Estudios de Deusto

Revista de Derecho Público

Vol. 74/1 enero-junio 2026

DOI: https://doi.org/10.18543/ed7412026

ESTUDIOS

USO DE DATOS BIOMÉTRICOS EN LA DISCRIMINACIÓN DE PERSONAS CON FINES DE PREVENCIÓN DELICTIVA

Use of Biometric data in the discrimination of individuals for crime prevention purposes

Silvia I. Verdugo Guzmán
Profesora Titular (acreditada ANECA) de Derecho Penal
Universidad Internacional de La Rioja (UNIR), Logroño. España
https://orcid.org/0000-0001-9851-4795

https://doi.org/10.18543/ed.3586

Fecha de recepción: 21.11.2025
Fecha de aceptación: 02.02.2026
Fecha de publicación en línea: junio 2026

USO DE DATOS BIOMÉTRICOS EN LA DISCRIMINACIÓN DE PERSONAS CON FINES DE PREVENCIÓN DELICTIVA

Use of Biometric data in the discrimination of individuals for crime prevention purposes

Silvia I. Verdugo Guzmán[1]
Profesora Titular (acreditada ANECA) de Derecho Penal
Universidad Internacional de La Rioja (UNIR), Logroño. España
https://orcid.org/0000-0001-9851-4795

https://doi.org/10.18543/ed.3586

Fecha de recepción: 21.11.2025
Fecha de aceptación: 02.02.2026
Fecha de publicación en línea: junio 2026

Resumen

El derecho a la intimidad se encuentra inmerso en una sociedad digital que reconoce derechos humanos de cuarta generación. Diariamente se recopilan infinitos datos personales altamente sensibles mediante sistemas informatizados de biometría, por su exactitud y precisión. Sin embargo, puede suceder que los algoritmos de estas tecnologías presenten sesgos o tendencias respecto a personas de ciertas características, lo cual puede dar lugar a discriminación por motivos de género, origen étnico u otros patrones. Existen casos de sistemas biométricos que han llevado erróneamente a acusar a personas de ser autoras de un delito o les han causado perjuicios en el ámbito laboral o sanitario. En este trabajo se analizan estas cuestiones, y se centra la exégesis en la exposición de la normativa vigente, propuestas de mejora y también sobre implementación de medidas para un correcto uso de datos biométricos que sea respetuoso con los derechos humanos y la protección de la intimidad.

[1] Correo electrónico: silvia.verdugo@unir.net

Palabras clave

Derechos humanos; datos biométricos; algoritmos y sesgos; discriminación algorítmica; prevención de delitos.

Abstract

The right to privacy is embedded in a digital society that recognises fourth-generation human rights. Every day, vast amounts of highly sensitive personal data are collected using biometric computer systems due to their accuracy and precision. However, the algorithms underlying these technologies may exhibit biases or tendencies towards people with certain characteristics, which can lead to discrimination on the grounds of gender, ethnic origin or other factors. There are cases where biometric systems have wrongly led to people being accused of committing a crime or have caused them harm in the workplace or in healthcare settings. This paper analyses these issues by examining current legislation, proposals for improvement, and the implementation of measures to ensure the correct use of biometric data in a manner that respects human rights and the protection of privacy.

Keywords

Human rights; biometric data; algorithms and biases; algorithmic discrimination; crime prevention.

I. INTRODUCCIÓN

La necesaria protección del derecho a la intimidad de las personas estaba perfectamente identificada desde el año 1948, con el origen de los transistores, que se utilizaron de forma cada vez más masiva a nivel mundial especialmente para obtener información personal y con la posibilidad de ser transmitida a cualquier lugar del planeta. En este sentido, la Sociedad del riesgo de la última década del siglo XX se dirige hacia una nueva modernidad tecnológica (Beck, 1992), y que actualmente permite confirmar que es cada vez más común y constante el manejo de todo tipo de datos en el ciberespacio, pues la información de millones de sujetos se mueve libremente por el mundo digital con diversos fines de manera instantánea. En efecto, ya en los años '80 se vislumbraba que la intimidad personal acabaría perdiéndose en un océano estadístico de computadoras donde la informática convertiría a los individuos en números localizables y casi controlados por terceros (Fariñas Matoni, 1983: 69).

En la década de los 90 se manifestaba que los efectos del uso de la informática sobre la identidad y dignidad humana serían difusos e implacables, e incidirían también en el disfrute de los valores de la libertad e igualdad. Según expone Pérez Luño (1991: 209), "la *primera*, porque en las sociedades más avanzadas se hallaba acechada por el empleo de técnicas informáticas de control individual y colectivo que comprometen o erosionan gravemente su práctica. Contemporáneamente, se produce una agresión a la *segunda*, la igualdad, más implacable que en cualquier otro período histórico, desde el momento en que se desarrolla una profunda disparidad entre quienes poseen o tienen acceso al poder informático y los que se hallan marginados de su disfrute". Efectiva y acertadamente, la dignidad de las personas como derecho humano aparece recogida a partir de 1948 cuando se reconoce en la Declaración Universal de los Derechos Humanos (Miranda Gonçalves, 2020: 151). Y es ese el derecho que se debe proteger en estos tiempos de nuestra sociedad digital.

En el siglo XXI encontramos plenamente vigentes los derechos de cuarta generación en una sociedad que debe proteger datos personales, privacidad

digital, acceso a internet, entre otros. Continuamente se están implementando distintas tecnologías en nuestros hábitos y rutina, que incluyen sistemas sofisticados tales como geolocalización (GPS), inteligencia artificial (IA[2]), el uso de dispositivos electrónicos inteligentes, y otros que, inevitablemente se alimentan de datos de diversa índole para su puesta en funcionamiento y que son almacenados con ese fin. Por ejemplo, el *Big Data* permite intercambiar en forma simultánea datos e información de distintas características, pues crea su espacio en diferentes materias que se pueden gestionar y almacenar indefinidamente. De los 90 minutos que dura un partido de fútbol, es posible medir el rendimiento de cada jugador, los kilómetros que recorre, el porcentaje de pases acertados, cantidad de tiros libres que ejecuta, entre otros datos. Todo esto le sirve al entrenador para realizar los cambios que estime necesarios de cara a obtener el triunfo del equipo.

Con los sistemas tecnológicos disponibles, es relativamente sencillo compartir diversos datos de una persona, pues a través de internet es posible obtener todo tipo de información: etnia, parentesco, posibles enfermedades, etc. lo cual puede influir a nivel laboral e incluso a la hora de contratar un seguro de salud o un crédito bancario. Así también, tradicionalmente se utilizan contraseñas, documentos de identidad y códigos o números PIN con una cantidad de dígitos que pueden ser fácilmente conocidos por terceros, e incluso a nivel delictivo, ciberdelincuentes pueden acceder a sistemas que los contienen, adivinándolos o inutilizando información incorrecta varias veces (Natgunanathan, Mehmood, Xiang, Beliakov y Yearwood, 2016: 880 y ss.).

Por lo que respecta al derecho a la intimidad de las personas, se relaciona directamente con el uso cada vez más masivo de las tecnologías de la información y comunicación (TIC) que, en materias tan importantes como son los datos e información personal han pasado a ser un bien inmaterial muy preciado para los Estados, empresas, y en definitiva, terceras personas de distintas clases, porque son un conjunto importante de información que, con el transcurso del tiempo se han convertido en una herramienta poderosa que puede ser utilizada con diversos fines. Por ejemplo, hoy en día la discusión se

[2] Artículo 3.1. «sistema de IA»: un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales; Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), DOUE núm. 1689, 12 de julio de 2024.

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 74/1, enero-junio 2026, págs. 435-457
https://doi.org/10.18543/ed.3586 • http://www.revista-estudios.deusto.es/

encuentra en torno a la red social *TikTok* y el dominio de los algoritmos que contienen poderosa información de millones de usuarios conectados, cuyo dueño es China y que Estados Unidos quiere poseer.

En línea con lo anterior, cabe precisar que un dato personal es el nombre de una persona, su dirección, teléfono, el Documento Nacional de Identidad, su imagen, la clave asociada a un usuario, el nombre de usuario –*nickname*–, la dirección de correo electrónico, etc. (Andreu Martínez, 2022: 201). De estos, se pueden obtener datos sensibles tales como los de salud, genéticos, biométricos, etc. Por este motivo, son custodiados por aseguradoras, líneas aéreas, tiendas de ropa, de comida, etc. Generalmente, tomados sin consentimiento del titular de esos datos, por ejemplo, cuando se acepta el uso de las *cookies* por parte de quien navega en internet con su autorización (viciada en muchos casos, cuando se deben aceptar o de lo contrario no se puede acceder a la *web* que se quiere consultar). Esto otorga total libertad a terceros para obtener información privilegiada sobre gustos y preferencias, para así ofrecer productos incluso a costos más altos que lo normal. LESSIG señalaba que es como el caso de un viajero frecuente, pues su perfil puede abarcar información acerca del asiento que prefiere o si le gusta la comida vegetariana, e indicar la frecuencia con que viaja esa persona, y compañías aéreas pueden efectuar discriminaciones basadas en esta información (Lessig, 2009: 356).

Cobra importancia analizar en este trabajo los problemas que existen en torno a los datos biométricos, que, dentro de las clasificaciones de datos personales se consideran una categoría especial en la normativa europea. Si bien serán analizados, cabe definirlos sencillamente como, aquellos que consisten en la elaboración de perfiles, peligrosos por su cuestionable funcionamiento y probablemente discriminatorio de las personas, incluso cuando se usa IA, porque los sistemas que la incorporan son capaces de analizar, interpretar, segregar y utilizar la distinta información que captan, esto mediante la discriminación algorítmica o recogida masiva de datos.

También, se plantearía un problema no menor cuando se producen fallos o errores en el sistema de la misma IA que analiza la información que capta. Con razón, "como los resultados de estos sistemas tienen un carácter probabilístico no están exentos de errores y, esa tasa de error, aún respecto de aquellas herramientas más afinadas y con tasas bajas, puede suponer un enorme impacto en la vida y en los derechos de las personas afectadas" (Garriga Domínguez, 2024: 120). Y, en innumerables ocasiones esto ha quedado como una simple disculpa de la entidad en que se ha producido el fallo informático, sin mayor preocupación respecto de la persona que ha sido discriminada, por ejemplo, cuando el escáner facial no reconoce el color de piel de una persona.

Además, se plantean problemas respecto a la vulneración de la intimidad con el uso de sistemas tecnológicos que probablemente custodian

información con absoluta impunidad por bases deficientes de regulación normativa, por ejemplo, mediante el uso de la IA en el ámbito policial, ya que se deberían establecer límites claros en el desarrollo y aplicación de tecnologías que podrían justificarse en casos como es la persecución del terrorismo, pero que pueden causar discriminaciones de personas. Si bien cabe reconocer que también la integración generalizada de los datos biométricos es bastante útil para el reconocimiento de personas que están siendo buscadas por algún motivo (desaparición, autor de un delito, etc.), esto también plantearía nuevos retos en materia de seguridad y privacidad.

En definitiva, mediante una profunda revisión bibliográfica y legislativa, nuestra exposición va encaminada a describir algunos de los problemas planteados y advertir que no se puede dar vía libre a quienes conocen datos e información de terceros, ni siquiera con fines de prevención delictiva, por muy insegura que sea una calle o para evitar desórdenes en la vía pública si la excusa es una detención policial de "posibles" sujetos violentos detectados con un sistema de reconocimiento facial. Por estos motivos, finalmente, la propuesta se dirige a un llamado a implementar las medidas oportunas por quienes custodian datos biométricos de cara a la efectiva protección de un derecho humano tan importante como es el de la dignidad de las personas.

II. DATOS BIOMÉTRICOS COMO CATEGORÍA ESPECIAL DE PROTECCIÓN EN LA NORMATIVA EUROPEA

Cabe comenzar recordando que el art. 12 de la Declaración Universal de los Derechos Humanos de 1948[3] es clave al referirse expresamente al derecho a la intimidad de las personas, y que se encontraría, en efecto, adaptado hace décadas al uso de las TIC, que además nos acerca a su aplicación respecto al uso de los datos biométricos, que se tratarán más adelante.

En el ámbito europeo, la tutela de los datos personales está regulada desde hace décadas, y contiene en el Reglamento General de Protección de Datos (RGPD)[4] el eje central de su protección actualmente, e incluye como datos de especial protección aquellos que revelen el origen racial o étnico, en su

[3] "Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

[4] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD). Diario Oficial de la Unión Europea, L 119/1, 4 de mayo de 2016.

Considerando 51[5]. Aquí entonces localizamos los primeros asomos de protección de los datos biométricos personales.

En efecto, se advierte que procesar datos personales que revelen el origen racial o étnico a gran escala –sea con fines científicos o policiales[6]– puede representar una importante colisión con varios derechos y principios que se contemplan en torno a la protección de la privacidad de las personas. Más aún, se debe apuntar que en el caso del almacenamiento de datos genéticos derivados de un proceso penal es una actividad que se expande cada día más entre los Estados que ya cuentan con esta tecnología (Verdugo Guzmán, 2021: 96 y ss.). Si bien es cierto que pueden ser útiles para controlar la reincidencia de los individuos sospechosos o ya condenados por la comisión de un delito (Valerio Jiminián, 2019), en la identificación de personas desaparecidas, quienes han fallecido en un incendio, etc., en otros casos probablemente causarían problemas incluso a la hora de buscar trabajo o de tomar una póliza de seguro. Cuestión similar sucede con los datos biométricos, con énfasis en su utilización en distintos campos en que existen bases de regulación normativa difusas, y que no cuentan con un cumplimiento efectivo riguroso.

A continuación, cabe preguntarse, ¿qué son los datos biométricos?

Si bien ya se ha dado un avance de definición anteriormente, cabe precisar ahora que son aquellos datos que se obtienen a partir de un tratamiento que incluye dispositivos informáticos o tecnologías capaces de procesar información sobre los rasgos físicos o conductuales de una persona, y específicamente, según el art. 3. 34. RIA son, "datos biométricos: los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos"[7].

---

[5] *"*Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. (…). Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas*"*.

[6] En este sentido, *vid.* la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

[7] RIA. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia

Los datos biométricos efectivamente son de gran ayuda en la vida de las personas, y cabe reconocer, como destaca Casado (2014: 13), "las tecnologías de identificación que actualmente se manejan son poderosas y tienen una creciente potencialidad. La huella genética y la biometría en general –de la mano, del iris, el reconocimiento de voz, la huella digital…– constituyen herramientas cada vez más fiables que proporcionan datos de fácil almacenamiento y acceso, lo que conlleva que sean técnicas altamente intrusivas para la intimidad personal, ya que permiten fácilmente la disposición para usos indebidos y especialmente discriminadores".

Respecto al art. 4 RGPD el Tribunal de Justicia de la Unión Europea (TJUE) ha tenido ocasión de pronunciarse en relación con la definición de datos personales en reiteradas oportunidades y ha señalado que la utilización del término «toda información», debe entenderse en un sentido amplio de forma que, "(...) puede abarcar todo género de información, tanto objetiva como subjetiva, en forma de opiniones o apreciaciones, siempre que sean "sobre" la persona en cuestión"[8]. Esto significa que, independientemente de que se trate de datos personales, genéticos, de salud o biométricos, igualmente deben ser protegidos a cabalidad, sin posibilidad de ser tratada información obtenida en forma voluntaria o involuntaria por parte del titular: de ahí la importancia de los distintos principios reguladores del tratamiento de datos personales que se establecen especialmente a partir del art. 5 del RGPD[9].

III. DERECHO A LA INTIMIDAD DE LAS PERSONAS EN LA CONSTITUCIÓN ESPAÑOLA DE 1978

Conectada a la protección de los derechos fundamentales se encuentra el art. 18 CE que, en sus apartados 1 y 4[10], se refiere al derecho a la intimidad,

---

artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial-RIA), DOUE núm. 1689, 12 de julio de 2024.

[8] Apdo. 34 de la STJUE de 20 de diciembre de 2017, y apdo. 23 de la STJUE de 4 de mayo de 2023.

[9] Se encuentra el principio de licitud, lealtad y transparencia en la letra a); limitación de la finalidad de la letra b); minimización de datos en la letra c); exactitud de los datos de la letra d); limitación del plazo de conservación de la letra e); integridad y confidencialidad de los datos de la letra f); y de responsabilidad proactiva o *accountability* –art. 5.2–, del RGPD.

[10] "Art. 18. 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. (…).

4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

el cual está estrechamente vinculado al derecho a la protección de datos, también, biométricos. En cualquier caso, la regulación y protección de derechos fundamentales como el que se encuentra en el art. 18.4 CE, requieren de una adaptación y custodia de la libertad, intimidad personal y familiar, además de la propia imagen, incluida la protección de los datos personales, y en general, de todos los derechos humanos que deben armonizarse a la sociedad digital en que nos encontramos (Verdugo Guzmán, 2023: 35 y ss.). Lo mismo cabe plantear respecto a los datos biométricos y los distintos sistemas de reconocimiento facial que se utilizan por distintas entidades hasta que son intervenidos por las autoridades competentes.

En relación al art. 18 CE, cabe recordar la Sentencia del Tribunal Constitucional núm. 292/2000, de 30 de noviembre, pues estableció que, "este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, (…) atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran"[11].

De lo expuesto se colige que el derecho a la protección de datos se configura como una facultad del titular para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención, y decidir cuáles de esos datos se pueden proporcionar a un tercero, sea el Estado, una empresa o un particular, o cuáles datos puede recabar un tercero, el tiempo de conservación, efectiva eliminación, y que también se permita fácilmente al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso por parte de terceros, sin necesidad de formularios o gestiones burocráticas que en general llevan a que las personas no tomen medidas efectivas. Así, las denominadas llamadas *spam*, se realizan diariamente a infinitos ciudadanos, si bien existe la "Lista Robinson", pero que, después de rellenar un formulario en que se solicita no sean realizados llamados telefónicos por parte de compañías, poca o nula utilidad parece ser 100% cierta.

El enlace constitucional a las normas del ordenamiento jurídico se encuentran hace ya décadas, con la regulación de la protección de datos personales principalmente en la Ley Orgánica 15/1999, de 13 de diciembre, de

[11] Sentencia del Tribunal Constitucional, núm. 292/2000, 30 de noviembre. Ponente: J. D. González Campos.

Protección de Datos de Carácter Personal[12], que fue derogada con la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)[13], cuyo objeto fue adaptar el ordenamiento español al propio RGPD y así también para completar sus disposiciones jurídicas al efecto. Ha sido una difícil tarea, que se encuentra con ese océano de datos e información personal que circulan por las redes del ciberespacio sin rumbo conocido en muchas ocasiones, o que son captados en terceros países (que están fuera de la Unión Europea, y, por tanto, que no se ven obligados por el RGPD). Un ejemplo está porque muchos hoteles exigen el documento de identidad a los huéspedes para sacarle copia con distintos fines.

Así entonces, si bien la situación de los datos personales en poder de terceros se encuentra medianamente protegida en España, los riesgos para los derechos de las personas siguen estando latentes, y más aún, la cuestión regulatoria sobre los datos biométricos está en un limbo jurídico difícil de delimitar aún. Incluso empresas como Mercadona o La Liga (de fútbol) han sido multadas por la Agencia Española de Protección de Datos (AEPD) debido al uso de estos sistemas en espacios públicos. En el mes de noviembre de 2025 la propia AEPD multó con 10 millones de euros al gestor aeroportuario AENA, por usar sistemas de reconocimiento facial en varios aeropuertos del país, que captaban datos de los pasajeros en contra del principio de proporcionalidad del RGPD y la normativa española. Se impuso una sanción de 10.043.002 euros vinculada al art. 35 RGPD, por no disponer de una evaluación de impacto en la protección de datos válida (EIPD) en relación con el sistema de reconocimiento facial. Además, se ordenó la suspensión temporal del tratamiento biométrico hasta que se subsanaran los errores mediante una EIPD.

IV. DATOS BIOMÉTRICOS, RECONOCIMIENTO FACIAL Y SESGOS ALGORÍTMICOS

Existen varios casos documentados que se refieren al uso de tecnologías que ha llevado a un sinnúmero de posibles vulneraciones a un derecho tan importante como es el de la intimidad personal que se desprotege cuando se capta conscientemente (o de forma involuntaria) un dato personal. Al comienzo fue mediante algoritmos[14] básicos, pero con el transcurso del

[12] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE núm. 298, de 14 de diciembre de 1999.

[13] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE núm. 294, de 6 de diciembre de 2018.

[14] Algoritmo: conjunto ordenado y finito de operaciones que permite hallar la solución de un problema. Diccionario de la Real Academia Española (DRAE, 2025).

tiempo están siendo cada vez más complejos y sofisticados, permitiendo una adaptación dinámica mucho más precisa en el caso de los algoritmos de reconocimiento facial que se impulsan mediante IA (Cuadrado Gamarra, 2024: 347).

Distintos sistemas de IA permiten captar datos biométricos de forma muy precisa. Mediante el uso de técnicas de escaneo del iris ocular, la huella digital, el reconocimiento de voz y otros, se captan, a través de equipos tecnológicos cada vez más cantidad de datos biométricos cuyo destino final y almacenamiento suelen ser inciertos. Según la AEPD (2022) la aplicación conjunta de todas las tecnologías –redes sociales, IA, interfaces neuronales, etc.– puede provocar efectos individuales y sociales que generen riesgos para los derechos y libertades a una escala difícil de imaginar *a priori;* así, por ejemplo, la vigilancia masiva, la discriminación, la pérdida de autonomía, el fraude o la suplantación de identidad.

Las alarmas en las personas 'físicas' se encienden porque, según Cuadrado Gamarra (2024: 346), "los sistemas de identificación biométrica automatizados, especialmente aquellos basados en IA o reconocimiento facial, tienden a facilitar la vigilancia masiva o exhaustiva". Así pues, un mal uso de los datos biométricos puede causar suplantaciones de identidad, acceso a información confidencial, daños físicos o psicológicos, especialmente con la discriminación algorítmica por razón de sexo o raza; pero no todo es negativo, pues también sirven para identificar enfermedades, gustos o hábitos de las personas.

En términos sencillos, básicamente, los datos biométricos se crean, forman y "entrenan" con algoritmos para descubrir patrones y conocimientos de la máquina (aprendizaje automático o *machine learning*). El problema está cuando existen sesgos[15] de un algoritmo, que se produce por diversas causas, por ejemplo, debido a sesgos en los datos de un entrenamiento defectuoso que cause repetidamente errores, en el diseño de los algoritmos específicos, en los datos *proxy* o incluso en la evaluación final, cuya consecuencia es que, "los errores sistemáticos en los algoritmos de *machine learning* producen resultados injustos o discriminatorios. A menudo refleja o refuerza los sesgos socioeconómicos, raciales o de género existentes" (IBM, 2025). En definitiva, cuando los datos están mal registrados e inducen a errores.

Ya ha quedado claro que, según el RGPD los datos biométricos son considerados como una categoría especial de datos. Esto significa que en principio está prohibido el uso de datos biométricos si su tratamiento no se produce dentro del marco legal (siendo fundamental el consentimiento del titular o dueño de aquellos) porque el objetivo final de estos sistemas que los captan

[15] Sesgo: Torcido, cortado o situado oblicuamente (DRAE, 2025).

utiliza tratamientos técnicos para identificar y revelar de forma inequívoca a una persona física determinada.

En línea con lo anterior, el RIA señala en el art. 3. 35 que identificación biométrica es, "*El reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos*".

Mediante las técnicas de identificación biométrica se permite identificar a una persona sin necesidad de contacto físico: es posible a distancia ya que la información captada es transmitida a una base de datos con la cual está conectada. Así entonces, según Pizzolo (2024: 7), "las mediciones realizadas con una videocámara o un micrófono son adquiridas por IA y procesadas comparando las características biométricas con los datos previamente adquiridos y almacenados en una base de datos y/o diferentes bases de datos".

Y cabe preguntarse, en la práctica, ¿quién controla tales sistemas?

Si bien probablemente hay un sistema operativo o programa informático, cabe suponer que detrás de ello hay una persona física, que es quien toma las decisiones finales. Sin embargo, en no pocos casos se ha excusado la responsabilidad de la persona que confía ciegamente en la decisión de una máquina. Por ejemplo, hace un tiempo Amazon utilizó una herramienta de IA que discriminaba y descartaba currículos que incluían palabras como "mujeres", dando preferencia a perfiles de hombres.

La utilidad de los datos biométricos se relaciona al rastreo digital del movimiento corporal, de ondas cerebrales e incluso de respuestas fisiológicas de una persona. En general, estos se captan mediante la huella dactilar, el reconocimiento facial, del iris ocular, la retina, de la geometría de la mano, la forma de las orejas, vascular o geometría del árbol de las venas en dedos o de la mano, de firma, de escritura, de voz, de escritura de teclado, la forma de andar, y probablemente habrá otras más. Por ejemplo, mediante la Autentificación Biométrica (AB), es posible verificar la identidad de una persona, "(…) considerando detalles morfológicos que sólo existen en ese sujeto. A través de la AB se recoge información referente a un rasgo distintivo de una persona (su voz, su huella dactilar), para cotejar esa muestra con otra, recogida normalmente en el mismo momento, y poder comprobar si son iguales o no" (https://ayudaleyprotecciondatos.es, 2019).

En este orden de ideas, el reconocimiento facial mediante el uso de *software* con IA que permite captar patrones del rostro humano es el que presenta una especial preocupación en este instante. Ello porque implica el tratamiento de datos personales especialmente protegidos (según el RGPD), y pueden verse afectados cuando un algoritmo presenta sesgos cognitivos y

provocan discriminación[16], hacen recomendaciones a personas de cierto perfil[17] o descartan a otras[18], especialmente si la IA no es capaz de identificar a una persona como tal. Más aún, recuerda la AEPD (2020: 37), "en el estudio *Discrimination, artificial intelligence, and algorithmic decision-making* publicado por el Consejo de Europa, se enumeran los siguientes ejemplos: el *software* de seguimiento facial de *Hewlett Packard* no reconoció los rostros oscuros como caras, la aplicación *Google Photos* etiquetó una foto de una pareja afroamericana como "gorilas", una cámara Nikon seguía preguntando a personas de origen asiático: ¿alguien parpadea?, un hombre asiático tuvo su foto de pasaporte rechazada, automáticamente porque "los ojos del sujeto están cerrados", Buolamwini y Gebru descubrió que "las mujeres de piel más oscura son el grupo más mal clasificado (con error tasas de hasta el 34,7%). La tasa de error máxima para los hombres de piel más clara es del 0,8%".

Para utilizar los sistemas de biometría es necesario contar con unas plantillas biométricas. En este sentido, "se configuran como presupuesto esencial del funcionamiento de los sistemas de identificación y autenticación basados en biometría, en un primer momento se captan y almacenan los datos biométricos, los cuales de manera posterior se comparan con una o más plantillas según sea el caso. El uso de sistemas de reconocimiento facial supone la previa realización de una evaluación de impacto a través de la cual se pueda examinar la necesidad y proporcionalidad en relación con el fin del tratamiento" (González Mendoza, 2025: 460).

El impacto del uso de sistemas de identificación biométrica ha sido ampliamente abordado por la AEPD (2020: 37), y señaló que la exactitud de la información biométrica es primordial en relación a la protección de los datos personales y se deben tener en cuenta factores de rendimiento en los sistemas biométricos, es decir, falsos positivos, negativos y otros, pero además el impacto sobre la recogida de datos de personas con alguna discapacidad o particularidad física que impidan una identificación adecuada o producen un perfilado erróneo incluso antes del tratamiento personal de los datos.

[16] En Buenos Aires el año 2019 fueron usadas más de 300 cámaras con *software* de reconocimiento facial bajo el argumento de utilizarlos con fines de seguridad pública. Sin embargo, el sistema tuvo acceso a millones de personas y en varios casos falsamente se les identificó como prófugas, por lo que sin respaldo legal se estaba utilizando un sistema que vulneraba evidentes derechos constitucionales.

[17] En China es común que las policías utilicen gafas de reconocimiento facial conectadas con la sede central, y que permiten identificar a personas perseguidas por un delito o una situación particular.

[18] Hace unos años *Facebook*, utilizó un algoritmo en *Meta*, su filial de Metaverso que despidió a 60 empleados al azar en la sucursal Accenture en Texas a través de una videollamada, sin indicarles alguna justificación ni motivo del cese laboral.

V. BIOMETRÍA Y PREVENCIÓN DELICTIVA

Corresponde analizar dónde y hasta qué punto se justifica el uso de los sistemas tecnológicos de biometría en espacios abiertos, como puede ser en estadios de fútbol, salas de conciertos o aeropuertos, por ejemplo. Quizás, en el último caso (igual que en estaciones de trenes, autobuses y lugares fronterizos) se justifica por razones de orden y seguridad pública (evitar atentados terroristas o perseguir sujetos que han cometido un delito), pero en los otros casos parece ser que no. En este sentido, explica Garriga Domínguez (2024: 148), "las posibilidades del seguimiento omnipresente de las personas en espacios públicos a través de la videovigilancia de reconocimiento facial, además de una grave injerencia en sus derechos a la vida privada y a la protección de datos personales, impactará negativamente en la libertad de expresión y a la libertad de reunión y asociación".

En el caso de España, la propia AEPD (2022) señaló que no toda instalación pública justifica el uso de tales sistemas, pues según el principio de proporcionalidad (en materia de protección de datos), se deben valorar alternativas que sean menos intrusivas (que puedan vulnerar derechos fundamentales) y justificar la necesidad del uso de un sistema biométrico en un sitio concreto. En este sentido, el Preámbulo de la Ley Orgánica 7/2021, señala que, "los datos biométricos (como las huellas dactilares o la imagen facial) sólo se consideran incluidos en esta categoría especial cuando su tratamiento está dirigido a identificar de manera unívoca a una persona física. El propósito es singularizar los autores o partícipes de infracciones penales, así como poder reconocer si son las personas que se supone o se busca, y de esta forma, atribuir o exonerar, sin género de dudas, la participación en determinados hechos, gracias a posibles indicios o vestigios biométricos"[19].

Para evitar discriminaciones injustificadas de una persona que es identificada gracias a biometría, por ejemplo, directamente como autor de un delito (no como "posible autor" sino que con 100% de certeza de quién se trata), es clave un entrenamiento adecuado de los algoritmos, esto es, cuando los sistemas de IA aprenden a tomar decisiones basándose en datos de entrenamiento con 100% de precisión. Entonces, será esencial evaluar los conjuntos de datos que se custodien para detectar la presencia de sesgos, y en este sentido, un método consiste en revisar el muestreo de datos previamente recolectados para detectar grupos sobrerrepresentados o infrarrepresentados en los datos de entrenamiento para evitar justamente esas desviaciones algorítmicas. Por ejemplo, "los datos de entrenamiento de un algoritmo de reconocimiento facial que representa en exceso a las personas de raza blanca pueden dar

[19] *Preámbulo*, Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, BOE núm. 126, de 27 de mayo de 2021.

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 74/1, enero-junio 2026, págs. 435-457
https://doi.org/10.18543/ed.3586 • http://www.revista-estudios.deusto.es/

lugar a errores al intentar el reconocimiento facial de personas de color. Del mismo modo, los datos de seguridad que incluyen información recopilada en zonas geográficas predominantemente negras podrían crear un sesgo racial en las herramientas de IA utilizadas por la policía" (IBM, 2025). Estas conductas son las que se deben evitar.

Cabe plantear ahora los casos en que un tercero no autorizado (ciberdelincuente o un pirata informático) accede a sistemas informáticos que contienen datos biométricos, como puede suceder en caso de un sabotaje a los sensores biométricos a una empresa que interrumpe el funcionamiento de autenticación y compromete la seguridad de los datos y confiabilidad de esos procesos (INCIBE, 2025). Más allá de la responsabilidad administrativa de la persona física que custodia esa información y de la entidad en la cual se utilizan (aplicando multas), debido a ese incumplimiento del deber de custodia y poca precaución en relación con datos personales de terceros, sin duda hay que avisar al interesado o titular de esos datos, de cara a evitar suplantaciones de identidad que signifiquen incluso accesos no autorizados a cuentas bancarias o contratación de seguros, bienes o servicios. Más aún, por los riesgos que puede acarrear la comisión delictiva atribuyendo falsamente la autoría del hecho. Así, es posible plantear que, ese "no" aviso de intromisión a la base de datos de la entidad donde se alojan y custodian los datos de clientes (por ejemplo), sí que puede acarrear responsabilidad penal del encargado del sistema y de la propia empresa o persona jurídica (y la sanción entonces será mucho más perjudicial que una multa administrativa). Por esto, además son fundamentales los escudos de ciberseguridad para garantizar la protección y custodia segura de información personal, evitando una excesiva dependencia en la inteligencia artificial.

Por otra parte, respecto a las amenazas y problemas de seguridad relacionados con los puntos de ataque de un sistema biométrico, se encuentra la siguiente enumeración (Wencheng Yang, Song Wang, Jiankun Hu, Guanglou Zheng & Craig Valli, 2019):

1) Suplantación de identidad: presentar datos biométricos falsos al sensor.
2) Aprovechar la similitud, por ejemplo, utilizando la cara de gemelos idénticos.
3) Intento de cero esfuerzos: el atacante utiliza su propia muestra biométrica para hacerse pasar por un usuario autorizado.
4) Destruir físicamente el sensor biométrico para dejarlo fuera de servicio.
5) Ataque de repetición: el atacante intercepta una señal biométrica y la reproduce en el sistema.
6) Cortar el canal de comunicación para que el sistema no esté disponible.
7) Ataque de denegación de servicio: altera la información del canal para impedir que un usuario genuino se autentique.
8) Ataque de escalada: modificar convenientemente la imagen de consulta hasta obtener el puntaje de coincidencia deseado.

9) Inyectar continuamente muestras para impedir que usuarios genuinos accedan al sistema.
10) Inyectar programas troyanos.
11) El atacante obtiene ilegalmente plantillas biométricas originales.
12) El atacante modifica la plantilla biométrica, por ejemplo, agregando o reemplazando información.
13) Leer plantillas biométricas de un canal de comunicación y reproducirlas.
14) Alterar la información transmitida a través de un canal de comunicación con el fin de negar a usuarios genuinos el acceso al sistema.
15) Cortar el canal de comunicación para que el sistema no esté disponible.
16) Alterar la información transportada coincidentemente o no coincidente para denegar el acceso de un usuario genuino o permitir el acceso de un impostor.

De la información expuesta, se colige que los datos biométricos se obtienen por diversos motivos, y, en última instancia, su uso indebido puede acarrear consecuencias perjudiciales para el titular. Entonces, las medidas de prevención por quien los posee, además de una custodia seria y eficaz, se vuelven fundamentales para un correcto uso de las tecnologías de biometría. Pero por otra parte, la persecución de ciberdelitos tales como la usurpación de identidad, daños informáticos, ciberestafas, sabotajes, etc., se tornan esenciales para una adecuada protección de la sociedad digital.

VI. PRIVACIDAD DE LAS PERSONAS EN EL MARCO DE SEGURIDAD "CIDAR"

Ante los problemas de intromisión ilegítima a los datos biométricos son deficientes las regulaciones normativas en muchos países, principalmente por desconocimiento o falta de especialización y actualización por quienes acceden y custodian esos datos, cuya consecuencia produce la violación de la privacidad de las personas que ceden su información a terceros. A ello se suma que, en muchas ocasiones por desconocimiento o un exceso de confianza de los interesados en saber para qu**é** serán utilizados, o cuando se les indica que será con fines lícitos pero que finalmente son mal utilizados, se tornan como fundamentales unas correctas medidas especialmente de protección.

Llegados a este punto se torna interesante verificar el reciente marco de seguridad sobre la Confidencialidad, Integridad, Disponibilidad, Autenticidad y Responsabilidad (CIDAR), que sirve para evaluar la seguridad en torno a los datos biométricos[20], y así entonces tenemos:

[20] En inglés *CIAAA (Confidentiality, Integrity, Availability, Authenticity and Accountability)*.

CONFIDENCIALIDAD	La protección de la información biométrica es crucial debido a las amenazas y graves consecuencias que pueden producirse debido a su filtración. Debe fomentarse todo tipo de iniciativas que mantengan segura e íntegra la información.
INTEGRIDAD	Es esencial proteger los datos biométricos de modificaciones no autorizadas. Por lo tanto, cabe disuadir a los actores maliciosos de comprometer la integridad de los datos, y a la vez incentivar a las autoridades competentes a mantener protegida la información biométrica.
DISPONIBILIDAD	Los datos biométricos deben ser accesibles en cualquier momento pero de forma segura, si bien en el ámbito privado puede ser más difícil (si por ej. no se tienen buenos sistemas de ciberseguridad). En cualquier caso, cualquier sistema (público o privado) puede ser objeto de intromisiones ilegales.
AUTENTICIDAD	La identificación precisa de los usuarios autorizados (o propietarios de esos datos biométricos) es fundamental para el control de acceso a ellos en aplicaciones o sistemas. Junto con la confidencialidad, cualquier fallo en la autenticidad de los datos biométricos podría tener consecuencias negativas.
RESPONSABILIDAD	Cuando una persona es autorizada al acceso de la información biométrica, es importante actualizar un registro de auditoría para mantener un historial de accesos. La responsabilidad sobre los sistemas es crucial durante investigaciones por incidentes de seguridad (acceso no autorizado) y para la recuperación posterior a los ataques de seguridad. Por esta razón, autoridades (que custodian estos datos) deben ser conscientes de su responsabilidad sobre ellos.

Fuente: Jung & Virgil (2024): 50.

A raíz de lo anterior, se considera primordial contemplar un correcto marco de ciberseguridad CIDAR, pues se vuelve fundamental para la eficacia de cualquier sistema de seguridad que se refiera al manejo y custodia de información biométrica. Por lo tanto, es importante identificar las cuestiones pertinentes dentro de cada aspecto de la seguridad, evaluar el alcance de la cobertura de dichas cuestiones en el marco jurídico vigente en materia de privacidad y debatir las posibles mejoras para promover el desarrollo de una legislación más eficaz (Jung & Virgil, 2024: 49-50).

Ciertamente, las tecnologías de identidad digital pueden vulnerar derechos humanos, por lo que es importante minimizar los riesgos de posible discriminación y promover estándares de alta seguridad en la privacidad y protección de datos personales (Beduschi, 2019). Está claro que al mostrar transparencia y prácticas honestas en materia de privacidad de las personas (a la hora de obtener y custodiar datos) es una forma de generar confianza y la reputación de las empresas (Li, Yu & He, 2019). Así también, es clave considerar al sujeto responsable del tratamiento de los datos personales, que conforme al principio de responsabilidad proactiva del art. 24 RGPD, debe implementar las medidas adecuadas para asegurar y evidenciar la conformidad del tratamiento con el Reglamento europeo. Y es que, en definitiva, "estas medidas deben revisarse y actualizarse siempre que sea necesario, en función de los riesgos que puedan afectar a los derechos y libertades de los interesados" (García Antón, 2025: 10).

Pero también es importante abordar los prejuicios algorítmicos y no descartarlos, pues, según IBM (2025) cuando no se hace, "se obstaculiza la capacidad de las personas para participar en la economía y la sociedad. También reduce el potencial de la IA. Las empresas no pueden beneficiarse de sistemas que producen resultados distorsionados y fomentan la desconfianza entre las personas de color, las mujeres, las personas con discapacidad, la comunidad LGBTQ u otros grupos de personas marginadas". En este sentido, un seguimiento efectivo del correspondiente sistema, por parte de una persona física, se torna fundamental para no incurrir en discriminaciones.

VII. EVALUACIÓN DE IMPACTO EN LA PRIVACIDAD O *PRIVACY IMPACT ASSESSMENT*

Finalmente, cabe referirse a la necesidad de mantener una especial protección de la privacidad de las personas a nivel estatal, pues, si bien en muchos casos se puede justificar la posesión de datos biométricos por necesidades de seguridad nacional u orden público, por ejemplo, de todas maneras, es importante un respeto por este derecho tan fundamental, y es tarea de los Estados desarrollar un marco de especial protección de la privacidad, el denominado PIA (*Privacy Impact Assessment*), o EIPD (Evaluación de Impacto de la Protección de Datos).

Lo anterior se refiere al análisis de los riesgos que puede llevar el tratamiento de datos personales. Así pues, una EIPD consiste en identificar, evaluar y mitigar los riesgos que pueden existir por parte del responsable y encargado del tratamiento (o autoridad de control), a realizar antes de poner en marcha un sistema informático o nuevo proceso que involucre el manejo

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 74/1, enero-junio 2026, págs. 435-457
https://doi.org/10.18543/ed.3586 • http://www.revista-estudios.deusto.es/

de datos personales utilizando nuevas tecnologías[21]. En particular, la EIPD se requerirá en caso de tratamientos automatizados, como la elaboración de perfiles, según el art. 35.3 RGPD[22].

En relación con lo expuesto, el art. 35.4 RGPD, señala que se debe realizar un listado de los tratamientos que requieren una EIPD, entre los cuales se encuentran, "*Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física*"[23].

Si bien el RGPD establece la obligación de una EIPD, de todas formas, la creación de un listado no es de un carácter vinculante, y podrá llevarse a cabo si el responsable o la autoridad de control lo considera oportuno, o no, y es que los términos del art. 35.1 RGPD, "*alto riesgo para los derechos y libertades*"[24], son una cuestión discutible cuando se trata de seguridad nacional u orden público. En nuestra opinión, sí es fundamental que sea obligatoria una EIPD en toda entidad o persona que maneje datos biométricos, como un compromiso de todos los involucrados, incluyendo los Estados, para una correcta y efectiva protección de los derechos humanos.

VIII. CONCLUSIONES

Desde la Declaración Universal de los Derechos Humanos de 1948 se reconoce normativamente el derecho a la intimidad de las personas, y en la Unión Europea existe un alto nivel de protección de éste. El imparable uso de las TIC en las propias personas significa que están cada día más expuestas a

[21] "Art. 35.1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares" RGPD.

[22] "Art. 35.3. a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o c) observación sistemática a gran escala de una zona de acceso público", RGPD.

[23] Art. 35.4 RGPD.

[24] Art. 35.1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

sistemas que se alimentan de datos para su funcionamiento. Concluimos que, gracias al marco normativo existente, encabezado por el RGPD y el reciente RIA, existe mayor preocupación por la captación de información mediante sistemas biométricos. Por lo tanto, su uso debe ser respetuoso con este derecho fundamental y sólo pueden controlarse por interesados legítimos (personas, empresas, autoridades o Estados) con consentimiento del titular o dueño de ellos, respetando los márgenes legales y principios del RGPD.

En este trabajo se ha profundizado sobre el uso de IA, los datos biométricos y los problemas en torno a los sesgos, además de la consecuente discriminación de ciertas personas. Por lo expuesto, se concluye que el uso de la biometría está cada vez más extendido por su precisión y alto grado de certeza en el reconocimiento de un individuo, que es único e irrepetible. Ahora bien, su implementación y uso debe ser con fines estrictamente permitidos y siempre vigilando que sean captados los datos estrictamente necesarios. Propuestas como la obligación de implementar una EIPD son fundamentales.

Se evidencia que el incumplimiento del deber de custodia no puede eximir de responsabilidad, más aún, si se debe al actuar negligente del autor, su exceso de confianza en el sistema automatizado o descuidos frente al mal funcionamiento de un sistema de IA. Como recomendación, se deben considerar unas oportunas medidas de prevención y ciberseguridad, pues se tornan fundamentales para respetar los derechos humanos, incluyendo aquellos de cuarta generación que están vigentes en nuestra sociedad digital.

Como recomendación final, y a nivel personal, quien voluntariamente cede sus datos biométricos, debe tomar ciertas precauciones, las cuales giran en torno a cuidados a la hora de instalar aplicaciones que solicitan acceso a esos datos personales. Se debe evitar compartirlos innecesariamente, rechazar peticiones de acceso a ellos si no son necesarias, mantener las aplicaciones de sistemas inteligentes actualizadas. Asimismo, es fundamental implementar soluciones de ciberseguridad y antivirus capaces de detectar accesos no autorizados, o que puedan ser un peligro para la intimidad personal.

IX. REFERENCIAS BIBLIOGRÁFICAS

Andreu Martínez, María. "Lección 8. Intimidad, confidencialidad y documentación clínica". En Romeo Casabona, C. (dir.). *Manual de Bioderecho*. Madrid: Dykinson, 2022.

Beck, Ulrich. *La Sociedad del riesgo: hacia una nueva modernidad.* Barcelona: Paidos, 1992.

Beduschi, Ana. "Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights". *Big Data & Society,* vol. 6, núm. 2 (2019). DOI: https://doi.org/10.1177/2053951719855091

Casado, María. "Reflexiones bioético-jurídicas sobre el uso de muestras, perfiles, datos y bancos de ADN". En Casado, M. / Guillén, M. (dirs.), *ADN forense: pro-*

blemas éticos y jurídicos. Barcelona: Publicacions i Edicions de la Universidad de Barcelona, 2014.

Cuadrado Gamarra, Nuria. "Desafíos ético-jurídicos en el uso de Inteligencia Artificial para el tratamiento masivo de datos biométricos". *Revista Deusto de Derechos Humanos*. Bilbao: Universidad de Deusto, diciembre (2024). DOI: https://doi.org/10.18543/djhr.3199.

Fariñas Matoni, Luigi. *El Derecho a la Intimidad*. Madrid: Trivium, 1983.

García Antón, Elena. "Inteligencia Artificial y protección de datos: análisis jurídico del reconocimiento biométrico en el acceso a los estadios de fútbol". *Revista de Derecho*, Thomson Reuters – Aranzadi, Cizur Menor (Navarra), 2025.

Garriga Domínguez, Ana. "Los derechos ante los sistemas biométricos que incorporan inteligencia artificial". *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 51 (2024), época II. DOI: https://doi.org/10.20318/dyl.2024.8585

González Mendoza, Diana. "Los datos biométricos y las tecnologías que los utilizan para su funcionamiento". *Revista Vasca de Administración Pública*, (132), 427-464 (2025). DOI: https://doi.org/10.47623/ivap-rvap.132.2025.12.

Jung, Young y Virgil, Ethan. "Analysis of Legislative Framework Governing Biometric Data". *Procedia Computer Science,* vol. 241 (2024). DOI: https://doi.org/10.1016/j.procs.2024.08.009.

Lessig, Lawrence. *El Código 2.0 (trad. del libro "El Código y Otras Leyes del Ciberespacio" de 2001)*. Málaga: *Traficantes de Sueño*, Universidad de Málaga, 2009.

Li, He, Yu, Lu & He, Wu. "El impacto del RGPD en el desarrollo tecnológico global". *Journal of Global Information Technology Management*, 22 (1), 1–6 (2019). DOI: https://doi.org/10.1080/1097198X.2019.1569186.

Miranda Gonçalves, Rubén. "La protección de la dignidad de la persona humana en el contexto de la pandemia del Covid-19". *Revista Justiça do Direito*, vol. 34, núm. 2, mai-ago (2020). DOI: https://doi.org/10.5335/rjd.v34i2.11013

Miró Llinares, Fernando. "El modelo policial que viene: Mitos y realidades del impacto de la inteligencia artificial y la ciencia de datos en la prevención policial del crimen", *Libro blanco de la prevención y seguridad local valenciana.* Valencia: Instituto Valenciano de Seguridad Pública y Emergencias, 2019.

Natgunanathan, I., Mehmood, A., Xiang, Y., Beliakov, G. y Yearwood, J. "Protección de la privacidad en datos biométricos". *IEEE Access*, vol. 4 (2016), pp. 880-892. DOI: https://doi.org/10.1109/ACCESS.2016.2535120.

Pérez Luño, Enrique. "Las generaciones de derechos humanos*". Revista del Centro de Estudios Constitucionales,* núm. 10, septiembre-diciembre (1991).

Ortiz Pradillo, Juan Carlos. "Capítulo V. Inteligencia Artificial, *Big Data*, Tecnovigilancia y Derechos Fundamentales en el proceso penal". En Villegas Delgado, César / Martín Ríos, Pilar (dirs.), *El Derecho en la Encrucijada Tecnológica*. Valencia: Tirant lo Blanch, 2022.

Pizzolo, Calógero. "¿Cuándo el fin justifica los medios? Inteligencia Artificial (IA) y datos biométricos en pasaportes y documentos de identidad". *Revista Integración Regional & Derechos Humanos*, vol. 12, núm. 2 (2024), Universidad de Buenos Aires.

Recuero Linares, Mikel. "Transferencias internacionales de datos genéticos y datos de salud con fines de investigación". *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada* (2019).

Valerio Jiminián, Miguel. *Registros de ADN y prevención del delito.* Barcelona: Atelier, 2019.

Verdugo Guzmán, Silvia. "Reflexiones sobre la expansión de la bio-delincuencia y el almacenamiento del perfil genético para investigaciones criminales". *Ius et Scientia*, 7 (2), 96-116 (2021). Disponible en: https://institucional.us.es/revistas/Ius_Et_Scientia/vol7_2/Art_07.pdf

Verdugo Guzmán, Silvia. *Ciberespacio, Metaverso y nuevos delitos que gravitan sobre los derechos humanos.* Valencia: Tirant lo Blanch, 2023.

Yang, Wencheng, Wang, Song, Hu, Jiankun, Zheng, Guanglou, & Valli, Craig. "Security and Accuracy of Fingerprint-Based Biometrics: A Review". *Symmetry,* 11(2):141 (2019). DOI: https://doi.org/10.3390/sym11020141.

Normas citadas

Constitución Española de 1978.

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, BOE núm. 126, de 27 de mayo de 2021.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE núm. 294, de 6 de diciembre de 2018.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE núm. 298, de 14 de diciembre de 1999.

Pacto Internacional de Derechos Civiles y Políticos, Asamblea General de las Naciones Unidas, Nueva York, 16.XII.1996.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Diario Oficial de la Unión Europea, L 119/1, 4 de mayo de 2016.

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), DOUE núm. 1689, 12 de julio de 2024.

Documentos

Agencia Española de Protección de Datos, *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción* (febrero 2020). Disponible en: https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf.

Agencia Española de Protección de Datos, "Metaverso y Privacidad", 29.IX.2022. Accesible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/metaverso-y-privacidad.