Revista Ius et Praxis
Talca, Chile, 2025
Artículo de Investigación
Fecha de recepción: 2024-11-04; fecha de aceptación: 2025-04-03
DOI: 10.4067/S0718-00122025000200003

TUTELA DE LA INFORMACIÓN PERSONAL: DESAFÍOS PARA LA PROTECCIÓN DE LOS DATOS BIOMÉTRICOS EN CHILE

Protection of personal information: challenges for the protection of biometric data in Chile

SANZ-SALGUERO, FRANCISCO J. *
Universidad Santo Tomás, Chile

Resumen

Este artículo tiene por objeto describir el estado del arte de la protección de los datos biométricos en el derecho chileno, teniendo en cuenta el escenario que surge con la aprobación de la nueva Ley sobre Protección de Datos Personales. Para estos efectos se abarca un amplio espectro doctrinal y legal, análisis que comienza con un panorama general de la biometría, y prosigue con un ejercicio de comparación entre la Ley 19.628 sobre Protección de la Vida Privada y la nueva Ley sobre Protección de Datos Personales. La investigación, también aborda la situación de los datos biométricos desde el punto de vista del derecho de la Unión Europea y su incidencia en el ordenamiento jurídico chileno, contrastando la nueva Ley sobre Protección de Datos Personales chilena y el Reglamento General de Protección de Datos, analizando los efectos de la vocación de extraterritorialidad atribuible al Reglamento Europeo, y revisando el tratamiento de la información biométrica por parte de la Ley de Inteligencia Artificial. En el marco de sus conclusiones, el presente trabajo reconoce que, no obstante los avances generados con la aprobación de la nueva Ley sobre Protección de Datos Personales, el texto legal podrá dar una mejor respuesta a la pretensión de resguardo de la información biométrica, si aprovecha la experiencia del derecho de la Unión Europea en el ámbito de los datos personales y la inteligencia artificial.

Palabras clave

Datos biométricos; Nueva Ley sobre Protección de Datos Personales; Reglamento General de Protección de Datos de la Unión Europea.

Abstract

This article aims to describe the state of the art of the protection of biometric data in Chilean law. For these purposes, a broad doctrinal and legal spectrum is covered, an analysis that begins with a general overview of biometrics, and continues with a comparison exercise between Law 19,628 on the Protection of Private Life and the new Law on the Protection of Personal Data. The investigation also addresses the situation of biometric data from the point of view of European Union law and its impact on the Chilean legal system, contrasting the new Chilean Law on Personal Data Protection and the General Data Protection Regulation, analyzing the effects of the extraterritoriality vocation attributable to the European Regulation, and reviewing the treatment of biometric information by the Artificial Intelligence Law. Within the framework of its conclusions, this work recognizes that, despite the advances generated with the approval of the new Law on the Protection of Personal Data, the legal text will be able to provide a better response to the claim of safeguarding biometric information, if it takes advantage of the experience of European Union law in the field of personal data and artificial intelligence.

Key words

Biometric data; New Law on Protection of Personal Data; General Data Protection Regulation.

* Doctor en Derecho por la Pontificia Universidad Católica de Valparaíso, Académico Investigador en la Universidad Santo Tomás, Santiago, Chile. Correo electrónico: fjsanzsalguero@hotmail.com; ORCID: https://orcid.org/0000-0002-3082-3863. La investigación es parte del proyecto: ANID/FONDECYT/Iniciación 11221089.

1. Introducción

A nivel universal, en especial desde los inicios de la llamada *época de la información*[1], el interés por el tratamiento de la información personal ha sido permanente[2]. La protección de los datos personales debe estudiarse de forma simultánea con los avances alcanzados en el ámbito de la *transformación digital*, proceso enraizado en la innovación tecnológica que trae aparejada nuevas oportunidades, pero que a la vez puede generar, reproducir o reforzar desigualdades[3]. El funcionamiento de la interconexión informática que representa el internet depende de la creación, almacenamiento y administración de contenidos como los datos personales, escenario en los que una vasta cantidad de información sobre las personas pueda ser interceptada, almacenada y analizada por los Estados y por terceros[4]. Dentro del espectro de la información personal, el tratamiento de los datos biométricos constituye una de las preocupaciones surgidas en el marco de la señalada evolución digital.

Los argumentos esgrimidos respaldan la importancia de la tutela de los datos personales, significancia reconocida por el Derecho continental europeo con la reciente aplicación (2018) del Reglamento General de Protección de Datos de la Unión Europea RGPD, legislación más avanzada en la materia[5]. El efecto del RGPD adquiere mayor relevancia teniendo en cuenta la vocación de eficacia extraterritorial que se le reconoce[6], vocación capaz de otorgarle alcances que superan las fronteras comunitarias.

En el caso chileno, el interés por el resguardo de la vida privada o privacidad y, consecuentemente, la protección de los datos personales, se manifiesta en una evolución legal con dos hitos clave: en primer lugar, tenemos la aprobación de la Ley N° 19.628 de 1999, sobre protección de la vida privada (en adelante LPD), estatuto que en su trámite parlamentario surgió bajo la pretensión de tutelar la vida privada, pero que luego de un complejo desarrollo legislativo terminó limitándose a la protección de los datos personales[7]. En segundo término, observamos la Ley 21719 que "regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales" (en adelante Nueva LPDP), aprobada por el Parlamento chileno[8] y publicada el 13 de diciembre del 2024, estatuto cuya vigencia está diferida hasta el primero de diciembre del 2026.

Simultáneamente, y a diferencia de lo que ocurre en Europa en donde el RGPD define expresamente a los datos biométricos y regula su tratamiento[9], uno de los problemas acreditados en el ordenamiento jurídico chileno (puntualmente en la LPD) lo representaba la falta de claridad sobre la situación de estos datos en particular, información de naturaleza sensible que permite reconocer (o hacer reconocible) a una persona, gracias a alguna característica biofísica o de comportamiento. Sobre este punto, es oportuno reiterar lo expresado por Jijena, autor que recuerda como en el escenario nacional las clínicas de salud, tiendas de *retail*, empresas de telefonía, gimnasios, bancos, recintos deportivos, administraciones de edificios y otros, aplican como estándar cotidiano al cliente el (i) "deme su RUT", el (ii) "ponga su huella" o el (iii) "mire la cámara"[10]. Son evidentes las ventajas que implica la utilización de la biometría, ya que la aplicación de esta ciencia del análisis de las características físicas o del comportamiento permite, de forma inequívoca, demostrar nuestra identidad individual (o *Identidad Digital*), lo que redunda en la posibilidad de operar y acceder a todo tipo

[1] PÉREZ (2013), p. 48.
[2] SANZ (2023 b), p. 1.
[3] Este concepto de *trasformación digital*, es acuñado por la Secretaría General Iberoamericana en la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales, adoptada en la XXVIII Cumbre Iberoamericana de Jefas y Jefes de Estado y de Gobierno, realizada en Santo Domingo, República Dominicana, el 25 de marzo de 2023. SECRETARÍA GENERAL IBEROAMERICANA (2023), p. 6.
[4] FRANCO Y VELOZ (2022), p. 53.
[5] MILANÉS (2017), p. 20.
[6] SANZ (2023b), p. 2.
[7] SANZ (2023a), p. 4.
[8] Aprobación generada el 26 de agosto del 2024.
[9] QUINTANILLA (2020), p. 83.
[10] JIJENA (2024).

de información, y realizar transacciones de manera segura[11]. No obstante la utilidad derivada del uso de estos datos sensibles, en el caso de la LPD su falta de precisión exigía desarrollar una legislación que abordara, en especial, la creación de mecanismos que garanticen a los individuos el uso correcto de esta información, factor que involucra elementos como el otorgamiento real de su consentimiento y la recuperación de los datos biométricos cuando así lo requiera[12]. En este contexto, es necesario llevar a cabo un trabajo de contraste entre la LPD y la Nueva LPDP, a fin de verificar los cambios alcanzados con el trabajo del legislador respecto a la información biométrica.

Finalmente, otro desafío en el ámbito de la biometría consiste en establecer los efectos del Reglamento (UE) 2024/1689, o Ley de Inteligencia Artificial (en adelante Ley de IA) de la Unión Europea, directiva que entre sus aspectos aborda el uso de esta faceta de la evolución tecnológica en el tratamiento de los datos biométricos.

Con las anteriores premisas, y a fin de aportar a la discusión respecto al tratamiento de la información biométrica en el modelo chileno, en su primera fase la investigación desarrolla un panorama general de la biometría. En su segunda etapa, se examina el tratamiento de los datos biométricos en el ordenamiento jurídico chileno, abarcando temas como los desafíos enfrentados durante la redacción de la LPD, los esfuerzos del legislador para mejorar la protección de la información personal (lo que incluye un ejercicio de comparación entre la LPD y la Nueva LPDP), y la reciente controversia interna generada a propósito del escaneo del iris ocular. En su capítulo final, el trabajo aborda la situación de los datos biométricos desde el punto de vista del derecho comparado, llevando a cabo un trabajo de contraste entre el tratamiento de esta información en el RGPD y la Nueva LPDP, examinando la vocación de eficacia extraterritorial atribuida al RGPD, y estudiando los efectos de la Ley de IA de la Unión Europea sobre la información biométrica. En cuanto a su estructura, la investigación está dividida en una introducción, tres apartados principales y las conclusiones.

2. Aspectos generales de la biometría

Explicar los retos que enfrenta la protección de los datos biométricos en Chile, exige en primer lugar abordar los aspectos generales de la biometría, ciencia encargada de establecer la identidad de un individuo según sus atributos físicos, químicos, o comportamentales[13]. La importancia de esta disciplina, va de la mano con los avances de sistemas masivos para el manejo de la identidad de los individuos, factor asociado al desarrollo de instrumentos de seguridad cada vez más complejos. Desde el punto de vista de la informática, la biometría está basada en el principio de que cada individuo es único y posee rasgos físicos distintivos (rostro, huellas digitales, iris ocular, entre otros) o de comportamiento (como la voz o la manera de firmar), los cuales pueden ser utilizados para identificarla o validar restricciones de acceso[14]. Con base en los anteriores argumentos, los rasgos biométricos están representados en atributos conductuales o *biometría conductual*[15] (como ocurre con la firma o la forma de teclear), atributos físicos o *biometría fisiológica*[16] (como ocurre con el rostro, las huellas digitales o el iris) u otros atributos (como lo son la voz, el ADN[17] e, incluso, las *bioseñales*, entendidas estas como las señales fisiológicas que se producen a consecuencia de los cambios electroquímicos en el organismo)[18].

[11] AZANZA (2021).
[12] QUINTANILLA (2020), p. 88.
[13] LUCERO et al. (2020), p. 44.
[14] RUIZ et al. (2009), p. 29.
[15] RUIZ Y RUIZ (2021), p. 294.
[16] RUIZ Y RUIZ (2021), p. 294.
[17] Con respecto al ADN y desde la vigencia de la LPD, Donoso le reconoce la naturaleza de información sensible en su carácter de dato de salud, aclarando la autora que la información sobre el ADN *"no revela estados de salud sino predisposiciones de una persona a ciertas afecciones"*. DONOSO (2011), p. 85.
[18] LUCERO et al. (2020), p. 44.

La identificación de los datos biométricos depende de la presencia de indicadores biométricos, es decir, de alguna característica que permita realizar biometría. En este orden de ideas, cualquier característica humana puede ser considerada como un dato biométrico, siempre que satisfaga las siguientes propiedades: universalidad, unicidad, permanencia y la mensurabilidad [19]. A partir del cumplimiento de estas propiedades, la doctrina clasifica a los datos biométricos en tres grupos[20]:

- datos estáticos, grupo que incluye aquéllos que se extraen de las características físicas de cualquier individuo (como por ejemplo las huellas dactilares, la imagen del rostro o el iris);

- datos dinámicos, grupo que incluye aquéllos que se concentran en el comportamiento (como por ejemplo la forma de caminar, manera en la que se firma o utilización del teclado de un computador), mecanismos que detectan patrones de conducta para vincularlos con una persona especifica;

- datos mixtos, grupo en el que se combinan las técnicas ya mencionadas [como por ejemplo, el patrón de voz, que mezcla técnicas estáticas (características fisiológicas de los apéndices que se utilizan en la creación del sonido) y dinámicas, como el comportamiento del discurso[21]].

Finalmente, desde una perspectiva práctica, la identificación de personas mediante el uso de los datos biométricos se puede llevar a cabo mediante *autentificación* (o *verificación*) *de identidad*, o a través de *identificación*. El primer caso (autentificación o verificación de identidad), implica la recolección de uno o más datos biométricos (por ejemplo, datos estáticos) para que sean procesados y almacenados en una base de datos. Esta fase es conocida en el ordenamiento jurídico de la Unión Europea como "inscripción", la cual permite la generación de una *plantilla* biométrica[22]: la plantilla biométrica es comparada con el dato entregado y, si coinciden, será verificada la identidad de la persona. El segundo caso, determina que la identificación de una persona funciona a través del contraste de una muestra biométrica con una gran cantidad de plantillas biométricas: si coincide el dato biométrico con alguna de las plantillas almacenadas, se habrá identificado al individuo[23].

Llevado a cabo un panorama general de la biometría, los elementos inherentes a la noción de dato biométrico y los usos prácticos de este tipo de información, otro paso exige indagar el tratamiento de los datos biométricos en el ordenamiento jurídico chileno. En el siguiente capítulo, desarrollamos este objetivo.

3. Tratamiento de los datos biométricos en el ordenamiento jurídico chileno

Abordar los desafíos asociados a la tutela eficaz de los datos biométricos en Chile, exige revisar el tratamiento de esta información en el marco jurídico interno. Con esta pretensión y como punto de partida de la discusión, en la primera parte del capítulo nos enfocamos en las dificultades presentes durante la redacción de la LPD. En una siguiente fase, teniendo en cuenta los esfuerzos del legislador para mejorar los estándares de protección de la información personal, en el trabajo se efectúa un ejercicio de comparación entre la LPD y la Nueva LPDP, identificando elementos vinculados directamente con la información biométrica, enfatizando en la situación de los datos sensibles. En sintonía con la fase anterior, la investigación avanza revisando el tratamiento de los datos biométricos en la Nueva LPDP. El capítulo concluye abordando la situación del iris ocular, revisión necesaria a propósito de la reciente controversia por el ofrecimiento de pagos en criptomonedas, a cambio de escanear el iris de los usuarios. A continuación, llevamos a cabo el recorrido propuesto.

[19] ALONSO (2008), pp. 167-168.
[20] GARRIDO Y BECKER (2017), pp. 69 y 70.
[21] ASOCIACIÓN POR LOS DERECHOS CIVILES ADC (2015), p. 3.
[22] La plantilla es una reducción estructurada de una imagen biométrica, es decir, la medida biométrica registrada de una persona. Lo que debe almacenarse es la plantilla, presentada en forma digitalizada, y no el propio elemento biométrico. UNIÓN EUROPEA, GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS (2003), p. 4.
[23] GARRIDO Y BECKER (2017), p. 70.

3.1. Del tratamiento de la vida privada o privacidad a la protección de los datos personales, en el ordenamiento jurídico chileno

En el escenario interno, abordar los retos asociados a la protección eficaz de los datos biométricos, exige inicialmente revisar la posición doctrinal con respecto al resguardo de la vida privada o privacidad. Como comentario preliminar y para facilitar la lectura del documento, advertimos que en adelante utilizaremos indistintamente las expresiones *vida privada* o *privacidad*, lo que se justifica observando la falta de univocidad en los contenidos que la literatura jurídica propone a estos conceptos (de hecho, parte de la doctrina estima que esta diferenciación parece carecer de efectos jurídicos en la legislación interna[24]), llegándose incluso al uso indistinto de las nociones de privacidad y vida privada en algunos modelos normativos[25].

Son diversas las actividades humanas vinculadas al interés fundamental de la vida privada, entre la que se distingue la *protección de datos personales*. En efecto, al concentrarnos en el concepto de *privacidad* o *vida privada*, se reconoce la existencia de un interés jurídicamente protegido a la no intromisión en la vida propia (en diferentes ámbitos: corporal, familiar y espacial) y sobre la información relativa a una persona (es decir, sobre los datos personales)[26].

Al enfocarnos en el resguardo de la información personal, es una categoría que emerge como respuesta ante determinados usos de las nuevas tecnologías[27], avances técnicos que van de la mano del permanente intercambio de información en una sociedad digital. De esta manera, no se trataría del *"derecho a ser dejado en paz"* propuesto por Brandeis y Warren[28]: consistiría en el derecho a la autodeterminación informativa, esto es, el derecho de las personas a controlar sus datos personales[29]. No obstante, el derecho de las personas a controlar su propia información no es un estándar que se cumpliera en la LPD chilena, siendo una de las deficiencias atribuibles a la labor del legislador en la esfera normativa interna[30].

En este orden de ideas, y desde la perspectiva jurídica nacional, la preocupación por la tutela de la vida privada y, consecuentemente, de los datos de naturaleza personal, tiene un hito relevante con la promulgación en 1999 de la LPD, estatuto que en su trámite parlamentario surgió bajo la pretensión de resguardar la privacidad, pero que luego de un intenso trabajo legislativo terminó enfocándose en la protección de los datos personales[31]. Al respecto, compartimos la opinión de Anguita, quien reconoce la presencia de fallas en la técnica legislativa, y una *"falta de claridad en torno a los objetivos del proyecto de ley como una efectiva tutela de los datos personales y derechos conferidos a sus titulares"*[32]. Las fallas atribuibles a la LPD no se limitan a su proceso de construcción legislativa. En este sentido, el incumplimiento de los compromisos adquiridos por el Estado chileno al momento de ingresar (el año 2009) a la Organización para la Cooperación y el Desarrollo Económicos OCDE, compromisos consistentes en la obligación de implementar las Directrices relativas a la protección de la privacidad y el flujo transfronterizo de datos personales, le valió al país ser objeto de advertencias por parte de este organismo[33]. A lo anterior, debe sumarse el listado de críticas planteadas por la doctrina al contenido de la ley[34].

---

[24] Este pensamiento no es nuevo, ya que vemos opiniones en ese sentido desde principios de la década de los 90 del siglo pasado. JIJENA (1992), p. 37

[25] En la escena constitucional chilena, la dificultad para distinguir estos conceptos tiene como ejemplo la redacción del artículo 19 N° 4 de la Carta Política de 1980, proceso de confección normativa en el que se propusieron expresiones como *intimidad* y *privacidad*, hasta llegar a la definitiva *vida privada.* SANZ (2013), pp. 461-462.

[26] LARA et al. (2014), p. 11.

[27] GARCÍA (2007), p. 747.

[28] GLANCY (1979), pp. 3-4.

[29] RAJEVIC (2011), pp. 142-143.

[30] SANZ (2013), p. 476.

[31] SANZ (2023 a), p. 4.

[32] ANGUITA (2007), pp. 277-278.

[33] VIOLLIER (2017), p. 39.

[34] A título de ejemplo, entre las fallas que se imputan al contenido de la LPD, la doctrina incluye la no descripción exacta del objeto regulado por la ley, la falta de un órgano administrativo fiscalizador, la ausencia de un procedimiento de reclamo idóneo, la inexistencia de un catálogo de infracciones y sanciones efectivas, las deficiencias en el tratamiento de las excepciones al consentimiento, solo por mencionar algunas deficiencias. VERGARA (2017), p. 136.

Los problemas identificados, en conjunto, son factores que inciden en la naturaleza deficiente de la normativa sobre protección de datos. Subrayando que no es la pretensión del presente trabajo hacer un examen exhaustivo de la protección de la información personal, si es posible encontrar elementos que aporten a la discusión sobre el tratamiento de la información biométrica en Chile. En este sentido, lo primero que debe indicarse es que los datos biométricos no se encuentran regulados expresamente en la LPD. Teniendo en cuenta esta realidad, el siguiente paso de la investigación consiste en realizar un ejercicio de contraste entre la LPD y la Nueva LPDP, identificando elementos vinculados directamente con la información biométrica, con énfasis en el tratamiento de los datos sensibles. A continuación, llevamos a cabo el ejercicio propuesto.

3.2. Análisis comparativo entre la LPD y la Nueva LPDP: situación de los datos sensibles

Como comentario inicial, debemos señalar que el artículo 2° de la LDP aborda dos categorías: los datos personales y los datos sensibles. La norma [en la letra f)] identifica el dato de carácter personal como el relativo *"a cualquier información concerniente a personas naturales, identificadas o identificables"*, definición en exceso genérica. El carácter genérico de esta noción estaría superado con lo estipulado en la Nueva LPDP, estatuto que no obstante mantener el concepto de dato personal de la LDP, realiza dos innovaciones: agrega el criterio para que una persona física se considere identificable (es identificable *"toda persona cuya identidad pueda determinarse, directa o indirectamente"*), y describe un amplio listado de identificadores que permiten determinar esa identidad[35].

Con respecto al dato sensible, el mismo artículo 2° [pero en la letra g)] lo define como *"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"*, datos cuyo tratamiento está proscrito por la LPD, salvo que el régimen legal lo autorice, se trate de datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares o exista consentimiento del titular (artículo 10). Sobre esta categoría especialmente protegida de la información personal, una primera labor consiste en justificar el carácter de dato sensible atribuible a la información biométrica, desde la perspectiva de la LPD. En este sentido, desde una interpretación literal de la norma, se deduce que los datos que describen *"las características físicas* (…) *de las personas* (es decir, los atributos físicos o biometría fisiológica)*"* poseen carácter sensible. Teniendo en cuenta que los datos sensibles son *"aquéllos que están esencialmente (no excluyentemente) vinculados a la privacidad"*, lo que les otorga *"una mayor potencialidad discriminatoria"*[36], la necesidad de una protección legal radica en que su tratamiento puede afectar la intimidad de los titulares o generar discriminaciones arbitrarias[37]. En consecuencia, el uso indebido o la recolección indiscriminada de los datos biométricos (entre otro tipo de información[38]), pueden generar perfilamientos discriminatorios por entidades privadas u organismos públicos[39]. Finalmente, no obstante conforme a lo explicado está justificada la naturaleza sensible de la información biométrica desde el punto de vista de la LPD, la Nueva

[35] La Nueva LPDP incluye como identificadores, entre otros, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social.
[36] PUCCINELLI (2004), p. 170.
[37] Al discutir los riesgos del uso de datos biométrico y su relación con los derechos fundamentales, para Franco y Veloz la biometría plantea potenciales vulneraciones a derechos de naturaleza iusfundamental como la libertad de expresión y asociación (aunque no profundizan sobre esta afirmación). FRANCO Y VELOZ (2022), p. 67.
[38] Como, por ejemplo, información sobre el origen étnico o racial, convicciones políticas o estados de salud.
[39] GARRIDO Y BECKER (2017), p. 74.

LPDP incorpora expresamente los datos biométricos dentro del espectro de los datos personales sensibles[40].

Siguiendo con la información sensible, y en otra materia de interés con respecto a la LPD, tenemos la necesidad que los *datos sensibles* se encuentren claramente definidos, sin dar espacio para que la interpretación de la ley haga partícipe de esta categoría a otro tipo de datos. La presencia de este *espacio para la interpretación* creemos que se presenta en el artículo 2° letra g) de la LPD, norma que acude a la expresión *"tales como"* al abordar los *"hechos o circunstancias de su vida privada o intimidad",* otorgándole entonces a esta enumeración[41] el carácter de ejemplos. La Nueva LPDP permite resolver esta anomalía ya que, junto con omitir la expresión *"tales como"*, otorga expresamente la condición de sensible a los datos personales referidos a las características físicas o morales de las personas, o a hechos o circunstancias de su vida privada o intimidad, que revelen *"el origen étnico o racial, la afiliación política, sindical o gremial, situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural"*.

Culminado el trabajo de contraste entre la LPD y la Nueva LPDP, desde el punto de vista del concepto y los alcances de la información sensible, a continuación nos concentramos en el tratamiento de la información biométrica dentro del marco de la nueva ley de protección de datos personales.

3.3. La Nueva LPDP y el tratamiento de los datos biométricos

Con respecto a su génesis, la nueva ley de protección de datos personales tiene origen en la iniciativa contenida en el Boletín N°11144-07 (refundida con el Boletín 11092-07). El texto, es un avance en la pretensión por mejorar las disposiciones sobre la tutela de la información personal. La anterior afirmación se justifica, teniendo en cuenta que la Nueva LPDP incorpora aspectos sustantivos que actualmente no poseen regulación alguna. Este factor debe asociarse al hecho que, desde la perspectiva de la técnica legislativa, la estructuración y redacción mejora en comparación con la LPD[42].

Con relación a los datos biométricos en particular, la Nueva LPDP en su artículo 16 ter. señala cuales datos tienen esta calidad, junto con las obligaciones del responsable de su tratamiento. En este ámbito, el inciso primero del artículo 16 ter. establece que son *"datos personales biométricos aquellos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona que permitan o confirmen la identificación única de ella, tales como la huella digital, el iris, los rasgos de la mano o faciales y la voz"*. El mismo artículo, agrega que el tratamiento de estos datos solo es posible si se cumple con lo dispuesto en el inciso primero del artículo 16 de la Nueva LPDP, *"y siempre que el responsable proporcione 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, y

d) La forma en que el titular puede ejercer sus derechos".

Simultáneamente, la nueva ley establece que un reglamento debe encargase de regular la forma y los procedimientos a utilizar para la implementación de los sistemas biométricos (este reglamento, se presupone como objeto orientador y guía en la implementación de las técnicas

[40] Artículo 2 letra g) Nueva LPDP.

[41] Es decir, *"a las características físicas o morales de las personas, 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".*

[42] VERGARA (2017), pp. 149-150.

biométricas[43]), advirtiendo que no se pueden crear o mantener bancos de huellas digitales o de otros datos biométricos, salvo autorización legal. En efecto, la exigencia de mandato legal para poder efectuar registros de datos, va en sintonía con el requerimiento de mayor protección a fin de evitar vulneraciones a los titulares de la información biométrica[44].

Adicionalmente, el artículo 16 ter. se remite al inciso primero del artículo 16[45], para indicar que el tratamiento de los datos personales *sensibles* sólo pueden realizarse *"cuando el titular a quien conciernen estos datos manifiesta su consentimiento en forma expresa, otorgado a través de una declaración escrita, verbal o por un medio tecnológico equivalente"*. Excepcionalmente, la norma admite el tratamiento de los datos personales biométricos sin consentimiento del titular *("respetando los principios y reglas establecidos en la presente ley"*, subraya la norma), sólo para los casos expresamente señalados en el inciso segundo del artículo 16 bis. Estos casos, involucran materias vinculadas con la salvaguarda de la vida o integridad física o psíquica del titular o de otra persona; situaciones de alerta sanitaria legalmente decretada; uso de datos con fines históricos, estadísticos o científicos; y el tratamiento de datos necesarios para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia o un órgano administrativo, entre otras hipótesis[46].

Para concluir el capítulo referido al tratamiento de los datos biométricos en Chile, a continuación examinamos la situación del iris ocular. El examen de este atributo en particular, se justifica teniendo en cuenta el interés mediático surgido a propósito de la reciente controversia por el ofrecimiento de pagos en criptomonedas, a cambio de escanear el iris de los usuarios. En esta parte, efectuamos el examen propuesto.

3.4. Tratamiento del iris ocular como dato biométrico en Chile

En la praxis nacional, el efecto de la falta de regulación de los datos biométricos se ve reflejada en diversas situaciones que involucran el tratamiento de esta información. Un primer ejemplo de ello, tiene que ver con la utilización de sistemas de video vigilancia y de reconocimiento facial, medios que (caracterizados por su rápido avance, gracias a los progresos computacionales que los transforman en sistemas inteligentes) van teniendo con el tiempo cualidades más intrusivas[47].

En un segundo ejemplo que consideramos de interés dada su repercusión mediática (y que refleja los más recientes avances informáticos), tenemos la casuística sobre el iris ocular como rasgo físico de carácter permanente (a diferencia de otros datos biométricos)[48], puntualmente la campaña de ofrecimiento de criptomonedas a cambio de escanear el iris de las personas. Esta campaña es impulsada a través del proyecto *Worldcoin*[49], desarrollado a su vez por la empresa *Tools for Humanity*[50], cuyo objetivo consiste en generar una base de datos mundial[51]. La posibilidad de escanear esta característica física plantea diversos interrogantes:

a) En primer lugar, ¿Qué tan legítimo es que una empresa recolecte este dato biométrico?: aprovechando las ventajas tecnológicas que ofrece la IA, el proyecto *Worldcoin* avanza con el

[43] LUCERO et al. (2020), p. 47.
[44] GARRIDO Y BECKER (2017), pp. 76 y 77.
[45] Regla general para el tratamiento de datos personales sensibles.
[46] Según Reusser, la Nueva LPDP no permite el uso de la información biométrica para controlar la asistencia a la jornada laboral de los trabajadores (incluyendo datos como la huella dactilar, el reconocimiento facial o el patrón del iris). En lo medular, el autor fundamenta su opinión argumentando, en primer lugar, que los datos biométricos (como la huella dactilar) son "datos sensibles" según la legislación, por lo que están especialmente protegidos ya que se relacionan con características físicas únicas de cada persona: en este contexto, su uso sólo está permitido si el trabajador otorga su consentimiento de forma expresa. En segundo lugar, para el autor el uso de la información biométrica para controlar la asistencia laboral puede generar una vulneración del derecho fundamental del artículo 19 N° 4 de la Constitución (el cual, recordemos, otorga un estatus iusfundamental a la protección de los datos personales). REUSSER (2024).
[47] CONSEJO PARA LA TRANSPARENCIA (2020), p. 118.
[48] En efecto, cada iris tiene un patrón distintivo de colores, fibras y anillos, y se define alrededor de los ocho meses de edad, permaneciendo constante a lo largo de la vida. UNIVERSIDAD DE CHILE (2024).
[49] Proyecto de criptomoneda biométrica con reconocimiento de iris.
[50] LOIZOS (2023).
[51] BIOMETRIC UP DATE.COM (2023).

propósito de reunir información biométrica para crear una red financiera y de identidad global[52]. El cumplimiento de este objetivo, permitiría verificar que cada persona tenga una *identidad digital* única[53]. Desde esta perspectiva, no hay duda de la utilidad que representa aprovechar una IA cada vez más realista y con la capacidad para simular las características de los seres humanos. No obstante, frente a este escenario de utilidad, se formula la pregunta sobre el grado de legitimidad de la actividad impulsada por *Worldcoin*. Establecer ese *grado de legitimidad*, debe resolverse examinando los riesgos a la privacidad que involucra el escaneo del iris, con el propósito de generar una base de datos global.

b) Con base en la pregunta anterior, ¿Qué riesgos trae aparejado el escaneo del iris con el objetivo de generar una base de datos global, a cambio de criptomonedas?: desde un punto de vista interno y en el marco de una casuística incipiente, un problema central tiene que ver con la identificación de la empresa responsable ante el posible mal uso de la información biométrica. Subrayando el carácter de protocolo de código abierto atribuido al *Worldcoin* (en palabras de *Tools for Humanity* para Latinoamérica, opera de forma similar al internet: *"La internet no es de nadie, allí se pueden tener varios sitios, por ejemplo. Eso es un protocolo"*[54]), dentro de ese sistema distintas organizaciones pueden colaborar desarrollando tecnologías a partir del código abierto, destacándose dos grandes colaboradores: *Worldcoin Foundation* y *Tools For Humanity*. La segunda empresa (*Tools For Humanity*), se encarga de operar la aplicación denominada *World App*, software que permite a una persona configurar su *World ID* o cédula de identidad digital que se consigue escaneando el iris. Con todo lo anterior, el usuario puede administrar sus criptomonedas, las WLD. En últimas, reiterando la naturaleza de protocolo de código abierto otorgado al *Worldcoin*, para el caso chileno el problema radica en que la actividad de escaneo del iris es desarrollada por la empresa Worldcoin SpA (constituida en Chile ante el Registro de Empresas en junio de 2021, con un capital de, apenas, un millón de pesos), la cual no es filial local de *Worldcoin Foundation* o de *Tools For Humanity*: de hecho, ninguna de estas dos últimas entidades existe realmente como empresa en el ámbito nacional[55]. En este orden de ideas, en la esfera jurisprudencial ya se ha dado algún tratamiento al escaneo del iris a cambio del pago de criptomonedas. No obstante, en estas sentencias (limitadas al nivel de Cortes de Apelaciones), la pretensión de los accionantes por "bloquear" la utilización de la información biométrica ha sido rechazada por los jueces, decisiones que abarcan sobre todo cuestiones de forma, más que de fondo[56]. En últimas, corresponderá a los tribunales de justicia chilenos ponderar la utilización de los medios digitales de intercambio (como las criptomonedas) y el resguardo de un rasgo físico como el iris, aplicando las directrices de la Nueva LPDP (una vez que esta normativa entre en plena vigencia).

Finalmente, y a diferencia de lo que ocurre en Chile, la legislación de la Unión Europea presenta mayores avances con relación al tratamiento de la información biométrica. Estos avances van de la mano con los desafíos que plantea la vocación de eficacia extraterritorial atribuible al RGPD, o los efectos de la Ley de IA europea. En este orden de ideas y como conclusión de la investigación, en el siguiente capítulo abordamos estas materias.

4. Tratamiento de los datos biométricos en el ámbito del derecho comparado

Aportar al debate sobre los desafíos que enfrenta la tutela de los datos biométricos en el ordenamiento jurídico interno, implica revisar el tratamiento de esta información desde la

[52] https://es-es.worldcoin.org/.

[53] Identidad entendida como el conjunto de información personal que se hace pública en internet, y que caracteriza a una persona o institución a partir de lo que es o dice ser en la red. HUERTA et al. (2021), p. 48.

[54] CIPER (2024).

[55] CIPER (2024).

[56] En efecto, al respecto tenemos la sentencia de la Corte de Apelaciones de Valparaíso, Rol N° 1474-2024, de 22 de julio de 2024, en donde la acción incoada se desestima *"por no haberse establecido la existencia del acto que motiva su interposición, no haberse podido establecer que se dedujo dentro de plazo y por haberse acogido la alegación de falta de legitimación pasiva de la recurrida"*. Igualmente, tenemos la sentencia de la Corte de Apelaciones de Valparaíso, Rol N° 1307-2024, de 27 de julio del 2024, en donde la acción presentada se rechaza por considerarse que existen otras vías jurídicas para resolver lo pretendido.

perspectiva del derecho europeo. Esta exigencia se justifica observando que los mayores avances en la protección de los datos personales se reconocen en la legislación de la Unión Europea, con énfasis en lo estipulado en su RGPD. Desde este punto de vista, a continuación estudiaremos el tratamiento de los datos biométricos en el citado Reglamento, pasando por el análisis de la vocación de eficacia extraterritorial del RGPD y su relación con este tipo de información sensible, finalizando con el examen de la Ley de IA de la Unión Europea y la situación de la información biométrica.

4.1. Datos biométricos y su tratamiento en el derecho comparado: alcances del RGPD

Con relación a la situación del derecho comparado, una primera observación es que en la legislación de América Latina (no obstante varias iniciativas, que permanecen en calidad de proyectos[57]), en general, hay ausencia de un marco jurídico para el tratamiento de la información biométrica[58]. Respecto a los Estados Unidos, algunos Estados cuentan con instrumentos legales para regular datos biométricos, como son los casos de Illinois y su *Biometric Information Privacy Act BIPA* (2008)[59], Texas y el Capítulo 503 *(Biometric Identifiers)* de su *Business and Commerce Code* (2009), y Washington y su *Biometric Privacy Protection Act* (2017)[60]. Sin embargo, estas normas tratan la privacidad y la seguridad de manera distinta, y hacen que los procesos y la recolección de los datos sean lentos, además de presentar otras diferencias al contrastar los contenidos de estos instrumentos[61], por lo que la doctrina considera más útil desarrollar una ley federal que unifique criterios en el país norteamericano[62]. Finalmente, en el marco de otras realidades jurídicas y políticas, ya han surgido temores sobre la utilización que regímenes autocráticos pueden hacer de estas tecnologías, como ocurre con el caso de China y la aplicación de vigilancia biométrica (por medio del uso de tecnología de reconocimiento facial, para identificar a las personas en lugares públicos)[63], o el caso de Irán y la utilización discriminatoria de la tarjeta de identidad nacional biométrica[64] (implementada el año 2015)[65].

Al concentrarnos en el modelo de la Unión Europea y su RGPD, un aspecto reconocido por la doctrina es que, *"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"*[66]. Formulada esa premisa, el RGPD define los datos biométricos y el tratamiento que se puede hacer de ellos. En efecto, el artículo 4 número 14 estipula que los datos de naturaleza biométrica son datos personales que se obtienen de un procesamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, información capaz de permitir o confirmar la identificación única de dicha persona. La norma, menciona como ejemplos las imágenes faciales y los datos dactiloscópicos. Al llevar a cabo un ejercicio de comparación entre el artículo 4 número 14 del RGPD, y el artículo 16 ter. de la Nueva LPDP, se subraya que el contenido de estas normas es muy similar. Como diferencia observable, tenemos que el Reglamento europeo indica que es una persona "*física"* de quien se puede obtener la información biométrica, mientas que la Nueva LPDP no menciona este carácter. Otra distinción, consiste en que la norma chilena agrega más ejemplos de datos biométricos, ya que incluye el iris (ejemplo relevante, dado el impacto que ha tenido su tratamiento recientemente), los rasgos de la mano y la voz.

[57] Por ejemplo, tenemos el caso de Costa Rica y su Proyecto de Ley N° 21321, presentado en marzo de 2019. PIEDRA (2023), p. 23.
[58] QUINTANILLA (2020), p. 75.
[59] 740 ILCS 14/1.
[60] Washington House Bill 1493.
[61] QUINTANILLA (2020), p. 75.
[62] NGUYEN (2018), pp. 71 y 73.
[63] PIEDRA (2023), p. 25.
[64] La tarjeta posee "chip" y almacena datos biométricos.
[65] PUTTICK (2020), p. 179.
[66] QUINTANILLA (2020), p. 82.

Igualmente, el RGPD otorga un mayor estándar de protección a los datos biométricos, dada su naturaleza de dato sensible[67]. Este carácter sensible, se deduce de su incorporación en el artículo 9 del Reglamento, artículo encargado del tratamiento de *categorías especiales* de datos personales[68]. En efecto, la norma proscribe el tratamiento de información personal que revele *"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 las orientaciones sexuales de una persona física"*. Con base en las explicaciones anteriores, la fortaleza del RGPD no es solo la inclusión expresa de los datos biométricos dentro de las *"categorías especiales de datos personales"*: otra fortaleza, subyace en la indicación taxativa de la información que posee el carácter de sensible.

Siguiendo con el carácter sensible de la información biométrica, la Unión Europea recomienda la adopción de principios orientadores de la protección de los datos biométricos. En este sentido, Iglesias y Becker señalan los parámetros en los que se sustentan esos principios. Estos parámetros incluyen el consentimiento del interesado, la legitimidad (determina que los datos deben ser tratados de manera lícita y leal en relación con su titular), la finalidad (implica que la información biométrica sólo será tratada con fines determinados, explícitos y legítimos), la calidad (parámetro conforme al cual los datos personales deben ser pertinentes, exactos y estar actualizados), la proporcionalidad (el tratamiento de datos deberá limitarse a aquéllos que resulten adecuados, necesarios y relevantes), la pertinencia, la transparencia (determina que el *responsable*[69] del tratamiento debe tomar las medidas oportunas para, en todo momento, facilitar al titular la información relativa a la finalidad del tratamiento e identidad de dicho responsable), la responsabilidad y rendición de cuentas (atribuible al responsable del tratamiento), la confidencialidad (atribuible a quienes trabajan en el tratamiento de datos personales, y al encargado de su acceso), la minimización de datos (toda recolección de datos debe limitarse a lo necesario), la temporalidad y la seguridad[70].

Conjuntamente, el procesamiento de datos biométricos esta proscrito, a menos que haya sido dado el consentimiento por el *interesado*, y que previamente el controlador de los datos haya realizado y documentado una evaluación de impacto de privacidad, o una evaluación de impacto de la protección de datos [71], conforme a lo expresado en artículo 9 número 2 del RGPD. Precisamente, con relación a esta norma encargada de las excepciones a la prohibición de tratamiento de los datos sensibles, surge la pregunta sobre la situación de los datos que se recolectan de *fuentes de acceso público* [artículo 14, número 2, letra f), RGPD][72]. Respecto a este punto, el Reglamento europeo no señala expresamente que *fuentes* tienen la calidad de ser accesibles al público. No obstante, en España la Ley Orgánica 15/1999 (o LOPD 15/1999) definía y señalaba inequívocamente cuales eran estas fuentes. Ahora bien, frente al hecho que la Ley Orgánica 3/2018 (o LOPD 3/2018, estatuto que derogó la LOPD 15/1999) carece de estas definiciones, la Agencia Española de Protección de Datos AEPD ha estimado que es posible seguir aplicando como criterio interpretativo la Ley Orgánica derogada, otorgando el carácter de *fuentes de acceso público* a las páginas Web y fuentes que pueden ser objeto de libre consulta, excluyéndose el acceso a los sitios restringidos a un círculo determinado de usuarios[73]. Como comentario final y a diferencia de lo que ocurre en el RGPD, la Nueva LPDP chilena define

[67] QUINTANILLA (2020), p. 82.
[68] Como lo anotan Iglesias y Becker, las etiquetas *sensible* y *especial categoría* son nociones equivalentes. De esta forma, mientras en Europa se habla de *especial categoría*, países como Colombia, Perú y Chile hablan de *dato sensible*. GARRIDO Y BECKER (2017), p. 74.
[69] Conforme a lo estipulado en el artículo 4 número 7 del RGPD, el *"responsable del tratamiento"* o *"responsable"* es *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento"*.
[70] GARRIDO Y BECKER (2017), pp. 78-80.
[71] QUINTANILLA (2020), p. 82.
[72] A propósito de la información que debe facilitarse cuando los datos personales no se han obtenido del interesado, y conforme a lo estipulado en el artículo 14 número 2 letra f) del RGPD, se impone al responsable del tratamiento la obligación de indicar la fuente de la que proceden los datos personales y, en su caso, si proceden de *fuentes de acceso público*.
[73] GRUPO ADAPTALIA (2019).

claramente las fuentes de acceso público, y enuncia ejemplos de estas [artículo 2° letra i)], de lo que se deduce una fortaleza en comparación con la norma europea.

Para finalizar esta parte relativa a los alcances del RGPD, un punto de interés lo constituye el tratamiento del iris ocular en el contexto del ordenamiento de la Unión Europea, en particular el caso español. De forma análoga a lo ocurrido en Chile, la empresa *Tools for Humanity* dentro proyecto *Worldcoin*, llevó el procesado de datos biométricos a través de la captura inicial de imágenes de los iris, ojos y rostro en toda España. Esta actividad afectó a numerosas personas, incluidos menores de edad, sin constar acreditado el consentimiento y la información proporcionada acerca de este tratamiento[74]. En consecuencia, y a raíz de un conjunto de reclamaciones formuladas en el marco de este proyecto, la AEPD impuso en marzo del año 2024[75] un conjunto de medidas cautelares[76] contra *Tools for Humanity*. Las medidas, consistieron en ordenar el cese de la recopilación y tratamiento de datos personales en el territorio español (concretamente aquellos que implicaban el escaneo de iris, ojos y rostro), y su posterior procesamiento, además de exigir el bloqueo de los datos captados. La decisión de la Agencia, se justificó en el *"tratamiento presuntamente ilícito"* que implicaba *"el procesamiento de datos personales sensibles a través de medios altamente opacos e intrusivos",* tratamiento que podría incluir *"operaciones de seguimiento y elaboración de perfiles, sin garantizar, además, el derecho de los interesados a la información adecuada"*. Además, La AEPD reconoció las amenazas sobre otras garantías concedidas por el RGPD, como *"el derecho a la retirada del consentimiento o el derecho de supresión"*. Por último, la decisión enfatiza que, dado que el caso involucra el tratamiento de datos de menores de edad, *"debe considerarse la necesidad de primar el interés superior del menor"*[77].

El análisis del RGPD adquiere un interés adicional, teniendo en cuenta la vocación de eficacia extraterritorial que se le reconoce. Frente a los efectos que pueda tener esa vocación en el ordenamiento jurídico chileno, a continuación, abordamos los alcances de esa eficacia.

4.2. Vocación de eficacia extraterritorial del RGPD y los datos biométricos

El artículo 3 del GDPR establece su ámbito de aplicación territorial, reconociendo una inclinación de eficacia que supera las fronteras de los miembros comunitarios[78]. Esta norma, incorpora al derecho positivo la doctrina expansiva del Tribunal de Justicia de la Unión Europea TJUE (originada en casuística vinculada a empresas que se dedican a ofrecer servicios exclusivamente a través de Internet[79]), y en consecuencia se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del *responsable* o del *encargado*[80] en la Unión Europea, independientemente de que el tratamiento tenga o no lugar en la comunidad política[81]. Los elementos del artículo 3 que deben observarse al momento de establecer los alcances de la vocación extracomunitaria, son los siguientes:

a) No importa si la operación o conjunto de operaciones realizadas sobre datos personales tiene lugar dentro o fuera de la comunidad política: el RGPD se aplica a ese

[74] Según se lee en el *"Acuerdo de adopción de medida provisional"* incorporado en el EXP202312448 de la AEPD (Disponible en: https://www.aepd.es/documento/co-000297-2023-medida-provisional.pdf).
[75] Con base en las atribuciones conferidas por el artículo 58 del RGPD, y de acuerdo a lo dispuesto en el artículo 69.2 de la LOPD 3/2018.
[76] Medida cautelar generada con carácter excepcional y dentro del marco habilitante del artículo 66.1 del RGPD.
[77] Según se lee en el "Acuerdo de adopción de medida provisional" incorporado en el EXP202312448 de la AEPD, pp. 3-4.
[78] Con relación a la vocación de extraterritorialidad, no abordamos instrumentos como los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales adoptados por la OEA (2021), o los *"Estándares de Protección de Datos de los Estados Iberoamericanos"* sugerido por la Red Iberoamericana de Protección de Datos RIPD (2017), dada su naturaleza no vinculante. Lo anterior, justifica que nos aboquemos en esta parte de la investigación a la vocación de eficacia extraterritorial atribuible al RGPD.
[79] Concretamente, tenemos las sentencias C-131/12 del 13 de mayo de 2014 (asunto Google Spain), y C-230/14 del 1 de octubre de 2015, (asunto Weltimmo).
[80] Recordemos que el *encargado del tratamiento* o *encargado* (el cual, según el artículo 4 numeral 8 del RGPD, puede ser una persona física o jurídica, autoridad pública, servicio u otro organismo) es quien trata la información personal *"por cuenta del responsable del tratamiento*".
[81] BAUZÁ (2019), p. 126.

tratamiento en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea.

b) El RGPD se aplica al tratamiento de la información personal del titular que resida en la Unión Europea, por parte de un responsable o encargado no establecido en la comunidad política, siempre y cuando las actividades de tratamiento estén relacionadas con[82]: (1) *"la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago"*, o (2) *"el control de su comportamiento, en la medida en que este tenga lugar en la Unión"*[83].

c) El Reglamento se considera aplicable al tratamiento de datos personales por parte de un responsable que no esté establecido en la comunidad de Estados, *"sino en un lugar en que el Derecho de los Estados miembros sea de aplicación"*[84], aspecto que determina como el RGPD no es ajeno a las normas de derecho internacional público[85].

Pese a la existencia de estos elementos incorporados en su artículo 3, poner en práctica la vocación extracomunitaria del RGPD supone generar herramientas que faciliten esa aptitud. En este contexto, la institucionalidad comunitaria ha reaccionado trabajando desde el 2020 en una serie de instrumentos que apuntan a delimitar los alcances de dicha vocación. Concentrados en aquellas iniciativas que pueden incidir en la situación de los datos personales de naturaleza sensible, debemos mencionar las *"Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, Versión 2.0"* (en adelante *Recomendaciones*)[86]. Este conjunto de propuestas, pese a que por su naturaleza no posee un carácter vinculante, tiene la virtud de abordar un punto que afecta a Estados extracomunitarios (hipótesis que, por cierto, incumbe al ordenamiento jurídico chileno): las *Recomendaciones* reconocen en el capítulo V del RGPD, encargado de regular las transferencias de datos personales a *"terceros países"*[87], la condición de que la transferencia no debe menoscabar el nivel de protección de las personas físicas garantizado por el mismo Reglamento[88]. Creemos que los progresos que se logren en la implementación efectiva de las *Recomendaciones*, deben ser tenidos en cuenta en el debate para la definición de los estándares que debe cumplir la legislación chilena en materia de tutela de los datos personales, incluyendo, por cierto, el tratamiento de los datos biométricos, a fin de hacerla coherente con las exigencias del RGPD. Adicionalmente, estos avances colaborarán en la pretensión para que la Unión Europea declare que Chile garantiza un nivel de protección adecuado y, en consecuencia, permita la transferencia internacional de datos personales sin requerir ninguna autorización específica[89].

Para finalizar este capítulo de la investigación, debemos indicar que en el ordenamiento jurídico comunitario ha surgido un texto que, dentro de la esfera de la IA, se encarga de los datos biométricos: hacemos referencia a la Ley de IA de UE. Teniendo en cuenta la importancia de esta faceta del desarrollo en la vida del ser humano, a continuación examinamos esta normativa en su relación con la información biométrica.

[82] BAUZÁ (2019), p. 126.
[83] Artículo 3, numeral 2 del RGPD.
[84] Artículo 3, numeral 3 del RGPD.
[85] BAUZÁ (2019), p. 126.
[86] *Recomendaciones* adoptadas el 18 de junio del 2021 por el Comité Europeo de Protección de Datos, y que tienen su origen en la sentencia del Tribunal de Justicia de la Unión Europea en el asunto Schrems II (C-311/18).
[87] La noción de *tercer país*, abarca cualquiera que no sea un Estado miembro del Espacio Económico Europeo, que incluye a los Estados miembros de la Unión Europea y a Islandia, Noruega y Liechtenstein. COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2021), p. 29.
[88] SANZ (2023 a), pp. 12-13.
[89] BORDACHAR (2022), p. 398.

4.3. Ley de Inteligencia Artificial de la Unión Europea y tratamiento de los datos biométricos

Como dimensión del progreso humano, la IA tiene la capacidad de incidir de manera positiva y negativa en la vida de las personas[90]. Son diversos los alcances de esta faceta de la evolución tecnológica, y su progreso se ha visto impulsado por una mayor disponibilidad de datos, recursos tecnológicos y financieros, así como de los avances en las técnicas de aprendizaje computacional.

En Chile, ya se han formulado algunas iniciativas para regular la IA. Estos esfuerzos, incluyen la presentación de los proyectos de ley Boletín N° 16638-19[91] y Boletín N° 16821-19[92], ambas iniciativas recién cursando el primer trámite constitucional. Igualmente, el año 2021 el Gobierno Nacional (a través del Ministerio de Ciencia, Conocimiento, Tecnología e Innovación) dio conocer su Política Nacional de IA, conjunto de directrices que, al abordar el ámbito de la ética, plantea la preocupación por los efectos del mal uso de sistemas de vigilancia basados en reconocimiento biométrico, y la posible afectación de nuestra personalidad en el mundo digital[93] (anotando que el tema de la información biométrica no fue incorporado en el texto de actualización de esta Política Nacional, dado a conocer en mayo del 2024). Continuando con el espectro interno y desde la perspectiva de la ciberseguridad, la aplicación de la IA podría fortalecer las defensas digitales del país, pero a su vez exponerlo a nuevas vulnerabilidades, factores que plantean un doble reto respecto a esta disciplina del conocimiento: su implementación como herramienta de protección (ejecución acompañada de un legislación adecuada) y la necesidad de prevenir su mal uso en actividades maliciosas, sobre todo en sectores críticos como la energía, la salud y el transporte, esenciales para la estabilidad del país (y especialmente vulnerables ante ataques potenciados por IA)[94]. En contraste, el derecho europeo establece un hito al ser el primero en generar una normativa sobre el tratamiento de esta dimensión tecnológica, gracias a la redacción del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 [Reglamento (UE) 2024/1689] o Ley de Inteligencia Artificial de la Unión Europea (Ley de IA de la UE). No obstante que el Reglamento entró en vigor el 1° de agosto de 2024, la norma será aplicable en su totalidad solo 24 meses después de esa fecha, dependiendo de variables como el nivel de "riesgo" que representa la IA (factor que se encuentra directamente vinculado al ámbito de la información biométrica, lo que expondremos más adelante), entre otros factores[95]. Como primera normativa integral en la materia, la Ley de IA de la UE tiene por objeto enfrentar los efectos perjudiciales de los sistemas de IA, mejorando el funcionamiento del mercado interior y promoviendo la adopción de una IA centrada en el ser humano y fiable. Lo anterior, garantizando un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de Derechos fundamentales de la Unión Europea, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente[96].

Al concentrarnos en la situación de la información biométrica, en primer lugar observamos que la Ley de IA de la UE, en su artículo 3° reitera, en general, el concepto de "dato biométrico" consagrado en el RGPD[97].

Siguiendo con la exposición, una de las señas de identidad del Reglamento europeo sobre la IA, es que se encuentra instalado en un enfoque basado en el riesgo. En este sentido, la Ley

[90] SÁNCHEZ Y TORO-VALENCIA (2021), p. 213.
[91] Que "Modifica el DFL N° 33, de 1981, del Ministerio de Educación Pública, para establecer inhabilidades de acceso a recursos del Fondo Nacional de Desarrollo Científico y Tecnológico", ingresado recién el 31 de enero del 2024.
[92] Que "Regula los sistemas de inteligencia artificial", ingresado recién el 4 de mayo del 2024.
[93] MINISTERIO DE CIENCIA, CONOCIMIENTO, TECNOLOGÍA E INNOVACIÓN (2021), p. 50.
[94] EL AGORA (2024).
[95] Por ejemplo, la Ley de IA de la UE establece un plazo de 6 meses para su aplicación respecto a las prohibiciones de sistemas de IA de *riesgo inaceptable*, y de 9 meses respecto de los códigos de prácticas. EUROPEAN PARLIAMENT (2024).
[96] Artículo 1°, Reglamento (UE) 2024/1689.
[97] La única diferencia observable al comparar el concepto de *datos biométricos* del RGPD con la Ley de IA de la UE, es que en el primero se agrega la expresión *"que permitan o confirmen la identificación única de dicha persona"*.

de IA de la UE consagra diferentes obligaciones para los proveedores y los usuarios según el nivel de *riesgo* que representa la IA, configurándose 3 categorías: riesgo inaceptable, alto riesgo y riesgo mínimo[98]. Con relación a los sistemas de IA de riesgo inaceptable, el artículo 5° establece una serie de *"prácticas de IA prohibidas"*, incluido un conjunto de sistemas que representan una amenaza a la seguridad pública. No obstante que estas prohibiciones abordan la utilización de aspectos biométricos para identificación y seguimiento en *tiempo real* (es decir, que se produce *sin una demora significativa*[99]) en espacios de acceso público, *"con fines de garantía del cumplimiento del Derecho"*, esa restricción no es aplicable a las Fuerzas y Cuerpos de Seguridad del Estado frente a la persecución de delitos de mayor impacto, incluyendo conductas como el secuestro y las actividades de carácter terrorista, entre otras[100].

Paralelamente, la Ley prohíbe los *"sistemas de categorización biométrica"*[101] que utilizan características sensibles de las personas (creencias políticas, religiosas, filosóficas, orientación sexual o raza). Igualmente, la norma proscribe los sistemas de vigilancia predictiva, los sistemas de extracción no dirigida de imágenes faciales de Internet o imágenes de circuito cerrado de televisión para crear bases de datos de reconocimiento facial, y los *"sistemas de reconocimiento de emociones"*[102] en el lugar de trabajo y en instituciones educativas (salvo que tengan finalidades médicas o de seguridad). De todas formas, en las hipótesis anteriores también se contemplan excepciones de estos sistemas en el ámbito policial[103]. Con relación a estas excepciones, la doctrina ha formulado su inquietud teniendo en cuenta la inexactitud de los algoritmos utilizados para identificar a las personas, identificándose un sesgo racial en detrimento de individuos afroamericanos: frente a esta preocupación, cuando fuerzas de seguridad acuden al uso de estos sistemas para reconocer personas humanas, o intentar encontrar sospechosos en una investigación criminal, debe observarse que no solo existe la probabilidad de errar, sino también de afectar diversas garantías fundamentales (como el principio de inocencia, la libertad de expresión, el derecho de protesta ante las autoridades y el derecho a la igualdad)[104]. Como reflexión final en este punto, creemos que el incipiente trabajo legislativo que se está llevando a cabo en Chile en el ámbito de la IA, debe observar con atención los avances alcanzados en el ordenamiento jurídico de la Unión Europea. Lo anterior, con miras a lograr el tratamiento adecuado de la información de naturaleza biométrica dentro del marco de esa dimensión del desarrollo tecnológico, en el escenario interno.

Conclusiones

1. Como consecuencia de la transformación digital, han surgido nuevos desafíos para la sociedad en materia de protección de la información personal. En ese contexto, lograr el adecuado tratamiento de los datos biométricos constituye una de las preocupaciones surgidas en el marco de la señalada trasformación. Bajo esta perspectiva, la pretensión de la investigación es aportar a la discusión sobre la protección de los datos biométricos en el derecho chileno. En este orden de ideas, el trabajo tiene como punto de partida la presentación de un panorama general de la biometría, etapa que involucró el examen de los elementos inherentes a la noción de dato biométrico, junto con las formas en que se puede lograr la identificación de las personas a partir del uso de este tipo de información (formas que incluyen la *autentificación* o *verificación*, y la *identificación*).

[98] CHAPARRO (2023), p. 49.
[99] GARRIGA (2024), p. 145.
[100] Artículo 5, apartado 1°, letra h), Reglamento (UE) 2024/1689.
[101] El concepto de *categorización biométrica* de la Ley de IA de la UE, hace referencia a la inclusión de personas físicas en categorías específicas en función de sus datos biométricos (considerando 16).
[102] El concepto de *sistema de reconocimiento de emociones* a que hace referencia la Ley de IA de la UE, debe definirse como un sistema de IA destinado a distinguir o deducir las emociones o las intenciones de las personas físicas a partir de sus datos biométricos (considerando 18).
[103] GARRIGA (2024), p. 146.
[104] COMMATTEO Y MOREYRA (2022), pp. 36-37.

2. El artículo indagada también en el tratamiento de los datos biométricos en el caso chileno, abordando diversas materias. En una primera parte del Capítulo, se lleva a cabo un recorrido jurídico en el que se exponen las particularidades que rodearon la redacción de la LPD, análisis que permite identificar diversas debilidades atribuibles a ese estatuto legal. En este escenario, no obstante a que los datos biométricos no se encuentran regulados expresamente en el señalado estatuto, con el examen de la LPD es posible identificar elementos que aportan al debate, elementos particularmente vinculados a la noción de *información sensible*: por un lado, se deduce que la LPD justifica de forma tácita el carácter de dato sensible atribuible a la información biométrica. Por otro lado, se subraya en la necesidad que los *datos sensibles* se encuentren claramente definidos, sin dar espacio para que la interpretación de la ley haga partícipe de esta categoría a otro tipo de datos, *espacio para la interpretación* que estaría dado con la presencia de la expresión *"tales como"* estipulada en el artículo 2° letra g) de la LPD.

Siguiendo con el Capítulo, el ejercicio de comparación entre la LPD y la Nueva LPDP permite identificar cambios con respecto al tratamiento de los datos biométricos. En primer término y con relación a los datos sensibles, la Nueva LPDP no solo incorpora expresamente los datos biométricos dentro del espectro de los datos personales sensibles: además, suprime la expresión *"tales como"* en la definición de dato sensible, superando así ese *espacio para la interpretación* presente en la LPD. En segundo lugar, la Nueva LPDP no se limita a definir cuales datos tienen la calidad de biométricos (*"aquellos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona que permitan o confirmen la identificación única de ella, tales como la huella digital, el iris, los rasgos de la mano o faciales y la voz"*), ya que formula otras directrices con relación a este tipo de información especialmente protegida: indica las obligaciones del responsable de su tratamiento, exige la redacción de un reglamento que se encargue de regular la forma y los procedimientos para la implementación de los sistemas biométricos, y determina los requisitos que permiten el tratamiento de estos datos personales sensibles. En la etapa final del Capítulo, a propósito de la situación del iris ocular como dato biométrico y el efecto mediático por la reciente campaña de ofrecimiento de criptomonedas (a cambio del escaneo de este rasgo físico), se concluye que los tribunales de justicia nacionales, pese a la incipiente jurisprudencia generada hasta la fecha, deben realizar una labor de ponderación entre el uso de los medios digitales de intercambio y la protección del iris, trabajo que exigirá aplicar los parámetros de la Nueva LPDP (una vez que esta normativa entre en vigencia).

3. Con respecto a la situación de la información biométrica en el derecho comparado y su incidencia en el ordenamiento jurídico chileno, el capítulo final de la investigación abarca tres esferas, con las siguientes conclusiones:

a) Como resultado de un ejercicio de contraste entre el RGPD y la Nueva LPDP, se evidencia que el contenido de la definición de dato biométrico presente en ambas normas es similar. No obstante, la nueva ley chilena agrega como ejemplo en esa definición al iris ocular, lo que va en sintonía con el interés que ha generado la situación de este rasgo físico en el último tiempo. Con respecto a la Unión Europea, la preocupación por el tratamiento del iris como dato sensible ha tenido mayores avances, teniendo en cuenta que (al menos en el modelo español) la AEPD, en una casuística que involucró a la empresa *Tools for Humanity* dentro del proyecto *Worldcoin* (escenario análogo al ocurrido en Chile), ya ha tomado medidas tendientes a la protección efectiva de este dato biométrico en particular.

En este mismo trabajo de comparación, se observa que tanto en la Nueva LPDP como en el RGPD, hay una expresa incorporación de la información biométrica dentro de la órbita de los datos sensibles. Simultáneamente, una debilidad identificada en la ley europea sobre protección de datos es la falta de definición de lo que son las *fuentes de acceso público*. Este aspecto es relevante, teniendo en cuenta que entre las excepciones a la prohibición de tratamiento de los datos sensibles, se incluyen los recolectados en estas fuentes. Por el contrario, la Nueva LPDP define claramente este tipo de fuentes, notándose una fortaleza con respecto al RGPD.

Finalmente, como reflexión general surgida del ejercicio de contraste entre el RGPD y la Nueva LPDP, se concluye que el texto de la nueva ley chilena de protección de datos tiene elementos comunes a los contenidos del Reglamento europeo, en lo que concierne al tratamiento de los datos biométricos. Lo anterior, confirma el avance que representa la Nueva LPDP en esta materia, en comparación con la LPD.

b) Con relación a la eficacia extraterritorial atribuida al RGPD, concluimos que no obstante el Reglamento europeo formula elementos para delimitar su vocación extracomunitaria (elementos incorporados en su artículo 3°), llevar a la práctica esa vocación supone generar herramientas que la faciliten, destacándose en este marco las propuestas contenidas en las *Recomendaciones 01/2020.* En efecto, estas *Recomendaciones* abordan las transferencias de datos personales a *terceros países* (entre los que se incluye a Chile), estableciendo que la transferencia es posible siempre y cuando no menoscabe el nivel de protección de las personas físicas garantizado por el RGPD. A este respecto, pensamos que los progresos que se logren en la implementación efectiva de las *Recomendaciones* (dado que actualmente no tienen un carácter vinculante), son insumos clave en el debate para el perfeccionamiento de los estándares que debe cumplir la legislación chilena en materia de tutela de la información personal, abarcando, por cierto, el tratamiento de los datos biométricos.

c) Una tercera esfera, tiene que ver la situación de la IA (faceta del desarrollo con amplios efectos en la vida del ser humano) y su relación con la información biométrica. Al respecto, el ordenamiento jurídico comunitario ya cuenta con un texto legal sobre la materia, identificado como la Ley de IA de la UE, norma que entrará en plena vigencia 24 meses después del 1° de agosto de 2024. En cuanto a los datos biométricos, la Ley de IA reitera la definición de este tipo de información sensible consagrada en el RGPD. Adicionalmente, y con relación a los sistemas de IA de riesgo *inaceptable*, la misma norma establece prohibiciones, entre las que se incluye la restricción de utilizar aspectos biométricos para identificación y seguimiento en *tiempo real* en espacios de acceso público, *"con fines de garantía del cumplimiento del Derecho"*, estipulándose que esta restricción no es aplicable a las Fuerzas y Cuerpos de Seguridad del Estado frente a la persecución de delitos de mayor impacto. Simultáneamente, la Ley de IA de la UE proscribe los *sistemas de categorización biométrica* que utilizan características sensibles de las personas, y prohíbe el uso de otros sistemas de IA basados en la recolección de rasgos biométricos (como pueden ser los sistemas de extracción no dirigida de imágenes faciales de Internet o imágenes de circuito cerrado de televisión para crear bases de datos de reconocimiento facial), aunque establece excepciones que permiten favorecer trabajos de naturaleza policial. Sobre este último aspecto, la doctrina plantea su preocupación por la inexactitud de los algoritmos utilizados para identificar a las personas, enfatizando en el sesgo racial generado en detrimento de individuos afroamericanos, y las consecuencias de ese sesgo. Finalmente, no obstante en el caso chileno se han generado algunos esfuerzos para dar tratamiento a la IA, avances que incluyen la presentación de dos proyectos de ley y la existencia de una Política Nacional de IA (política que esboza alguna preocupación por los efectos del mal uso de sistemas de vigilancia basados en reconocimiento biométrico), esta labor es aún incipiente, lo que obliga al legislador a observar atentamente los avances alcanzados en el ordenamiento jurídico de la Unión Europea, a fin de enriquecer el contenido de estas propuestas y de la Política Nacional de IA. Lo anterior con miras a que, a nivel nacional, se alcance en el futuro un tratamiento adecuado de la información de naturaleza biométrica dentro del marco de la IA.

BIBLIOGRAFÍA CITADA

ALONSO, FERNANDO (2008): Biometric Sample Quality and its Application to Multimodal Authentication Systems. Tesis Doctoral (Madrid, UPM).

ASOCIACIÓN POR LOS DERECHOS CIVILES (2015): "Si nos conocemos más, nos cuidamos mejor. Informe sobre políticas de biometría en la Argentina", en: Policy Papers, ADC (mayo de 2015), pp. 1-25.

AZANZA, EDUARDO (2021): "Identidad, Biometría e Inteligencia Artificial: Ética, mitos y realidades". Disponible en: https://veridas.com/es/biometria-etica-mitos-realidades/ [visitado el 3 de octubre de 2024].

BAUZÁ, FELIO (2019): "El modelo europeo de protección de datos. Experiencias para la regulación chilena presente y futura", en: Ars Boni et Aequi (Vol. 15, N° 1), pp. 121-148.

BIOMETRIC UP DATE.COM (2023): "Iris biometrics crypto project Worldcoin reportedly looks for $120M investment". Disponible en: https://www.biometricupdate.com/202302/iris-biometrics-crypto-project-worldcoin-reportedly-looks-for-120m-investment [visitado el 15 de julio de 2024].

BORDACHAR, MICHELLE (2022): "Comentarios al proyecto de ley chileno sobre protección de datos personales: Deficiencias e inconsistencias en los derechos ARCO", en: Revista Chilena de Derecho y Tecnología (Vol. 11, N° 1), pp. 397-414.

CHAPARRO, MILAGROS (2023): "La inteligencia artificial y los desafíos que presenta su regulación en el marco de la Unión Europea", en: Álvarez, María Victoria (Comp.), La dinámica de la Agenda de Unión Europea: nuevas prioridades, nuevas perspectivas (Rosario, Argentina, Universidad Nacional de Rosario), pp. 47-55.

CIPER (2024): "Datos personales a cambio de criptomonedas: padre presentó recurso porque escanearon el iris de su hija menor de edad". Disponible en: https://www.ciperchile.cl/2024/03/22/datos-personales-a-cambio-de-criptomonedas-padre-presento-recurso-porque-escanearon-el-iris-de-su-hija-menor-de-edad/#top [visitado el 15 de abril de 2024].

COMMATTEO, GABRIELA Y MOREYRA, PILAR (2022): "Discriminación 4.0: una aproximación a los problemas que suscitan la biometría y los sistemas de reconocimiento facial", en: Revista Internacional de Derechos (Vol. 12, N° 1), pp. 15-53.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2021): "Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, Versión 2.0". Disponible en: https://www.edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_es.pdf [visitado el 8 de julio del 2025].

CONSEJO PARA LA TRANSPARENCIA (2020): Estudios de transparencia. La protección de datos personales en contextos de avanzado desarrollo tecnológico, con énfasis en videovigilancia y tecnología de reconocimiento facial empleada por el sector público (Santiago, Consejo para la Transparencia).

DONOSO, LORENA (2011): "El problema del tratamiento abusivo de los datos personales en salud", en: Arrieta Cortés, Raúl (Coord.), Reflexiones Sobre el Uso y Abuso de los Datos Personales en Chile (Santiago, Expansiva), pp. 79-99.

EL AGORA (2024): "IA y seguridad digital: ¿está Chile preparado para los desafíos del 2025?". Disponible en: https://www.elagora.net/ia-y-seguridad-digital-esta-chile-preparado-para-los-desafios-del-2025/ [visitado el 19 de marzo de 2025].

EUROPEAN PARLIAMENT (2024): "Artificial Intelligence Act: MEPs adopt landmark law". Disponible en: https://web.archive.org/web/20240315034359/https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law [visitado el 7 de octubre de 2024].

FRANCO, KHALIL Y VELOZ, JOHAN (2022): "Posibles riesgos y problemas del uso de datos biométricos y su relación con los derechos fundamentales", en: Complejidades Del Ágora Jurídica (Vol. 2, N° 1), pp. 52-77.

GARCÍA, ARISTEO (2007): "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", en: Boletín Mexicano de Derecho Comparado (Vol. XL, N° 120), pp. 743-778.

GARRIDO, ROMINA Y BECKER, SEBASTIÁN (2017): "La biometría en Chile y sus riesgos", en: Revista Chilena de Derecho y Tecnología (Vol. 6, N° 1), pp. 67-91.

GARRIGA, ANA (2024): "Los derechos ante los sistemas biométricos que incorporan inteligencia artificial", en: Derechos y Libertades (N° 51, Época II), pp. 117-149.

GLANCY, DOROTHY (1979): "The Invention of the Right to Privacy", en: Arizona Law Review (Vol. 21, N° 1), pp. 1-40.

GRUPO ADAPTALIA (2019): "Fuentes de Acceso Público en la LOPD y el RGPD". Disponible en: https://grupoadaptalia.es/blog/fuentes-de-acceso-publico-en-la-lopd-y-el-rgpd-2/ [visitado el 7 de octubre de 2024].

HUERTA, GUSTAVO; TORRES, CARLOS Y LAGUNES, AGUSTÍN (2021): "Identidad digital en el ámbito educativo", en: Torres, Carlos y Lagunes, Agustín (Coords.), Sistemas y ambientes educativos: estado del conocimiento (Veracruz, Universidad Veracruzana), pp. 46-61.

JIJENA, RENATO (2024): "Responsables y encargados del tratamiento de DP biométricos huellas dactilares: la necesaria fiscalización frente a consentimientos obligatorios (no libres) y para fines no exclusivos". Disponible en: https://www.diarioconstitucional.cl/articulos/responsables-y-encargados-del-tratamiento-de-dp-biometricos-huellas-dactilares-la-necesaria-fiscalizacion-frente-a-consentimientos-obligatorios-no-libres-y-para-fines-no-exclusivos/ [visitado el 19 de marzo de 2025].

JIJENA, RENATO (1992): La protección penal de la intimidad y el delito informático (Santiago, Editorial Jurídica de Chile).

LARA, CARLOS; PINCHEIRA, CAROLINA Y VERA, FRANCISCO (2014): "La privacidad en el sistema legal chileno", en: Policy Papers, ONG Derechos Digitales (N° 8), pp. 1-93.

LOIZOS, CONNIE (2023): "Worldcoin, co-founded by Sam Altman, is betting the next big thing in AI is proving you are human". Disponible en: Worldcoin, co-founded by Sam Altman, is betting the next big thing in AI is proving you are human. Disponible en: https://techcrunch.com/2023/03/07/worldcoin-cofounded-by-sam-altman-is-betting-the-next-big-thing-in-ai-is-proving-you-are-human/ [visitado el 3 de octubre de 2024].

LUCERO, BORIS; SARACINI, CHIARA; MORA, MARCO Y MUÑOZ-QUEZADA, MARÍA (2020): "Aspectos éticos del uso de identificadores biométricos", en: Acta Bioethica (Vol. 26, N° 1), pp. 43-50.

MILANÉS, VALERIA (2017): "Desafíos en el debate de la protección de datos para Latinoamérica", en: Revista Transparencia & Sociedad del Consejo para la Transparencia (N° 5), pp. 13-31.

MINISTERIO DE CIENCIA, CONOCIMIENTO, TECNOLOGÍA E INNOVACIÓN (2021): Política Nacional de Inteligencia Artificial (Santiago, MinCiencia).

NGUYEN, FIONA (2018): "The standard for biometric protection", en: Journal of Law and Cyber Warfare (Vol. 7, N° 1), pp. 61-84.

PÉREZ, ÁNGEL (2013): "Educarse en la era digital. Adelanto del nuevo libro de Ángel Pérez Gómez (Separata)", en: Sinéctica (Vol. 40, N° 1), pp. 47-72.

PIEDRA, JONATHAN (2023): "La recopilación de datos biométricos en Costa Rica: controversias éticas a partir del Proyecto de Ley N° 21321", en: Revista Enfoques: Ciencia Política y Administración Pública (Vol. 21, N°. 38), pp. 23-49.

PUCCINELLI, OSCAR (2004): Protección de datos de carácter personal (Buenos Aires, Editorial Astrea).

PUTTICK, MIRIAM (2020): "Iran: For religious minorities, biometric identity cards threaten to become a new tool for surveillance and discrimination", en: Grant, Peter (Ed.), Minority Rights Group International: Focus on Technology (London, Minority Rights Group International), pp. 178-180.

QUINTANILLA, GABRIELA (2020): "Legislación, riesgos y retos de los sistemas biométricos", en: Revista Chilena de Derecho y Tecnología (Vol. 9, N° 1), pp. 63-91.

RAJEVIC, ENRIQUE (2011): "Protección de datos y transparencia en la administración pública chilena: Inevitable y deseable ponderación", en: Arrieta Cortés, Raúl (Coord.), Reflexiones Sobre el Uso y Abuso de los Datos Personales en Chile (Santiago, Expansiva), pp. 137-159.

REUSSER, CARLOS (2024): "¿Se puede seguir usando la huella dactilar y datos biométricos para registrar la asistencia de los trabajadores?". Disponible en: https://www.derechoinformatico.cl/seguir-con-huella-dactilar/ [visitado el 19 de marzo de 2025].

RUIZ, MARÍA ELENA Y RUIZ, EDGAR (2021): "Método de búsqueda eficiente para resolver el problema de identificación de huella dactilar aplicando machine learning", en: Revista Industrial Data (Vol. 24, N° 2): pp. 293-317.

RUIZ, MILTON; RODRÍGUEZ, JUAN CARLOS Y OLIVARES, JUAN CARLOS (2009): Una mirada a la biometría, en Revista Avances en Sistemas e Informática (Vol. 6, N° 2), pp. 29-38.

SÁNCHEZ, CAROLINA Y TORO-VALENCIA, JOSÉ (2021): "El derecho al control humano: Una respuesta jurídica a la inteligencia artificial", en: Revista Chilena de Derecho y Tecnología (Vol. 10, N° 2), pp. 211-228.

SANZ, FRANCISCO (2023a): "Desafíos para la modernización de la Ley N° 19.628 de 1999, de cara al alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea GDPR", en: Revista CES Derecho (Vol. 14, N° 1), pp. 3-16.

SANZ, FRANCISCO (2023b): "Protección de los datos personales en la era digital: situación de las redes sociales en el caso chileno". Disponible en: https://riej1812.com/wp-content/uploads/2023/04/Comunicaciones-Sanz-Salguero.docx [visitado el 4 de noviembre del 2024].

SANZ, FRANCISCO (2013): "Solicitud de acceso a la información y tutela de los datos personales de un tercero", en: Revista de Derecho de la Pontificia Universidad Católica de Valparaíso (Vol. 41, N° 2), pp. 457-502.

SECRETARÍA GENERAL IBEROAMERICANA (2023): "Carta Iberoamericana de Principios y Derechos en los Entornos Digitales (SEGIB)". Disponible en: https://www.segib.org/wp-content/uploads/Carta_iberoamericana_derechos_digitales_ESP_web.pdf [visitado el 8 de julio del 2025].

UNIÓN EUROPEA, GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS (2003): "Documento de trabajo sobre biometría". Disponible en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_es.pdf [visitado el 3 de octubre de 2024].

UNIVERSIDAD DE CHILE (2024): "Entre la innovación y la intrusión: Investigadoras U. de Chile advierten sobre los riesgos del escaneo de iris por criptomonedas en nuestro país". Disponible en https://uchile.cl/noticias/215213/investigadoras-u-de-chile-advierten-sobre-riesgos-del-escaneo-de-iris [visitado el 10 de agosto de 2024].

VERGARA, MANUEL (2017): "Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales", en: Revista Chilena de Derecho y Tecnología (Vol. 6, N° 2), pp. 135-152.

VIOLLIER, PABLO (2017): El estado de la protección de datos personales en Chile (Santiago, Derechos Digitales).

JURISPRUDENCIA CITADA

Tribunal de Justicia de la Unión Europea, 13 de mayo de 2014, sentencia C-131/12.

Tribunal de Justicia de la Unión Europea, 1° de octubre del 2015, sentencia C-230/14.

Berrios y Otros con Worldcoin Spa (2024): Corte de Apelaciones de Valparaíso 22 de julio de 2024 (acción de protección), Rol: 1474-2024, en: www.pjud.cl.

Kamanau y otro con Worldcoin (2024): Corte de Apelaciones de Valparaíso 27 de julio de 2024 (acción de protección), Rol: 1307-2024, en: www.pjud.cl.

NORMAS JURÍDICAS CITADAS

Biometric Information Privacy Act BIPA. Illinois, 2008.

Biometric Privacy Protection Act. Washington, 2017.

Business and Commerce Code. Texas, 2009.

Constitución Política de Chile.

Ley N° 19.628, sobre protección de la vida privada. Diario Oficial, 30 de agosto de 1999. Chile.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. España.

Boletín N°11144-07 y Boletín 11092-07, Proyecto de Ley sobre Protección de Datos Personales. Chile.

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo. 13 de junio de 2024.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. de 27 de abril de 2016.