otros autores agregan más elementos a considerar en la biometría: no sólo se trataría de características o rasgos físicos, sino además de comportamientos que permitirían una identificación. Así las cosas, en el presente trabajo se entenderá la biometría como aquellos mecanismos automatizados para determinar la identidad de una persona basada en sus aspectos fisiológicos o conductuales (Korja, 2006: 199).[3]

Los datos biométricos tienen dos características fundamentales:

- Son obtenidos por tratamientos automatizados para verificar o determinar la identidad de personas a través de características fisiológicas o conductuales (Korja, 2006: 199).
- Reconocen características fisiológicas, físicas, conductuales o psicológicas: las características fisiológicas o físicas se definen como medidas o mediciones a parte o partes del cuerpo humano (escáner al iris o huellas dactilares, patrones geométricos del rostro u orejas, reconocimiento de voz, etcétera). Por su parte, las características conductuales o psicológicas se basan en acciones derivadas directa o indirectamente de las características del cuerpo humano (Korja, 2006: 199).

Junto con lo anterior, para que los datos biométricos puedan cumplir la función de identificar a las personas, o bien autentificarlas, deben cumplir con las siguientes características:

- Medibles: la facilidad por la cual es posible leer el dato.
- Robustos: en cuanto a cómo el dato individual va modificándose con el tiempo.
- Aceptables: deben mostrar aspectos positivos del individuo.
- Universales: que toda población tenga aquel dato que se extrae del individuo.
- Distintivos: debe mostrar una gran variabilidad sobre el resto de la población para asegurar la individualidad del dato en cuestión (Korja, 2006: 200).

Así las cosas, los datos biométricos pueden clasificarse en tres grandes grupos:

- Datos estáticos: aquéllos que se extraen de las características físicas de cual-

3. En el mismo sentido se ha referido la Asociación por los Derechos Civiles (2015: 2).

quier individuo. Suelen ser huellas dactilares, imagen del rostro, iris de los ojos, etcétera, y se recolectan a través de programas de reconocimiento facial; por ejemplo, es posible identificar a una persona de acuerdo a las distancias que hay entre su nariz, su boca y sus ojos, y con ellas generar modelos geométricos de rostro para la identificación posterior.

- Datos dinámicos: aquéllos que se concentran en el comportamiento, forma de caminar, manera en la que firma o utilización del teclado de un computador, entre otras. Estos mecanismos detectan patrones de conducta para vincularlas con una persona en particular.
- Datos mixtos: Combina ambas técnicas ya mencionadas, como por ejemplo el patrón de voz o comportamientos de discurso (Asociación por los Derechos Civiles, 2015: 3).

Usos de la biometría

Los datos biométricos son principalmente usados para la identificación de personas, la que puede ser a través de *autentificación* (o *verificación*) *de identidad* o a través de *identificación*.

La autentificación o verificación de identidad se da cuando en una primera fase es realizada la recopilación de uno o más datos biométricos (por ejemplo, la muestra del iris, huella digital o rostro de una persona) para que sea procesado y almacenado en una base de datos biométricos. Esta fase del proceso se llama «inscripción y elaboración de una planilla biométrica» (Unión Europea, 2003: 4). Posteriormente, se compara la plantilla biométrica con el dato entregado; si coinciden, será *verificada* la identidad de aquella persona. La técnica es conocida como «1:1», en cuanto se *autentifica* o *verifica* el dato biométrico obtenido con el ya almacenado.

Por otra parte, la identificación de una persona funciona a través de la comparación de una muestra biométrica con una gran cantidad de plantillas biométricas; en caso de que coincida el dato biométrico con alguna de las plantillas almacenadas, se habrá *identificado* a la persona. Aquí el contraste es uno en múltiples muestras o «1:N».

Lo anterior puede ser ilustrado en la figura 1 (Prabhakar y otros. 2003: 34; la traducción es propia). El primer esquema indica cómo se registra y recopila la muestra biométrica (*enrollment*), en este caso una huella dactilar. El segundo esquema ilustra el proceso de comparación, en el que se chequea si coincide una muestra obtenida con el dato previamente guardado, realizándose una verificación 1:1. Finalmente, el tercer esquema describe la identificación y cómo se verifica la huella digital obtenida con los múltiples datos biométricos almacenados, realizándose una identificación 1:N.

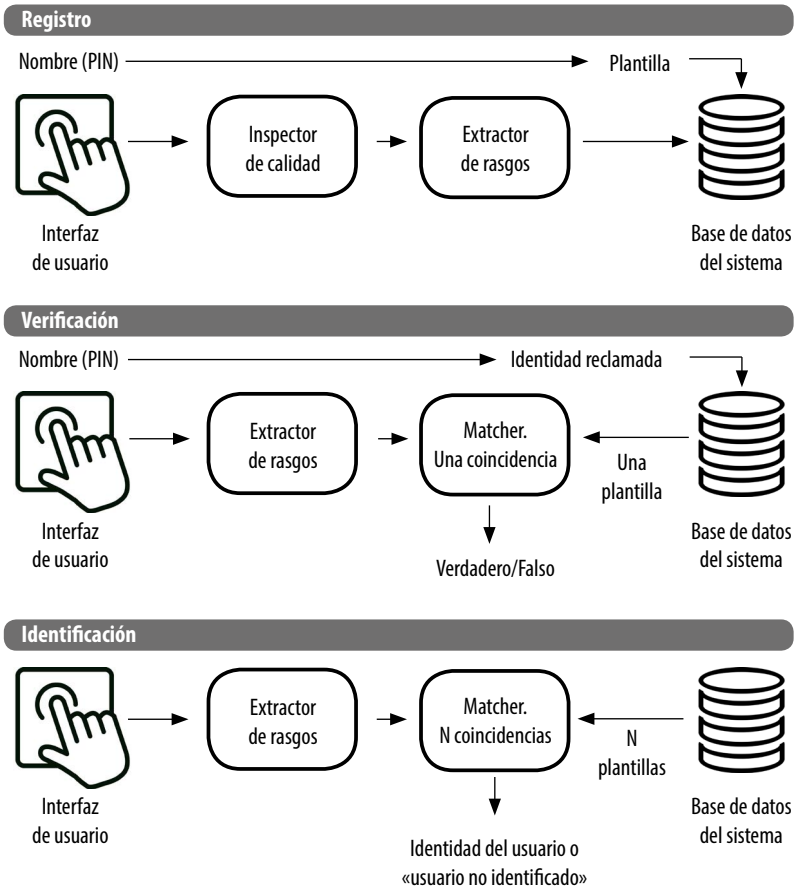

Figura 1. Funcionamiento de registro, verificación e identificación mediante datos biométricos (huella digital). Inspirado en Prabhakar y otros (2003: 34).

Una postura más bien crítica frente a este mecanismo de identificación o verificación de personas es la sostenida por la Asociación por los Derechos Civiles de Argentina (ADC), que en su *Informe sobre políticas de biometría en la Argentina* señala que la «identificación biométrica positiva no significa realmente una identificación positiva, sino una "probabilidad de identificación correcta"» (Asociación por los Derechos Civiles, 2015: 3). Ello debido a que la extracción de los datos biométricos no es perfecta, lo que hace que el dato obtenido no sea idéntico al sujeto en estudio, sino que en la mayoría de los casos se trabaja más bien con «rangos tolerables» (*tolerable range*) (Clark, 2001) o FAR (*False Acceptance Rate*) (Cavoukian, 2008: 1), el cual establecerá el rango de error de una muestra que no corresponda exactamente con la plantilla, por ejemplo, 1 en 10.000. Por lo tanto, la verificación e identificación de identidades biométricas dependerá del rango utilizado para identificar o verificar a una persona y de qué tan idénticas serán las planillas respecto del dato biométrico en

cuestión (Korja, 2006: 200).[4] Esto revela algo sumamente importante sobre las transferencias de los datos biométricos: en la medida que se multipliquen las copias de las plantillas obtenidas de una misma muestra, se pierden los rangos tolerables para identificar o autentificar a las personas. Los datos biométricos son más confiables si salen directamente de la muestra original y no de las plantillas.

Datos biométricos y su regulación

Naturaleza jurídica de los datos biométricos

Debe destacarse que los datos biométricos (como cualquier otro dato personal) son capaces de ser tratados; esto es, ser capturados, almacenados, analizados, transferidos y eliminados. Si bien parece obvio lo anterior, es necesario destacarlo para entender posteriormente los riesgos e implicancias del tratamiento de datos biométricos desde una óptica jurídica.

En la Ley, los datos biométricos no se encuentran regulados expresamente, por lo que resulta útil observar la regulación extranjera que brinde orientación sobre qué son los datos biométricos y en qué categoría se encuentran para la legislación chilena; y, conforme a ello, qué regulación les compete según su naturaleza jurídica.

El reciente reglamento de la Unión Europea (2016/679) de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, el Reglamento), su artículo 4 número 14 señala que los datos biométricos son: «Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las *características físicas*, *fisiológicas* o *conductuales* de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos» (el destacado es nuestro).

Cabe destacar que la Unión Europea entiende los datos biométricos como datos de carácter personal, porque —siguiendo la tendencia mundial— en la medida en que el dato sirva para identificar claramente a una persona, será un dato personal.

Podemos precisar que el concepto de dato personal corresponde a aquél que importa una posibilidad de identificación de un individuo, al permitir que «aunque no se haya identificado todavía [al individuo], sea posible hacerlo» (Unión Europea, 2007: 13). De esta manera, cabe destacar que las personas pueden ser identificadas

4. Esto parece ser de suma importancia en torno a los riesgos. En la medida que los datos biométricos se alejen de la muestra original, pierden la «probabilidad de identificación», por lo que el flujo indiscriminado de datos biométricos podría ser contraproducente con los objetivos que pretende la biometría, que es la identificación y autentificación de las personas. Sumado a eso, es necesario resaltar que no todas las personas tienen el mismo nivel de pulcritud de sus datos biométricos, por cuanto entre más exigente es el rango de fiabilidad, menos personas podrán utilizarlo para los fines que se requiere.

directa o indirectamente según datos precisos (nombre y apellido, por ejemplo) o datos indirectos que hagan posible su identificación, como a través de combinaciones únicas de datos personales (Unión Europea, 2007: 13-14).

A una conclusión equivalente puede arribarse respecto de nuestra legislación nacional, ya que —a pesar de no señalarlo explícitamente— entendería los datos biométricos como datos de carácter personal, atendido que los datos biométricos son datos concernientes a personas naturales que permiten identificarlas o hacerlas identificables. Lo anterior emana de lo señalado en el artículo 2 letra f) de la Ley, que contiene la definición de «datos personales»,[5] la cual permite abarcar perfectamente al dato biométrico. De la misma forma lo entiende la Unión Europea, en cuanto ha señalado que en «el contexto de la identificación biométrica, la persona es generalmente identificable, porque los datos biométricos se usan para identificar o autenticar/comprobar, al menos en la medida en que el interesado se distingue de cualquier otro» (Unión Europea, 2003: 6).

Datos biométricos: ¿datos sensibles?

Teniendo claro que los datos biométricos son datos de carácter personal tanto para la legislación comparada como para la nacional, cabe preguntarse si es que responden también a la etiqueta de «dato sensible» según las legislaciones comparadas y nuestra legislación local; así las cosas, señala el artículo 2 letra g) de la Ley que los datos sensibles son:

> Aquellos datos personales que se *refieren a las características físicas* o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual (los destacados son nuestros).

En este punto, ni nuestra jurisprudencia ni nuestro órgano legislador se han referido expresamente al tema. Sin embargo, desde una interpretación literal de la norma podemos desprender que los datos biométricos serían datos de carácter sensible en la medida que se refieren a «características físicas de las personas», esto es rostro, iris, retina, huellas dactilares, etcétera.

Los datos sensibles son «aquéllos que están esencialmente (no excluyentemente) vinculados a la privacidad y, por tanto, poseen una mayor potencialidad discriminatoria» (Puccinelli, 2004: 170). De allí la importancia de resguardar y darles una protección especial en la legislación: el tratamiento de datos sensibles podría afectar

5. Artículo 2 letra f) de la Ley 19.628: «Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables».

la intimidad de los titulares o bien generar discriminaciones arbitrarias. De esta manera, por ejemplo, el uso indebido o la colección indiscriminada de datos sobre el origen étnico o racial, convicciones políticas, estados de salud o datos biométricos podrían generar perfilamientos discriminatorios por entidades privadas u organismos públicos. He allí su especial regulación.

Para la Unión Europea, dentro de los datos de categoría especiales o especialmente protegidos —equivalente a nuestra categoría de datos sensibles— se encuentran los datos biométricos, según lo dispuesto en el artículo 9 número 1 del Reglamento.[6] En la actualidad, una gran parte de la legislación de protección de datos a nivel internacional se refiere a los datos sensibles también como una categoría distinta o particular de datos personales, denominándolos datos especialmente protegidos y entregándoles objetivamente una protección particular. Para efectos del presente trabajo, la nomenclatura específica utilizada en cada legislación para denominar a esta categoría de datos es indiferente, debiendo resaltarse que en la medida que los datos biométricos podrían revelar claramente la identidad y aspectos específicos de una persona, tales como su raza, etnia o estados de salud,[7] entre otras, debieran entenderse como datos de especial consideración (dato sensible o dato especialmente protegido). Así las cosas, el dato biométrico para la Unión Europea es un dato sensible o de especial categoría.[8] Señala el Comité Consultivo de la Convención para la Protección de las Personas respecto al Proceso Automatizado de los Datos de Carácter Personal (en adelante, el Comité Consultivo): «Los datos biométricos deben ser considerados como una categoría específica de datos en la medida en que proceden del cuerpo humano, siguen siendo los mismos en distintos sistemas y son inalterables de por vida» (Consejo de Europa, 2015: 25). Esto implica que los datos biométricos, al revelar datos procedentes del cuerpo humano, tienen una mayor propensión a derivar información sumamente sensible de la población como enfermedades, origen racial

6. Señala el artículo 9 número 1 del Reglamento (Unión Europea) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE: «Artículo 9, Tratamiento de categorías especiales de datos personales. 1) Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, y el tratamiento de datos genéticos, *datos biométricos dirigidos a identificar de manera unívoca a una persona física*, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física» (las cursivas son nuestras).

7. El 27 de marzo de 2017, el diario *El Mercurio* publicó en la página A11 una noticia en la cual se indica que, a través de software de reconocimiento facial, es posible diagnosticar el síndrome de DiGeorge con un 96,6% de certeza. También han podido identificar estados depresivos con el sólo tono y forma de hablar.

8. Las etiquetas «sensible» y «especial categoría» son aspectos que para efectos de este trabajo significan lo mismo. Mientras en Europa se habla de «especial categoría», países como Colombia, Australia, Perú y Chile hablan de «dato sensible».

o étnico o estados de salud, entre otros; en consecuencia, se entienden como datos de carácter sensible.

Lo expuesto anteriormente permite sostener dos aspectos relevantes en cuanto a los riesgos de los datos biométricos (que se verán más adelante). En primer lugar, los datos biométricos, a diferencia de una contraseña o una llave, son aspectos que están inherentemente circunscritos a la persona, la cual no es capaz de desligarse de ellos (salvo por alguna cirugía plástica). Esto quiere decir que, para efectos de clasificar mecanismos de seguridad, a diferencia de una llave (que se posee) o una contraseña (que se sabe), en el dato biométrico «se es» (Bennett, 2007: 16). El dato biométrico va ligado a la persona en su condición de tal y funciona como un identificador único, de manera que su pérdida o mal utilización pareciera ser irremplazable y terriblemente riesgosa para los derechos de las personas (Bennett, 2007: 17).

Sumado a lo anterior, el presente trabajo considera acertado afirmar que los datos biométricos son datos sensibles para efectos de la legislación chilena (a pesar de la omisión de su mención expresa), en la medida que es posible relacionar datos biométricos con otros datos (personales o no) y así obtener características únicas, tales como las raciales, étnicas o de otro tipo, que permitirían saber no sólo la identidad de un individuo, sino además aspectos sensibles relacionados a su físico o su estado de salud. A mayor abundamiento, datos como el iris o huella digital son conocidos en la doctrina extrajera como dato clave o *key data* (Liu, 2008: 47), por cuanto uno de estos datos biométricos permitiría saber absolutamente todo de una persona. El criterio de *key data* es el mismo que adoptó la Suprema Corte de California en el caso *Perkey versus Department of Motor Vehicles* (42 Cal. 3d 185, 187-8 (1986)): ella entendió que las huellas dactilares deben entenderse como datos de carácter sensible (Liu, 2008: 47).

En este sentido, entonces, el presente trabajo concluye que los datos biométricos —al ser información que puede develar todo de un individuo (*key data*) y que además puede asociarse a estados de salud u otros aspectos sensibles de las personas— son datos de carácter sensible, debiéndose por tanto tratar como tales (Liu, 2008: 48). Reforzando lo anterior, el Comité Consultivo destaca en sus conclusiones que el origen del dato biométrico proviene del cuerpo humano y reconoce su carácter de perpetuo e inherente a la persona, por lo que le entrega la categoría de «sensible» (Consejo de Europa, 2015: 6). De este modo, la relación que tienen los datos sensibles con los datos biométricos es una relación género-especie. Al ser los datos biométricos características físicas de las personas y además capaces de revelar sus aspectos íntimos o información susceptible a ser utilizada para discriminaciones arbitrarias, es que deberán ser considerados datos de carácter sensible.

La fórmula de datos biométricos como datos sensibles está asentada en diversas legislaciones extranjeras. La legislación colombiana ha establecido en su artículo 5 de

la Ley Estatutaria 1.581 de 2012 que los datos biométricos son datos sensibles.[9] El mismo criterio también ha tenido la legislación peruana, en cuanto señala en el artículo 2.2 de la Ley 29.733 (Ley de Protección de Datos Personales) que son datos sensibles:

> Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual». Por último, Australia también ha incorporado en su legislación a los datos biométricos como datos de carácter sensible, señalando, entre otros, que información sensible significa: «d) Información biométrica que se utiliza con el propósito de verificación o identificación automatizada y e) plantillas biométricas.[10]

En Chile, el más reciente proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales es el Boletín 11.144-07, presentado por el Ejecutivo. Si bien en su modificación al artículo 2 —que contiene la definición de datos personales sensibles— no incluye una mención expresa a los datos biométricos, sí se establece una regulación específica y taxativa a su respecto en el artículo 16 ter del proyecto, el cual señala:

> El responsable que trate datos personales biométricos, tales como la huella digital, el iris, los rasgos de la mano o faciales y la voz, deberá proporcionar al titular la siguiente información específica:
>
> a) La identificación del sistema biométrico usado.
>
> b) La finalidad específica para la cual los datos recolectados por el sistema biométrico serán utilizados.
>
> c) El período durante el cual los datos biométricos serán utilizados.
>
> d) La forma en que el titular puede ejercer sus derechos.
>
> Un reglamento regulará la forma y los procedimientos que se deben utilizar para la implementación de los sistemas biométricos.
>
> Con todo, no se podrán crear o mantener bancos de huellas digitales o de otros datos biométricos, salvo expresa autorización legal[11].

De este modo, el proyecto de ley apunta en la dirección correcta en cuanto a otorgarle una especial protección al tratamiento de esta clase de datos personales. Sumado a lo anterior, es acertado que el proyecto de ley entienda a los datos biométricos como una categoría amplia y no taxativa. Finalmente, el reglamento que establezca los procedimientos para la implementación de sistemas de identificación o autenti-

9. Véase el artículo 5 y la definición de datos sensibles, disponible en http://bit.ly/1C6Sx2w.

10. Véase la Division 1, «Definitions», de la Privacy Act (1988), disponible en http://bit.ly/2pwF3RM.

11. Véase Proyecto de ley que regula la protección y el tratamiento de los datos personales, 13 de marzo de 2017, Mensaje 001-365, Boletín 11.144-07. Disponible en http://bit.ly/2nG33Oa.

ficación de datos biométricos debiese incorporar una evaluación *ex ante* por la autoridad competente, la que pondere a través del sistema de proporcionalidad si es que la medida a adoptar es la más idónea, necesaria y proporcional a los fines específicos por los cuales requiere ser implementada. De esta manera, podría asegurar el pleno respeto de los derechos humanos de las personas afectadas o interesadas.[12]

Por otra parte, se destaca que sólo por mandato legal puedan ser realizados registros de datos biométricos. Al ser datos sensibles, los bancos centrales de datos biométricos merecen una especial protección, debido a las posibles vulneraciones en las que sus titulares pueden verse envueltos. Existen riesgos para los derechos y libertades básicas, por lo que el mandato legal permitiría, incluso, un control de constitucionalidad, lo que eleva el estándar normativo vigente.

Implicancias de considerar los datos biométricos como datos sensibles

Entender los datos biométricos como datos sensibles tiene consecuencias relevantes en cuanto a la manera en que deben ser tratados, esto es, recopilados, almacenados y traspasados, lo que debe acontecer siempre bajo una óptica respetuosa de los derechos humanos. En este sentido, es fundamental entender que, al ser datos de carácter sensible, los estándares para el tratamiento de datos biométricos serán muchos más estrictos, debido a que los riesgos que se corren por su mala utilización son mucho mayores. Es por ello que es necesario establecer, por una parte, cuál es el estándar legal en Chile, para luego complementar la Ley con guías normativas que impulsen una buena práctica en su tratamiento.

De acuerdo a la Ley, los datos sensibles se someten al régimen general de tratamiento con dos particularidades:

- Prohibición general del tratamiento: el artículo 11 de la Ley 19.628 señala: «No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares».
- Consentimiento: El artículo 4 de la citada ley señala que cuando una persona otorga el consentimiento debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público. La autorización debe constar por escrito. La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito.

Lo anterior, de cara a los derechos fundamentales de las personas, es insuficiente. Es por ello que urge una nueva institucionalidad y una ley más robusta en los princi-

12. Una visión más completa de este punto se verá en el siguiente acápite.

pios sobre protección de datos personales. Como se menciona más arriba, en el proyecto de ley es posible encontrar pautas normativas claras para afrontar los riesgos del uso de datos biométricos en Chile.

Sin perjuicio de lo anterior, el Reglamento sobre protección de datos personales de la Unión Europea ha establecido una serie de principios que sirven de orientación en la regulación del tratamiento de datos personales sensibles y, en particular, de los datos biométricos.

En primer lugar, siendo los datos biométricos datos de carácter sensible, la Unión Europea recomienda la adopción de los principios orientadores de la protección de datos bajo los parámetros indicados a continuación.[13]

Consentimiento. El interesado debe dar un consentimiento explícito para el tratamiento con los fines especificados.

Legitimidad. Los datos biométricos serán tratados de manera lícita y leal en relación con su titular. Es decir, la ley debe autorizar el tratamiento de datos con las debidas garantías para las personas interesadas.

Finalidad. Los datos biométricos sólo serán tratados con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

Calidad. Los datos personales deben ser adecuados, pertinentes y responder con veracidad a la situación real de la persona titular de los datos. Deberán ser exactos y actualizados, y los responsables deberán adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

Es fundamental aquí resaltar las características de los datos biométricos que se revisaron en el acápite sobre «concepto de la biometría», esto es, que son medibles, robustos, deben ser aceptables, son universales, permanentes y distintivos.

Sumado a lo anterior, parece clave vincular la calidad de los datos biométricos con el FAR: ¿cuál será el porcentaje de certeza que tendrá el dato biométrico para identificar o verificar la identidad? Si es que se requiere sistemas masivos de identificación, cabe recordar que no todas las personas tienen la misma calidad de muestra biométrica, por lo que los rangos tolerables de muestras deberán bajar para alcanzar a toda una población o masa de personas; esto implicaría una menor seguridad en la calidad del dato mismo, lo que aumentaría la probabilidad de falsas identidades u otras fallas en el sistema.

Proporcionalidad. El tratamiento de datos personales deberá circunscribirse a aquéllos que resulten adecuados, necesarios, relevantes y no excesivos en relación con las finalidades previstas en el tratamiento, y considerar, entre los medios con que pueda llevarse a cabo dicho tratamiento, el menos lesivo para los derechos de los

13. Basado en nuevo reglamento de la Unión Europea 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

titulares de dichos datos. Esto implica que deben buscar soluciones alternativas que supongan un menor atentado contra la privacidad (u otros derechos) de los interesados. La Agencia Española de Protección de Datos se ha manifestado en este punto señalando, por ejemplo, que es desproporcionado y excesivo el autentificar a niños con huellas dactilares para la entrada de un colegio (Agencia Española de Protección de Datos, 2006a: 1-2).

La proporcionalidad entonces es un razonamiento previo a la elaboración del registro, basado en tres supuestos o condiciones (Agencia Española de Protección de Datos, 2006b):

- Juicio de idoneidad: esto es, si con el tratamiento de datos y la creación del registro es posible conseguir el objetivo propuesto.
- Juicio de necesidad: si el tratamiento de datos y la creación del registro es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia.
- Juicio de proporcionalidad estricto: si la medida es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.

En consecuencia, deberá evaluarse, a través de la proporcionalidad bajo los parámetros anteriormente señalados, si el tratamiento de los datos sensibles es el medio idóneo para conseguir el objetivo propuesto. Estas comprobaciones previas debieran ser realizadas siempre por la autoridad de control de datos personales (que en Chile no existe hoy, por lo que, hasta la vigencia de una nueva ley, el análisis deberá realizarlo el mismo interesado en crear la base de datos) en su fiscalización del responsable o el encargado de la base de datos personales, cuando se trate de datos especialmente protegidos.

Pertinencia. Implica que el dato recolectado sea adecuado y concordante con dicha finalidad. Esto es, que el dato sirva para lo que se recogió, y que el o los datos sean los estrictamente necesarios para cumplir con esa finalidad específica en el tiempo presente. Un dato no es pertinente si sirve para el cumplimiento de otra finalidad relacionada o futura (Garriga Domínguez, 2004: 37).

Transparencia. El responsable del tratamiento de datos biométricos debe tomar las medidas oportunas para, en todo momento, facilitar al titular la información relativa a la finalidad del tratamiento e identidad del responsable. Además, el responsable deberá transparentar la comunicación relativa al tratamiento en forma concisa, inteligible, de fácil acceso y con un lenguaje claro y sencillo, en particular con cualquier información dirigida específicamente a un niño.

Responsabilidad y rendición de cuentas. El responsable del tratamiento es el responsable del cumplimiento de la ley y debe ser capaz de demostrarlo.

Confidencialidad. Quienes trabajen en el tratamiento de datos personales y el encargado que tenga acceso a los datos personales deberán guardar secreto de los mismos, obligación que no cesa por haber terminado sus actividades en ese campo.

Minimización de datos. Toda recolección de datos deberá limitarse a lo necesario en relación con los fines para los que serán tratados. Lo anterior está muy vinculado con la proporcionalidad: debe analizarse según la finalidad de generar la base de datos biométrica, limitándose al mínimo la recolección y las posibles cesiones de este tipo de datos.

Temporalidad. Los datos deberán ser conservados durante no más tiempo del necesario para los fines del tratamiento.

Seguridad. Los datos personales deberán ser tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Es conveniente que su detalle sea regulado en normas que den un margen de flexibilidad a quienes procesen datos, ya que se trata de medidas técnicas que podrán variar en el tiempo en la medida del avance tecnológico. Finalmente, las leyes de protección de datos deben exigir mayores medidas de seguridad en el tratamiento de datos sensibles y en aquellos casos en que la vulneración traiga consigo un grave riesgo para el titular de dichos datos. Para lo anterior, se puede optar por establecer seguridad por niveles concretos o seguridad por riesgos a evaluar por el responsable. El enfoque de riesgos es el contenido en las más modernas legislaciones de datos. Considerar la seguridad por riesgos implica que el responsable del tratamiento evalúa los riesgos que la organización afronta de manera de asumirlos, mitigarlos, transferirlos o evitarlos en forma eficiente, sistemática y estructurada. El responsable de los datos debe identificar el tipo de datos tratados: entre ellos habrá algunos que requieran un mayor o menor grado de confidencialidad, disponibilidad e integridad, lo que el responsable deberá asegurar. Sin embargo, los riesgos no sólo deben evaluarse desde lo organizacional, como pérdidas, inversión o costos concretos para el responsable, sino también desde la óptica de un custodio de los datos, y el perjuicio para los dueños en caso de vulneración de sus datos biométricos.

Algunas consideraciones del riesgo son:

- Legislación, tanto requisitos, restricciones y sanciones.
- Objetivos y competencias de la organización.
- Restricciones operacionales y presupuestarias.
- Costos de implementación de la reducción, mitigación o eliminación del riesgo.
- Balance de la inversión, frente al daño probable.

Los datos biométricos requerirán un enfoque de riesgo más estricto, uno que im-

pida su alteración, divulgación, destrucción o perdida, que asegure su conservación y acceso sólo por personal autorizado, obligando al responsable a hacer la mayor inversión posible en infraestructura, so pena de eventuales incumplimientos a los principios de protección de datos personales.

No hay una solución estándar para todos los casos, pues dependerá de los objetivos de ésta y de la naturaleza de la información que se maneja. Las medidas de seguridad podrán segregar los datos personales y se clasificarán en niveles de seguridad bajo, medio y alto según qué clase de dato personal o sensible se estará analizando. Si no es posible segregarlas, se aplicarán siempre las medidas del nivel más alto o el mayor riesgo, es decir, las contempladas para los datos sensibles.[14]

La adopción de estos principios para el tratamiento de datos biométricos en general permitiría tener un control más claro y respetuoso con los derechos fundamentales de las personas, al asumir quienes realizan el tratamiento los costos y riesgos que significa. Esto además implica la responsabilidad del Estado y las empresas en cuanto a articular estructuras tecnológicas robustas que permitan el ejercicio de los derechos fundamentales en el mundo digital.

En la medida que se responda con estas directrices normativas sobre el tratamiento de datos personales, se tendrá un sistema de identificación y autentificación más seguro y confiable, tanto para empresas como para organismos públicos que utilicen sistemas biométricos.

Riesgos del tratamiento de datos biométricos

Según lo expuesto hasta aquí, la biometría es un mecanismo para la identificación de individuos según sus características fisiológicas o conductuales. Como se analizó, la identificación de las personas se realiza a través de estándares probabilísticos, lo que deriva —como ha señalado la ADC de Argentina— en que la identificación a través de datos biométricos sea «esencialmente imperfecta» (Asociación por los Derechos Civiles, 2015: 4). Junto con ello, la naturaleza de los datos biométricos proviene del cuerpo, es decir, para lograr la identificación de una persona no es necesario que el individuo posea algo (tal como una llave) o sepa algo (como una contraseña), pues los datos biométricos son aspectos inherentes al ser humano, por lo cual la identificación se logra por algo «que se es». Es por ello sumamente importante el resguardo y protección de tales datos, debido a que en caso de robo o extravío de esta información generaría muchísimos problemas para poder revertir dicha situación.

14. Véase el artículo 81 número 1, 2, 3 y 8 del Real Decreto 1720/2007, del 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/199 de Protección de Datos de Carácter Personal, disponible en http://bit.ly/2s1le6d.

De esta forma, los datos biométricos pueden revelar muchísima información, por lo que su tratamiento es altamente sensible. Un mal uso de datos biométricos podría poner en jaque nuestra personalidad en el mundo digital, lo que significaría un riesgo inminente a los derechos humanos de las personas; es por lo anterior que la Unión Europea ha fijado principios normativos respecto a cómo deben ser tratados los datos sensibles (incluidos los biométricos).

Los riesgos de la biometría vienen dados por las vulnerabilidades que los mismos sistemas informáticos o de Internet poseen, como ciberataques en redes sociales, vulnerabilidades de software o redes, *spoofing*, cómo se procesan los datos biométricos, etcétera. También aparecen riesgos debido a las vulnerabilidades intrínsecas de la biometría, esto es, información que no es secreta, no pueden anularse o puede tener usos secundarios. De este modo, se expondrán una serie de riesgos que conlleva la biometría en sus usos y prácticas.

Riesgos intrínsecos de los datos biométricos

Los datos biométricos son información de carácter público a la que es fácil acceder: las fotografías de nuestros rostros se encuentran en cada red social que poseemos, las huellas digitales son fácilmente extraíbles de las cosas que tocamos, nuestra voz es reconocible y grabable, etcétera. Esta característica es precisamente uno de sus riesgos: se ha demostrado que es posible falsificar el iris de una persona mediante la captura de fotografías de alta resolución (Galbally, Fierrez y Ortega García, 2007: 4-5) o falsificar huellas digitales mediante fotografías de personas imitando el símbolo de la paz (Asociación por los Derechos Civiles, 2017: 7). De esta forma, se hace patente lo señalado previamente: ¿Cómo hacemos para reemplazar un dato biométrico que fue falsificado? ¿Cómo lograr reemplazar algo «que se es»? (Asociación por los Derechos Civiles, 2017: 8). No es posible, una vez falsificada una huella digital o un iris, reemplazarlo; esta es la principal y extrema vulnerabilidad que aqueja a los sistemas de identificación y autentificación biométricos.

Esta vulnerabilidad va de la mano de los ataques en redes sociales, del *spoofing*, la adquisición encubierta y otros. En la medida que no puedan anularse o reemplazarse, los sistemas de identificación o autentificación biométricos podrán ser interceptados por terceras personas, con los ciberataques como más lesivos, pues podrán ser utilizados para fines no previstos, harán más fácil la suplantación de identidad, etcétera. Junto con ello, la ADC advierte que, en la medida que los bancos de datos sean centralizados, existirá aún más riesgo para la seguridad de la información, lo que dejaría a las personas vulnerables a los ataques antes expuestos; además, en los casos en que las bases de datos sean usadas para efectos de vigilancia, existen riesgos como la criminalización ilícita o la exclusión social (Asociación por los Derechos Civiles, 2017: 11).

Riesgos en el tratamiento de datos biométricos

Los datos biométricos están siendo utilizados hoy día para garantizar rigurosos estándares de seguridad al entrar a sistemas de información altamente seguros o lugares comunes como trabajos, escuelas, estadios u otros; sirven para facilitar la autentificación a usuarios en internet y realizar compras. En la actualidad existe autentificación con huellas digitales o reconocimiento facial, tecnologías que han permitido mayor seguridad en las industrias de *retail*, financiero y otras; incluso se utiliza para entrar a un puesto de trabajo o probar hechos en materia procesal penal.

Para la OCDE, la biometría en sí no implica necesariamente un aspecto dañino o benigno para la privacidad, sino que deviene necesariamente de los usos que se le den y cómo hacemos frente a sus desafíos para la privacidad de las personas (OCDE, 2004b: 12). De este modo, la OCDE sugiere que, con diseños y políticas apropiadas al respecto (*privacy by design*), no es necesario escoger entre privacidad o seguridad, sino que es posible encontrar soluciones que permitan mejorar los aspectos económicos y sociales de los países (OCDE, 2004b: 12). Es decir, para la OCDE existen claros aspectos positivos de la biometría (seguridad) que merecen continuar por su senda, sin perjuicio de enfrentar los riesgos que sus vulnerabilidades permiten.

Como hemos dicho ya, la tecnología biométrica entrega información intrínseca de la persona, por lo que para obtener dichas muestras debe necesariamente ser realizada por mecanismos invasivos y, algunas veces, incluso degradantes. Desde la obtención de una huella digital a través de introducir un dedo o mano a una máquina, hasta la obtención de muestras de ADN por fluidos corporales, éstos son métodos que se entrometen con el derecho a la privacidad.

Por otro lado —y como vimos— la información privada de las personas puede ser capturada, almacenada, transferida y analizada por distintas agencias o empresas para su tratamiento; lo anterior puede llevar a malas prácticas por parte de las empresas u organismos que tratan estos datos biométricos, debido a que, en la medida que existan más intermediarios o terceros que utilicen o traten datos biométricos, es mayor el riesgo a vulnerar aspectos del derecho de la privacidad de las personas (Liu, 2008: 49). Sumado a lo anterior, al ser las plantillas biométricas «esencialmente imperfectas», la reproducción o copia indiscriminada de plantillas reduce las probabilidades de identificar o verificar identidades, por lo que es fundamental mantener el control sobre las copias y transferencias de las plantillas biométricas.

En nuestro contexto nacional, como se vio, no existe una legislación adecuada, lo cual es el mayor riesgo para el desarrollo de la biometría en Chile y, por ende, para el tratamiento de estos datos frente a una creciente industria a la que se le permite almacenar, transferir y analizar toda clase de información sin mayores estándares de seguridad o control frente a tratamiento indebidos. Las empresas y el Estado están capacitadas para almacenar grandes cantidades de datos personales y biométricos sin

que exista un control de parte de un órgano regulador respecto a cómo es llevado a cabo, si es que se cumplen con los principios de finalidad, proporcionalidad, transparencia, seguridad o consentimiento. El marco regulatorio por el cual debiesen ceñirse las empresas es sumamente débil, y el que existe no consta que se esté cumpliendo, a pesar de que extraer huellas dactilares para realizar compras simples sea una práctica comercial habitual. Esto implica que hay riesgos de divulgaciones no autorizadas, flujos de datos biométricos interempresas, discriminación en la entrega de servicios, robo de identidades, etcétera. Todos estos riesgos conllevan que puedan existir múltiples identidades digitales, vulneraciones a derechos humanos y otras lesiones a los derechos de las personas.

A modo de ejemplo, se ilustrarán algunos de los riesgos involucrados a los derechos humanos por los datos biométricos:

Divulgación no autorizada

Como se analizó, tanto nuestra ley nacional como los principios de la Unión Europea establecen como fundamental el consentimiento expreso para la utilización de datos biométricos. En caso de que no existan autorizaciones correspondientes por las personas dueñas de los datos biométricos, su derecho fundamental a la privacidad u otros derechos fundamentales será vulnerado. Todos los individuos tienen derecho a tener el control de sus datos personales y, en la medida que éstos sean transferidos o divulgados sin su consentimiento, existe una vulneración a los derechos de las personas. La divulgación de datos provenientes de bancos centralizados de datos podría llevar consigo todos los riesgos mencionados en el acápite anterior y discriminaciones arbitrarias por la sensibilidad de los mismos, tales como la criminalización de personas.

Vigilancia y rastreo clandestino

Existe un gran potencial de que los datos biométricos sirvan para el rastreo clandestino de las personas a través del reconocimiento facial y los Circuitos Cerrados de Televisión (CCTV). Incluso en nuestro país se han instalado políticas de seguridad basadas en globos de vigilancia y drones con sistemas de videovigilancia. Ambos sistemas con software de identificación biométricos podrían atentar contra la privacidad de las personas, debido a que la utilización de videovigilancia en espacios públicos coarta las expectativas de privacidad que las personas tienen derecho a conservar. Es más, nuestro mismo Tribunal Constitucional lo ha señalado de esta forma:

> Cualquiera entiende que está a salvo en su legítima discreción para circular anónima e indistinguiblemente de los demás, sin chequeos o registros […] que la intimidad no sólo puede darse en los lugares más recónditos, sino que también se extien-

> de, en algunas circunstancias, a determinados espacios públicos donde se ejecutan específicos actos con la inequívoca voluntad de sustraerlos a la observación ajena.[15]

De la misma forma se ha manifestado la Unión Europea, en cuanto a que la vigilancia en espacios públicos a través de mecanismos de videovigilancia genera lo que se conoce como *chilling effect* o «efecto panóptico», es decir, que al sentirse observadas o saber que pueden ser observadas e identificadas por sistemas biométricos, las personas dejarán de actuar naturalmente, vulnerándose espacios creativos, políticos y de disidencia, entre otros; es por ello que la masificación de *softwares* de identificación biométricos vulneraría no sólo la privacidad de las personas sino además la libertad de expresión, el derecho a reunión, derecho a petición, entre otros (Unión Europea, 2014: 7). Eso implicaría que, por ejemplo, un elemento tan importante como la protesta podría verse seriamente mermado por esta clase de reconocimientos biométricos y la vigilancia.

Sumado a lo anterior, y en nombre de la «seguridad» y «orden público», múltiples personas se verían afectadas al ser grabadas sus actividades en espacios públicos, aunque en su mayoría no tienen ni tendrán alguna vinculación con actividades que justifiquen tal vigilancia. Es por ello que debe tenerse presente que la videovigilancia y el reconocimiento facial con sistemas biométricos deben situarse en un marco de derechos que no interfiera arbitraria ni ilegalmente con la privacidad u otros derechos de las personas, es decir, que cumpla con los principios de legalidad, necesidad y proporcionalidad, tal como señala el Alto Comisionado de Derechos Humanos en su informe «El derecho a la privacidad en la era digital (2014)» (ACNUDH, 2014: 8). Toda limitación al derecho a la privacidad debe estar prevista en la ley, y la ley debe ser lo suficientemente accesible, clara y precisa para que una persona pueda leerla y saber quién está autorizado a realizar actividades de vigilancia de datos y en qué circunstancias. El mismo informe señala que la limitación debe ser necesaria para alcanzar un objetivo legítimo y proporcional al mismo, buscando la opción menos perturbadora y lesiva de las disponibles. Añade el informe que debe demostrarse que la limitación impuesta al derecho tiene posibilidades de alcanzar ese objetivo. Agregando, a su vez, que las limitaciones al derecho a la privacidad no deben «vaciar» el derecho en su esencia y deben ser compatibles con otras normas de derechos humanos, incluida la prohibición de la discriminación. De esta forma, si la limitación no cumple esos criterios sería ilegal y/o arbitraria (Rayman, 2015: 214).

En definitiva, la biometría y sus utilizaciones en videovigilancia o rastreo son verdaderas amenazas al derecho de la privacidad y otros derechos humanos, por lo que una utilización de tales medidas debiese traer consigo altos estándares normativos que condicionen su ejercicio; tanto gobiernos como empresas pueden establecer y

15. Sentencia Tribunal Constitucional, rol 1.984-2011, considerando vigésimo tercero.

crear perfiles según sus datos biométricos para estar en un constante monitoreo de actividades o acciones que las personas realizan, afectando enormemente no sólo el derecho a la privacidad, sino otros derechos fundamentales como la libertad de expresión, petición o reunión.

*Usos secundarios (*function creep*)*

Al ser los datos biométricos transferibles y almacenables, y bajo su condición de ser permanentes, es posible que la información sea recopilada por terceras personas ajenas para propósitos distintos a aquéllos por los que fueron entregados. Pueden ser transferidas sin permiso ni autorización a otros almacenadores, tratando los datos biométricos para fines no autorizados. Como se ha identificado, la información que otorgan los datos biométricos representa aspectos sensibles de las personas, por lo que, en la medida que puedan identificarlas de forma tan exhaustiva, entrega un enorme poder sobre la población (Korja, 2006: 208). Ello implica que deben existir mecanismos de resguardo y una verdadera gobernabilidad de los datos personales que circulen en el mundo digital, para evitar vulneraciones graves a los derechos fundamentales de las personas.

Disminución del anonimato

El que existan varias fuentes con datos biométricos fluyendo en el mundo digital hace que disminuya paulatinamente el anonimato en espacios públicos y privados. Los datos biométricos son información que va esencialmente contra el anonimato, debido a la facilidad y exactitud con que pueden identificar, rastrear o distinguir a las personas. Es una realidad el que Facebook es capaz de rastrear a personas con reconocimiento biométrico para puedan ser identificadas y etiquetadas. La recopilación de datos biométricos de nuestros rostros aumenta la capacidad de ser vigilados e identificados, lo que disminuye nuestro derecho a la privacidad y, en particular, a pasar anónimamente en espacios públicos o digitales. Ya existe la tecnología suficiente para, por ejemplo, detectar enfermedades a través de datos biométricos del rostro o bien diferenciar estados depresivos con sólo datos de la voz; es decir, en manos equivocadas la información de datos biométricos puede ser extremadamente reveladora frente a personas. En Venezuela, por ejemplo, el año 2014 se implementó el «sistema digitalizado de abastecimiento seguro», el cual consiste en un sistema biométrico para registrar a las personas cuando realicen compras de mercadería. De este modo, el Estado conoce qué cosas compran los ciudadanos y ciudadanas venezolanas y las autentifica con el registro del Consejo Nacional Electoral de Venezuela (CNE) (Abadi y Obuchi, 2014), lo que imposibilita la anonimización para compras de medicamentos u otras mercaderías.

Discriminación

El uso de datos biométricos para rastrear e identificar acertadamente a personas en distintos espacios puede ser utilizada también para discriminar a personas según atributos físicos o intelectuales, según su estado salud, según lugares que visita o personas que frecuenta. Para la ADC de Argentina, «un sistema mal diseñado puede violar la igualdad si promueve o facilita una distribución inequitativa de recursos que debería ser equitativa. Un sistema mal diseñado se puede prestar más fácilmente a abusos por parte de las autoridades encargadas de aplicarlo» (Asociación por los Derechos Civiles, 2015: 4). Se explica este riesgo en virtud de que el poseer datos tan sensibles como la huella digital, rostro de las personas u otros permitiría generar *discriminaciones arbitrarias* a personas en la entrega de productos, servicios o en el otorgamiento de derechos por parte del Estado. Junto con lo anterior, podría ocurrir que agentes del Estado o empresas que obtengan datos biométricos generarán bancos de datos con información en torno a la raza, etnia, orientación sexual u otros, lo que generaría riesgos de discriminación como consecuencia de la información almacenada. Un ejemplo ilustrador al respecto es el manejo de datos sensibles que podría manejar una compañía de seguros para aumentar la póliza según los datos sensibles que la compañía pudiere tener del potencial cliente, por ejemplo, dónde vive el usuario y la exposición a mayor delincuencia de un sector (Asociación por los Derechos Civiles, 2015: 15). De la misma forma, el sistema de identificación indio Aadhaar (voz hindi para la palabra «credencial») fue pensada para que los ciudadanos de la India pudieran votar, pagar impuestos, tener prestaciones de salud u otros; sin embargo, la Corte Suprema de ese país determinó que el sistema no podía ser obligatorio para el acceso a beneficios sociales (Asociación por los Derechos Civiles, 2017: 16).

Vigilancia y represión

Sumado a lo anterior, la Asociación por los Derechos Civiles advierte que las políticas de registro y clasificación de los ciudadanos(as) pueden servir como mecanismos represivos para la población (Asociación por los Derechos Civiles, 2015: 14), de la misma manera se ha expresado la OCDE al señalar que las tecnologías biométricas y la acumulación ilegítima de tales datos son atentatorias con la privacidad y permiten la identificación precisa de los ciudadanos, por lo que la vigilancia y el control social son el costo de autentificar a las personas con datos biométricos (OCDE, 2004: 12). Lo anterior queda de manifiesto cuando los gobiernos tratan de recolectar la mayor cantidad de datos biométricos posible para tener vigilada a la población, y que una identificación individual sea rápida. La biometría está sirviendo a muchos para rastrear y monitorear a las personas, lo cual no debiera ser tolerado en relación a garantizar los derechos humanos. Por ejemplo, distintas ONG latinoamericanas han

denunciado que el «sistema digitalizado de abastecimiento seguro» venezolano o el proyecto de ley brasileño 1775/2015 que crea un registro centralizado (Registro Civil Nacional) puede llevar consigo mecanismos de control y vigilancia para la población (Rena y Varón, 2015; Díaz, 2015).

Conclusiones

El presente trabajo parte por establecer que la biometría es un sistema de identificación o verificación de personas. Ella puede realizarse a través de sistemas 1:1, en el que se compara una muestra extraída de una persona con una plantilla previamente obtenida en una base de datos para ver si son compatibles (verificación); o a través del sistema 1:N, en el que se compara una muestra extraída con una serie de datos previamente obtenidos (identificación). La biometría permite, a través de sistemas de reconocimiento facial, de iris, huellas digitales u otros, lograr mayores estándares de seguridad para distintas industrias, como también para agentes del Estado. Sus funciones son múltiples y la OCDE ha promovido su uso, siempre y cuando sea compatible con la privacidad de las personas.

Así las cosas, el panorama en Chile sobre los datos biométricos desde una óptica normativa es poco claro y atrasado a nivel latinoamericano. No existe una definición expresa sobre qué son los datos biométricos dentro de la normativa chilena —a diferencia de Perú o Colombia— ni tampoco si se los considera datos personales sensibles o no. A pesar de ello, y luego de un análisis hermenéutico de la Ley, este trabajo entiende que los datos biométricos, al revelar características físicas y morales de las personas (según el artículo 2 de la Ley), son datos personales sensibles; dicha conclusión sigue la tendencia de las legislaciones comparadas e incluso del proyecto de ley presentado en el Congreso el pasado mes de marzo.

La conclusión anterior no es baladí frente al panorama en general de los datos biométricos en Chile; su tratamiento debe seguir lineamientos que permitan una gobernanza de datos personales que respeten los derechos humanos de todos los ciudadanos, pues de lo contrario se estaría generando un contexto inseguro para las transacciones electrónicas y desenvolvimiento digital. Es por ello que la Unión Europea ha generado lineamientos para el tratamiento de datos sensibles —categoría a la cual los datos biométricos pertenecen— que considera la legitimidad, finalidad, calidad, proporcionalidad, transparencia, responsabilidad y rendición de cuentas, confidencialidad, minimización, temporalidad y seguridad del tratamiento de datos personales como principios rectores para el uso y almacenamiento de datos biométricos.

Los principales riesgos son de dos tipos. Uno es la falibilidad de los sistemas biométricos por la naturaleza de los datos (públicos, únicos, muy difíciles de reemplazar), y el otro es sus usos o tratamiento: el uso indiscriminado de los datos biomé-

tricos para finalidades distintas por las cuales fueron recabados, la interceptación de datos biométricos que generan falsas identidades, la divulgación no autorizada de información, la revelación masiva de datos biométricos, la discriminación en el otorgamiento de servicios o derechos por parte de empresas o entidades estatales que poseen y analizan datos biométricos. Todos estos riesgos asociados a la biometría comprometen no sólo la privacidad de los ciudadanos, sino además otros derechos fundamentales de las personas, como la no discriminación arbitraria, lo que afecta el marco normativo que debiese tener un Estado de derecho democrático.

Referencias

Abadi, Anabella y Richard Obuchi (2014). «Todo lo que debe saber sobre el sistema biométrico». *Prodavinci*. Disponible en http://bit.ly/2rNNWng.

ACNUDH, Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2014). «El derecho a la privacidad en la era digital». Disponible en http://bit.ly/1HpMZlr.

Agencia Española de Protección de Datos (2006a). «Proporcionalidad del tratamiento de la huella dactilar de alumnos de un colegio. Informe 368/2006». Disponible en http://bit.ly/2rBDaW6.

—. (2006b). «Instrucción 1/2006, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras». Disponible en http://bit.ly/2siHKaC.

Asociación por los Derechos Civiles (2015). «Si nos conocemos más, nos cuidamos mejor. Informe sobre políticas de biometría en la Argentina». *ABC Digital*. Disponible en http://bit.ly/2sHTR1B.

—. (2017). «La identidad que no podemos cambiar. Cómo la biometría afecta nuestros derechos humanos». Disponible en http://bit.ly/2tksUil.

Bennett, Steven (2007). «Privacy implications of biometrics». *The Practical Lawyers*, 53 (3): 13-18.

Clark, Roger (2001). «Biometrics and privacy». *Roger Clarke's Web-Site*. Disponible en http://www.rogerclarke.com/DV/Biometrics.html.

Cavoukian, Ann (2008). «Fingerprint biometric: Address privacy before deployment». Information and Privacy Commissioner of Ontario. Disponible en http://bit.ly/2rwszYg.

Consejo de Europa (2015). «Informe de situación relativo a la aplicación de los principios de la Convención 108 a la recogida y al proceso de los datos biométricos» Disponible en http://bit.ly/2scgf2t.

Díaz, Marianne (2015). «Tu huella digital por un kilo de harina: biométrica y privacidad en Venezuela». *IFEX*. Disponible en http://bit.ly/2rwpRCl.

Galbally, Javier, Julián Fierrez y Javier Ortega-García (2007). «Vulnerabilities in biometric systems: Attacks and recent advances in liveness detection». Disponible en http://bit.ly/2rZtOUh.

Garriga Domínguez, Ana (2004). *Tratamiento de datos personales y derechos fundamentales*. Madrid: Librería-Editorial Dykinson.

Herrán Ortiz, Ana Isabel (2003). «El derecho a la protección de datos personales en la sociedad de la información». *Cuadernos Deusto de Derechos Humanos*, 26: 9-93. Disponible en http://bit.ly/2tFPv8d.

Korja, Juhani (2006). «The privacy risks of biometric identification». En Ahti Saarenpää y Aleksander Wiarowski (editores), *Society trapped in the network, does it have a future?* Rovaniemi: University of Lapland.

Liu, Yue (2008). «Identifying legal concerns in the biometric context». *Journal of International Commercial Law and Technology*, 3 (1): 45-54. Disponible en http://bit.ly/2sKn225.

OCDE, Organización para la Cooperación y el Desarrollo Económicos (2004a). «Background material on biometrics and enhanced network systems for the security of international travel». Directorate for science, technology and industry Committee for information, computer and communication policy. Disponible en http://www.oecd.org/internet/ieconomy/34661198.pdf.

—. (2004b). «Biometric-based technologies», *OECD Digital Economy Papers*, 101. DOI: 10.1787/232075642747.

Prabhakar, Saul, Sharath Pankanti y Anil K. Jain (2003). «Biometric recognition: Security and privacy concerns». *IEEE Security & Privacy*, 1 (2): 33-42. Disponible en http://bit.ly/2tFJ2tY.

Puccinelli, Oscar (2004). *Protección de datos de carácter personal*. Buenos Aires: Editorial Astrea de Alfredo y Ricardo Depalma.

Rayman Labrín, Danny (2015). «Chile: Vigilancia y derecho a la privacidad en internet». *Revista Chilena de Derecho y Tecnología*, 4 (1): 187-232. DOI: 10.5354/0719-2584.2015.36007.

Rena, Paulo y Joana Varon (2015). «Brasil anuncia proyecto para identificación única con la biometría. ¿Cómo está el tema en América Latina?». *Oficina Antivigilancia*. Disponible en https://antivigilancia.org/es/2015/07/1430/.

Unión Europea, Grupo del Artículo 29 sobre Protección de Datos (2003). «Documento de trabajo sobre biometría». 12168/02/ES WP 80. Disponible en https://www.apda.ad/system/files/wp80_es.pdf.

—. (2007), «Dictamen 4/2007 sobre el concepto de datos personales». Disponible en http://bit.ly/2tXsUEu.

—. (2014). «Opinion 01/2014 on privacy and data protection issues relating to the utilization of drones», 01673/15/EN, Bruselas. Disponible en http://bit.ly/2sHOhMz.

Sobre los autores

Romina Garrido Iglesias es abogada. Licenciada en Ciencias Jurídicas por la Universidad de Valparaíso. Magíster en Derecho y Nuevas Tecnologías por la Universidad de Chile. Fundadora y directora ejecutiva de ONG Datos Protegidos. Su correo electrónico es romina@datosprotegidos.org.

Sebastián Becker Castellaro es abogado. Licenciado en Ciencias Jurídicas y Sociales por la Universidad de Chile. Investigador de ONG Datos Protegidos. Becario del Programa de Perfeccionamiento Académico Facultad de Derecho, Programa de Magíster en Derecho con y sin mención (2015-2017). Su correo electrónico es sebastian@datosprotegidos.org.