REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 9 NÚM. 1 (2020) • PÁGS. 63-91 • DOI 10.5354/0719-2584.2020.53965
RECIBIDO: 28/7/2019 • APROBADO: 23/4/2020 • PUBLICADO: 30/6/2020

DOCTRINA

Legislación, riesgos y retos de los sistemas biométricos

Legislation, risks and challenges of biometric systems

Gabriela Quintanilla Mendoza
Universidad Pedagógica Nacional, México

RESUMEN La identificación personal ha obligado a los individuos a tener múltiples contraseñas, *tokens* y números o documentos personales de identificación, que han resultado no ser lo más adecuado para actividades en línea. Las tecnologías biométricas han ofrecido formas de identificación y validación eficientes, pero también han resultado ser inseguras ante posibles trasgresiones o mal uso que pudieran realizar los controladores. Si bien existe legislación para reglamentar esta información, resulta todavía limitada. Con el nuevo Reglamento General de Protección de Datos (RGPD) europeo, se espera que se extienda la protección de los datos biométricos a todos los países, para que los riesgos y retos actuales sobre seguridad, privacidad y derechos humanos sean atenuados.

PALABRAS CLAVE Biométrica, identificación, privacidad, seguridad, legislación.

ABSTRACT Personal identification has forced individuals to have multiple passwords, tokens and personal identification numbers or documents, which have proved not to be the most appropriate for online actions. Biometric technologies have offered efficient forms of identification and validation but have also proved to be unsafe in the face of possible transgressions, or misuse that the controllers can make. Although there is legislation to regulate this information, it is still limited; therefore, with the new European General Data Protection Regulation (GDPR), the protection of biometric data is expected to be extended to all countries, and the current risks and challenges in security, privacy and human rights be mitigated.

KEYWORDS Biometrics, identification, privacy, security, legislation.

Introducción

La identificación personal es la asociación entre la identidad y el individuo, que se observa en forma de verificación o autentificación y reconocimiento (Jain, Bolle y Pankati, 1996: 1). Los instrumentos utilizados tradicionalmente para la identificación personal han sido los *tokens*, es decir, objetos que los individuos poseen y sirven para identificarse, como el pasaporte o la carta de identificación; y el conocimiento, aquello que la persona sabe y que utiliza, como códigos, contraseñas y números de identificación personal (PIN) (Jain, Hong y Pankati, 2000: 91; Miller, 1994: 22). Sin embargo, el uso de estos instrumentos de identificación personal ha conducido a grandes problemas por el robo, pérdida, olvido u suplantación, lo que pone en riesgo la seguridad personal.

El uso de la biométrica[1] como método de identificación en la ejecución de las operaciones diarias ha demostrado ser un mecanismo más seguro que reduce el fraude y reporta resultados con más certidumbre y confianza, aunque a su vez conlleva riesgos de privacidad y de seguridad. Basada en técnicas utilizadas durante mucho tiempo, la biométrica empezó a ser desarrollada en la segunda mitad del siglo XX como método de autentificación sobre todo en criminalística, aunque en realidad se hizo presente sobre todo hacia principios de siglo XXI, tras el ataque a las Torres Gemelas en Nueva York en septiembre de 2001, momento en que los avances biométricos existentes empezaron a reforzarse para evitar la presencia, por segunda vez, de actos terroristas de esa naturaleza. Es decir, se buscó modernizar la seguridad, prevenir el terrorismo y la falsificación de documentos a través del empoderamiento de la biométrica, la cual fue utilizada en un principio en aeropuertos, fronteras y puertos, para luego extenderse a operaciones que facilitaran la identificación y salvaguardaran a la población (figura 1).[2]

Con el aumento de los datos biométricos y la creación de sistemas y bases de datos para su almacenamiento, empezó a emerger la posibilidad de sufrir ataques informáticos y, con ellos, la pérdida de datos y de privacidad. A partir de entonces, la legislación existente ha tenido que ser reevaluada y modificada, así como innovada de tal manera que los datos sean protegidos de intrusiones y ataques (Sánchez Pérez y Rojas González, 2012). Si bien existen organizaciones que tratan de regular su uso y administración, además de establecer un sistema tecnológico de protección de la privacidad (*privacy enhancing technologies*, PET) (Federrath, 2005: 1),[3] no hay

1. *Biométrica* es un término utilizado en las tecnologías de la información respecto de seguridad. La *biometría* es la aplicación de análisis estadístico en datos biológicos.

2. George W. Bush, «President Bush commemorates Fifth Anniversary of U.S. Department of Homeland Security», The White House President George W. Bush, 6 de marzo de 2008, disponible en https://bit.ly/3c3gRuW.

3. «Summary of privacy enhancing technologies: A survey of tools and techniques», Cranium, disponible en https://bit.ly/2WYwHm9.

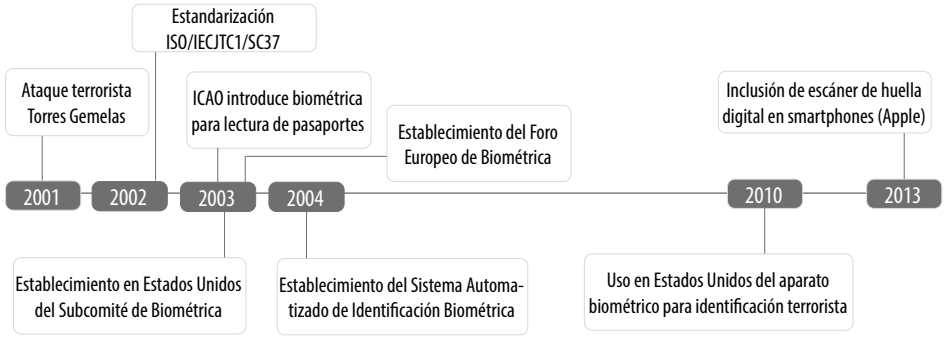

Figura 1. Principales eventos en el desarrollo de la biométrica. Fuentes: Elaboración propia a partir de Chris Burt, «Crossmatch explores history and future of biometrics», *Biometric Update,* 26 de febrero de 2018, disponible en https://bit.ly/2Xd5nR8; y Stephen Mayhew, «History of biometrics», *Biometric Update,* disponible en https://bit.ly/3cgHIDE.

en todos los países un marco legal que regule tanto la compilación de datos biométricos, el almacenamiento, el uso y las sanciones por el incumplimiento, como los riesgos de pérdida de privacidad, seguridad y libertad. La mayoría de los países tiene leyes de protección de datos personales, y en algunas de ellas simplemente se insertó el término «datos biométricos» intentando darle el mismo tratamiento que se da a los datos personales de otra naturaleza. Solo algunos estados de Estados Unidos y miembros la Unión Europea decretaron leyes y regulación para proteger los datos biométricos (Sánchez Pérez y Rojas González, 2012). Para 2018, a partir del establecimiento del Reglamento General de Protección de Datos creado por la Unión Europea (RGPD), los países empezaron a desarrollar legislación más concreta para regular la biométrica.

Existe mucha información sobre la biométrica, pero es escasa la referida a la legislación y las acciones que ejecutan los Gobiernos para regular el uso (bueno o malo) de los datos biométricos. Esta investigación se desarrolló a partir una búsqueda exhaustiva y el análisis de diversos artículos en revistas, sitios web, blogs, libros, organizaciones y la propia legislación. Se encontró que si bien la legislación sanciona la recopilación, almacenamiento y gestión de los datos sin consentimiento de los individuos, en la práctica no se regula el consentimiento, almacenamiento, uso y control de los datos biométricos, los cuales están aumentando considerablemente y poniendo en riesgo la privacidad, libertad y seguridad de los individuos.

Este artículo cuenta con una introducción; un apartado titulado «Datos biométricos» para definirlos; una sección llamada «Biométrica», en la que se explica su historia, conformación, definiciones y contenidos; un aparatado sobre las tecnologías de protección de privacidad y su aprovechamiento; un apartado de legislación, en el cual se presentan las leyes sobre protección de datos biométricos existentes en América Latina, Estados Unidos y las leyes que regularon la protección de los datos en la

Unión Europea hasta la creación del RGPD, que regula además los datos biométricos; un apartado sobre el propio Reglamento y sus aspectos más relevantes; y, por último, un apartado de retos y riesgos que deben ser superados, seguido de conclusiones.

Datos biométricos

Los datos son cualquier información computarizada o manual que es recabada por organizaciones públicas, privadas o académicas (Millard y Hon, 2012: 68). Los datos personales han sido definidos en la legislación como la información que hace a una persona ser identificada o identificable y pertenecer a un grupo determinado de individuos, como nombre, domicilio, filiación, patrón de voz o forma de mano (Sánchez Pérez y Rojas González, 2012). Los datos personales deben ser procesados bajo principios como el consentimiento, propósito definido, acceso a ellos por el individuo que los posee y restricciones en la transferencia. Deberá tenerse en cuenta que, si se almacenan de manera que ninguna persona utilizando medios razonables pueda identificar al dueño de los datos, entonces pierden su característica de dato personal (Jasserand, 2016: 303).

La definición engloba otros tipos de datos personales, aunque cada uno tiene sus propias características. Así, los datos sensibles están relacionados con la intimidad de las personas, como su origen étnico, religión o preferencias sexuales. Su divulgación pone en riesgo al individuo y lo hace susceptible de discriminación. Los datos biométricos también son parte de los datos personales. Han sido definidos en la literatura como los rasgos físicos, sicológicos y de comportamiento que identifican de manera única a un individuo. Al igual que los otros datos, los datos biométricos pueden ser afectados por muchas fuentes, pero la violación puede tener un nivel más alto y presentar fuertes riesgos, como la pérdida de identidad.[4] Como se verá más adelante, al tratar la nueva legislación europea, los procedimientos para proteger los datos biométricos, tratarlos, almacenarlos y usarlos son específicos y diferentes a los utilizados para los datos personales en general, dado que la mayor parte no cuenta con el consentimiento ni el control del individuo.

En la mayoría de los casos, los datos personales, biométricos o sensibles son recolectados, analizados, almacenados, usados o compartidos con poco conocimiento y control de los individuos (Kindt, 2010: 136), lo que compromete la privacidad, seguridad y confianza. Estos datos pertenecen sin embargo a los individuos que identifican, son una extensión informacional de ellos relativa a su vida privada, pública y profesional y no deberían ser tratados como propiedad de una organización de ningún carácter, sino como un derecho que ya es reconocido en el artículo 8 de la Carta de los

4. Luke Irwin, «GDPR: Things to consider when processing biometric data», *IT Governance European Blog*, 15 de septiembre de 2017, disponible en https://bit.ly/2zwhm3f.

Derechos de la Unión Europea y por el artículo 16 del Tratado de Lisboa, por lo que debería ser reconocido y protegido a nivel mundial (Kosciejew, 2014: 27).[5]

Al ser únicos, los datos biométricos tienen mayor veracidad; no obstante, debe considerarse que las características de los individuos cambian con la edad, por lo que los datos biométricos no son infalibles y pueden ocasionar problemas de identificación (Kindt, 2007: 168).

Biométrica

No existe una definición clara de biométrica, y puede ser considerada como ciencia o un simple término. Como ciencia, la biométrica establece la identidad de un individuo a través de las características físicas, químicas o de comportamiento individual por medio del análisis estadístico (Jain, 2006: 37). Como término, se usa para describir características o procesos. En este sentido, *características* se refiere a las características biológicas y de conducta medibles, utilizadas para lograr un reconocimiento automatizado; y *proceso,* a los métodos automatizados de reconocimiento de un individuo, basados en características biológicas y sicológicas medibles (Rosenker y Hirshey, 2008: 7).

En ambos casos, la biométrica busca identificar de manera automática a las personas a través de sus características biológicas y sicológicas, normalmente para facilitar el control de acceso. La biométrica ha sido reforzada con el establecimiento de sistemas de gestión[6] que permiten la determinación precisa de la identidad de un individuo para diversos servicios y aplicaciones, como transacciones financieras, acceso a edificios o a vuelos, o el ejercicio del voto (Jain, 2001: 1; Pato y Millet, 2010: 18; Zhang, 2000: 2).

La biométrica utiliza un conjunto de tecnologías que miden y analizan datos de reconocimiento únicos que facilitan los procesos de verificación o autenticación y de identificación. La *verificación* o *autenticación* biométrica es una comparación uno a uno que permite validar la identidad de un individuo mediante la comparación de datos entre las características de un individuo con su plantilla biométrica existente, para determinar el parecido y crear un modelo de referencia que se guarda en un sistema de gestión de identidad o *template*, el que posteriormente permite la autenticación. Se utiliza para reconocimientos positivos que permiten evitar duplicidades o

5. «Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses», Comisión Europea, 25 de enero de 2012, disponible en https://bit.ly/2Ab2HL6.

6. Un sistema de gestión de identidad es un programa que administra la recolección, autentificación o uso de identidad e información vinculada a la identidad. Se implementa en los sectores público y privado para controlar los mecanismos de autentificación y autorización (Hansen, Schwartz y Cooper, 2008: 38).

multiplicidades, esto es, muchos individuos con una misma identidad (Jain, 2001: 6). Esta función permite que los datos biométricos sean guardados en forma local y queden en control de los individuos. La autenticación o verificación biométrica responde a la pregunta «¿soy la persona que pretendo ser?» (Jain, Hong y Pankati, 2000: 91).

La *identificación*, por otra parte, es la comparación de uno a muchos que permite saber si la característica biométrica se encuentra en la base central. Se centra en la información contenida en las características físicas o de conducta de cada individuo, misma que se convierte en identificador biométrico mucho más confiable que los basados en conocimiento y los *tokens*. Esta función es de mayor riesgo, dado que los datos quedan fuera del control de los individuos y conforman grandes bases de datos, especialmente gubernamentales, con características biométricas obligatorias que se vinculan con bases de datos que contienen nombres y direcciones, las que terminan un tanto expuestas para quien tiene acceso a una de las bases de datos. La identificación responde a las preguntas «¿quién soy?» o «¿quién es esa persona?» (Jain, Hong y Pankati, 2000: 91). La identificación es un componente crítico en el reconocimiento negativo cuando un individuo niega ser quien es, por lo que su propósito es prevenir que un individuo tenga múltiples identidades (GT29, 2003: 3).[7]

El desarrollo de sistemas de identificación basados en biométrica ha ido en aumento con el avance de las tecnologías y las computadoras, y su objetivo último es lograr la identificación de los individuos en movimiento en cualquier contexto (Jain, 2006: ix). Los sistemas biométricos son métodos basados en el reconocimiento de patrones que distinguen las características físicas, sicológicas y de conducta, para lograr la identificación personal (Jain, Hong y Pankati, 2000: 92; Miller, 1994: 22). Con un sistema biométrico se comparan características con otras referencias almacenadas. Cuando esas características y las referencias anteriores coinciden porque provienen del mismo individuo, entonces se otorga la autorización (Pato y Millet, 2010: 22).

Existen dos tipos de mediciones biométricas: fisiológica y de comportamiento (figura 2). La medición fisiológica codifica las características físicas de los individuos, ya sea a través de la morfología que estudia el organismo y sus características, como huella digital, forma de la mano, patrón venoso, iris y retina, forma de la oreja o forma de la cara; o a través de la biología, que analiza el origen, evolución y propiedades de los organismos, como su ADN, sangre, saliva u orina, características normalmente de uso forense o médico. Estas mediciones por lo general son más confiables porque permanecen estables a lo largo de la vida del individuo; sin embargo, solo tres son consideradas en verdad únicas y de precisión: retina, iris y huella digital (Woodward, 1997: 1.481).

La medición del comportamiento o conducta se orienta al reconocimiento de la

7. «Biometrics: Authentication & identification (definition, trends, use cases, laws and latest news), 2020 review», Thales Group, disponible en https://bit.ly/2B12B9a.

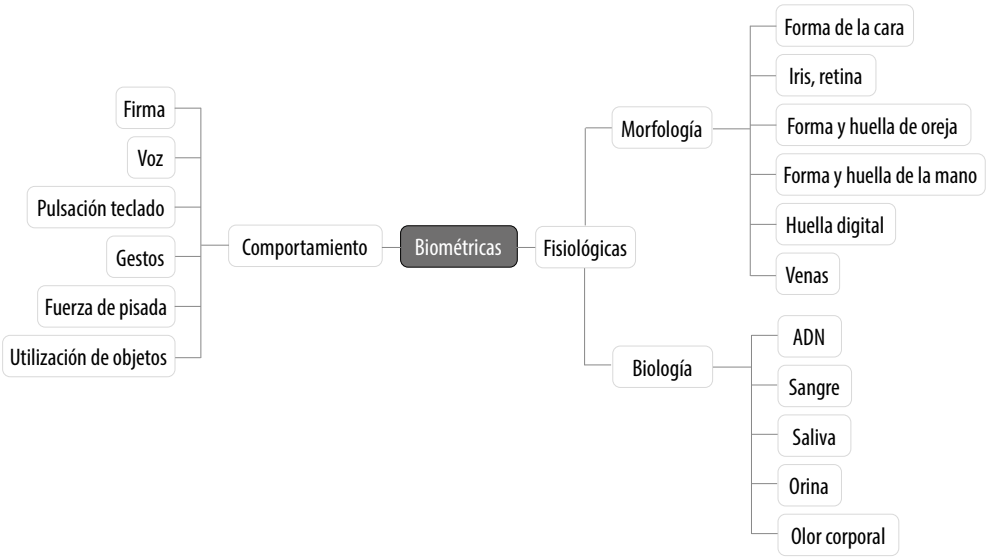

Figura 2. Sistemas biométricos. Fuentes: Elaboración propia a partir de «Biometrics: Authentication & identification (definition, trends, use cases, laws and latest news), 2020 review», Thales Group, *Biometric Update*, 15 de mayo de 2020, disponible en https://bit.ly/2B12B9a; y Jain, Bolle y Pankati (2000).

voz, la dinámica de la firma (velocidad del movimiento de la pluma, aceleración, presión, inclinación), la pulsación de teclas, la forma de utilización de objetos, los gestos o la fuerza de la pisada, entre otros. Estas mediciones varían conforme el individuo se desarrolla y cambia su estado físico y social.

Las mediciones biométricas deben satisfacer cuatro propiedades, a las que en la práctica se les suman otras tres (Jain, Bolle y Pankati, 1996: 4):

- Universal: Todo individuo tiene esa característica.
- Única: La característica es original, no se repite en dos personas al compararlas.
- Permanente: La característica se conserva en el tiempo.
- Coleccionable: Medible cuantitativamente.
- Verosímil: Referida a la precisión de la identificación alcanzable, los recursos para lograrla y los factores ambientales o de trabajo que afectan esa precisión.
- Aceptable o tolerable: El grado en que las personas aceptan y toleran un sistema biométrico.
- Ineludible: La facilidad de engañar al sistema.

Los datos biométricos que se obtienen a partir de estos sistemas posibilitan el desarrollo de tecnologías para la identificación única de los individuos. El Instituto de Biométrica divide los datos biométricos en dos tipos:[8]

Identificación física y fisiológica:

- ADN, identificación a partir del análisis de segmentos de ADN (químico).
- Oreja, identificación a partir de su forma (visual).
- Reconocimiento mediante las características encontradas en el iris para identificación (visual).
- Reconocimiento de retina mediante patrones de las venas de la parte trasera del ojo (visual).
- Reconocimiento facial a través del análisis de las características o patrones para la autenticación o reconocimiento de la identidad de un individuo (visual). Muchos de los sistemas de reconocimiento facial usan interfaces o análisis de características locales.
- Huella dactilar, basado en el uso de las crestas y valles precisos encontrados en la superficie de las puntas de los dedos humanos (visual).
- Geometría de los dedos, usando la geometría de los dedos en tercera dimensión para determinar la identidad (visual y espacial).
- El uso de las características geométricas de la mano (visual-espacial).
- El olor que expiden los individuos, para determinar su identidad.
- Reconocimiento venoso, a partir de los patrones que conforman las venas en la palma de la mano o en los dedos.

Identificación de comportamiento:

- Paso, a partir de la forma de caminar o de los pasos de los individuos para determinar la identidad (conductual).
- Escritura de teclado, mediante el uso de características únicas de teclear que tienen las personas (conductual).
- Identificación de voz o habla. Permite identificar la identidad de quien habla a través de la comparación de la voz con plantillas existentes (1:N) (auditivo). Se utiliza en ocasiones sin el consentimiento del parlante para identificar interlocutores en una discusión o para verificar la inscripción de un individuo en un sistema.

8. «Types of biometrics», Biometrics Institute, disponible en https://bit.ly/2LWlTyL.

- Autenticación de voz o habla. Es un método para determinar la identidad de la persona que habla, para control de acceso. Es también conocido como modelo de voz o voz impresa. Cuando el parlante reclama una identidad, la voz se usa para verificar con un *template* (o referencia digital) el hecho (1:1). Normalmente es empleada como «portero» para proveer acceso a sistemas de seguridad, como sucede en los bancos vía telefónica. Opera con el conocimiento del individuo y requiere de su cooperación (auditivo).
- Reconocimiento de firma mediante el análisis de la escritura manual (visual-conductual). Existen dos tipos de autenticación de la firma digital, estático y dinámico. El primero es normalmente una comparación visual entre dos firmas escaneadas o una firma escaneada y otra hecha con tinta. La segunda es más popular a medida que los datos rituales se capturan junto con las coordenadas X, Y, T y P del firmante desde un dispositivo de firma. Se utiliza en la corte judicial o para crear una plantilla biométrica que sirva para autenticar las firmas dinámicas.

La biométrica es susceptible a errores. Sin embargo, entrega pruebas de identificación lo más seguras posible, que son usadas principalmente por los Gobiernos en áreas de relaciones exteriores al expedir pasaportes y visas; en el control en fronteras; en identificación nacional, en los «e-servicios», en finanzas y en algunos espacios educativos. Las cámaras en espacios públicos como supermercados o cruces en la vía pública se utilizan para identificar a los individuos de manera inmediata (Toli y Prennel, 2015: 2). En el sector privado se han utilizado básicamente como medios de identificación en organizaciones bancarias y el comercio electrónico (*e-commerce*).

La propiedad, la privacidad y la seguridad son transversales a las tecnologías de autenticación y autorización y resultan de gran importancia para los datos biométricos.

La *propiedad* es un concepto vinculado a la defensa y control de la información personal, que prevalece aun cuando el individuo fallezca. Esta idea conforma el modelo europeo de protección de datos personales (Sánchez Pérez y Rojas González, 2012).

Reconocida en el artículo 12 de la Declaración Universal de Derechos Humanos y en otros documentos de carácter internacional, la *privacidad* es un derecho humano esencial que permite al individuo establecer límites para la protección de intromisiones, por lo que su protección queda determinada en múltiples documentos constitucionales.[9] La privacidad tiene carácter multidimensional (Wang y Kobsa, 2009: 203), por lo que puede ser determinada como un proceso de regulación de límites entre diferentes esferas de acción (Palen y Dourish, 2003: 130-131) o la protección

9. «What is privacy?», Privacy International, 23 de octubre de 2017, disponible en https://bit.ly/36vU5KP.

de un conjunto de actividades interconectadas que afectan a un grupo de personas relacionadas en un momento dado (Solove, 2006: 484). Para los propósitos de este documento, la privacidad será entendida como un principio fundamental de los sistemas legales, un derecho a decidir y controlar la información personal y una filosofía política que valora la libertad de los individuos, su autonomía, intimidad e imparcialidad (Kent y Millet, 2003: 62; Wang y Kobsa, 2009: 203). La privacidad conforma el modelo americano que, a diferencia del anterior (la propiedad), se pierde cuando el individuo fallece (Sánchez Pérez y Rojas González, 2012). Debe enfatizarse que la protección de la privacidad depende de lo que cada país entiende por privacidad, lo que la hace efímera y vaga (Solove, 2008: 3-4).

Al igual que sucede con la propiedad, la privacidad denota que los datos biométricos pertenecen a cada individuo y éste tiene control sobre ellos. Con el surgimiento de las tecnologías de la información y los cambios sociales, estos dos conceptos obtuvieron más atención y se modificaron. Entonces empezaron a demandarse prácticas justas de información, que establezcan principios que aseguren la protección contra la recopilación secreta de información y provean seguridad (Kent y Millet, 2003: 71).

La *seguridad* es la razón por la que la autenticación se hace necesaria y es vital para salvaguardar la privacidad. Integrados a este concepto se encuentran no solo los mecanismos de seguridad, sino los procesos y políticas que administran quién y cómo tiene acceso a los datos personales. La creación de sistemas de seguridad depende de: i) la vulnerabilidad que ocurre como resultado de errores procedimentales, personales o problemas físicos de seguridad; ii) ataques técnicos, procedimentales, físicos o de programas maliciosos (*malware*); iii) la presencia de crackers y hackers; o iv) un mecanismo de seguridad o procedimiento diseñado para contrarrestar ataques (Kent y Millet, 2003: 82). Al establecer medidas de seguridad, se reduce la posibilidad de que los datos biométricos sean distribuidos sin consentimiento de los individuos y utilizados para fines distintos a los cuales fueron recolectados.

Tecnologías para mejorar la privacidad

Una forma de protección de identidad real del usuario y para los controladores de los datos son las tecnologías para mejorar la privacidad (*privacy enhancing technologies*), más conocidas como PET (Shen y Pearson, 2011: 2). Estas tecnologías se basan en la creación de seudoidentidades que asume el usuario para protegerse de ser perseguido cuando hace una transacción o un servicio en línea, lo que proporciona el control sobre la información que se tiene de su persona y permite decidir cómo y cuándo ésta puede ser utilizada por terceros (Federrath, 2005: 1-2; Hes y Borking, 1998: 11-13, 29).

Las PET consideran tanto los principios de privacidad que sirven como guía para la evaluación conceptual de soluciones técnicas, como las inquietudes[10] sobre privacidad que constituyen las necesidades de los usuarios, las que deben ser abordadas como mecanismos de privacidad (Wang y Kobsa, 2009: 222). Las PET buscan eliminar el uso de datos personales por completo o dar el control total de los datos a la persona interesada (Agre y Rotenberg, 1998: 125). Es decir, tienen la finalidad de permitir a los usuarios proteger su privacidad (informativa) permitiéndoles decidir, entre otras cosas, qué información están dispuestos a compartir con terceros (como los proveedores de servicios en línea) y en qué circunstancias se compartirá esa información (GT29, 2003).[11] Una de sus ventajas es que su uso reduce el incumplimiento de las reglas de protección de datos.

Las PET son categorizadas conforme a la funcionalidad y capacidad que ofrecen al usuario final en línea y se enlistan de manera sintética: consentimiento informado, minimización de los datos para una transacción, anonimato, control, negociación de términos y condiciones, aplicación técnica, que va de la mano de la revisión remota de cumplimiento y el uso de los derechos legales.[12] Por lo tanto, las PET ayudan a proteger la privacidad al reducir los datos personales en línea y prevenir el procesamiento innecesario de datos sin perder la funcionalidad del sistema de información, además de asegurar que el consentimiento para el procesamiento de datos sea informado.[13]

Ahora bien, el reconocimiento basado en los datos biométricos depende de lo que un individuo es o hace, a diferencia de otros modos de autenticación como las contraseñas. Los procesos biométricos son modelos de identificación y autentificación modernos y parecieran estar más lejos de fraude o falsificación. Muchos esfuerzos se han llevado a cabo, particularmente en la legislación, para lograr la protección biométrica; sin embargo, todavía existe un desfase de privacidad y seguridad, además de la atención que debe darse al almacenamiento de los datos biométricos para la autenticación humana o el acceso limitado de terceros (Toli y Prennel, 2015: 1-3).

Las PET para la biométrica son desarrolladas a partir de suposiciones que involucran al usuario y al controlador de la identificación. Se clasifican, según la protección

10. Los principios de privacidad aplican cuando los datos personales son procesados con la finalidad de identificar a un individuo, como la especificación del propósito, los límites para la recolección y uso, transferencia, consentimiento, acceso, integridad, seguridad, anonimato o negación. Las inquietudes se presentan particularmente en la recolección de datos que se realiza, analiza o transfiere de manera impropia, como rastrear, perfilar, recomendar entre sitios web o el intercambio de datos con terceros (Wang y Kobsa, 2009: 205, 210-11).

11. «Summary of privacy enhancing technologies», Cranium.

12. «Privacy enhancing technologies: A review of tools and techniques», Office of the Privacy Commissioner of Canada, noviembre de 2017, disponible en https://bit.ly/3gq41dq.

13. «Summary of privacy enhancing technologies», Cranium.

de plantillas y a criptosistemas biométricos (encriptación criptográfica y descifrado de algoritmos) en:

- Transformación de características, para proteger plantillas durante el registro, con la finalidad de lograr un almacenamiento seguro.
- Biometría cancelable y renovabilidad, para proteger los datos después de robo, a través del almacenamiento de una versión transformada de la plantilla biométrica.
- Criptobiometría, gestión de claves para la protección de datos biométricos basados en claves utilizando algoritmos criptográficos de cifrado y descifrado. Solo tienen acceso las entidades involucradas a ciertos componentes.
- Identidades biométricas seudónimas múltiples, para lograr una vinculación controlada, como sucede con las llaves públicas. El usuario crea este seudónimo de forma secreta y puede ser usada como elemento verificador dentro del sistema (Toli y Prennel, 2015: 8-12).

Las PET traen ventajas de costo, reducción de riesgos por errores humanos, confianza y cumplimiento con la protección de datos. Por ello, su uso correcto permite al individuo decidir, entre otras cosas, sobre la información que desea compartir con terceros, las circunstancias en las cuales esa información es compartida y los fines para los cuales los terceros pueden usar esa información.[14]

Legislación

Es indiscutible que los avances tecnológicos han obligado a los países a considerar el tratamiento y la protección de los datos biométricos, en particular porque los sectores público y privado han incrementado el uso de las tecnologías biométricas de identificación personal para proveer mayor seguridad, incrementar la eficiencia y mejorar los servicios (Woodward, 1997: 1.480). Cada vez más los individuos son identificados de modo biométrico, ya sea de forma voluntaria u obligatoria y, en el caso de la identificación facial, sin autorización alguna, como sucede en aeropuertos, puertos, centros comerciales o comercios donde existen cámaras.

Poca legislación en materia de protección de datos biométricos existe a nivel internacional. La legislación para usar, almacenar y proteger los datos biométricos de los individuos no va de la mano con el avance de la biométrica, por ser relativamente nueva para el campo legislativo. Pero la renovación de esta última puede reducir el

14. «Privacy enhancing technologies», Office of the Privacy Commissioner of Canada; «Privacy enhancing technologies: An absolute necessity for effective compliance with data protection laws», Data Protection Office, diciembre 2012, volumen 7, p. 9, disponible en https://bit.ly/2TG3479.

fraude y salvaguardar los derechos humanos (Liu, 2008: 45). Si bien los datos biométricos son datos personales, en pocas legislaciones son considerados de manera explícita (Rojas González y Sánchez Pérez, 2012). Para no extender demasiado el artículo, se mencionan algunas legislaciones que consideran los datos biométricos.

Legislación latinoamericana

En América Latina, la recopilación y el uso de los datos biométricos es evidente en los sectores público y privado; pero en general se observa la ausencia de un marco jurídico para el tratamiento de los datos biométricos. Las políticas públicas en la materia son implementadas con escasa transparencia hacia la ciudadanía. No hay información respecto de la recolección, uso o almacenamiento de los datos ni del acceso que tienen terceros sobre ellos. La mayoría de los países no ha introducido el término en su legislación de privacidad y protección de datos personales, y los que lo han hecho los confunden con datos sensibles. Se observa la recopilación de datos biométricos principalmente en las áreas financiera, tributaria y de seguridad, aunque con poca transparencia, dado que en general se desconocen las tecnologías y mecanismos para la recolección, análisis y almacenamiento de los datos biométricos, así como su gestión, uso, acceso y transferencia. El individuo no es consultado ni otorga consentimiento alguno (Ucciferri y Ferreyra, 2017: 5).

Un caso que vale la pena mencionar es el de Chile. Este país ha sido pionero en el trato de los datos personales y se ha esforzado por destacar los datos biométricos. En los proyectos de ley 11.144-07 y 11.092-07-2[15] (Legislatura 364 de 2017) se ha buscado modificar la Ley 19.628, sobre Protección de la Vida Privada, adicionando los datos biométricos como una categoría amplia y no taxativa (Garrido y Becker Castellaro, 2017: 76) y un tratamiento especial para su protección. Sin embargo, estas ideas continúan en proyecto.

Legislación norteamericana

A nivel local, solo tres instrumentos legales han servido en Estados Unidos para regular la biométrica: el Acta de Privacidad de Información Biométrica de Illinois, la Ley de Privacidad Biométrica de Texas y la Ley de Biométrica de Washington. Estas leyes tratan la privacidad y la seguridad de manera diferenciada y hacen que los procesos y la recolección de los datos sean lentos, además de tener diferencias en las definiciones, tratamiento y sanciones. De ahí que la legislación estado por estado no

15. En el artículo 16 ter del proyecto 11.044-07 se menciona el tratamiento que debe hacer el responsable de los datos biométricos, aunque no se menciona en las definiciones. En el artículo 3 del proyecto 11.092.07 se incluyen específicamente como parte de los datos sensibles y el consentimiento de éstos en los artículos 5 y 9.

sea el ideal, y se considere que sería de mayor utilidad el desarrollo de una ley federal, que abarque al país y unifique criterios (Nguyen, 2018: 71, 73).

La primera y más importante ley se dio en Illinois en 2008, cuando se aprobó el Acta de Privacidad de Información Biométrica (BIPA) (740 ILCS 14/1), cuyo fin es regular la recolección de identificadores biométricos por parte de las organizaciones. De manera acotada, señala que un identificador biométrico se refiere a la imagen de retina o iris, a la huella digital, a la voz, a la imagen de la mano o la geometría de la cara.[16] Asimismo, esta Ley regula la información biométrica desde la manera en que es capturada, convertida, almacenada y compartida, para asegurar la protección, privacidad y seguridad de los individuos. Es la única ley americana que no solo permite protección a los individuos contra la violación de la privacidad de la información biométrica, sino que además les permite demandar a personas u organizaciones por no obtener autorización en la recopilación, uso y almacenamiento de la información biométrica.[17] Características importantes son que prohíbe la recolección de datos biométricos sin consentimiento previo por escrito y salvaguarda los datos biométricos, al prohibir a entidades comerciales el uso, intercambio, venta o préstamo de estos datos. De manera sintética, la BIPA se caracteriza por:

- Solicitar consentimiento informado antes de la recolección de datos.
- Permitir un derecho limitado de apertura y acceso.
- Ordenar obligaciones de protección y otorgar recomendaciones.
- Prohibir la obtención de beneficios con los datos biométricos.
- Crear un derecho de acción privado para las personas perjudicadas por las violaciones de la BIPA.[18]

Por otra parte, la Ley de Privacidad Biométrica de Texas de 2009 (Texas Business and Commerce Code § 503.001, Capture or Use of Biometric Identifier) regula por igual los identificadores biométricos de la BIPA, aunque solo protege los identificadores biométricos. Esta Ley demanda el consentimiento verbal del individuo, prohíbe el traspaso de información y especifica la destrucción de los datos cuando ya cumplieron con su propósito. Es aplicable a organizaciones que recolectan datos biométricos para fines comerciales y restringe la venta o traspaso de datos a menos

16. «Biometric Information Privacy Act», Illinois General Assembly, 2018, disponible en https://bit.ly/2ZAcFQJ.

17. Nicole O., «Biometrics laws and privacy policies», Privacy Policies, 4 de septiembre de 2019, disponible en https://bit.ly/2XBrG1W; «Biometric information privacy», Technology Safety, 15 de marzo de 2018, disponible en https://bit.ly/2AZEzv3.

18. «Illinois Biometric Information Privacy Act FAQs», Jackson Lewis, disponible en https://bit.ly/2zBgM4r.

que existan ciertas condiciones. Los identificadores biométricos deben ser destruidos en un lapso no mayor a un año (Browning, 2018: 675).[19]

En Washington, la Ley de Biométrica establecida en 2017 (Washington House Bill 1.493) establece los requisitos para la recopilación y uso de identificadores biométricos con fines comerciales. Refiere a la información biométrica como los datos que provienen de mediciones automáticas de las características biológicas de los individuos, como la voz, iris, retina y examen de la mano. Se adicionaron las características biológicas exclusivas que permiten la identificación única de un individuo. Esta Ley exige la inscripción de los identificadores biométricos a una base de datos de propósito comercial, además de señalar que el consentimiento puede no ser por escrito; asimismo, señala que se debe evitar el acceso a los datos biométricos y eliminarlos cuando cumplieron con el propósito.[20]

Si bien estas leyes (Illinois, Texas y Washington) establecen sanciones por violaciones, la diferencia básica entre ellas es que sólo la ley de Illinois ofrece un derecho de acción privada en caso de violación, esto es, presentar una demanda, recibir una recompensa por daños y recuperar gastos por pago de abogado, por lo que un individuo afectado puede recibir hasta mil dólares por cada violación negligente y hasta cinco mil por violación imprudente o deliberada.[21]

Recientemente, siguiendo el modelo de la ley europea del RGPD, en California se expidió la Ley de Privacidad de los Consumidores de California (California Consumer Privacy Act of 2018, CCPA), puesta en marcha el primero de enero de 2020. Esta ley se enfoca en los datos que otorgan los consumidores cuando compran. Para asegurar los datos personales, se otorgó a las compañías un plazo de doce meses para organizar los sistemas de datos, de manera que el consumidor pueda solicitar los datos recolectados por ellas cuando así lo requiera.

Por consiguiente, esta Ley provee control a los consumidores tanto de sus datos biométricos como de cualquier otra información personal que identifica, se refiere, describe, es asociada o vinculada, ya sea directa o indirectamente, con un consumidor.[22] Esta Ley especifica que la información biométrica recolectada por una empresa sin el conocimiento y consentimiento del individuo no puede ser pública. Asimismo, provee el derecho a promover una acción privada cuando la información ha sido divulgada o existe una intromisión por la presencia de una violación a la seguridad de la organización.

---

19. Annemaria Duran, «Understanding the Texas Biometric Privacy Law as an employer», Swipelock, 29 de diciembre de 2017, disponible en https://bit.ly/2zxmC6R; Danny Thakkar, «Biometric regulations in the U.S. States: The state of play», Bayometric, disponible en https://bit.ly/2ZEEass.

20. «June 2019: The rise of biometrics laws and litigation», JD Supra, 28 de junio de 2019, disponible en https://bit.ly/3ejHpJO; Thakkar, «Biometric regulations».

21. Niya T. McCray, «The evolution of U.S. Biometric Privacy Law», *The Defense Magazine*, mayo de 2018, disponible en https://bit.ly/36uDcjU; Nicole O., «Biometrics laws».

22. «June 2019: The rise of Biometric laws», JD Supra.

En el resto del país, la práctica del reconocimiento facial y el uso de software para identificar a un individuo utilizando imágenes obtenidas en áreas públicas atenta contra la privacidad, anonimato y autonomía de los individuos, porque ésta es llevada a cabo sin consentimiento. Si bien en Illinois y Texas no están permitidas para uso comercial, en Washington y en el resto del país resulta un procedimiento invasivo.[23] Pese a todo, cabe decir que Alaska, Connecticut, Massachusetts y New Hampshire se encuentran en proceso de crear leyes para protección de los datos biométricos que buscan la implementación de una legislación biométrica integral similar a BIPA y el Reglamento europeo.[24]

Legislación europea

En la legislación europea, el Convenio 108 de 1981 (vigente) es un tratado internacional legalmente vinculante que obliga a las partes a llevar a cabo medidas en la legislación nacional para aplicar los principios que aseguren la protección de los derechos humanos con respecto al procesamiento de datos personales.[25] El documento Data Protection Directive 95/46/EC [EE95] de 1995, vigente hasta antes de 2018, sentó las bases para la protección de los datos biométricos. Este documento puntualizaba la protección de los individuos en materias de tratamiento y circulación de los datos y establecía, entre otros aspectos, que: i) los responsables debían aplicar medidas técnicas y de organización adecuadas contra la destrucción y pérdida accidental, y contra la alteración, difusión o acceso no autorizado; ii) los principios de protección de datos eran aplicables tanto al tratamiento como al procesamiento de los datos cuando éstos pertenecían a un sistema de archivo, pero no cuando eran procesados individualmente; iii) los datos personales debían ser recolectados para un propósito específico, explícito y legítimo y ser asequibles por el tiempo necesario para alcanzar ese propósito, además de ser proporcionados, adecuados, relevantes e ir de acuerdo al propósito (principio de propósito y proporcionalidad establecido en el artículo 6) (GT29, 2012: 6).[26]

El Documento sobre Biométrica (WP80) de 2003 buscó contribuir a la aplicación homogénea y efectiva en la protección de datos en conjunto con la Data Protection Directive 95/46/EC [EE95]. En el documento se señalaba que los datos biométricos

23. «Biometric data and data protection regulations (GDPR and CCPA)», Thales Group, 12 de mayo de 2020, disponible en https://bit.ly/2XAif2H.

24. McCray, «Sensitive to the touch», p. 79.

25. «Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data», Consejo de Europa, 28 de enero de 1981, disponible en https://bit.ly/2XvDXF7.

26. «EU Data Protection Directive (95/46/EC)», EUR-Lex, disponible en https://bit.ly/2A7tW9l. En derecho público, la proporcionalidad se refiere al establecimiento de ciertas reglas para justificar la intervención estatal con los derechos y libertades fundamentales del individuo.

son datos personales y sólo pueden ser tratados y procesados si existe una base legal y el conocimiento y consentimiento de los individuos para la recolección de los datos biométricos, por lo que los sistemas que no cumpliesen con estas normas debían ser evitados (GT29, 2012: 17). Sin embargo, el documento no establecía cómo el propósito y la proporcionalidad (idoneidad, necesidad y adecuación en un contexto dado) debían ser aplicados a los datos biométricos (Kindt, 2007: 169; Pato y Millet, 2010: 86).

Los datos biométricos en el Reglamento General de Protección de Datos

El Reglamento General de Protección de Datos 2016/679 fue aprobado en abril de 2016 por el Parlamento Europeo, para entrar en vigor el 25 de mayo de 2018. Esta Ley regula en el sistema legal europeo la protección de datos y privacidad para los individuos de la Unión Europea y el Área Económica Europea, como sustitución de la Directiva 95/46/EC.[27] Esta Ley fue diseñada para (artículo 1):

- Regular la forma como las empresas protegen los datos personales de los europeos.
- Empoderar la privacidad de los ciudadanos europeos.
- Reconciliar las leyes europeas específicas de privacidad de datos.
- Cambiar la forma como las organizaciones visualizan la protección de los datos que recolectan, con especial atención en el procesamiento de los datos y en la libre movilidad de esos datos.

El Reglamento es aplicable a todas las organizaciones, ubicadas en territorio europeo o fuera de éste, cuando ofrecen bienes o servicios que procesan datos personales de las personas que residen en la Unión Europea (tabla 1).

En esta Ley, los datos personales son definidos como la información que permite identificar a una persona o la hace identificable, es decir, puede ser identificada directa o indirectamente, por medio de una referencia sobre el identificador como el nombre o el número de identificación e incluso mediante factores físicos, sicológicos, económicos, culturales, genéticos o sociales. Los datos personales incluyen identificadores en línea (dirección IP, identificadores de telefonía móvil) y datos de localización que deben protegerse como todos los datos personales (artículo 4).

En el artículo 1 de la Ley se protegen los derechos y libertades fundamentales de las personas físicas y se establece el derecho humano a la protección de datos personales. En los siguientes tres artículos se introducen nuevos conceptos:

27. En Tikkinen-Piri, Rohunen y Markkula (2018) se elabora un análisis minucioso sobre los cambios entre ambas legislaciones.

Tabla 1. Conceptos del Reglamento General de Protección de Datos

Propósito	Permitir el libre movimiento de datos personales dentro de la Unión Europea protegiendo los derechos fundamentales y las libertades de las personas naturales, así como su derecho a la protección de los datos personales.
Alcance material	Se aplica al procesamiento de datos personales, ya sea en totalidad o en partes, dentro del ámbito de aplicación del derecho de la Unión Europea.
Alcance territorial	Aplica al procesamiento de datos que se lleva a cabo dentro de la Unión Europea en el contexto de sus actividades y fuera de ella cuando se ofrecen bienes y servicios a individuos que pertenecen a la Unión Europea.
Datos personales	Información relativa a una persona natural identificable o identificada.
Datos sensibles	Los datos biométricos son datos sensibles que se utilizan para identificar de forma única a una persona natural.
Consentimiento	Las compañías no pueden usar términos ilegibles y condiciones ilegales. El requerimiento exige un formato claro y accesible.
Controlador de datos	Persona natural o legal o autoridad que determina, junto con otros, los propósitos del procesamiento de datos personales.
Oficiales de Protección de Datos	Persona de seguridad y legal responsable de vigilar que las compañías cumplan con los requisitos y establezcan una adecuada estrategia de implementación.
Acceso a los datos	Los dueños de los datos tienen derecho de obtener del controlador información y comunicación sobre el estado que guarda el procesamiento de los datos personales que los conciernen de manera clara, y de acceder a los datos personales y ejercer los derechos de eliminación y rectificación de los datos personales, el derecho a presentar una queja ante un DPA, la fuente de los datos.
Transferencia de datos a otros países	Los datos personales solo pueden ser transferidos a otros países que la Unión Europea considere que tienen leyes que proveen adecuada protección o cuando estén protegidos por normas vinculantes.*
Nuevas provisiones y principios	Transparencia del procesamiento de datos, rendición de cuentas y procesamiento de datos que no requieren identificación.

* Al momento en que el Reglamento empezó a ser aplicable, los países que cumplían con una adecuada protección eran Andorra, Argentina, Canadá (solo organizaciones comerciales), Islas Feroe, Guernsey, Israel, Isla de Man, Jersey, Nueva Zelanda, Uruguay y Estados Unidos (si el destinatario es parte del Escudo de Privacidad). La transferencia de datos a estos países está expresamente permitida. El Escudo de Privacidad provee a las compañías que se encuentran a ambos lados del Atlántico, de un mecanismo para cumplir con los requisitos para la protección de datos cuando éstos son transferidos entre y por la Unión Europea y Suiza, o la Unión Europea y Estados Unidos, para soportar el comercio trasatlántico. «Privacy Shield overview», Privacy Shield Framework, disponible en https://bit.ly/2X96K3n.

Primero, datos seudónimos referentes a los datos que han sido expuestos a medidas tecnológicas, como la encriptación. Estos datos ya no pueden ser sinónimo de identificación, porque requieren de información adicional —que está separada— para ello. La ley fomenta estos datos con la finalidad de lograr mayor seguridad y privacidad por diseño.

Segundo, la privacidad por diseño se refiere a la inclusión de la protección de datos desde el principio del diseño de los sistemas, de tal manera que solo sean procesados los datos necesarios para terminar las obligaciones y limitar el acceso a ellos a cualquier persona fuera del proceso; los datos genéticos considerados datos personales sensibles que requieren consentimiento explícito para ser procesados.

Tercero, la portabilidad de los datos, referida al derecho de los sujetos a recibir datos personales concernientes a su persona, mismos que fueron provistos con anterioridad en otro formato.

Por último, la violación de los datos personales cuando existe una transgresión en la seguridad que conduce a una destrucción accidental o intromisión en los datos almacenados (artículos 1 a 4). El procesamiento de datos biométricos y sensibles está prohibido a menos que la Ley lo permita expresamente o haya sido dado el consentimiento por el sujeto en cuestión.

En los principios considera la transparencia del procesamiento de datos, lo que incluye la legalidad, equidad y transparencia; propósito específico, explícito y legítimo; recolección adecuada, relevante y limitada de acuerdo con el propósito; datos precisos y actualizados, la rendición de cuentas y el procesamiento que no requiere identificación (artículo 5).

Las organizaciones y las administraciones públicas se sujetan a las reglas de esta Ley cuando procesan datos personales, y al cumplimiento y observancia de los principios clave: procesamiento justo, transparente y legal; recolección para propósitos específicos, explícitos y legítimos; minimización de datos y retención de datos; seguridad de los datos personales; así como información al individuo sobre el procesamiento (artículo 5).

Un aspecto de gran importancia para el empoderamiento de los individuos sobre sus datos personales se encuentra referido en el artículo 13, el cual señala la necesidad de que el controlador,[28] al obtener los datos, provea al sujeto de la siguiente información y le permita el ejercicio de sus derechos:

- Identidad y detalles de contacto.
- Detalles de contacto del oficial de protección de datos.
- Propósitos del procesamiento y su base legal.
- Beneficiarios de los datos personales.
- Razones sobre la posible transferencia de datos personales.
- Período de tiempo que esos datos serán guardados o el criterio utilizado para determinarlo.
- Derecho a solicitar el acceso, rectificación o borrado de los datos personales o a la restricción del procesamiento en relación con el interesado u objeto de procesamiento.
- Derecho a solicitar la portabilidad de los datos y a retirar el consentimiento.

28. Persona jurídica, autoridad, agencia o cualquier otro organismo que solo o en conjunto con otros, determine los fines y medios del procesamiento de datos personales (artículo 4).

Infringir la Ley lleva a multas del 4% de la facturación global anual[29] o de 20 millones de euros, lo que sea más alto. Las compañías deben solicitar el consentimiento de los individuos de forma inteligible y con fácil acceso, usando lenguaje claro, de manera que sea posible distinguirlo de otros asuntos y pueda ser removido sin dificultad. Cuando el procesamiento de datos cuenta con el consentimiento del individuo, éste debe ser hecho sobre la base de una decisión informada y expresada a través de una acción afirmativa, es decir, a través de una política que no discrimine.

Si bien pareciera que la Ley se refiere en todos los casos a los datos personales, al ser parte de ellos datos biométricos, esta regulación los abarca en su totalidad. Por otra parte, por tener características diferentes, son mencionados en varios artículos, aunque no se dedique a ellos en forma concreta. Los datos biométricos fueron identificados y definidos como cualquier información que permite identificar o reconocer a una persona natural a partir de un identificador existente, como el nombre. En este sentido, los datos biométricos son los datos personales que resultan de un procesamiento técnico específico concerniente a características físicas, sicológicas y de conducta de una persona natural, que permiten o confirman la identificación única de esa persona, como la imagen facial (artículo 4). Los datos biométricos como parte de los datos personales son considerados datos sensibles, y por tanto están sujetos a altos índices de protección (artículo 4).

Según señala el artículo 9, el procesamiento de los datos biométricos está prohibido a menos que exista consentimiento explícito para un propósito determinado y que previamente el controlador de los datos haya realizado y documentado una evaluación de impacto de privacidad (DIA) o una evaluación de impacto de la protección de datos (DPIA). El consentimiento requiere ser informado cuando existe la posibilidad de una transferencia (artículo 6), lo que implica conocer la identidad del controlador, propósito, tipo de datos y derecho a retirar el consentimiento, además de existir la posibilidad de presentarse riesgos específicos por la inexistencia de protección de los datos en otro país (GT29, 2018: 7). La evaluación de impacto de la protección de datos solo es obligatoria cuando pone en riesgo los derechos y libertades de los individuos y resulta particularmente importante llevarla a cabo cuando se utiliza nueva tecnología para el procesamiento de datos (GT29, 2017: 7).

Es importante destacar que, si bien el consentimiento es la base legal para el procesamiento, la Ley señala también el contrato, las obligaciones legales, los intereses vitales del interesado, el interés público y el interés legítimo (artículo 6). Finalmente, cabe destacar que el acceso a los datos es clave en esta Ley, porque permite el ejercicio de los derechos de consulta, ratificación o eliminación y porque, al ser los datos omitidos o incompletos, los controladores pueden hacerse acreedores a multas (artículos

29. La facturación global anual es sinónimo del total de ingresos de una empresa en la Unión Europea en un año. Es un movimiento financiero anual en el mundo.

12 y 15). Por tanto, esta Ley no solo define los datos biométricos, sino que regula el tratamiento que puede hacerse de ellos.

Retos y riesgos

El uso de las computadoras, la World Wide Web e internet abrieron el camino a riesgos de privacidad y seguridad de gran relevancia, como la compilación no autorizada de datos biométricos sin conocimiento ni consentimiento de los individuos (cámaras ocultas); la compilación biométrica con fines no necesarios para obtener una verificación contundente; el uso y distribución de los datos biométricos sin autorización o con propósitos diferentes a los autorizados, para monitorear la actividad y la expansión del sistema biométrico en áreas no pensadas desde el origen; la recopilación secreta; las tasas de aceptación falsa y de reconocimiento falso (medidas que se crean ante la probabilidad de que el sistema de seguridad biométrica acepte o rechace incorrectamente un intento de acceso por parte de un usuario no autorizado o autorizado, conocidas como FAR (*false acceptance rate* o porcentaje de instancias de identificación no autorizadas que son aceptadas incorrectamente) y FRR (*false rejection rate* o porcentaje de instancias de identificación autorizadas que son rechazadas incorrectamente); el robo y el fraude; la vigilancia; el reuso incompatible; el movimiento imperceptible de datos y el uso de un identificador único para conectar bases de datos (Breebaart, Kindt y Busch, 2008: 26; GT29, 2012: 17; Kindt, 2007: 167).

Estos riesgos están asociados con el tratamiento que se hace de los datos, el propósito para el cual estos datos son utilizados, el almacenamiento, la protección que se hace de ellos por parte de los responsables y el acceso y control de los datos por parte de sus dueños.

Tratamiento

El tratamiento se refiere a la recolección, uso, almacenamiento, modificación, consulta, transmisión, cotejo, limitación y destrucción de los datos. Incluye el procesamiento con consentimiento del individuo para llevar a cabo una contratación, una queja, la protección de intereses vitales o una tarea de interés público. También señala las acciones a llevar a cabo en los casos de procesamiento de categorías especiales de datos personales, el procesamiento de datos relativos a crímenes y el procesamiento que no requiere identificación (artículos 4-6, 9-11).

Los riesgos en el tratamiento inician con el diseño de sistemas biométricos para reconocer y rastrear a los individuos sin su consentimiento (Pato y Millet, 2010: 11). Pero el consentimiento es un principio clave de la legislación para la protección de los datos biométricos, por lo que requiere de la información al individuo respecto de lo que se hará con esos datos.

Otro riesgo se presenta con el uso de las tecnologías para mejorar la privacidad, que no resulta ser una solución para evitar riesgos en el tratamiento de los datos, porque no son conocidas y utilizadas por la mayoría de las personas, muchas veces fallan y otras involucran a terceros desconocidos que ponen en riesgo la privacidad y la seguridad de los datos del individuo.[30]

El reconocimiento facial es un sistema biométrico que se caracteriza por medir y registrar de manera automática nombre, lugar y tiempo (Maden, 2019: 227). Con este sistema se desarrolla un problema enorme para la privacidad de los individuos. Si bien su uso para desbloquear sistemas electrónicos como el móvil o la computadora facilita muchas actividades individuales, el uso que hacen múltiples organizaciones privadas y públicas para monitorear las actividades individuales es violatorio (Garrido y Becker Castellaro, 2017: 85).[31]

De la misma manera, la información grabada es vulnerable. La distribución de cámaras en eventos culturales, religiosos, sociales y políticos invade la esfera privada de los individuos y muchas veces pone en riesgo su seguridad y libertad, por lo que quebrantan los derechos humanos. La recolección, almacenamiento y manipulación de estos datos se presenta de manera cotidiana sin que la Ley intervenga.

A pesar de que el Reglamento General de Protección de Datos trajo considerables cambios a las compañías en materia de tratamiento de los datos personales y privacidad, el cumplimiento de requisitos por parte de compañías no europeas e internacionales debe hacerse en corto tiempo, lo que pone en riesgo la información por la falta de conocimiento y entendimiento sobre la manera de implementarlos (Tikkinen-Piri, Rohunen y Markkula, 2018: 136).

Propósito

Referido a las acciones que se realizan con los datos recolectados. Los problemas de privacidad, seguridad y libertad por el uso de datos para propósitos desconocidos son inminentes cuando se habla de biométrica, principalmente porque los factores sociales, legales y culturales no son considerados al momento de diseñar y desarrollar sistemas biométricos, lo que los convierte en tópicos de preocupación ante la pérdida de conciencia sobre los riesgos de protección de datos, la pérdida de derechos y el impacto en la vida de los individuos (Pato y Millet, 2010: 12, 89). Asimismo, el hecho de que los datos no sean precisos o actualizados y no tengan un propósito definido en el que se explicite para qué serán procesados, pone en riesgo la integridad del individuo al ser sujeto de una mala autenticación (Kindt, 2007: 168).

30. «Privacy enhancing technologies», Office of the Privacy Commissioner of Canada.

31. Enrique Dans, «Do we need to recognize that we have a facial recognition problem?», *Forbes,* 28 de junio de 2019, disponible en https://bit.ly/2XHLOiS.

El Reglamento obliga a las organizaciones privadas a establecer el propósito y no compartir los datos personales con ningún tercero a menos que haya una causa justificada, en cuyo caso, debe avisar al dueño de los datos personales para su conocimiento y consentimiento. Con esta legislación, las compañías deben cambiar la mentalidad, gestión y acciones, lo que está resultando un tanto complicado, no solo en cuanto a los costos, personal, capacitación y diseño tecnológico, sino también en cuanto al cambio, al establecimiento de propósitos específicos que acotan su mercado, y principalmente al cumplimiento de los requisitos que conducen a nuevas acciones y responsabilidades (artículo 6).

Almacenamiento

Referido a la manera en que los datos biométricos son guardados, el almacenamiento de los datos biométricos trae riesgos a la seguridad y privacidad cuando se lleva a cabo en una base de datos central. El reuso de la información con otros propósitos o el acceso accidental pueden alterar los datos incluso cuando se encuentren encriptados. Por tanto, es aconsejable guardar la información en un *token* personal y que el individuo sea quien lo conserve, aunque en este caso se presentan dos problemas: i) el controlador tiene el derecho legal de la propiedad y el contenido del dispositivo, lo que puede traer abusos e invasión de la privacidad; ii) el individuo no solo desconoce lo que está guardado en el *token,* sino que no sabe cómo acceder a esos datos (Liu, 2008: 49).

Los sistemas de almacenamiento corren el riesgo de que alguna persona (un cracker) tenga acceso al sistema y comprometa o robe los datos cuando éstos son recopilados y comparados con datos ya capturados.[32] El RGPD señala que los datos deben ser almacenados por el tiempo que sea necesario su procesamiento, o por períodos más largos cuando el propósito del almacenamiento sea de interés público o por razones científicas proveyendo a los datos de las medidas de seguridad necesarias (artículo 5).

Protección

La protección involucra los derechos de los individuos para obtener información y acceso a los datos; para corregirlos o borrarlos cuando ya no sean necesarios; oponerse a uso con fines comerciales; limitar el tratamiento para ciertas situaciones, y la portabilidad de los datos. También involucra las obligaciones que tienen organizaciones públicas, privadas y académicas y los principios aplicables.

Cabe agregar que parte de los riesgos que se presentan en la protección se debe a

32. «Biometric authentication benefits and risks», Identity Management Institute, disponible en https://bit.ly/2MdSEHz.

que los sistemas biométricos no son perfectos, y puede existir el riesgo importante de identificación errónea y consecuentes daños irrefutables, por lo que borrar al sujeto de la base de datos no es la mejor solución. Lo mismo sucede cuando las tasas de aceptación falsa dan lugar a que gente inocente sea detenida. El problema está latente y no se ha encontrado alguna solución que elimine el riesgo.[33]

Por otra parte, los riesgos pueden ser ocasionados por el controlador de los datos biométricos, lo que puede llevar a discriminación y abusos en la prestación de servicios, entrega de productos o en el goce de los derechos y a la pérdida paulatina del anonimato (Garrido y Becker Castellaro, 2017: 86-87). Una violación a los sistemas de datos biométricos compromete los datos y pone a los individuos en riesgo ante la posible presencia de ataques de identificación (Kindt, 2007: 168). Entonces, corresponde a la legislación proveer de medios a los individuos para que la protección se lleve a cabo.

En el RGPD se establece que para ejercer los derechos de protección de datos, el individuo debe solicitarlos al tenedor de los datos, quien tiene un mes para su entrega. Cuando los derechos son violentados, entonces se puede presentar una reclamación o emprender acciones legales ante las autoridades responsables de la aplicación de la regulación (artículos 60, 77-80).

Control

Como sistema de identificación para el reconocimiento y autorización que facilita el acceso biométrico y la verificación de datos, normalmente es manejado de forma superficial. Sin embargo, a partir del RGPD se busca que los individuos tengan más control sobre los datos que recopilan las empresas a través de: i) reglas establecidas para el cumplimiento de la protección y el tratamiento de los datos biométricos; ii) la transparencia como principio, que establece que los datos y la información dirigida a los usuarios deben ser claros y de fácil acceso; y iii) la rendición de cuentas, que obliga al controlador a ser responsable ante la perdida, daño o mal uso de los datos e información en su poder. Cuando se presenta un fraude y los datos son utilizados, no es posible emitir una nueva identidad para un individuo (ADC, 2017: 11).

A pesar de la legislación, se ha observado que el empoderamiento de los individuos para el control de sus datos es una irrealidad. El manejo de los datos personales es llevado a cabo de forma irresponsable por parte de las empresas y, hasta ahora, las regulaciones sobre datos personales son infringidas. Los datos personales no son utilizados con un propósito definido, por lo que son distribuidos hacia terceros, sin que el individuo conozca los propósitos para los cuales sus datos serán utilizados. Asimismo, el individuo difícilmente puede tener acceso a sus datos personales para

33. «Types of biometrics», Biometrics Institute.

rectificar o borrar la información, y recuperarlos es prácticamente imposible. Los individuos han dejado de ser dueños de sus datos personales.[34]

En este sentido, los datos biométricos están incluidos. En la actualidad, la libertad de expresión se puede ver afectada por los datos biométricos ante la posible vigilancia en actos públicos, en especial en la zona de interacción humana dentro del ámbito de la privacidad determinada por el Tribunal Europeo de Derechos Humanos (ADC, 2017: 14).[35]

Conclusiones

Las tecnologías de la información han modificado la forma en que los individuos obtienen productos y servicios. La identificación ha evolucionado desde la contraseña y tarjeta *token*, pasando por la encriptación, hasta la biométrica. La biométrica ha cambiado la manera en que se desarrolla la identidad de los individuos. La recolección, almacenamiento y uso de los datos biométricos que llevan a cabo las organizaciones públicas, privadas o académicas han puesto en riesgo la privacidad, seguridad y libertades de los individuos.

La biométrica exige un procesamiento diferente al que se otorga en la legislación de protección de datos personales. Aunque los datos biométricos están contenidos en estos últimos, no hay que olvidar que tienen características que obligan a atender los cambios y proceder de manera diferente.

Varios países se han preocupado por el impacto que traen estos avances y las implicaciones en materia de derechos humanos, privacidad y seguridad. No obstante, aún faltan acciones por realizar, así como promover la renovación e incremento de legislación que regule la recopilación de datos biométricos. Así, falta desarrollar y establecer candados de seguridad al almacenamiento de datos biométricos, de manera que los fraudes, robos o uso de programas maliciosos no afecten la información contenida en las bases de datos. También se hace indispensable informar a los individuos sobre el propósito y las acciones que se ejecutarán con los datos biométricos y que éstos otorguen su consentimiento, porque, de otra manera, como ha sucedido hasta ahora con los datos personales, serán diseminados con propósitos desconocidos, mientras que los individuos no solo desconocen que sus datos se encuentran en un mar de organizaciones, sino que no pueden tener acceso a ellos para ejercer sus derechos. Hace falta legislar concretamente sobre datos biométricos y sus consecuencias para evitar pérdida de identidad.

34. Carl Miller, «Would you recognise yourself from your data?», *BBC News,* 29 de mayo de 2019, Disponible en https://bbc.in/3dc4ePD.

35. «Guide on article 8 of the European Conventio on Human Rights», Tribunal Europeo de Derechos Humanos, 31 de agosto de 2019, párrafo 68, disponible en https://bit.ly/2TOv7Bq.

Si bien las tecnologías de mejora de la privacidad han ayudado a reducir el acceso indeseado a los datos biométricos, continúan existiendo riesgos que dañan los derechos humanos de los individuos con posibilidades de ser vigilados, perder autonomía, ser discriminados o incluso ser susceptibles de intromisiones en su intimidad.

Las legislaciones analizadas son ejemplos a seguir por los países en que las organizaciones hacen uso de la biométrica para identificar a los individuos. No es suficiente adicionar el término al azar en la legislación de protección de datos personales, sino que es necesario integrar un apartado específico para su protección, dado que no es lo mismo tener los datos básicos de un individuo a tener datos sensibles como los datos biométricos. De ahí que no solo sea garantía de seguridad y privacidad el crear una ley para la protección de los datos biométricos, sino realmente aplicarla cuando los individuos son afectados. No basta con legislar en la materia, se necesita un mecanismo que garantice a los individuos el uso correcto de la información, el otorgamiento real de su consentimiento, en formato claro y conciso, y la recuperación de los datos biométricos cuando así lo requiera.

Referencias

ADC, Asociación de los Derechos Civiles (2017). «La identidad que no podemos cambiar: Cómo la biometría afecta nuestros derechos humanos». Disponible en https://bit.ly/3dfoVtH.

Agre, Philip y Marc Rotenberg (editores) (1998). *Technology and privacy: The new landscape*. Cambridge: MIT Press.

Breebaart, Jeroen, Els Kindt y Christoph Busch (2008). «A reference architecture for biometric template protection based on pseudo identities». En *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures* (pp. 25-37). Darmstadt: Gesellschaft für Informatik. Disponible en https://bit.ly/3dirqMa.

Browning, John (2018). «The battle over biometrics». *Texas Bar Journal,* 81 (9): 674-76. Disponible en https://bit.ly/3cdK5Y5.

Federrath, Hannes (2005). «Privacy enhanced technologies: Methods, markets, misuse». En *Second International Conference, TrustBus 2005* (pp. 1-9). Copenhague: Springer.

Garrido, Romina y Sebastián Becker Castellaro (2017). «La biometría en Chile y sus riesgos». *Revista Chilena de Derecho y Tecnología,* 6 (1): 67-91. DOI: 10.5354/0719-2584.2017.45825.

GT29, Grupo de Trabajo sobre Protección de Datos del Artículo 29 (2003). «Working document on biometrics». Documento de trabajo, WP80. Disponible en https://bit.ly/2Xfabpu.

—. (2012). «Opinion 3/2012 on developments in biometric technologies». Documento de trabajo, WP193. Disponible en https://bit.ly/2XcM6iL.

—. (2017). «Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of regulation 2016/679». Documento de trabajo. Disponible en https://bit.ly/2WsdTui.

—. (2018). «Guidelines on Article 49 of Regulation 2016/679». Documento de trabajo. Disponible en https://bit.ly/2zScaHq.

Hansen, Marit, Ari Schwartz y Alissa Cooper (2008). «Privacy and identity management». *IEEE Security & Privacy,* 6 (2): 38-45. DOI: 10.1109/MSP.2008.41.

Hes, Ronald y John J. Borking (editores) (1998). *Privacy-enhancing technologies: The path to anonymity*. La Haya: Registratiekamer.

Jain, Anil K. (editor) (2006). *Biometrics: Personal identification in networked society*. Volumen 1. Nueva York: Springer.

Jain, Anil K., Ruud Bolle y Sharath Pankati (1996). «Introduction to biometrics». En *Biometrics*. Boston: Springer.

Jain, Anil K., Lin Hong y Sharath Pankati (2000). «Biometric identification». *Communications of the ACM,* 43 (2): 91-98.

Jain, Arvind K. (editor) (2001). *The political economy of corruption*. Londres: Routledge.

Jasserand, Catherine (2016). «Legal nature of biometric data: From "generic" personal data to sensitive data». *European Data Protection Law Review,* 2 (3): 297-311. DOI: 10.21552/EDPL/2016/3/6.

Kent, Stephen y Lynette Millet (editores) (2003). *Who goes there?: Authentication through the lens of privacy*. Washington DC: National Academies Press. DOI: 10.17226/10656.

Kindt, Els (2007). «Biometric applications and the data protection legislation: The legal review and the proportionality test». *Datenschutz Und Datensicherheit,* 31 (3): 166-70. DOI: 10.1007/s11623-007-0064-6.

—. (2010). «The use of privacy enhancing technologies for biometric systems analysed from a legal perspective». En *Privacy and identity 2009: Privacy and identity management for life* (pp. 134-145). Berlín: Springer. DOI: 10.1007/978-3-642-14282-6_11.

Kosciejew, Marc (2014). «Proposing charter of personal data rights». *Information Management*, 48 (3). Disponible en https://bit.ly/2McCz5e.

Liu, Yue (2008). «Identifying legal concerns in the biometric context». *Journal of International Law and Technology,* 3 (1): 45-54. Disponible en https://bit.ly/36HArLY.

Maden, Mike (2019). *Tom Clancy's Line of sight*. Nueva York: Berkley.

Millard, Christopher y W. Kuan Hon (2012). «Defining "personal data" in e-social science». *Information, Communication & Society,* 15 (1): 66-84. DOI: 10.1080/1369118X.2011.616518.

Miller, Benjamin (1994). «Vital signs of identity». *IEEE Spectrum,* 31 (2): 22-30. DOI: 10.1109/6.259484.

Nguyen, Fiona (2018). «The standard for biometric protection». *Journal of Law and Cyber Warfare, 7* (1): 61-84. Disponible en https://bit.ly/36Loh54.

Palen, Leysia y Paul Dourish (2003). «Unpacking "privacy" for a networked world». En *Proceedings of the Conference on Human Factors in Computing Systems* (pp. 129-136). Florida: ACM Press. DOI: 10.1145/642611.642635.

Pato, Joseph y Lynette Millet (editores) (2010). *Biometric recognition: Challenges and opportunities*. Washington DC: National Academies Press. DOI: 10.17226/12720.

Rojas González, Isai y Gabriel Sánchez Pérez (2012). «Leyes de protección de datos personales en el mundo y la protección de datos biométricos, parte 2». *Seguridad*, 14. Disponible en https://bit.ly/2ApiGVC.

Rosenker, Heather y Megan Hirshey (2008). *Biometrics in government post-9/11. Advancing science, enhacing operations*. Washington DC: National Science and Technology Council.

Sánchez Pérez, Gabriel e Isai Rojas González (2012). «Leyes de protección de datos personales en el mundo y la protección de datos biométricos, parte 1». *Seguridad*, 13. Disponible en https://bit.ly/2AoGQQ5.

Shen, Jun y Siani Pearson (2011). «Privacy enhancing technologies: A review». Hewlet Packard Development Company. Disponible en https://bit.ly/3cfpAKz.

Solove, Daniel J. (2006). «Taxonomy of privacy». *University of Pennsylvania Law Review,* 154 (3): 479-560. Disponible en https://bit.ly/2MaomCy.

—. (2008). *Understanding privacy*. Cambridge: Harvard University Press.

Tikkinen-Piri, Christina, Anna Rohunen y Jouni Markkula (2018). «EU General Data Protection Regulation: Changes and implications for personal data collecting companies». *Computer Law & Security Review,* 34 (1): 134-53. DOI: 10.1016/j.clsr.2017.05.015.

Toli, Christina-Angeliki y Bart Prennel (2015). «Biometric solutions as privacy enhancing technologies». En *Amsterdam Privacy Conference (APC) 2015* (pp. 1-16). Amsterdam. Disponible en https://bit.ly/3guOidj.

Ucciferri, Leandro y Eduardo Ferreyra (2017). *Cuantificando identidades en América Latina: Un breve repaso acerca de cómo las sociedades latinoamericanas se enfrentan a la implementación de las tecnologías biométricas*. Buenos Aires: Asociación por los Derechos Civiles. Disponible en https://bit.ly/2BgBs2b.

Wang, Yang y Alfred Kobsa (2009). «Privacy enhancing technologies». En *Handbook of research on social and organizational liabilities in information security* (pp. 203-227). Hershey: IGI Global. Disponible en https://bit.ly/2XFogby.

Woodward, J. D. (1997). «Biometrics: Privacy's foe or privacy's friend?». *Proceedings of the IEEE,* 85 (9): 1.480-1.492. DOI: 10.1109/5.628723.

Zhang, David D. (2000). *Automated biometrics: Technologies and systems*. Nueva York: Kluwer Academic Publishers. DOI: 10.1007/978-1-4615-4519-4.

Sobre la autora

Gabriela Quintanilla Mendoza es administradora pública. Licenciada en Ciencia Política y Administración Pública, Universidad Nacional Autónoma de México. Maestrías en Gobierno y Asuntos Públicos por la Universidad Nacional Autónoma de México y en Pedagogía por la Universidad Pedagógica Nacional, México. Doctorado en Ciencias Políticas y Sociales por la Universidad Nacional Autónoma de México. Su correo electrónico es gabrielllaq@yahoo.com. https://orcid.org/0000-0002-7456-4242.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL
Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB
rchdt.uchile.cl

CORREO ELECTRÓNICO
rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).