LOS DERECHOS ANTE LOS SISTEMAS BIOMÉTRICOS QUE INCORPORAN INTELIGENCIA ARTIFICIAL*

RIGHTS IN THE FACE OF BIOMETRIC SYSTEMS INCORPORATING ARTIFICIAL INTELLIGENCE

Ana Garriga Domínguez
Universidad de Vigo
https://orcid.org/0000-0003-2846-3448

Fecha de recepción: 29-1-24
Fecha de aceptación: 19-2-24

Resumen: *Partiendo de un enfoque desde los riesgos que el tratamiento de los datos biométricos y los sistemas de IA biométricos implican para los derechos humanos, se analiza su protección en la legislación sobre protección de datos personales y en la Propuesta de Reglamento sobre Inteligencia Artificial de la Unión Europea.*

Abstract: *Starting from an approach based on the risks that the processing of biometric data and biometric AI systems imply for human rights, the protection of human rights is analysed in the legislation on the protection of personal data and in the Proposal for a Regulation on Artificial Intelligence of the European Union.*

Palabras clave: identidad y dignidad humana, derechos humanos, democracia, inteligencia artificial, sistemas biométricos.
Keywords: identity and human dignity, human rights, democracy, artificial intelligence, biometric systems.

* Este trabajo ha sido realizado en el marco del Proyecto de Investigación de la Agencia Estatal de Investigación sobre "La conciliación del derecho a la protección de datos con el cumplimiento por los poderes públicos del deber de transparencia y de lucha contra la corrupción (PID2021-128309NB-I00).

1. INTRODUCCIÓN: INTELIGENCIA ARTIFICIAL Y DERECHOS FUNDAMENTALES

La complejidad de las diferentes tecnologías y sistemas, que pertenecen al ámbito de la Inteligencia Artificial (IA), plantean riesgos importantes para los derechos fundamentales y los valores democráticos durante todo el ciclo de vida del sistema, es decir, desde el momento de su diseño y desarrollo hasta el de su despliegue y uso. Ello requiere que desde el mismo instante de su concepción se asuma la necesidad de incorporar requisitos que garanticen el respeto a esos valores y derechos, tanto en su planificación, diseño y confección, como en la fase posterior de despliegue. Como ha señalado Rafael de Asís, los derechos humanos "constituyen el marco ético, jurídico y político de referencia para las sociedades contemporáneas y, en este sentido, son los referentes a tener en cuenta la hora de estudiar los criterios que deben regular y guiar el desarrollo tecnológico"[1]. En el ámbito de la protección de datos personales, esta filosofía se incorpora a través de principio de privacidad desde el diseño[2] recogido en el artículo 25 del Reglamento general de protección de datos[3] (RGPD) y deberá incorporarse cuando los sistemas de IA utilicen en alguna de sus fases de creación, entrenamiento o uso, datos de carácter personal[4].

---

[1] R. DE ASÍS ROIG, *Una mirada a la robótica desde los derechos humanos*, Dykinson, Madrid, 2014, pp. 54-55. Igualmente. S. ÁLVAREZ GONZÁLEZ, "La necesaria protección de los derechos fundamentales como punto de partida en las propuestas de regulación de la inteligencia artificial, en T. DAMO CERVI (dir.), *Interfaces dos direitos humanos no Século XXI*, Metrics, Santo Ângelo Brasil, 2022.

[2] Vid. A. CAVOUKIAN, *Privacy by Design. The 7 Foundational Principles Implementation and Mapping of Fair Information Practices, Information and Privacy Commissioner of Ontario*, Canadá, 2010.

Asimismo, J. MEGÍAS TEROL, "Privacy by desing, construcción de redes sociales garantes de la privacidad", en A. RALLO LOMBARTE y R. MARTÍNEZ MARTÍNEZ, (coord.), *Derecho y redes sociales,* Civitas, Madrid, 2010.

[3] 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 libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

[4] Su implementación se explica pormenorizadamente en varios documentos elaborados por la Agencia Española de Protección de Datos (AEPD). Entre otros: de Privacidad desde el Diseño (*https://www.aepd.es/documento/guia-privacidad-desde-diseno.pdf*), Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción (*https://www.aepd.es/documento/adecuacion-rgpd-ia.pdf*) y Requisitos para Auditorías de Tratamientos que incluyan IA (*https://www.aepd.es/sites/default/files/2021-01/requisitos-auditorias-tratamientos-incluyan-ia.pdf).*

No existe una única definición de IA por lo que recojo dos complementarias[5]. Una más amplia, recogida en la Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO de noviembre de 2021, según la cual, *"los sistemas de IA son tecnologías de procesamiento de la información que integran modelos y algoritmos que producen una capacidad para aprender y realizar tareas cognitivas, dando lugar a resultados como la* predicción y la adopción de decisiones en entornos materiales y virtuales". Otra más precisa, la del artículo 3 del Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial de la Unión (RIA) y se modifican determinados actos legislativos de la Unión, que define un sistema de inteligencia artificial o sistema de IA como aquel sistema "basado en máquinas diseñado para funcionar con diversos niveles de autonomía y que puede mostrara capacidad de adaptación tras su despliegue y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales" (artículo 3)[6].

Hoy tenemos identificados los principales problemas que, con carácter general, la IA plantea para los derechos; asimismo los de sistemas o tecnologías determinadas, como las biométricas, que por su alta sensibilidad implican un elevado riesgo para los éstos. Los diversos riesgos se encuentran sistematizados en la Recomendación sobre la ética de la inteligencia artificial de la UNESCO como los riesgos de discriminación, que puede derivarse del denominado sesgo algorítmico[7]. Especialmente preocupantes para el derecho a la igualdad son los sistemas de IA que proporcionan calificaciones sociales de

[5] Sobre la distinción entre de la IA general y fuerte o IA débil y las diferentes posiciones críticas vid. S. CHURNIN, *Inteligencia artificial: retos éticos y jurídicos, y la influencia de los derechos humanos*, Servicio de Publicaciones de la Facultad de Derecho de la Universidad Complutense, Madrid, 2012.

[6] Esta última está más alineada con la definición de IA propuesta por la OCEDE en 2022. "OECD Framework for the Classification of AI systems", *OECD Digital Economy Papers*, núm. 323, OECD Publishing, Paris. Puede consultarse en: *https://doi.org/10.1787/cb6d9eca-en*.

[7] El sesgo es un reflejo del conjunto de datos que los desarrolladores de los algoritmos deciden utilizar, así como de sus métodos de combinación de esos datos, sus prácticas de elaboración de modelos y de la forma en que se aplican e interpretan los resultados. C. O'NEIL, *Armas de destrucción matemática. Cómo el Big Data aumenta la desigualdad y amenaza la democracia*, Capitán Swing, Madrid, 2017.

Pueden proceder, por lo tanto, de los datos de entrenamiento, pero también derivarse de la elección del algoritmo utilizado, por la forma en la que se determinan y ajustan determinados parámetros (sesgo algorítmico propiamente dicho) y, tiene como consecuencia que los resultados que ofrece el sistema de IA sean sesgados, reforzando determinados prejuicios

personas y cuya aplicación en el ámbito privado o por autoridades públicas pueden resultar discriminatorias e, incluso, abocar a la exclusión a determinados grupos; riesgos para la autonomía y la toma de decisiones libres[8]; riesgos en el ámbito del empleo y del mercado laboral que vendrá derivada de la automatización de numerosos puestos de trabajo; para los sistemas democráticos y el Estado de Derecho, la seguridad y el orden público; para la diversidad cultural y riesgos medioambientales y riesgos para otros derechos fundamentales[9].

Otro problema que plantean los sistemas de IA es el derivado de los fallos o errores del sistema. 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. Finalmente, la complejidad y opacidad de los sistemas dificultan su comprensión por la sociedad, pero también su validación independiente para auditar su seguridad.

Una única "aplicación de Inteligencia Artificial puede impactar en una gran cantidad de derechos"[10] y los sistemas de IA biométricos pueden verse afectados por cada uno de los problemas descritos, planteando dificultades específicas para el derecho a la privacidad y el derecho a la protección de datos personales. Estos sistemas pueden estar sesgados y ser discriminatorios, pue-

---

o estereotipos. Vid. G. L. NELSON, "Bias in Artificial Intelligence", *North Carolina Medical Journal*, vol. 80, núm. 4, 2019, p. 221 y 222.

[8] Se señala en la Recomendación que, a largo plazo, los sistemas de IA "podrían disputar al ser humano el sentido especial de la experiencia y la capacidad de actuar que le son propios, lo que plantearía nuevas inquietudes sobre la autocomprensión, la interacción social, cultural y ambiental, la autonomía, la capacidad de actuar, el valor y la dignidad del ser humano, entre otras". Pero, de manera más inminente la IA podría limitar la capacidad para tomar decisiones autónomas en el ámbito de la salud, la educación, el acceso a los servicios y prestaciones sociales o en el ámbito sancionador, por ejemplo.

[9] En el RIA se recogen los siguientes: el derecho a la dignidad humana, el respeto de la vida privada y familiar y la protección de datos de carácter personal, la no discriminación y la igualdad entre hombres y mujeres, la libertad de expresión y de reunión, a la tutela judicial efectiva y a un juez imparcial, la presunción de inocencia y los derechos de la defensa.

En su Informe "El derecho a la privacidad en la era digital", de octubre de 2021, la Alta Comisionada de las Naciones Unidas para los Derechos Humanos identifica las principales repercusiones de la inteligencia artificial en el derecho a la privacidad y otros derechos humanos, señalando como "el funcionamiento de los sistemas de IA puede facilitar y agravar de diversas maneras las intrusiones en la privacidad y las injerencias en otros derechos", como el de reunión pacífica, el de manifestación o la libertad de expresión.

[10] R. DE ASÍS ROIG, *Derechos y tecnologías*, Dykinson, Madrid, 2022, p. 102.

den agravar las vulnerabilidades de las personas afectadas o producir errores con consecuencias importantes en los derechos. Por otra parte, su uso en determinados ámbitos como la seguridad o la investigación policial presenta riesgos específicos particularmente cuando sirven para la adopción de decisiones automatizadas, ya que si la respuesta que facilita el algoritmo genera decisiones injustas, en muchos casos significará la discriminación o estigmatización de ciertos grupos de personas o colectivos"[11]. En el epígrafe siguiente analizaré determinadas características de los datos biométricos y los riesgos inherentes al uso de sistemas biométricos que incorporen IA con especial referencia a los sistemas de reconocimiento facial. Se ha optado por un enfoque desde el riesgo porque, no solo viene determinado por la normativa europea y española de protección de datos personales, sino que también es la perspectiva adoptada el RIA, así como en los principales textos que establecen criterios éticos en materia de IA[12]. En concreto, en las Directrices éticas para una IA fiable [13], se advierte que, *pese a que aportan beneficios sustanciales a las personas y a la sociedad, los sistemas de IA también entrañan determinados riesgos y pueden tener efectos negativos, algunos de los cuales pueden resultar difíciles de prever, identificar o medir (por ejemplo, sobre la democracia, el estado de Derecho y la justicia distributiva, o sobre la propia mente humana)*, por ello se deberán adoptar las medidas adecuadas para mitigarlos, que deberán ser proporcionales a la magnitud de los mismos.

2. TECNOLOGÍAS BIOMÉTRICAS Y TRATAMIENTO DE DATOS BIOMÉTRICOS: RIESGOS ESPECÍFICOS DERIVADOS DE SU PARTICULAR NATURALEZA

Los sistemas de IA que se utilizan con fines de reconocimiento facial utilizan una categoría especial de datos personales: los datos biométricos. Su

[11] N. BELLOSO MARTÍN, "La problemática de los sesgos algorítmicos (con especial referencia a los de género). ¿Hacia un derecho a la protección contra los sesgos?", en F. I. LLANO ALONSO, *Inteligencia artificial y Filosofía del derecho*, Laborum, 2022, p. 49. En el mismo sentido M. J. AÑÓN ROIG, "Desigualdades algorítmicas. Conductas de alto riesgo para los derechos humanos", *Derechos y Libertades,* núm. 47, 2022.

[12] Así se indica en las Directrices éticas para una IA fiable y en la Recomendación sobre la Ética de la Inteligencia Artificial de la Unesco. Igualmente, en la Declaración Europea sobre los Derechos y Principios Digitales, del Parlamento Europeo, el Consejo y la Comisión, de 26 de enero de 2022.

[13] Comisión Europea, Directrices éticas para una IA fiable, Oficina de Publicaciones, 2019, *https://data.europa.eu/doi/10.2759/14078*.

concepto se encuentra definido en el RGPD, como aquellos *datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*. El artículo 9 del RGPD los considera una categoría especialmente protegida, cuando estén dirigidos a identificar de manera unívoca a una persona física[14]. La definición legal de dato biométrico incluye, tanto propiedades físicas o fisiológicas (huellas digitales, voz, forma de las orejas o el rostro[15], parámetros de la retina o del iris, etc.), como psicológicas o comportamentales (como tics, análisis de pulsaciones de teclas, la firma manuscrita o la forma de caminar, entre otros) siempre que permitan la identificación unívoca de una persona. Los criterios que se habrán de valorar para situar un dato personal entre los biométricos son tres: su naturaleza, esto es, las características físicas, fisiológicas o conductuales de un individuo; los medios y las formas de tratamiento, han de obtenerse a partir de un tratamiento técnico específico; y la finalidad del tratamiento: la identificación unívoca de una persona física[16].

La preocupación por la recopilación y usos de los datos biométricos no es reciente. El *WP29* señalaba que uno de los rasgos esenciales de los datos

[14] Esta definición es idéntica a la que se recoge en 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 en el RIA. En el Considerando 7 del RIA se indica que "a noción de datos biométricos utilizada en el presente Reglamento debe interpretarse a la luz de la noción de datos biométricos definida en el artículo 4, apartado 14 del del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo; en el artículo 3, punto 18, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo; y en el artículo 3, punto 13, de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo". No obstante, existe alguna diferencia en estas normas. Así, en el Reglamento (UE) 2018/1862 sobre la información de Schengen (SIS) 6, se añade a la definición la mención explícita de "fotografías", además de imágenes faciales y de perfiles de ADN. En el Reglamento (UE) 2019/8178 se incluyen los datos dactiloscópicos o las imágenes faciales y se definen las imágenes faciales como las imágenes digitales del rostro de una persona.

[15] En el Considerando 51 del RGPD, se indica que el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de datos sensibles y sólo se incluyen en la definición de datos biométricos cuando se tratan a través de un medio técnico específico que permite la identificación o autenticación únicas de una persona física.

[16] Comité Europeo de Protección de Datos (CEPD), Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo, adoptadas el 29 de enero de 2020, p. 19-20.

biométricos es que "cambian irrevocablemente la relación entre el cuerpo y la identidad, ya que hacen que las características del cuerpo humano sean legibles mediante máquinas y estén sujetas a un uso posterior"[17]. Esta propiedad hace que los sistemas biométricos sean capaces de identificar unívocamente a una persona utilizando determinadas cualidades fisiológicas o comportamentales únicas. Al ser únicos para cada persona, son mucho más fiables que otros tipos de datos personales, pero al mismo tiempo, su utilización inadecuada supondrá mayores peligros para los derechos. Ello es así por su conexión directa con los valores de autonomía y dignidad humanas, directamente ligadas a la idea de identidad y autodeterminación personal[18]. Señala Rafael de Asís que la identificación biométrica emplea las dos dimensiones de la identidad, la condición y la situación, puesto que "se analizan características físicas, pero también características de comportamiento"[19]. No es esta la única propiedad de los datos biométricos que los hace enormemente sensibles y, como ocurre con otras categorías especialmente protegidas[20], son datos susceptibles de aportar mucha más información sobre los interesados que la de aquellos parámetros que servirían simplemente para identificarlas.

---

[17] Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, del 27 de abril de 2012, p. 4.

[18] Resulta pertinente recordar, que la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) ha venido reconociendo de forma reiterada, una noción de vida privada amplia, que incluye el derecho a la identidad y al desarrollo o realización personal, con independencia de que se presente en forma de desarrollo de la personalidad o en términos de autonomía individual (STEDH de 20 diciembre 2005, Wisse c. Francia). Pues, en la medida en que la dignidad humana y la libertad son la esencia misma del Convenio, en el artículo 8 en particular, el concepto de autonomía personal refleja un principio importante que subyace a la interpretación de las garantías de dicha disposición, por lo que se protege la esfera personal de cada individuo, incluido el derecho a establecer los detalles de su identidad como ser humano (entre otras, SSTEDH de 11 de julio de 2002, Christine Goodwin c. Reino Unido; de 29 de abril de 2002, Pretty c. Reino Unido o de 15 de abril de 2009, Reklos and Davourlis c. Grecia). En concreto y en relación con los datos biométricos, debemos tener presente que, de acuerdo esta doctrina, la imagen de una persona, obtenida por ejemplo a través de una fotografía, constituye "un atributo esencial de la personalidad" y, por lo tanto, no puede quedar "en manos de terceros sin que el interesado tuviera control alguno sobre su posible uso posterior" (STEDH 15 de abril de 2009, Reklos and Davourlis c. Grecia).

[19] R. DE ASÍS ROIG, "Ética, tecnología y Derecho", en F. I. LLANO ALONSO, *Inteligencia artificial y Filosofía del derecho*, cit., p. 27.

[20] Los datos genéticos, como los biométricos, tienen un carácter dual ya que, al corresponder exclusivamente a una única persona, permiten la identificación inequívoca de esa persona, pero al mismo tiempo posibilitan la obtención de "información sobre el cuerpo humano". Vid. WP29: Dictamen 4/2007 sobre el concepto de datos personales, del 20 de junio, p. 9.

Mucha de esta información secundaria tendrá igualmente carácter sensible: sobre el origen étnico, la salud, el consumo de drogas o, incluso, sobre el estado emocional de las personas en un momento determinado y, solos o combinados con otros, sirven para la elaboración de perfiles[21]. Otra peculiaridad, que les hace altamente sensibles, es que se trata de rasgos que, en su mayoría, son inmodificables por su poseedor.

La biometría incluye el conjunto de "tecnologías que permiten la captura o registro de algún rasgo del cuerpo humano, la conversión en información digital de ese registro y su almacenamiento en grandes bancos de datos que podrán estar disponibles para autentificación, identificación y verificación por parte de Estados o empresas"[22]. La biometría abarcaría todos los procesos automatizados que se utilizan para identificar a un individuo mediante patrones físicos, fisiológicos o comportamentales y, estas características, se definen como datos biométricos, ya que permiten o confirman la identificación única de una persona[23]. Estas tecnologías han ido evolucionando desde la biometría fisiológica o de primera generación, que "registra características físicas que permiten individualizar al sujeto como las huellas digitales, la estructura venosa, geometría o impresión de la palma de la mano, el reconocimiento facial, de iris o de retina, o el ADN, entre otros"[24] para establecer la identidad de una persona permitiendo su verificación y autenticación, hasta la biometría con-

[21] En el caso de las huellas dactilares, que depositan un patrón característico de las crestas presentes en la punta del dedo y están hechas de las sustancias que se han tocado y de las que el propio cuerpo excreta, permiten detectar el consumo de cocaína, heroína y morfina a partir de una única huella dactilar, así como los medicamentos que haya tomado el sujeto. (M. BAILEY y otros, "Rapid detection of cocaine, benzoylecgonine and methylecgonine in fingerprints using surface mass spectrometry", *Royal Society of Chemistry*, vol. 140, 2015, p. 6254-6259.

En un futuro, podrían ofrecer una firma molecular que podría revelar aspectos del estilo de vida y entorno de una persona, tipo de trabajo que desempeña, problemas médicos e incluso ámbitos alimenticios (en M. BAILEY,"A fingerprint could give a molecular signature revealing aspects of a person's lifestyle and environment, such as their job, eating habits or medical problems", *The Conversation US*, 27 de abril de 2018).

[22] E. SCHINDEL, "Biométrica, normalización de los cuerpos y control de fronteras en la Unión Europea", *Athenea Digital. Revista de Pensamiento e Investigación Social*, vol. 18, núm. 1, 2018, pp. 11-31.

[23] En CEPD: Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, del 12 de mayo de 2022, p. 7.

[24] Ibidem, p. 15.

ductual. Esta biometría de segunda generación o de medición de la conducta[25] (*behaviometrics*) analiza características relacionadas con el patrón de comportamiento con el objetivo de "predecir conductas sospechosas o intenciones hostiles, sobre todo en el marco de una mayor securitización (y) uno de sus objetivos es establecer perfiles de personas con base en la predicción de sus acciones y conductas mediante cámaras capaces de "reconocer" esos rasgos"[26]. De esta forma, la definición de biometría se ha ampliado para incluir características invisibles de una persona, como el comportamiento y las emociones, la dinámica facial, los estados psicológicos, los niveles de excitación (miedo, ansiedad, intención) y las células, fluidos o rastros corporales (como el ADN o las imágenes cerebrales en medicina forense), con el análisis de los gestos anticipatorios, la paralingüística y las imágenes térmicas[27].

Los sistemas biométricos también pueden ser usados para realizar procesos de categorización o segmentación con la finalidad de establecer si un individuo pertenece a un grupo con unas características específicas (raza, sexo, edad, etc.) con el fin de adoptar alguna medida determinada[28]. Muchos de los nuevos sistemas biométricos permitirán la categorización o identificación de individuos y la recogida a distancia de sus rasgos y se utilizarán "para la elaboración de perfiles, la vigilancia a distancia o incluso tareas más complejas como los entornos inteligentes"[29].

El objetivo principal de la biometría ha sido la búsqueda de sistemas que permitan la identificación de individuos y, si bien este es el campo de investigación mayoritario, se han ido mejorando los sistemas biométricos predictivos[30], que incluiría la inferencia de los estados de ánimo o psicoló-

---

[25] Según la clasificación de J. LODGE, y M. SNIJDER, *Developing Biometrics in the EU, Parlamento Europeo*, 2010, p. 9.

[26] E. SCHINDEL, "Biométrica, normalización de los cuerpos y control de fronteras en la Unión Europea", cit., p. 15.

[27] J. LODGE, y M. SNIJDER, *Developing Biometrics in the EU*, cit., p. 18.

[28] Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, cit., p. 6.

[29] Ibidem, p. 17.

[30] Además de determinar la edad, la raza o el sexo, permiten la predicción de del estado emocional o mental de un sujeto (si está feliz o triste, estresado o relajado). Varios estudios han demostrado las capacidades de los algoritmos de predecir la edad y el sexo del sujeto a partir de la voz, el rostro o la marcha, otros a través del iris identifican edad y etnia, pero actualmente muchas investigaciones se centran en las denominadas predicciones de nivel superior, que suelen referirse a condiciones que pueden describirse de forma genérica como estados mentales o emocionales. Por ejemplo, puede inferir el estado emocional del trazo de un dibujo o de la escritura, del uso del teclado o el ratón, de la forma de caminar, de la voz y, por

gicos. Determinados sistemas biométricos emplearán estos rasgos, que solos o combinados con otros sistemas, constituirían sistemas multimodales[31]. En consecuencia, los sistemas de verificación de la identidad que utilizan datos biométricos son más intrusivos que los sistemas tradicionales, ya que además de permitir la autenticación de una persona pueden aportar información sobre "su estado emocional, enfermedades, discapacidades y características genéticas, consumos de sustancias[32] o "que indiquen pensamiento inconsciente como mentir" [33]. Además, al estar implícita, el usuario no podrá impedir que se obtenga esta información suplementaria"[34]. La propia naturaleza de estos datos personales coloca a la persona en una situación particularmente vulnerable, en particular cuando se utilizan para el seguimiento, rastreo o elaboración de perfiles y, por ello, su potencial impacto la vida privada y el derecho a la protección de datos es tan elevado. Existen tecnologías de reconocimiento facial que analizan las expresiones faciales a partir de imágenes estáticas y vídeos para obtener información sobre estados emocionales y que pueden ser combinadas con otras tecnologías biométricas que incorporan IA[35]. El grado de fiabilidad de estas tecnologías ha sido cuestionado[36], sin embargo, se están utilizando en diversos ámbitos. En el informe del SEPD *Facial Emotion Recognition*[37] se recogen varias aplicaciones: para el análisis del comportamiento de los usuarios y publicidad, en el ámbito de la salud, para la prestación de servicios personalizados (mensajería, elecciones musicales, etc.), en el ámbito de los seguros para detectar el fraude, en el ámbito educativo, en el control de las fronteras[38] y en la lucha contra

supuesto, del análisis del rostro. En M. FAIRHURST, L. CHENG y M. DA COSTA-ABREU, "Predictive biometrics: a review and analysis of predicting personal characteristics from biometric data", *IET Biometrics*, vol. 6, 2017, pp. 369-378. Asimismo en AA.VV., "Emotion recognition based on pressure sensor keyboards", *IEEE Int. Conf. on Multimedia and Expo*, June 2008, pp. 1089–1092.

31 WP29, Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, cit., p. 17.

32 AEPD, 14 equívocos con relación a la identificación y autenticación biométrica, junio de 2020, p. 1.

33 WP29, Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, cit., p. 4.

34 AEPD, 14 equívocos con relación a la identificación y autenticación biométrica, cit., p. 1.

35 Vid. Supervisor Europeo de Protección de Datos (SEPD), *TechDispatch #1/2021 - Facial Emotion Recognition*, de 26 mayo de 2021.

36 HEAVEN, Douglas: "Why faces don't always tell the truth about feelings", *Nature*, vol. 578, núm. 7796, 2020.

37 SEPD: *TechDispatch #1/2021 - Facial Emotion Recognition,* cit., p. 2.

38 En el año 2019, varios países (Grecia, Hungría y Letonia) comenzaron a probar el sistema iBorder Crtl System, que analizando el tono de voz, las expresiones faciales y otros

el terrorismo o para detección de actitudes políticas. Estos sistemas, como ha señalado el Supervisor Europeo plantean problemas específicos para los derechos de las personas y, al tratarse de tecnologías cuyo objetivo principal no es la identificación, serán mayores los riesgos relacionados con su grado de precisión en la interpretación de las emociones para adoptar decisiones sobre las personas.

Otros riesgos concretos identificados por las autoridades de control son los derivados de la recogida encubierta y no transparente de los datos con la consiguiente falta de control sobre sus datos e invasión de su intimidad. Igualmente la posibilidad de que los datos se utilicen de forma distinta a la inicialmente prevista o los riesgos derivados de su usos para la adopción de decisiones automatizadas o para predecir el comportamiento o para determinar las preferencias individuales en una situación concreta y, en la medida en que algunos datos biométricos pueden revelar información física, podrían "utilizarse para la selección de objetivos y la elaboración de perfiles, pero también puede dar lugar a discriminación, estigmatización y confrontación no deseada con información inesperada o no querida"[39]. Además, como ocurre con otros atributos, físicos o fisiológicos humanos, son inmodificables por sus poseedor por lo que la pérdida de control sobre estas categorías de datos personales son irreversibles[40]. Finalmente otros daños se derivarán de la identificación o verificación de identidad incorrecta que, en algunos casos como los sistemas basados en huellas dactilares los errores pueden aumentar por el envejecimiento del individuo[41] y de la posible la suplantación de identidad a través de sistemas de reproducciones de huellas o el uso de máscaras y las propiciadas por brechas de seguridad[42].

---

datos detecta si un viajero miente. Vid. "Esta inteligencia artificial detecta si mientes al pasar una frontera", *El Español*, el 2-11-2018.

[39] CEPD: Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, cit., p. 19.

[40] A diferencia, por ejemplo en un sistema de autenticación o de verificación de la identidad, en el caso de que se pierda el control de una contraseña por una brecha de seguridad, es posible modificarla o cambiarla por otra de forma sencilla; sin embargo, en caso de que se pierda el control de un dato biométrico, va a tener consecuencias necesariamente más graves para el interesado.

[41] AEPD: 14 equívocos con relación a la identificación y autenticación biométrica, cit., p. 2.

[42] Así ocurrió en 2019 cuando un problema de seguridad en el software de identificación biométrica BioStar 2, expuso 27,8 millones de registros con los datos de más de un millón de personas, entre los que se encontraban huellas dactilares y datos de reconocimiento facial ("Un fallo de seguridad expone 27,8 millones de registros de datos biométricos", en Europa

En el caso particular de los sistemas de reconocimiento facial, el aumento de su uso, podría poner fin al anonimato en los espacios públicos y haría posible el seguimiento continuo de las personas. Estos riesgos han llevado al SPED y al CEPD a reclamar "la prohibición general del uso de la IA para el reconocimiento automatizado de rasgos humanos en espacios de acceso público, como los rostros, pero también la marcha, las huellas dactilares, el ADN, la voz, las pulsaciones de teclas y otras señales biométricas o conductuales, en cualquier contexto"[43]. Por su potencial invasivo, el uso de las tecnologías de reconocimiento facial en tiempo real son ampliamente rechazas por la población europea y de terceros estados según un estudio de la FRA[44]. En su informe sobre reconocimiento facial[45] se destaca la implicación de la protección de los datos personales biométricos, en especial los que son objeto de tratamiento por los sistemas de reconocimiento facial en tiempo real, como condición esencial para el ejercicio de otros derechos fundamentales, como la libertad de pensamiento, conciencia y religión, la libertad de expresión e información y la libertad de reunión[46] y asociación, pues como ya se ha indicado, a través del derecho fundamental a la protección de datos personales se protege en último término la autonomía y la dignidad humana de los individuos, concediéndoles una esfera privada en la que pueden desarrollar libremente su personalidad, pensar y a formar sus propias opiniones[47].

Los riesgos para los derechos de las personas serían mayores en el caso de la aplicación de estas tecnologías a gran escala ya que la discriminación algorítmica o la identificación errónea puede crear un elevado número de personas afectadas en su conducta y en su vida cotidiana. De hecho, como ha indicado el CEPD en sus *Directrices sobre el uso de tecnologías de recono-*

Press, 14 de agosto de 2019 (*https://www.europapress.es/portaltic/ciberseguridad/noticia-fallo-seguridad-expone-278-millones-registros-datos-biometricos-20190814142303.html*).

[43] Dictamen conjunto 5/2021 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) del 18 de junio de 2021.

[44] Agencia Europea de Derechos Fundamentales (FRA, por sus siglas en inglés).

[45] Facial recognition technology: fundamental rights considerations in the context of law enforcement, del 21 de noviembre de 2019, p. 20 y ss.

[46] En el mismo sentido, el Informe sobre el "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas" del Alto Comisionado de las Naciones Unidas para los Derechos Humanos de 24 de junio de 2020.

[47] Ibídem, p. 26 y ss.

cimiento facial en el ámbito policial, su uso ya está produciendo importantes implicaciones para los individuos y los grupos de personas, entre ellos las minorías y podrán tener un gran impacto en nuestras formas de convivencia, así como en nuestra estabilidad política y democrática, en la que tienen un papel relevante el pluralismo y la oposición política[48]. Su nivel de eficiencia resulta relevante para determinar el grado de impacto en los derechos de las personas. Tanto las posibilidades de "engañar" a la tecnología[49], como la tasa de errores (ya sean falsos negativos o falsos positivos) puede suponer graves perjuicios[50]. En el caso de las tecnologías de reconocimiento facial, el impacto de la tasa de errores afecta mayoritariamente a determinados grupos de personas, las mujeres y las personas de color, lo que produce resultados sesgados que en última instancia pueden conducir a su discriminación[51] y, si los algoritmos funcionan según factores demográficos, el sesgo del reconocimiento facial podría amplificarse[52]. Asimismo, como ocurre con cualquier dato personal es susceptible de ser usado con más de una finalidad y en diferentes contextos, entre ellos la categorización de los interesados y, los daños posibles de los efectos para sus derechos derivados de esos usos secundarios, dependerán de su capacidad para ejercer un control real de sus datos personales y de la efectividad de las facultades que permitan ese control real y, por lo tanto, de garantía del derecho fundamental a la protección de datos personales[53].

---

[48] CEPD: Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, cit., p. 6.

[49] Vid. *Cuatro trucos para engañar a un sistema de reconocimiento facial*, en *https://elpais.com/retina/2019/10/22/innovacion/1571730281_157570.html*; *Una máscara para solucionar el problema de la privacidad*, en *https://www.tecnonews.info/noticias/una_mascara_para_solucionar_el_problema_de_la_privacidad*; *Huellas dactilares falsificadas con impresión 3D imposibles de detectar*, en *https://impresiontresde.com/huellas-dactilares-impresion-3d/*.

[50] Como se recoge en el Informe de la FRA, las tasas deben evaluarse teniendo en cuenta el número real de casos, ya que *"si se comprueba un gran número de personas en masa, una tasa de falsos positivos potencialmente baja significa que un número significativo de personas sigue siendo identificado incorrectamente. Por ejemplo, una tasa de identificación de falsos positivos del 0,01 significa que de 100.000 personas, 1.000 serán identificadas erróneamente"* En *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, pp. 9 y 10.

[51] Ibidem, p. 4.

[52] Vid. P. DROZDOWSKI y otros, "Demographic Bias in Biometrics: A Survey on an Emerging Challenge", *IEEE Transactions on Technology and Society*, vol. 1, núm. 2, 2020.

[53] CEPD: Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, cit., p. 9.

3. REQUISITOS PARA EL TRATAMIENTO DE LOS DATOS BIOMÉTRICOS EN LA LEGISLACIÓN SOBRE PROTECCIÓN DE DATOS PERSONALES

La utilización de los datos biométricos se encuentra regulada en la legislación sobre protección de datos personales. Este corpus normativo es de aplicación cuando los sistemas de IA impliquen el tratamiento de datos personales, con el fin de garantizar los derechos fundamentales a la intimidad y a la protección de los datos personales, a menudo inextricablemente ligados a la protección de otros derechos fundamentales, como el derecho a la dignidad o a un recurso judicial efectivo y a un juicio justo[54]. Su relevancia en el ámbito de los sistemas de IA que emplean datos personales en alguna fase de su ciclo de vida es indiscutible y su utilidad en la protección de los derechos fundamentales se hace evidente con la actuación de las autoridades de control[55] y su aplicación por los tribunales. Y si bien, en mi opinión, es insuficiente para enfrentar todos los problemas que presentas los sistemas biométricos que incorporan IA, "la protección de datos sigue siendo por defecto la regulación aplicable cuando estos sistemas traten datos personales"[56] y así se prevé en el RIA que recuerda su plena vigencia[57]. Por ello, de la forma más concisa posible, trataré

[54] SEPD, Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments, de 23 de octubre de 2023, p. 20.

[55] Prueba de ello son las numerosas resoluciones sancionadoras de las diferentes autoridades de control de los estados miembros de la UE por usos ilícitos de los datos biométricos. Una relación de ellas., puede consultarse a través de la web oficial del CEPD (*edpb.europa.ue*). Por ello, en su dictamen 44/2023, el SEPD aboga por que se designe como 5.6. Autoridades de protección de datos como autoridades nacionales de control en el RIA, puesto que, "además de tener experiencia en la evaluación de los riesgos para los derechos fundamentales que plantean las nuevas tecnologías como la IA (por ejemplo, la IA que utiliza datos biométricos) son también, debido a su total independencia, las autoridades que pueden proporcionar una supervisión independiente eficaz de los sistemas de IA que pueden afectar a los derechos y libertades fundamentales" (la traducción es mía). Ibidem.

[56] L. COTINO HUESO, "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial. Los altos estándares que exigen el Tribunal Constitucional alemán y otros tribunales, que no se cumplen ni de lejos en España", *Revista General de Derecho Administrativo*, núm. 63, 2023, p. 5.

[57] En el Considerando 24 se recuerda que *Todo tratamiento de datos biométricos y otros datos personales que conlleve el uso de sistemas de IA para la identificación biométrica, que no esté relacionado con el uso de sistemas de identificación biométrica a distancia "en tiempo real" en espacios de acceso público con fines policiales, tal como se regula en el presente Reglamento, debe seguir cumpliendo todos los requisitos derivados del artículo 10 de la Directiva (UE) 2016/680. Para fines distintos de la aplicación de la ley, el artículo 9, apartado 1, del Reglamento (UE) 2016/679 y el artículo 10, apartado 1, del Reglamento (UE) 2018/1725 prohíben el tratamiento de datos biométricos, salvo las excepciones limitadas previstas en dichos*

aquellos requisitos y garantías más relevantes en el contexto de los sistemas biométricos de IA, refiriéndome preferentemente a la regulación del RGPD, aunque realizando las aclaraciones precisas cuando sea procedente respecto de la LOPDGDD[58], de la Directiva (UE) 2016/680[59] y la 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, en sus respectivos ámbitos de aplicación.

De acuerdo con la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE), la licitud del tratamiento de los datos personales vendrá determinada por una doble exigencia: contar con una base de legitimación adecuada para ese tratamiento y respetar los principios relativos al tratamiento[60]. Ambos requisitos son necesarios para cualquier tratamiento de datos personales, pero al tratarse de una categoría especial, será necesario además que se cumplan las condiciones establecidas en el artículo 9 del RGPD y del 9 de la LOPDGDD. Solamente se podrán tratar datos sensibles, cuando el responsable del tratamiento pueda cumplir una de las condiciones establecidas en el apartado segundo del artículo 9 del RGPD y ese tratamiento se ampare en una de las bases jurídicas de legitimación previstas en el artículo 6 (artículo 8 de la Directiva, 11 de la Ley Orgánica 7/2021), pero además, se realice de acuerdo con los principios relativos al tratamiento del artículo 5 y respetando el principio de proporcionalidad[61].

---

artículos. En aplicación del artículo 9, apartado 1, del Reglamento (UE) 2016/679, el uso de la identificación biométrica a distancia para fines distintos de la aplicación de la ley ya ha sido objeto de decisiones de prohibición por parte de las autoridades nacionales de protección de datos.También, en el Considerando 23, se hace referencia a la vigencia de la legislación de protección de datos personales, si bien *las normas del presente Reglamento que prohíben, con algunas excepciones, ese uso, basadas en el artículo 16 del TFUE, deben aplicarse como lex specialis con respecto a las normas sobre el tratamiento de datos biométricos (…).*

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

[59] 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, en su caso, a las establecidas por los derechos nacionales.

[60] Entre otras, sentencias de 24 de noviembre de 2011y de 20 de octubre de 2022.

[61] En el ámbito de aplicación de la Directiva 2016/680, estos requisitos se encuentran recogidos en los artículos 6 (Principios relativos al tratamiento de datos personales), 11 (Licitud del tratamiento) y 13 (Tratamiento de categorías especiales de datos personales) de la Ley Orgánica 7/2021.

3.1. La aplicación de los principios relativos al tratamiento de los datos biométricos

El artículo 5 del RGPD regula los principios básicos que deberán respetarse en la recogida, tratamiento, uso y almacenamiento de los datos personales. De su aplicación al tratamiento de los datos biométricos podemos extraer las siguientes consideraciones:

a) El *principio de licitud, lealtad y transparencia*[62] se concreta, en primer término, en la necesidad de los interesados sean conscientes de que sus datos biométricos estas siendo recogidos y utilizados y, por lo tanto, no será lícito recoger datos biométricos sin su conocimiento. La lealtad en la recogida y tratamiento de los datos personales está íntimamente relacionada con la transparencia de todo el proceso situando a la persona titular de los datos en una posición central que le permita controlar *"de una manera más intensa todas las circunstancias que rodean al tratamiento"*[63].

b) Un elemento esencial en el tratamiento de los datos biométricos es el *principio de limitación de la finalidad,* que requiere de una definición previa y clara de los objetivos de su obtención y tratamiento y, en este contexto, deberá valorarse si la finalidad es entrenar un sistema de IA, si los datos biométricos servirán para la verificación, la autenticación o la categorización, por ejemplo, debiendo desde un primer momento valorar los riesgos para los derechos y la libertades de los interesados en cada caso. También prohíbe que los datos biométricos sean tratados ulteriormente de manera incompatible con los fines que legitimaron su tratamiento[64].

c) El *principio de minimización de datos* exigirá que no se recojan ni almacenen más datos de los estrictamente necesarios para cada finalidad determinada y que sean adecuados y no excesivos para la

[62] La obligación de transparencia se configura como "una expresión del principio de lealtad en relación con el tratamiento de los datos personales plasmado en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea (En Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679 del WP29, adoptadas el 29 de noviembre de 2017 y revisadas por última vez y adoptadas el 11 de abril de 2018, p. 5.

[63] J. PUYOL MONTERO, "Los principios del derecho a la protección de datos", en J. L. PIÑAR MAÑAS, *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, REUS, Madrid, 2016, p. 138.

[64] En el ámbito policial y penal se establecen las condiciones para finalidades distintas de la inicial en el apartado 3 del artículo 6 de la Ley Orgánica 7/2021.

misma. Por ejemplo, cuando se obtengan datos biométricos a partir de imágenes será necesario que "todo el material de vídeo que no sea pertinente para la finalidad del tratamiento se elimine siempre o se anonimice (por ejemplo, mediante una difuminación sin posibilidad de recuperar los datos con carácter retroactivo) antes de su utilización"[65]. El principio de minimización también operará en relación a cómo se van a almacenar los datos personales o a quiénes van a tener acceso a los datos biométricos de forma que su aplicación conjunta con los principios de protección de datos desde el diseño y por defecto determinará la forma menos intrusiva de su tratamiento[66].

d) El *principio de exactitud* plantea dificultades diversas en función de la tecnología biométrica de que se trate. En concreto, en el caso de las tecnologías de reconocimiento facial, debe partirse de la premisa de que no es una tecnología exacta sino que se basa en un determinado porcentaje de probabilidad de que dos rostros pertenezcan a la misma persona. Pero, además y como ya se ha señalado, no solamente no proporcionan un resultado definitivo, sino que "numerosos estudios también han puesto de manifiesto que estos resultados estadísticos del procesamiento algorítmico también pueden estar sujetos a sesgos[67]; en particular, la falta de suficiente calidad de los datos[68] propiciará un sesgo social cuando se utilicen muestras de

[65] CEPD: Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, cit., p. 5.

[66] Por ejemplo, en el caso de que la finalidad del tratamiento de los datos biométricos sea la verificación de la identidad de una persona para garantizar su acceso a una zona física restringida, no se sería necesario que las características biométricas se almacenen en una base de datos central, bastando que se almacenen en una tarjeta o en el documento de identidad de una persona. Vid. FRA: Facial recognition technology: fundamental rights considerations in the context of law enforcement, cit.

[67] Derivado del sesgo de los datos, del propio algoritmo de aprendizaje o del bucle de retroalimentación entre el sistema y el usuario. Vid. R. BAEZA-YATES, "Ethical Challenges in AI", *WSDM '22: Proceedings of the Fifteenth ACM International Conference on Web Search and Data Mining*, 2022. La persistencia de estos sesgos ha llevado a afirmar la necesidad de que en el desarrollo de sistemas de minería de datos se sea consciente de la frecuente discriminación por diseño. En S. HAJIAN, F. BONCHI y C. CASTILLO, "Algorithmic Bias: From Discrimination Discovery to Fairness-aware Data Mining", *KDD '16: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2016, p. 2125.

[68] En ocasiones porque no se cuenta con un volumen suficiente de datos de entrenamiento o porque se utilizan directamente los datos de internet. Pero, si bien el tamaño de los

datos no representativas del conjunto de la población[69], ya sea en los datos de origen, o en las bases de datos de entrenamiento[70]. El principio de exactitud exige los responsables del tratamiento utilicen información exacta y actualizada y esta obligación lo es, tanto para los datos utilizados para crear y entrenar el software como para los datos utilizados en su despliegue. En el caso de los sistemas de reconocimiento facial, que se basa en modelos pre-entrenados a partir de una base de datos de imágenes faciales, la calidad de las imágenes es un aspecto fundamental ya que la tasa de error de los sistemas está directamente relacionada "con la calidad de los datos y la precisión de su procesamiento"[71] y, la calidad de los datos requerirá también "un conjunto representativo de rostros que representen a diferentes grupos de personas"[72].

Directamente relacionada con la exigencia de una suficiente calidad de los datos, el artículo 10. 3 del RIA contienen obligaciones muy precisas para los datos utilizados en los sistemas biométricos de alto riesgo para su entrenamiento validación o prueba, habiendo de

datos disponibles en la web ha permitido a los modelos de aprendizaje profundo alcanzar una alta precisión en aplicaciones como las del procesamiento del lenguaje natural (PNL) dan lugar a modelos que codifican prejuicios estereotipados y peyorativos en función del género, la raza, la etnia y la discapacidad. En E. M. BENDER, T. A. GEBRU, MCMILLAN-MAJOR, S. SHMITCHELL, "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?", *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, March 2021.

[69] L. JIMENA QUESADA, "Inteligencia artificial, protección de datos y derecho a la salud en la era post-covid", en AA.VV., *La implementación del reglamento general de protección de Datos en España y el impacto de sus cláusulas abiertas*, Tirant lo Blanch, Valencia, 2023, pp. 105 y ss.

[70] CEPD: Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, cit., p. 19.

[71] FRA: Facial recognition technology: fundamental rights considerations in the context of law enforcement, cit., p. 11 y 12.

[72] Ibidem, p. 40. Así mismo, para el cumplimiento de este principio será necesaria una actuación diligente por parte del responsable del tratamiento. Esta diligencia se traducirá en la necesidad de adoptar todas las medidas razonables para que se supriman o rectifiquen los datos inexactos, pero también en la necesidad de que los datos biométricos que se utilicen sean de alta calidad ya que eso garantizará la calidad del algoritmo de reconocimiento de la identidad. Además subraya el CEPD que las exigencias derivadas de la exactitud de los datos y del principio de responsabilidad proactiva y de rendición de cuentas supondrán asimismo para los responsables del tratamiento *"la evaluación periódica y sistemática del tratamiento algorítmico con el fin de garantizar, en particular, la exactitud, la equidad y la fiabilidad del resultado"* (En CEPD: Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, cit., p. 19; la traducción es mía).

ser *pertinentes, suficientemente representativos y, en la medida de lo posible, estarán exentos de errores y serán completos con vistas a la finalidad prevista*[73].

e) La aplicación del *principio de limitación del plazo de conservación*[74] va a determinar la necesidad de que se establezcan límites temporales para la conservación de los datos biométricos basados en criterios objetivos de acuerdo con la finalidad que justificó su tratamiento y en función de las categorías de personas a las que se refieran[75]. En su ámbito de aplicación, el artículo 8 de la Ley Orgánica 7/2021 regula los criterios y los plazo máximos de conservación.

f) En el RGPD, la seguridad de los tratamientos es un tema central para cualquier categoría de datos personales, aunque si se trata de categorías especiales debe extremarse el rigor en la evaluación y adopción de las medidas, técnicas y organizativas, para garantizar una seguridad adecuada de los datos.

g) El *principio de responsabilidad proactiva* supuso un cambio de paradigma desde un sistema de protección reactivo frente al incumplimiento a un modelo preventivo y proactivo[76]. En el ámbito del

---

[73] Además, se prevé que los datos *deberán tener las propiedades estadísticas adecuadas, incluso, en su caso, en lo que respecta a las personas o grupos de personas en relación con los cuales está previsto utilizar el sistema de IA de alto riesgo. Estas características de los conjuntos de datos podrán cumplirse a nivel de conjuntos de datos individuales o de una combinación de los mismos. mismos*.

Este mismo artículo del RIA, en sus apartados 4 y 5, respectivamente, contiene requisitos específicos para evitar sesgos algorítmicos derivados de los conjuntos de datos utilizados. Se establece *que los conjuntos de datos deberán tener en cuenta, en la medida en que lo exija la finalidad prevista, las características o elementos propios del entorno geográfico, contextual, conductual o funcional específico en el que esté previsto utilizar el sistema de IA de alto riesgo*. Y, que cuando sea estrictamente necesario para garantizar la vigilancia, la detección y la corrección de los sesgos asociados a los sistemas de IA de alto riesgo, *los proveedores de dichos sistemas podrán tratar las categorías especiales de datos personales que se mencionan en el artículo 9, apartado 1*, del RGPD ofreciendo siempre las salvaguardias adecuadas para los derechos y las libertades fundamentales de las personas físicas.

[74] Vid., entre otras, STJUE de 13 de mayo de 2014 (asunto Google vs AEPD y Mario Costeja).

[75] La necesidad de que se determine un período de conservación concreto es una exigencia del RGPD y que han señalado tanto el TEDH (STEDH de 4 diciembre 2008, Caso S. y Marper contra Reino Unido), como el TJUE y habrá de basarse "*en criterios objetivos para garantizar que ésta* (la vida privada de los interesados) *se limite a lo estrictamente necesario"* (STJUE de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12).

[76] S. LORENZO CABRERA, "Posición jurídica de los intervinientes en el tratamiento de datos personales. Medidas de cumplimiento", en AA.VV., *Protección de datos, responsabilidad activa y técnicas de garantía*, REUS, Madrid, 2018, p. 123 y ss.

tratamiento de los datos biométricos establece determinadas obligaciones concretas para el responsable del tratamiento[77]como la realización de una evaluación de impacto sobre la protección de datos (EIPD), ya que nos encontramos antes sistemas de alto riesgo para los derechos humanos[78] o, en determinados casos, realizar una consulta previa a la autoridad de control[79].

3.2. La insuficiencia de las bases de legitimación del artículo 6 del RGPD para el tratamiento de los datos biométricos

El artículo 9.1 del RGPD establece la prohibición del tratamiento de determinadas categorías de datos personales especialmente protegidos entre los que están los *"datos biométricos dirigidos a identificar de manera unívoca a una persona física"*. Con independencia de que el dato biométrico se utilice para la identificación (uno-a-varios) o para la autenticación (uno-a-uno), se trataría de datos personales que encajarían en la definición del artículo 4.14) del RGPD[80] ya que el artículo 9 no distingue entre las diferentes posibilidades

[77] Junto con la general prevista en el artículo 24 del RGPD de aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas. Igualmente habrán de aplicarse los principios de privacidad desde el diseño y por defecto.

[78] Así se recoge en la lista de la AEPD de tratamientos de datos que requieren evaluación de impacto relativa (art 35.4 del RGPD). Vid., asimismo, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679, adoptadas el 4 de abril de 2017 y revisadas por última vez y adoptadas el 4 de octubre de 2017 del CEPD.

[79] Esta consulta será obligatoria cuando el legislador nacional pretenda crear una nueva base jurídica para cualquier forma de tratamiento de datos biométricos mediante reconocimiento facial de acuerdo con lo previsto en el artículo 28, apartado 2 de la Directiva 2016/680. Vid. CEPD: Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, cit.

[80] Al respecto hay que señalar que no ha sido una cuestión pacífica, existiendo disparidad de posiciones entre las distintas autoridades de control. En el caso de la AEPD de forma reiterada venía sosteniendo que "los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno)" (en Informe jurídico: 0036/2020, p. 19 y Resolución de la AEPD PS/00120/2021, p. 39.) Actualmente, la AEPD ha modificado su criterio y es coincidente con el del CEPD (Guidelines 05/2022) o, por ejemplo la Autoridad Catalana (Dictamen CNS 21/2020), el *Garante per la protezione dei dati personali* (*Ordinanza ingiunzione nei confronti di*

de uso del dato biométrico y simplemente establece una condición para su aplicación: que los datos biométricos estén dirigidos a identificar de manera unívoca a una persona física. Esta consideración tiene importantes consecuencias prácticas, ya que va a determinar su régimen jurídico aplicable, que podemos concretar en las siguientes:

a) Existe una prohibición general para su tratamiento salvo que nos encontremos ante alguna de las excepciones previstas en el apartado segundo del artículo 9 del RGPD, puesto que la prohibición general del artículo 9.1 del RGPD tiene como consecuencia la insuficiencia de las causas de licitud del artículo 6 para tratar esta categoría de datos personales.

b) Una segunda consecuencia derivada de esa prohibición general es que, cualquiera de las excepciones previstas en el apartado segundo del artículo 9, deberá interpretarse de forma restrictiva. El carácter restrictivo que dimana de dicha prohibición viene recogido también en los Considerandos 51 y 52 del RGPD.

c) La especial importancia que reviste la aplicación del principio de necesidad y proporcionalidad en orden a calibrar la legitimidad de la injerencia en el derecho fundamental a la protección de datos personales derivada del tratamiento de los datos biométricos.

Es imposible en un trabajo de esta naturaleza, analizar en detalle cada una de las excepciones[81] previstas en el RGPD[82] por lo simplemente señalaré que el apartado 4 del artículo 9 deja abierta la posibilidad de que los Estados miembros mantengan o introduzcan condiciones adicionales o nuevas limitaciones para el tratamiento de los datos biométricos, que en el caso español han sido concretadas en el artículo 9 de la LOPDGDD. En todo caso, habría

---

Azienda sanitaria provinciale di Enna - 14 gennaio 2021) o la *Commission Nationale de l'informatique et des libertés* (*Délibération n° 2019-001, du 10 janvier 2019*) y así se recoge en su *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*, de noviembre de 2023, p. 13.

[81] Me remito al estudio realizado en un trabajo anterior: "La especial posición de los datos biométricos en el RGPD: peculiaridades derivadas de su naturaleza y riesgos asociados a su tratamiento", en C. PAUNER CHUVI, R. GARCÍA MAHAMUT y B. TOMÁS MALLÉN; J. A. VIGURI CORDERO (coords.), *La implementación del reglamento general de Protección de Datos en España y el impacto de sus cláusulas abiertas*, Valencia, Tirant lo Blanch, 2023.

[82] Las excepciones previstas en la Ley Orgánica 7/21 (artículo 13) y en la Directiva 2016/680 (artículo 10) son las siguientes: a) Que el tratamiento se encuentre previsto por una norma con rango de ley o por el Derecho de la Unión Europea; b) Que el tratamiento resulte necesario para proteger los intereses vitales, así como los derechos y libertades fundamentales del interesado o de otra persona física y c) Que dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

que cumplir otro requisito adicional, ya que será necesario que el tratamiento de los datos biométricos se ampare en alguna de las bases de legitimación del artículo 6. Ambas condiciones han de darse simultáneamente, pues como ha indicado la AEPD, de no concurrir alguna de las excepciones del artículo 9.2 no habría "legitimación para tratar los datos biométricos de nadie, con independencia de las acusas de licitud señaladas en el art. 6 del RGPD"[83].

c.1. **El tratamiento de los datos biométricos deberá ajustarse a las exigencias derivadas del principio de necesidad y proporcionalidad**

Cuando nos situamos ante las posibilidades de tratamiento de los datos sensibles, el principio de proporcionalidad cobra una importancia capital al afectar a los aspectos más íntimos de la personalidad del interesado, que inciden sobremanera en su desarrollo personal y su instrumentalización puede conculcar derechos "y principios como el de la igualdad y no discriminación"[84]. De acuerdo con la jurisprudencia del TEDH, el principio de proporcionalidad, derivado de la consideración de que la medida limitativa de los derechos amparados por el artículo 8 del Convenio ha de ser necesaria en una sociedad democrática, implica una doble consideración, tanto de procedimiento como de fondo[85]. Primero, habrá de examinarse "la decisión material de las autoridades internas para asegurar que es compatible con el artículo 8"[86] y, en segundo lugar, se estudiará el proceso de decisión para establecer si se han tenido suficientemente en cuenta los intereses de las personas. Será preciso verificar "si el proceso de toma de decisiones que llevó a la medida de la injerencia fue justo y de tal forma concedió el debido respeto a los intereses garantizados por el artículo 8 para el individuo"[87]. El principio de proporcionalidad exige, en definitiva, que "los Estados que minimicen, hasta donde sea posible, la injerencia en estos derechos, intentando encontrar soluciones alternativas y buscando en general, alcanzar los fines de la forma menos onerosa para los derechos humanos"[88]. El TEDH

[83] Resolución del procedimiento nº PS/00120/2021 de la AEPD, p. 33.

[84] I. CANO RUIZ, "Principios de protección de datos. Art. 9", en M. ARENAS RAMIRO y A. ORTEGA GIMÉNEZ, *Protección de Datos*, Sepín, Madrid, 2019, p. 82. Asimismo, A. E. PÉREZ LUÑO, "La tutela jurídica de los datos personales en España", *La Toga*, núm. 131, Ilustre Colegio de Abogados de Sevilla, diciembre de 2001, p. VIII.

[85] Entre otras, STEDH de 5 de diciembre de 2013 (caso Skrtic contra Croacia).

[86] STEDH de 10 de noviembre de 2004 (caso Taskin y otros contra Turquía).

[87] STEDH de 27 de mayo de 2004 (caso Connors contra el Reino Unido).

[88] STEDH de 2 de octubre de 2001 (caso Hatton y otros contra el Reino Unido).

requiere que se aplique el principio de proporcionalidad comprobando, si la injerencia está justificada, es racional y es proporcionada, en la búsqueda del imprescindible equilibrio que en las sociedades democráticas deben tener las actuaciones restrictivas de derechos fundamentales y los propios derechos de las personas, que forman un conjunto de valores fundamentales en nuestras sociedades democráticas y de Derecho[89].

En términos semejantes se ha expresado nuestro Tribunal Constitucional, que exige que la medida limitativa de un derecho fundamental sea necesaria para conseguir el fin perseguido[90], atienda a la proporcionalidad entre el sacrificio del derecho y la situación en la que se encuentra aquel a quien se le impone[91] y, en todo caso, respete su contenido esencial[92]. Es decir, para cumplir la finalidad legítima se debe utilizar un medio idóneo para lograrla, pero además se debe valorar si no existe otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad)[93] y, esta valoración se debe realizar, si cabe con mayor rigor, cuando nos encontramos ante un tratamiento de los datos especialmente protegidos, tal y como tuvo ocasión de señalar en su sentencia 76/2019, de 22 de mayo.

---

[89] Igualmente, el TJUE, de acuerdo con lo dispuesto en el artículo 52, apartado 1, de la Carta, recuerda *"que pueden introducirse limitaciones al ejercicio de derechos como los consagrados de los artículos 7 y 8 de la misma, siempre que tales limitaciones estén establecidas por la ley, respeten el contenido esencial de dichos derechos y libertades y, respetando el principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás" (*STJUE de 9 de noviembre de 2010, asuntos acumulados C-92/09 y C-93/09,Volker und Markus Schecke GbR, Hartmut Eifert y Land Hessen). Son muy pertinentes también las consideraciones del TJUE respecto de las medidas de vigilancia masiva e indiscriminada en su sentencia de 8 de abril de 2014, que anuló la Directiva 2006/24/CE por establecer un sistema de vigilancia masivo incompatible con los principios de necesidad y proporcionalidad derivados de los derechos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea. Asimismo, el TJUE se pronuncia sobre la proporcionalidad de la injerencia en los derechos de los artículos 7 y 8 de la Carta de derechos fundamentales que supone la inclusión de datos biométricos en los pasaportes en sus sentencias El TJUE se pronuncia sobre la proporcionalidad de la injerencia en los derechos de los artículos 7 y 8 de la Carta de derechos fundamentales que supone la inclusión de datos biométricos en los pasaportes en su sentencia de 17 octubre de 2013 y en su sentencia de 12 de diciembre de 2013. Muy interesante es la STJUE de 31de enero de 2023 sobre la aplicación rigurosa de los principios de minimización y proporcionalidad en el ámbito de la recogida de datos biométricos y genéticos a efectos de su inscripción en el registro policial.

[90] SSTC 61/1982, de 13 de octubre y 13/1985, de 31 de enero.

[91] STC 37/1989, de 15 de febrero.

[92] Entre otras, STC 11/1981, de 8 de abril o 57/1994, de 28 de febrero.

[93] SSTC 66/1995, de 8 de mayo, 186/2000, de 10 de julio, 17/2013, de 31 de enero o 292/2000, de 30 de noviembre.

c.2. **La elaboración de perfiles y la adopción de decisiones automatizadas basadas en datos biométricos**

En el ámbito de los sistemas de IA, la legislación sobre protección de datos personales prevé una serie de garantías interesantes, pero con limitaciones, frente a la adopción de decisiones automatizadas. El artículo 22 del RGPD garantiza el derecho del interesado *a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar*. No estamos ante un derecho absoluto, ya que no se aplicará este derecho cuando la decisión sea necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento, cuando esté autorizada por el Derecho de la Unión o de los Estados miembros y establezcan asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o cuando se base en el consentimiento explícito del interesado. Y, si bien establece una limitación en razón de la naturaleza de los datos personales prohibiéndose la adopción de decisiones automatizadas basadas en datos especialmente protegidos, entre los que estarían los biométricos, salvo que el interesado haya prestado su consentimiento explícito y esta posibilidad no esté prohibida por el Derecho de la Unión o de los Estados miembros, también se permitirá la elaboración del perfiles o la adopción de una decisión automatizada cuando el tratamiento sea necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. Por otra parte, el artículo 22 garantiza al interesado tres derechos en relación con la decisión automatizada: a obtener intervención humana por parte del responsable[94], a expresar su punto de vista y a impugnar la decisión.

Se ha cuestionado el potencial real del artículo 22 del RGPD para proteger eficazmente a las personas de la adopción de la IA[95]: por la limitación

[94] Señala el Comité Europeo que dicha intervención humana ha de ser significativa, es decir, la "revisión debe ser llevada a cabo por una persona con la autorización y capacidad adecuadas para modificar la decisión. El revisor debe llevar a cabo una evaluación completa de todos los datos pertinentes, incluida cualquier información adicional facilitada por el interesado". En Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 del GT29, Adoptadas el 3 de octubre de 2017 y revisadas por última vez y adoptadas el 6 de febrero de 2018, p. 30.

[95] G. GONZÁLEZ FUSTER, y M.A. NADOLNA PEETERS, *Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence*, cit., p. 26.

del ámbito de aplicación de la disposición[96], porque no recoge expresamente el principio de transparencia algorítmica[97] y porque solamente se aplicará cuando las decisiones produzcan un efecto jurídico o *o le afecte significativamente de modo similar*[98]. Sin embargo, la reciente sentencia del TJUE de 7 de diciembre de 2023 (asunto C-634/21)[99] supone "un"corrimiento del velo" de las decisiones "únicamente" automatizadas"[100], superando una interpretación restrictiva para aplicar las garantías de este precepto a muchos supuestos de decisiones parcialmente automatizadas y, así, "las garantías de este precepto también se darán si los resultados del sistema automatizado, el perfilado o la ponderación automatizada de datos (o con inteligencia artificial) se conectan materialmente con la decisión finalmente adoptada por quien tiene que adoptarla respecto del afectado por dicha decisión"[101].

---

[96] Que exige que se den tres requisitos acumulativos: que exista una decisión, que esté basada únicamente en un tratamiento automatizado de datos incluida la elaboración de perfiles y que produzca efectos jurídicos que afecten al interesado o que lo afecten significativamente de modo similar (STJUE de 7 de diciembre de 2023).

[97] L. GÓMEZ ABEJA, "Inteligencia artificial y derechos fundamentales", en *Inteligencia artificial y Filosofía del Derecho,* cit., p. 108. En este mismo sentido se pronuncia el Tribunal Federal Administrativo de Austria, en una sentencia de 29 de junio de 2023, considerando que "ese derecho a la información no incluye una completa revelación del algoritmo matemático utilizado, pues ello equivaldría a la divulgación de la fórmula matemática que rige la elaboración de perfiles, un aspecto que no está cubierto por el RGPD". En C. B. FERNÁNDEZ, "Alcance de la obligación de facilitar al interesado 'información significativa sobre la lógica aplicada' en la toma de decisiones automatizadas (art. 15.1, letra g, del RGPD), *Diario La Ley*, 31-8-2023.

[98] La aplicabilidad del artículo 22 dependerá de que se produzcan o se puedan derivar esas consecuencias relevantes para la persona; es decir, cuando produzca efectos jurídicos que afecten al interesado (por ejemplo, afecte a sus derechos, se le deniegue una prestación, produzca efectos en un contrato en el que sea parte) o le afecte significativamente de modo similar, es decir que sea suficientemente importante, como por ejemplo, que se le deniegue un crédito, que le afecte a su acceso a determinados servicios, en el acceso o promoción en el empleo, etc.

[99] El TJUE, considera que, en virtud del artículo 22 del RGPD, el responsable del tratamiento tiene la obligación "de utilizar procedimientos matemáticos o estadísticos adecuados, de aplicar las medidas técnicas y organizativas apropiadas para garantizar que se reduzca al máximo el riesgo de error y se corrijan errores, y de asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado e impedir, entre otras cosas, los efectos discriminatorios en las personas físicas. Estas medidas incluyen, por otro lado, como mínimo el derecho del interesado a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión".

[100] L. COTINO HUESO, "La primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de inteligencia artificial", *Diario La Ley*, núm. 80, Sección Ciberderecho, 17-1-2024.

[101] Ibidem.

Una previsión semejante, aunque no equivalente, se encuentra recogida en el artículo 11 de la Directiva 2016/680 y en el artículo 14 de la Ley Orgánica 7/2021, que regulan el *mecanismo de decisión individual automatizado*. Una particularidad de estas normas es que se establecen expresamente la prohibición de elaboración de perfiles *que dé lugar a una discriminación de las personas físicas sobre la base de categorías especiales de datos personales*.

4. REQUISTOS PARA LOS SISTEMAS BIOMÉTRICOS EN LA LEGISLACIÓN ESPECÍFICA SOBRE IA

4.1. La Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación

No es este el lugar para un análisis exhaustivo de las obligaciones que establece la Ley Orgánica 15/2022. Baste señalar, como muy relevante, que en su ámbito objetivo de aplicación (artículo 3) se incluye la *Inteligencia Artificial y gestión masiva de datos, así como otras esferas de análoga significación*. No obstante y si bien esta inclusión debe valorarse positivamente, como señala Lorenzo Cotino, su alcance será limitado ya que en principio "*esta ley sólo sería aplicable para los supuestos de discriminación y sesgos algorítmicos vinculados con las categorías especialmente sospechosas de discriminación*"[102].

El conjunto de previsiones normativas para garantizar que los sistemas de IA en su ámbito de aplicación sean respetuosos con el derecho a la igualdad y la no discriminación se encuentran recogidas en su artículo 23[103]. Este precepto prevé determinadas obligaciones para los sistemas de IA involucrados en los procesos de toma de decisiones, que serían aplicables a los sistemas biométricos. Se

[102] L. COTINO HUESO, "Los usos de la inteligencia artificial en el sector público, su variable impacto y categorización jurídica", *Revista Canaria de Administración Pública*, núm. 1, 2023, p. 236.

[103] Además, nuestro país cuenta ya con varias normas de rango reglamentario, que tienen alguna incidencia en los sistemas de inteligencia artificial: el Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial y el Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial, contine alguna previsión para los sistemas biométricos en ANEXO II, incluyéndolos en el Listado de áreas de sistemas de inteligencia artificial de alto riesgo específicos y en su artículo 5 sobre Requisitos de elegibilidad para la participación en el entorno.

trata de prevenir las decisiones automatizadas discriminatorias derivadas de los sesgos algorítmicos, en particular en el ámbito de las administraciones públicas. Para ello, se establece que, en el marco de la Estrategia Nacional de Inteligencia Artificial, de la Carta de Derechos Digitales y de las iniciativas europeas en torno a la Inteligencia Artificial, las administraciones públicas deberán de favorecer que se adopten determinados mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones públicas incorporen los criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente. Estas referencias junto con las del apartado tercero a un IA ética y confiable implicaría la necesidad de incorporar determinadas garantías concretas durante el desarrollo y todo el ciclo de vida del sistema: "como es la no discriminación en las decisiones y en el uso de datos y procesos, deben procurarse unas condiciones de transparencia, auditabilidad, aplicabilidad, trazabilidad, supervisión humana y gobernanza, siendo la información facilitada accesible y comprensible"[104].

Debe señalarse que este precepto no establece obligaciones concretas[105] sino que se limita a indicar que las administraciones públicas favorecerán que se incorporen esos criterios siempre que sea factible técnicamente. Dichos mecanismos se incluirán en el diseño del algoritmo y se aplicarán a los datos de entrenamiento, abordando su potencial impacto discriminatorio, *para lo que se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio*.

En el segundo apartado del artículo 23 se establece que, en su ámbito de competencia, las administraciones públicas priorizarán para los algoritmos involucrados en procesos de toma de decisiones, *la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos*. Por último y en este caso, tanto para el sector público como para el privado, se establece la promoción del *uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido.*

Puede afirmarse que esta norma, pionera en nuestro país, aporta algunos elementos innovadores para hacer frente a las situaciones de discrimi-

[104] A. T. ESTER SÁNCHEZ, "El desafío de la Inteligencia Artificial a la vigencia de los derechos fundamentales", *Cuadernos Electrónicos de Filosofía del Derecho*, núm. 48, 2023, p. 126.

[105] En R. Mª. GONZÁLEZ DE PATTO, "Inteligencia artificial y empleo. Análisis crítico del marco regulatorio europeo y español impulsado por el Pilar Europeo de Derechos Sociales", *Temas laborales: Revista andaluza de trabajo y bienestar social,* núm. 168, 2023, p. 387.

nación algorítmica, como la implementación de medidas para la prevención y eliminación de sesgos, que garanticen la transparencia y la rendición de cuentas. En contra, se debe indicar que se ha desaprovechado la oportunidad de establecer con mayor rotundidad los requistos que necesariamente deberán cumplir algoritmos y sistemas de IA para garantizar los objetivos de la ley; pues resulta obvio reconocer que el conjunto de éstos no se configuran como "*deberes imperativos: los términos legales* "favorecerán", "promoverán" o "priorizarán" utilizados en el precepto (…) apuntan tan solo a un desiderátum o a buenas prácticas desprovistas de fuerza vinculante, lo que indudablemente merma la efectividad de la tutela antidiscriminatoria integral pretendida por la Ley, que, por ello, nace ya obsoleta a este respecto[106].

4.2. Su regulación en el Reglamento sobre IA: un enfoque basado en los riesgos y el reforzamiento de la transparencia.

El pasado día 9 de diciembre de 2023 se anunciaba la aprobación de una acuerdo provisional entre la Presidencia del Consejo y el Parlamento Europeo sobre la Propuesta de Reglamento sobre inteligencia artificial (IA)[107]. Finalmente, el Parlamento Europeo lo aprobó el día 13 de marzo de 2024.

La preocupación por las implicaciones de los sistemas biométricos para los derechos humanos y los valores democráticos impregnan el Reglamento, que adopta un enfoque desde el riesgo para la calificación de algunos sistemas como de riesgo inaceptable y, en consecuencia los prohíbe, o de riesgo alto, estableciendo unas obligaciones específicas para su desarrollo e implantación. Como ya he señalado, la definición de dato biométrico del RIA es la misma que la que se recoge en las normas europeas sobre protección de datos personales, optando por establecer una clasificación de los sistemas biométricos desde un punto de vista funcional. De acuerdo con las disposiciones del artículo 3 del Reglamento,

[106] Ibidem, p. 388.

[107] Si bien ha sido presentada como la primera Ley sobre IA, el pasado mes de agosto, la República Popular China aprobó una Ley general reguladora de la IA y, una regulación específica de la IA generativa y, en octubre pasado, el presidente de EE.UU. emitió Orden Ejecutiva para gestionar los riesgos de la IA: la *Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*. En J. EGUILUZ CASTAÑEIRA y C. FERNÁNDEZ HERNÁNDEZ, "Cinco aclaraciones necesarias sobre el Reglamento de IA (con un prólogo para tecnólogos y un epílogo para optimistas)", *Diario La Ley*, núm. 79, Sección Ciberderecho, 15-12-2023.

los sistemas biométricos pueden ser clasificados por su finalidad, distinguiendo entre[108]:

a) *Sistemas de identificación biométrica remota:* sistemas de IA utilizados con el fin de identificar a distancia a personas físicas mediante la comparación de los datos biométricos de una persona con los datos biométricos contenidos en una base de datos de referencia, y sin que el usuario del sistema de IA sepa previamente si la persona estará presente y podrá ser identificada. El Reglamento distingue "entre sistemas"en tiempo real" y"en diferido", con características y riesgos distintos"[109]. En la primera clase de estos sistemas, la comparación y la identificación se producirían sin una demora significativa, englobando la identificación instantánea y las demoras mínimas limitadas, a fin de evitar su elusión. Los sistemas de identificación biométrica remota a distancia "posterior" se definen por contraposición a la primera clase, estos es, cualquier *sistema de identificación biométrica remota que no sea un sistema de identificación biométrica remota"en tiempo real"*.
b) *Sistemas de reconocimiento de emociones*: aquellos sistemas de IA utilizados *con el fin de identificar o inferir emociones o intenciones de personas físicas a partir de sus datos biométricos*; y, en tercer lugar;
c) *Sistemas de categorización biométrica*: aquel sistema de IA destinado a asignar a personas físicas a categorías concretas, como un sexo, edad, color de pelo, color de ojos, tatuajes, origen étnico u orientación sexual o política, en función de sus datos biométricos.

Por lo que respecta a los sistemas biométricos, al considerar que éstos presentan riesgos inaceptables para los derechos humanos y los valores democráticos, el artículo 5 del Reglamento prohíbe *el uso de sistemas de identificación biométrica remota"en tiempo real" en espacios de acceso público con fines de aplicación de la ley.* No se trata de una prohibición absoluta, pues van a estar permitidos cuando uso sea estrictamente necesario para alcanzar determinados objetivos. En primer lugar, cuando sea necesario para la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos. En segundo lugar, para la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista. Y,

[108] Se sigue la clasificación propuesta en G. GONZÁLEZ FUSTER y M. A. NADOLNA PEETERS, *Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence. European Parliament,* cit. pp. 3 y ss.

[109] Ibidem, p. 4.

finalmente, será posible su uso para la localización o identificación de una persona sospechosa de haber cometido una infracción penal, con el fin de llevar a cabo una investigación penal, el enjuiciamiento o la ejecución de una sanción penal por las infracciones contempladas en el anexo II bis y castigadas en el Estado miembro de que se trate con una pena privativa de libertad o una medida de seguridad privativa de libertad de un máximo de al menos cuatro años.

Antes de su utilización para la consecución de los objetivos anteriores, será necesario valorar *la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema*, pero también, *las consecuencias que utilizar el sistema tendría para los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias.*

Otros requisitos que se establecen en el artículo 5 del Reglamento, para los usos permitidos de estos sistemas de identificación biométrica, son: la adopción de salvaguardias y condiciones necesarias y proporcionadas en relación con el uso, en particular en lo que respecta a las limitaciones temporales, geográficas y personales y la autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente del Estado miembro donde vaya a utilizarse, salvo situaciones de urgencia debidamente justificadas.

Asimismo se prohíben los sistemas de categorización biométrica que utilizan características sensibles de las personas (por ejemplo, creencias políticas, religiosas, filosóficas, orientación sexual, raza); a los sistemas de vigilancia predictiva; los sistemas de extracción no dirigida de imágenes faciales de Internet[110] o imágenes de CCTV para crear bases de datos de reconocimiento facial y, también, a los sistemas de reconocimiento de emociones en el lugar de trabajo y en instituciones educativas[111], salvo que tengan finalidades médicas o de seguridad. No obstante, se seguirán contemplando excepciones de estos sistemas en el ámbito policial. Otra novedad respecto de la Propuesta es la de la inclusión de un procedimiento de urgencia, debidamente justificada (apartado 3 del artículo 5), si bien, si bien "*también se ha introducido un me-*

[110] Esta práctica ya llevó a varias autoridades europeas a sancionar a la empresa *Clearwiew* por recolectar, violando el RGPD, datos biométricos y de geolocalización de ciudadanos europeos: entre ellas las autoridades italiana y francesa le impusieron cada una sanción de 20 millones de euros.

[111] Así mismo se habría acordado prohibir: los sistemas de puntuación social basada en el comportamiento social o en características personales; los sistemas de IA que manipulan el comportamiento humano para eludir su libre albedrío y los dedicados a explotar las vulnerabilidades de las personas (por su edad, discapacidad, situación social o económica).

canismo específico para garantizar que los derechos fundamentales estarán suficientemente protegidos contra cualquier posible uso indebido de los sistemas de IA" [112].

Respecto de los sistemas biométricos calificados en el RIA de alto riesgo, en su Anexo III, de acuerdo con lo establecido en el artículo 6.2, tendrán tal consideración los sistemas de IA de identificación biométrica y categorización de personas destinados a utilizarse en la identificación biométrica remota"en tiempo real" o"en diferido" de personas físicas, cuando su uso esté permitido por la legislación nacional o de la Unión Europea. Para estos sistemas, el RIA establecen una serie de requisitos específicos en su artículo 9:

a) La implantación de un sistema de gestión de riesgos durante todo el ciclo de vida del sistema, identificando, analizando y evaluando los riesgos y adoptando las medidas necesarias para su gestión y minimización
b) Que se garantice la calidad de los datos para aquellos sistemas que utilicen técnicas que implican el entrenamiento de modelos con datos.
c) Se prevén obligaciones específicas para la redacción de la documentación técnica.
d) Que se diseñen e implementen archivos de registro que garanticen la trazabilidad del funcionamiento del sistema de IA durante su ciclo de vida.
e) Se prevé el reforzamiento de las obligaciones de transparencia e información para garantizar la correcta interpretación y uso de su información de salida por parte de los usuarios y, asimismo, para que el usuario y el proveedor cumplan las obligaciones previstas en la Propuesta.
f) Se obliga a diseñar y desarrollar los sistemas de forma que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, dotándolos de una interfaz humano-máquina adecuada a fin de prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando el sistema se utilice conforme a su finalidad prevista o cuando se le dé un uso indebido razonablemente previsible.
g) Que se diseñen y desarrollen de modo que alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera consistente en esos sentidos durante todo su ciclo de vida.

[112] C. B. FERNÁNDEZ, "Los negociadores europeos alcanzan el acuerdo definitivo sobre el Reglamento de inteligencia artificial", *Diario La Ley,* 9 de diciembre de 2023.

Este conjunto de obligaciones se habrían visto reforzadas en el acuerdo provisional, en particular respecto de aquellas que garantizarían la transparencia de los sistemas, "un elemento clave que incide directamente en la calidad y robustez del sistema, así como respecto de la posibilidad de controlar sesgos, errores o posibles discriminaciones"[113], incluyendo además la exigencia de que realice una evaluación del impacto en los derechos fundamentales antes de que un sistema de IA de alto riesgo sea introducido en el mercado por sus implementadores"[114].

5. CONSIDERACIONES FINALES

Las tecnologías biométricas basadas en la IA plantean riesgos significativos para numerosos derechos fundamentales, pero también para la propia democracia y el Estado de Derecho. El despliegue y utilización de los sistemas de reconocimiento facial entrañan un alto riesgo para los derechos y las libertades de los interesados[115]. La amplificación y perpetuación de los perjuicios y la discriminación, resultado de diversos factores, son un problema bien documentado en este ámbito. Como consecuencia del gran número de personas afectadas, el número de errores y de personas que se verán afectadas por estos errores y sesgos intrínsecos, también aumentará, desencadenando interferencias adicionales con el ejercicio de los derechos humanos de múltiples maneras[116]. Las posibilidades del seguimiento omnipresente de las personas en los espacios públicos a través de la vigilancia 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, alterando la forma en que determinados individuos y grupos pueden ejercer la protesta social y política, valores que, como señalara en el año 1983 el Tribunal Constitucional Federal alemán[117], limitarán el potencial de la

[113] L. COTINO HUESO, "Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida", *Revista Española de la Transparencia*, núm. 16, 2023, p. 33.

[114] C. B. FERNÁNDEZ, "Los negociadores europeos alcanzan el acuerdo definitivo sobre el Reglamento de inteligencia artificial",cit.

[115] CEPD: Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, cit., p. 9.

[116] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, de 8 de abril de 2020.

[117] En su conocida sentencia de 15 de diciembre de 1983 (ley del censo), en la que por primera vez se reconoce el derecho a la protección de datos personales (autodeterminación informativa),

democracia participativa[118]. Las tecnologías biométricas hacen hoy, más que nunca, que nuestra vida individual y social se encuentren sometidas a lo que Frosini calificó, "con razón, de "juicio universal permanente""[119].

Por estas razones, resulta una buena noticia la aprobación de la futura regulación legal de la IA en el seno de la Unión Europea. No solo porque ampliará los instrumentos de garantía de los derechos de las personas, sino porque aportará la necesaria seguridad jurídica para todos los actores implicados. Respecto de los sistemas biométricos supondrá mejoras respecto de su regulación inicial en la Propuesta, ya que parece acoger las demandas del SEPD y del CEPD, así como de otras organizaciones internacionales y europeas. Especialmente acertada parece la exigencia de evaluaciones de impacto en los derechos de las personas, instrumento que ya ha probado su utilidad en el ámbito de la protección de datos personales. También la ampliación de las obligaciones de transparencia durante todo el ciclo de vida del sistema resultan idóneas para generar una mayor confianza social[120], pues respecto de los sistemas biométricos resulta de capital importancia poder conocer quién diseña esas categorías, quién decide sus significado y quién decide bajo qué circunstancias esas categorías serán decisivas[121].

Ana Garriga Domínguez
Escuela Superior de Ingeniería Informática (ESEI).
Universidad de Vigo
Campus Universitario de Ourense s/n.
32004 Ourense
e-mail: agarriga@uvigo.es

ya alertaba de que, "quien sepa de antemano que su participación, por ejemplo, en una reunión o en una iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales (artículos 8º y 9º de la Ley Fundamental). Esto no sólo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda la comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos".

[118] G. GONZÁLEZ FUSTER y M. A. NADOLNA PEETERS, *Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence. European Parliament*, cit. p. IV.

[119] A. E. PÉREZ LUÑO, "Vittorio Frosini y los nuevos derechos de la sociedad tecnológica", en *Informatica e Diritto*, 1-2, Edizioni Scientifiche Italiane, 1992, p. 104.

[120] S. ÁLVAREZ GONZÁLEZ, "La necesaria protección de los derechos fundamentales como punto de partida en las propuestas de regulación de la inteligencia artificial", cit., p. 221.

[121] D. LYON, *Surveillance Studies. An overview*, Polity Press, Malden, 2014, p. 186.