TRABAJO FIN DE GRADO
MONOGRÁFICO

LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES ANTE EL USO DE LA INTELIGENCIA ARTIFICIAL POR PARTE DE LAS AUTORIDADES EN ESPACIOS PÚBLICOS: UN ESTUDIO JURÍDICO DEL SISTEMA DE IDENTIFICACIÓN BIOMÉTRICA

AUTOR: Eva María de Castro Grullón
TUTOR: Prof. Oscar Andrés Molina
CONVOCATORIA: Ordinaria

DOBLE GRADO EN DERECHO Y RELACIONES INTERNACIONALES
Curso académico 2022/2023

FACULTAD DE CIENCIAS SOCIALES Y DE LA COMUNICACIÓN
UNIVERSIDAD EUROPEA DE MADRID

ABREVIATURAS Y ACRÓNIMOS

Sigla	Español	Inglés
ACOES	Asociación de Constitucionalistas de España	Association of Constitutionalists of Spain
ADN	Ácido desoxirribonucleico	Deoxyribonucleic acid
AEPD	Agencia Española de Protección de Datos	Spanish Data Protection Agency
APD	Autoridad de protección de datos	Data Protection Authorities
Art./Arts.	Artículo/Artículos	Article/Articles
CEPD	Comité Europeo de Protección de Datos	European Data Protection Board
Dict.	Dictamen	Opinion
DPEJ	Diccionario panhispánico del español jurídico	Pan-Hispanic Dictionary of Legal Spanish
ENIA	Estrategia Nacional de Inteligencia Artificial	National Artificial Intelligence Strategy
FRA	Agencia Europea de los Derechos Fundamentales de la Unión Europea	European Union Agency for Fundamental Rights
GPDP	Autoridad italiana de protección de datos	Italian Data Protection Authority
HmbBfDI	Agencia de Protección de Datos de Hamburgo	Hamburg Data Protection Agency
IA	Inteligencia Artificial	Artificial Intelligence
INCIBE	Instituto Nacional de Ciberseguridad de España	National Institute of Cybersecurity of Spain
La Carta	Carta de los Derechos Fundamentales de la Unión Europea	Charter of Fundamental Rights of the European Union
Ley de IA	Propuesta de Reglamento del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de IA y se	Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence

	modifican determinados actos legislativos de la Unión	(artificial intelligence act) and amending certain Union legislative acts.
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales	Organic Law 3/2018 of December 5, 2018, on the Protection of Personal Data and guarantee of digital rights.
MINECO	Ministerio de Asuntos Económicos y Transformación Digital	Ministry of Economic Affairs and Digital Transformation
Núm.	Número	Number
ONU	Organización de las Naciones Unidas	The United Nations
Párr.	Párrafo	Paragraph
RGPD	Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE	Regulation (EU) 2016/679 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
STC	Sentencia del Tribunal Constitucional	Constitutional Court Judgment
SEPD	Supervisor Europeo de Protección de Datos	European Data Protection Supervisor
TEDH	Tribunal Europeo de Derecho Humanos	European Court of Human Rights
TFUE	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales	Organic Law 3/2018 of December 5, 2018, on the Protection of Personal Data and guarantee of digital rights.
TJUE	Tratado de funcionamiento de la Unión Europea	Treaty on the Functioning of the European Union
UE	Unión Europea	European Union
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura	United Nations Educational, Scientific and Cultural Organization

ÍNDICE GENERAL

RESUMEN

En un contexto en el que la inteligencia artificial se ha incorporado plenamente a nuestra vida cotidiana y el uso de nuevas tecnologías es habitual, me surge una pregunta: ¿hasta qué punto esto juega con nuestros derechos fundamentales? En este análisis jurídico exhaustivo, se profundizará en la manera en que las autoridades utilizan la tecnología en su propio interés y cómo esto repercute en la ciudadanía. Si bien se avecina una legislación al respecto, todavía resta por investigar y desarrollar para conseguir una coexistencia entre ambos mundos. En el marco de este proceso, se pondrán de manifiesto las consecuencias éticas y legales que se derivan de los sistemas de identificación biométrica, en especial cuando se aplican en espacios públicos, y se identificarán los desafíos que debemos afrontar para proteger nuestros derechos en una sociedad cada vez más digitalizada.

Palabras clave: Sistemas de identificación biométrica, Derechos Fundamentales, datos biométricos, Inteligencia Artificial y espacios de acceso público.

ABSTRACT

In a context where artificial intelligence has been fully incorporated into our daily lives and the use of new technologies is commonplace, a question arises for me: to what extent does this play with our fundamental rights? In this in-depth legal analysis, we will delve into how authorities use technology in their own interest and how these impacts on the citizenry. While legislation in this regard is on the horizon, there is still research and development to be done to achieve a coexistence between the two worlds. As part of this process, the ethical and legal implications of biometric identification systems, especially when applied in public spaces, will be highlighted and the challenges we face in protecting our rights in an increasingly digitized society will be identified.

Keywords: Biometric identification systems, Fundamental Rights, biometric data, Artificial Intelligence, and public access spaces.

1. INTRODUCCIÓN

1.1. Objetivo general

El objetivo principal de esta investigación consiste en llevar a cabo un exhaustivo análisis normativo, jurisprudencial y doctrinal en relación con el impacto de los derechos fundamentales frente a la utilización de la identificación biométrica remota por parte de las autoridades en espacios de acceso público.

Dado el notable progreso tecnológico experimentado en este ámbito en los últimos tiempos, el presente estudio se centrará geográficamente en el ámbito de España y Europa, en especial los Estados miembros a la Unión Europea, mientras que desde una perspectiva normativa, se abordarán los últimos 7 años con el fin de identificar las regulaciones más relevantes en este período, Asimismo, se persigue la identificación y estudio de los fallos más trascendentes emitidos por los tribunales en el marco de esta novedosa disciplina de la biometría.

1.2. Objetivos específicos

- Identificación y análisis de los puntos de interés de los cuerpos normativos en vigor, tales como el Reglamento 2016/679 relativo al tratamiento de datos personales, Carta de Derechos Fundamentales, etc.
- Examinar y evaluar las propuestas de regulación futura, específicamente en relación con la Ley de IA, para identificar sus aspectos positivos y oportunidades de mejora. Se busca analizar detenidamente el marco normativo propuesto y ofrecer recomendaciones basadas en un análisis riguroso.
- Reflexionar respecto a la capacidad de las autoridades públicas para implementar proyectos de este tipo, evaluando, en concreto, el papel que juegan los principios jurídicos. Además, se examinarán detalladamente los riesgos asociados al procesamiento de datos personales.
- Estudiar y determinar el posicionamiento de la jurisprudencia en el ámbito específico de los sistemas biométricos y su posible implicación en la vulneración de los derechos fundamentales. Particularmente, se pretende investigar y evaluar si existe jurisprudencia relacionada con este tema, y en caso afirmativo, examinar el papel desempeñado por los sistemas biométricos en los casos en los que se haya identificado una vulneración de los derechos fundamentales.

- Plantear propuestas con base en el análisis de la normativa existente, los principios legales aplicables y la jurisprudencia pertinente, con el fin de fomentar un marco normativo y práctico más sólido y garantista en el uso de la biometría por parte de las autoridades públicas.

1.3. Justificación

Nos encontramos en torno a uno de los eventos más significativos en el ámbito de las nuevas tecnologías y el Derecho, la aprobación de la primera normativa comunitaria respecto la IA, sin embargo, durante este proceso, los derechos fundamentales de los individuos se ven comprometidos. Esta investigación exhaustiva se basa en mi motivación por abordar esta problemática. A través de mi participación en espacios multidisciplinarios, he podido observar de cerca la aplicación de la Inteligencia Artificial en nuestra vida diaria, evidenciando la falta de consideración del impacto en los derechos en todas sus dimensiones. El creciente panorama de vigilancia gubernamental plantea la necesidad de abordar esta realidad paralela. Esta investigación me permite examinar de manera precisa y detallada esta supuesta realidad y contribuir al conocimiento sobre la protección de los derechos.

1.4. Estructura

El estudio está compuesto por 5 grandes apartados, con sus respectivos subapartados, para obtener los objetivos planteados con posterioridad. Estos siguen la siguiente estructura:

- Un acercamiento normativo a nivel nacional y comunitario, enfocado en la protección de datos y los derechos fundamentales que le rodean a la práctica.
- Estudio de la jurisprudencia relevante en esta misma materia.
- Los desafíos en relación con los sistemas de identificación biométrica.
- La exploración de posibles escenarios futuros.
- Los hallazgos obtenidos y recomendaciones derivadas del análisis.
- Fuentes normativas, jurisprudenciales, doctrinales y demás.

A esto se le debe añadir que el estudio se desarrolla conforme una sutil línea de tiempo, iniciando con el nacimiento de la Inteligencia Artificial, su panorama actual y lo que nos aguarda por delante gracias a su reinserción en nuestras vidas.

1.5. Metodología

Para la elaboración de este trabajo, se ha seguido una metodología dogmática, centrándose en los cuerpos normativos presentes en el Boletín Oficial del Estado y el Diario Oficial de la Unión Europea de los últimos 15 años. Además, se ha realizado una investigación monográfica de casos cruciales relacionados con la materia, como el Auto de la Audiencia Provincial de Barcelona 1448/2021 y la Sentencia de la Corte de Apelaciones de Inglaterra y Gales N° C1/2019/2670, los cuales se han obtenido de las bases de datos oficiales del cuerpo jurídico correspondiente.

En este estudio se empleará un enfoque principalmente cualitativo para analizar los supuestos, complementado con datos cuantitativos relevantes, como el volumen de información recopilada durante el procesamiento de los datos. Asimismo, se llevará a cabo una recopilación y análisis documental por parte de los organismos garantes de protección de datos, tanto a nivel nacional como internacional.

2. DESARROLLO DEL TRABAJO

2.1. APROXIMACIÓN A LA INTELIGENCIA ARTIFICIAL

2.1.1. Evolución histórica

El primer acercamiento a la inteligencia artificial (en adelante, IA) lo brindó Alan Turing, categorizado como uno de los padres de las ciencias de la computación, además, fue el primero en cuestionarse si las máquinas tienen la capacidad de aprender al igual que un ser humano. Este planteamiento está desarrollado en su artículo *Computing machinery and intelligence,* el que inicia preguntando si las máquinas piensan (Turing, 1950, p.1), de este modo, mediante el test de Turing, evaluó la habilidad que tiene la máquina de tener una conversación, idea que para aquel entonces era imposible, pero logró desarrollar exitosamente, hasta el punto de identificar un nivel de reconocimiento por parte de la máquina del lenguaje humano, a través la "inyección" de ideas y órdenes (Turing, 1950, p. 22).

No obstante, fue John McCarthy quien acuñó, por primera vez, la expresión IA durante lo que hoy se conoce como el germen de esta ciencia, en la Conferencia de Darmouth de 1956, en Nuevo Hampshire, Estados Unidos (McCarthy et al., 2006, p.1). A través de la colaboración de otros expertos, como Marvin Lee Minkey en representación de *Harvard University*, se plantearon los obstáculos que tendría que afrontar la IA, entre ellos, la automatización y el autoaprendizaje de la computadora (McCarthy et al., 2006, p.2).

Respecto con los sistemas biométricos, la línea de tiempo inició en 1858, cuando William Herschel decidió estampar la huella de todos sus trabajadores al reverso de los contratos, para poder identificarlos al momento de realizar los pagos correspondientes (Rodríguez, 2013, p.3). En 1869, Herschel envió este gran inventario a Francis Galton que, para aquel momento, era reconocido por sus contribuciones a la ciencia, destacando el sector de registro y correlación en las medidas biológicas. A efectos de esta contribución, "dos años más tarde se confirmó que las huellas dactilares de un individuo no cambian con el simple transcurso del tiempo" (Rodríguez, 2013, p.4), lo que solidifica el sistema de identificación biométrica más antiguo.

En la actualidad, conforme con el Instituto Nacional de Ciberseguridad de España (en adelante, INCIBE), existe una fusión de ambas ciencias con las tecnologías biométricas, así, a través de métodos automatizados reconocen a las personas, con base en sus características físicas o de comportamientos, asimismo, gracias a los procesos de autentificación, se captan muestras biométricas del sujeto para luego ser registrados (INCIBE, 2016, pp.4-6).

Uno de los puntos de inflexión de las tecnologías biométricas es el nacimiento del reconocimiento facial, en este sentido, el pionero en esta tecnología fue Woodrow Wilson, quien, a mediados de 1960, había prosperado en un sistema de clasificación de los rostros humanos por medio de una tabla de números aleatorios (Tucker, 2014, p.4). Ahora bien, este sistema se expone como semiautomatizado y lento, por lo que, en la décadas de 1990, los matemáticos, Michael Kirby y Lawrence Sirovich de la Universidad de Brown, y los informáticos Matthew Turk y Alex Pentland del Massachusetts Institute of Technology (MIT), decidieron desarrollar el primer sistema automatizado ¨basado en el álgebra lineal llamado Eigenfaces, que puede trazar un rostro humano de forma eficaz centrándose en las desviaciones que presenta con respecto a la media¨ (Tucker, 2014, p.4).

2.1.2. Conceptos primordiales

De acuerdo con el Ministerio de Asuntos Económicos y Transformación Digital, la aplicación de esta tecnología en empresas ha aumentado hasta el 11,8 % y se estima que, para el 2025, el 25 % de empresas españoles la utilicen (Ministerio de Asuntos Económicos y Transformación Digital, 2023, p.3). En efecto, es una ciencia prematura y requiere de precisión para su estudio, por ello, el siguiente apartado está enfocado en presenciar los conceptos básicos de esta investigación.

2.1.2.1. La IA

Precisar el significado de la IA puede ser un proceso complejo, pues algunos detalles pueden verse modificados, sin embargo, con el paso del tiempo y la necesidad de cuerpos normativos que regulen su aplicación, se ha podido llegar a un acuerdo. Para introducirse a la complejidad de esta práctica, es preciso acercarse al posicionamiento doctrinal; Lasse Rouhiainen, especialista internacional en la IA, en sus seminarios expone

una definición simplificada, es decir, la IA es "la habilidad de los ordenadores para hacer actividades que normalmente requieren inteligencia humana" (Rouhiainen, 2018, p.17)[1].

Una de sus características principales es el *machine learning,* uno de los avances de la informática, este le permite a las máquinas aprender independientemente de su programación. Un ejemplo típico es la capacidad de poder solicitarle a una máquina los resultados conforme con la experiencia y los conocimientos captados a través de los algoritmos[2] de los patrones de datos (Rouhiainen, 2018, p.19). Esta es la base de la IA, los datos y los algoritmos, estos últimos son "una serie lógica de pasos para organizar y actuar sobre un conjunto de datos con el objetivo de lograr rápidamente un resultado" (World Wide Web Foundation, 2018, p.8), es decir, son los encargados de comunicarle a la máquina qué debe hacer.

No obstante, este estudio se enfoca en la captación de su otra columna, los datos, concretamente, los de índole biométrico y cómo la obtención de dichos datos en espacios públicos interactúa con los derechos fundamentales. Para que el algoritmo se ponga en funcionamiento, este es el primer paso, la creación de una base de datos.

Ahora bien, a pesar de la creciente relevancia de la IA en el mundo académico, la industria y las instituciones públicas, no existe una definición estándar de lo que realmente implica. Por ello, la Comisión Europea examina las definiciones más acertadas y llega a la conclusión de que la IA se debe entender como sistemas de *software* y *hardware* que actúan en la dimensión física o digital:

> Percibiendo su entorno, a través de la adquisición e interpretación de datos estructurados o no estructurados, razonando sobre el conocimiento, procesando la información derivada de estos datos y decidiendo las mejores acciones para lograr el objetivo dado. Los sistemas de IA pueden usar reglas simbólicas o aprender un modelo numérico, y también pueden adaptar su comportamiento al analizar cómo

[1] A juicio de Lasse Rouhiainen, a esta definición se le pueden añadir los siguientes detalles: ¨la IA es la capacidad de las máquinas para usar algoritmos, aprender de los datos y utilizar lo aprendido en la toma de decisiones tal y como lo haría un ser humano. Sin embargo, a diferencia de las personas, los dispositivos basados en IA no necesitan descansar y pueden analizar grandes volúmenes de información a la vez¨ (Rouhiainen, 2018, p.17).

[2] Si busca profundizar respecto con el papel de los algoritmos y su funcionamiento, se recomienda observar el informe, *Algorithmic Accountability, Applying the concept to different country contexts* de World Wide Web Foundation (World Wide Web Foundation, 2017).

el medio ambiente se ve afectado por sus acciones previas (Comisión Europea, 2020, p.9).

Dicho concepto va de la mano con lo expuesto en la Comunicación de la Comisión, COM/2018/237 final, respecto con la IA para Europa, donde se reafirma que las nuevas tecnologías deben desarrollarse siempre respetando los valores[3], los derechos fundamentales de la Unión Europea, los principios éticos como rendir cuentas y la transparencia (Comisión Europea, 2018a, p.3). A esto se le debe añadir que exhorta la creación de directivas éticas en relación con la IA, donde se evalúe el impacto en los derechos fundamentales, en particular, la intimidad, la dignidad, la protección de los consumidores y la lucha contra la discriminación, pues estos son los que se han visto más afectados por estas nuevas tecnologías (Comisión Europea, 2018a, p.17).

2.1.2.2. Espacios de acceso público

La propuesta de Reglamento del Parlamento Europeo y del Consejo, por la que se establecen normas armonizadas en materia de IA y se modifican determinados actos legislativos de la Unión Europea (Ley de IA), brinda un significado a lo que se debería considerar como espacios de acceso público. En su Artículo (en adelante, Art.) 3 dedicado a las definiciones[4], afirma que es "cualquier lugar físico accesible para el público, con independencia de que deban cumplirse determinadas condiciones para acceder a él" (Art.3.39, Ley de IA).

Esta se desarrolla de forma más detallada en el número (en adelante, núm.) 9, donde se aclara que dicha definición no engloba aquellos lugares de carácter privado a los que, por regla general, no pueden entrar libremente terceros, tales como viviendas, clubes privados, oficinas, almacenes y fábricas, como tampoco cubre los espacios digitales, a efectos de su ausencia física[5]. Sin embargo, el hecho de que sean necesarias unas condiciones para acceder al espacio en cuestión no se traduce a que este no sea de acceso público, por consiguiente, tanto los típicos espacios públicos, como las calles, los

[3] Art. 2 del Tratado de la UE: "La Unión se fundamenta en los valores de respeto de la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías. Los Estados miembros tienen en común una «sociedad caracterizada por el pluralismo, la no discriminación, la tolerancia, la justicia, la solidaridad y la igualdad entre mujeres y hombres¨.
[4] Art.3, Ley de IA
[5] Ibid., Considerando 9

edificios gubernamentales, infraestructuras de transporte y los cines, teatros y tiendas tienen esta consideración[6].

Esto puede crear confusión a la hora de la práctica, por lo que la Ley de IA señala que se debe determinar cada caso de manera particular, para saber si se debe englobar en los espacios de acceso público o no[7].

2.1.2.3. Datos biométricos

Este es uno de los elementos clave para profundizar en el estudio, así, diferentes cuerpos normativos lo definen: por un lado, la Directiva sobre protección de datos en el ámbito penal[8], en su Art. 3.13, afirma que son los "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" (Directiva 2016/680 del Consejo, de 27 de abril de 2016).

La misma formulación se encuentra en el Art.4.14 del Reglamento 2016/679, del 27 de abril de 2016, relativo con la protección de las personas físicas respecto con el tratamiento de datos personales y la libre circulación de estos datos[9], al igual que en el Reglamento 2018/1725 del Parlamento Europeo y del Consejo, del 23 de octubre de 2018, relativo con la protección de las personas físicas respecta con el tratamiento de datos personales por las instituciones, órganos y organismos de la Unión Europea, y a la libre circulación de esos datos[10], además de encontrarse en la Ley de IA[11].

De este modo, su descripción ha evolucionado positivamente, pues, en el Dictamen (en adelante, Dict.) 3/2012 sobre la evolución de las tecnologías biométricas, se define como aquellas "propiedades biológicas, características fisiológicas, rasgos de la

[6] Ibid.
[7] Ibid.
[8] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa con la protección de las personas físicas en lo que respecta con el 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.
[9] Art.4.14 del Reglamento (UE) N°2016/679 del Consejo, de 27 de abril de 2016
[10] Art.3.18 del Reglamento (UE) N°2016/679 del Consejo, de 27 de abril de 2016
[11] Art.3.33, Ley de IA

personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad" (Dict. 3/2012 Consejo de la UE, de 27 de abril 2012, p.3). Sin embargo, desde aquel momento, se comprende el nivel de peligrosidad que supone la captura de estos datos elementales para los derechos de la personalidad[12].

El mismo dictamen presenta ambos lados de la moneda, por un lado, señala las facilidades que ha aportado el desarrollo de estas tecnologías, como adquirir lectores de huellas dactilares en precios asequibles u obtener análisis de ácido desoxirribonucleico (en adelante, ADN) en una rapidez considerable, asimismo, asegura que la discriminación genética y la usurpación identidad han dejado de ser un temor hipotético (Dict. Consejo de la UE, de 27 de abril 2012, p.3).

Uno de los componentes que ha añadido el perfeccionamiento de esta tecnología es la diversificación de los datos aptos de captación. Conforme con la guía de tecnologías biométricas aplicadas a la ciberseguridad de INCIBE, existen las tecnologías biométricas fisiológicas y de comportamiento. Las primeras abarcan el reconocimiento de la huella dactilar, facial, de iris, de la geometría de la mano, de retina, vascular, de líneas de la palma de la mano, de la forma de las orejas, la piel, el ADN y las composiciones químicas del olor corporal, mientras que las tecnologías biométricas de comportamiento son las encargadas del reconocimiento de la firma, escritor, voz, escritura de teclado y forma de andar (INCIBE, 2016, pp.7-12).

2.1.2.4. Identificación biométrica remota y ¨en tiempo real¨

El Reglamento (UE) 2016/679, del 27 de abril de 2016, relativo con la protección de las personas físicas respecto con el tratamiento de datos personales y la libre circulación de estos datos, por el que se deroga la Directiva 95/46/CE (en adelante, RGPD), indica, en su Art. 9.1, cuáles son aquellos datos personales de categoría especial, también denominados datos sensibles[13]. Uno de estos son ¨los datos biométricos dirigidos a identificar, de manera unívoca, a una persona física¨ (RGPD, de 27 de abril de 2016).

[12] Conforme Xavier O´Callaghan, magistrado del Tribunal Supremo jubilado y catedrático de Derecho Civil, los derechos de la personalidad son las manifestaciones inherentes a la persona, reconocidos por su trascendencia e intimidad, tanto física (vida, integridad física) como moral (honor, intimidad, imagen), siendo de interés digno de resguardo (O´Callaghan, 1996, párr.1).

[13] Art.9.1 del RGPD: ¨Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el

Dicha regulación abrió un gran debate, debido a que no se aclaraba si todo tratamiento de datos biométricos debe estar sujeto a la protección estipulada por el Art.9; la Agencia Española de Protección de Datos (en adelante, AEPD) lo ha podido desarrollar en múltiples informes[14], no obstante, se llega a la conclusión de que se estaba frente a un error interpretativo/técnico, por ello, se trae a colación la delimitación entre los términos de "identificación biométrica" y "verificación/autenticación biométrica", ambos definidos en la Directiva 3/2012.

En este sentido, la identificación biométrica es el proceso en el que un individuo es identificado, a través de un sistema característico, por comprar los datos con una serie de plantillas biométricas conservadas en una base de datos, en pocas palabras, un proceso de rastreo. Por su parte, la verificación/ autenticación biométrica es la comprobación de un individuo por un sistema biométrico entre sus datos contra una única plantilla biométrica, es decir, un proceso de detección uno-a-uno (Dict. 3/2012 Consejo de la UE, de 27 de abril 2012, p.6).

La misma delimitación se menciona en el Libro Blanco sobre IA de la Comisión Europea[15], en el Convenio para la Protección de Individuos respecto con el procesamiento de datos personales aprobado por el Comité de Ministros en su núm. 128 [16] y en la Resolución 940/0419 del procedimiento núm. E/03925/2020 de la AEPD, la que indica el amparo de los factores discutidos al afirmar lo siguiente:

---

tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física¨.

[14] Algunos de los escritos más destacados son el informe 36/2020 relativo con el reconocimiento facial de alumnos universitarios para la ejecución de pruebas telemáticas, el informe 47/2021, en materia del reconocimiento por parte de una entidad bancaria, además de la Resolución E/03925/2020 referente con el acceso biométrico en el ámbito laboral.

[15] En la nota de pie núm.56 del Libro Blanco sobre AI sostiene que: en lo que se refiere al reconocimiento facial, por «identificación», se entiende que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella. La «autenticación» (o «verificación»), por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; así, las dos plantillas se comparan para determinar si la persona de las dos imágenes es la misma.

[16] El Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Consejo de Europa, 1981).

> El concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación/autenticación. Sin embargo, y con carácter general, 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 (AEPD, 2020a, p.5).

De esta distinción nace el cuidado añadido a los procedimientos de identificación, es decir, el funcionamiento de este depende de una cantidad de datos significativos para obtener resultados. Por el contrario, los tratamientos de verificación o autenticación biométrica se utilizan, exclusivamente, para confirmar, mediante la comparación pertinente, si dicha persona es la misma de la que proceden los datos biométricos (Veridas, 2022, p.14).

Uno de los mercados que utiliza especialmente el tratamiento de identificación son los asistentes de voz virtuales, estos, conforme con el Comité Europeo de Protección de Datos (en adelante, CEPD) respecto con las Directrices 2/2021, implican el método al que se recurre para la identificación de los hablantes (CEPD, 2021a, p.25). Esta es una cuestión de peso, pues, gracias a la penetración de este tipo de *software* al mercado, se prevé que, para el 2024, se utilicen cerca de 8 400 asistentes que emplean el tratamiento de la voz de cada uno de sus consumidores (Fernández, 2021).

Con esto fijado y con el soporte de la Ley de IA, se entiende como sistema de identificación biométrica remota como aquella IA orientada a la identificación de personas físicas a distancia a través de la comparación de sus datos biométricos con los que integran "una base de datos de referencia, y sin que el usuario del sistema de IA sepa de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada" (Art.3.36, Ley de IA). Asimismo, los sistemas de identificación biométrica remota "en tiempo real" se definen de la misma forma, con la particularidad de que "la comparación y la identificación se producen sin una demora significativa[17]. Este término

[17] Otra figura son los sistemas de identificación biométrica remota "en diferido¨, el art.3.38 de la Ley de AI, lo define como ¨todo sistema de identificación biométrica remota que no sea un sistema de identificación biométrica remota en tiempo real¨ (Art.38, Ley de IA).

engloba no sólo la identificación instantánea, sino también demoras mínimas limitadas, a fin de evitar su elusión" (Art.3.37, Ley de IA).

2.2. MARCO NORMATIVO: LOS DERECHOS FUNDAMENTALES FRENTE A LA IDENTIFICACIÓN BIOMÉTRICA

El informe de la Agencia Europea de los Derechos Fundamentales de la Unión Europea (en adelante, FRA), *Getting the future right - Artificial intelligence and fundamental rights*[18], afirma que el uso de los sistemas de IA siempre pondrá en peligro a una gran diversidad de derechos fundamentales, indistintamente del campo de aplicación, así, los más afectados son la privacidad, la protección de datos, la no discriminación y el acceso a la justicia (FRA, 2021, p.5). Por esta razón, existe la urgente necesidad de regulación respecto con este campo, lo que conforma una de las obligaciones de la Unión Europea y sus Estados miembros.

Esta cuestión de normativa sobrepasa el territorio comunitario, pues los derechos fundamentales son inherentes al ser humano y el uso de esta tecnología es a nivel global. La Organización de las Naciones Unidas (en adelante, ONU) ha podido identificar la rigurosidad de la práctica, creando cuerpos exclusivos para su estudio, como el Grupo de Expertos *ad hoc* de la ONU para la Educación, la Ciencia y la Cultura (en adelante, UNESCO), el que es responsable de adoptar el primer acuerdo mundial sobre la ética de la IA[19], y el Panel de alto nivel sobre cooperación digital de la Secretaría General de la Organización (Drnas, 2022, p.9).

De acuerdo con la Revista de Estudios Jurídicos de la Facultad de la Universidad de Jaén, en su publicación, *Artificial intelligence in international law United Nations and European Union,* estas iniciativas hacia la regularización nacen como consecuencias de un *status* fragmentado. Este está compuesto por la inexiste coordinación y competencia en el sector, lo que es un efecto directo de "la globalización, la transnacionalización, la multiplicidad de redes transfronterizas no reguladas, el incremento del uso de la IA en el

[18] El que realizó su investigación en el terreno de cinco Estados miembros de la Unión Europea: España, Estonia, Finlandia, Francia y los Países Bajos, colectó información de los agentes responsables del diseño y uso de sistema de IA tanto en el sector público como privado (FRA, 2021, p.4).
[19] Titulado ¨Recomendación sobre la ética de la inteligencia artificial¨ y aprobado por los 193 países miembros de la UNESCO, fue adoptada el 23 de noviembre de 2021 y nos proyecta 11 ámbitos en los cuales la IA está implicada (UNESCO, 2021).

ámbito público y privado nacional, internacional y transnacional a nivel planetario" (Drnas, 2022, p.9).

2.2.1. Derecho comunitario

La Unión Europea es consciente de que se está abocado a un futuro sostenible y digital, donde los sistemas de IA participarán, activamente, en un sin número de ámbitos de la vida cotidiana, más de lo que ya intervienen. Esto fuerza, a los juristas a establecer un derecho capaz de comprender las necesidades nuevas y particulares que varían a máxima velocidad (García, 2021, p.305).

Por lo tanto, desde el 2018 comenzaron los actos preparatorios para una regulación efectiva, con el Comunicado de prensa *Artificial intelligence: Commission kicks off work on marrying cutting-edge technology and ethical standards*[20], el lanzamiento de la alianza europea de IA y el Plan coordinado sobre IA. Con el paso del tiempo, en abril de 2021, la Comisión Europea presentó un paquete de IA centrado en la excelencia y la confianza, conformado por un marco jurídico innovador basado en los derechos fundamentales y cuatros niveles de riesgo (Comisión Europea, 2023).

Así, este apartado se enfoca en los componentes del marco jurídico comunitario que están más interconectados con los sistemas de identificación biométrica en espacios públicos y los derechos fundamentales amenazados por el tratamiento.

2.2.1.1. La Carta (UE) 364/01, de 18 de diciembre de 2000 relativo a los Derechos Fundamentales

El marco global de los derechos fundamentales relativos con el uso de la IA en la Unión Europea se redactó en la Carta de los Derechos Fundamentales de la Unión Europea (en adelante, la Carta), juntamente con la Convención Europea de Derecho humanos (FRA, 2021, p.4). La misma pasó a ser jurídicamente vinculante en diciembre de 2009, por lo que tiene el mismo valor jurídico que los Tratados de la Unión Europea, además de que su obligatoriedad se encuentra recogida en su Art.51.1[21], el que vincula a

[20] Este comunicado fue el primer hito importante dentro de la línea de tiempo respecto al enfoque europeo de la IA (Comisión Europea, 2018b).
[21] Art.51.1 de la Carta: ¨Las disposiciones de la presente Carta están dirigidas a las instituciones y órganos de la Unión, respetando el principio de subsidiariedad, así como a los Estados miembros únicamente cuando

todas las instituciones, los órganos y los organismos comunitarios con el respeto de los derechos recogidos en el escrito.

Definitivamente, a la hora de emplear los sistemas de IA, se debe tomar en consideración un gran abanico de derechos, los que deben ser adaptados conforme con la tecnología utilizada y el ámbito aplicable (FRA, 2021). En el campo de aplicación, en el uso por parte de las autoridades públicas de los sistemas de identificación biométrica en espacios de acceso público, se destacan unos más que otros.

Tal como se dicta en las Conclusiones de la Presidencia del Consejo de la Unión Europea, la Carta de los Derechos Fundamentales en el contexto de la IA y el cambio digital[22], en el mundo digital deben aplicarse los mismos grados de protección a los Derecho Fundamentales que en el mundo físico. Por ende, el respeto de la vida privada y familiar (Art.7, la Carta) debe contemplarse en la aplicación de estos sistemas de identificación.

Como se puede observar en el apartado 2.1.2. sobre los Conceptos primordiales, los datos biométricos son datos personales de categoría especial, gracias a su capacidad de identificación de una persona física. Por consiguiente, nace un reto común para cualquier sistema de identificación/autentificación, debido a que los elementos recopilados en la base de datos deben estar protegidos de cualquier trazabilidad que suponga la violación del consentimiento prestado y la privacidad del individuo.

Esta es una de las cuatro brechas de seguridad del lector de huellas y el reconocimiento facial, ambos tratamientos de datos biométricos, de acuerdo con Helena Rifà Pous[23]. La autora asegura que los principales retos de seguridad y privacidad de la biometría son: a) la biometría no es un sistema inequívoco; b) los datos biométricos están más expuesto; c) los rasgos físicos identificativos no pueden modificarse; d) el uso de datos biométricos puede generar problemas de privacidad por la trazabilidad[24] (Subarroca, 2019). En este último punto, se afirma que el nivel de riesgos aumenta

apliquen el Derecho de la Unión. Por consiguiente, éstos respetarán los derechos, observarán los principios y promoverán su aplicación, con arreglo a sus respectivas competencias¨ (Art.51.1, la Carta).

[22] Consejo de la Unión Europea, Conclusiones de la Presidencia - La Carta de los Derechos Fundamentales en el contexto de la inteligencia artificial y el cambio digital, 11481/20, 2020.

[23]Directora del máster interuniversitario de Seguridad de las tecnologías de la información y la comunicación de la Universidad Abierta de Cataluña

[24] Helena Rifà Pous procede a realizar un ejemplo: ¨Si se extiende el uso de los datos biométricos y, por ejemplo, usas tu huella en muchos entornos, una persona con la plantilla de esta huella podría hacer consultas en varias bases de datos donde se haya registrado y saber dónde hemos estado¨ (Subarroca, 2019).

significativamente cuando la captura de datos es a través del registro de imágenes en la vía pública, debido a que se obtiene una traza automatizada de los movimientos realizados.

A pesar de lo señalado posteriormente, la Carta hace referencia al derecho a la protección de datos de carácter personal, como los datos biométricos. Como se consagra en el Art.8, "toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan" (art.8.1, la Carta), además, "estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación" (art.8.2, la Carta).

Asimismo, en el Art.16.1 del Tratado de Funcionamiento de la Unión Europea (en adelante, TFUE), se fija como uno de los principios de la Unión, además de confirmar que el Parlamento Europeo y el Consejo deberán establecer las normas sobre la protección de la persona física en materia de tratamiento de datos de carácter personal, siempre y cuando sea realizado por las instituciones, los órganos y los organismos de la Unión Europea, así como por los Estados miembros[25].

De estas protecciones se pueden extraer puntos significativos para este estudio, por un lado, se asegura que los datos de origen biométrico deben estar, en primera instancia, protegidos y tratados, así, deben estar dirigidos a un sistema leal, una finalidad determinada y a la luz del consentimiento del poseedor de dichos datos, los que pueden ser verificados posteriormente. Todos los Estados miembros de la Unión Europea deben ajustar su actividad conforme con estos requisitos, lo que daría como resultado la protección del derecho a una buena administración[26]. A esto se debe añadir que el respeto de dicha normativa recae en el control de una autoridad independiente (Art.8.3, la Carta), la que se denomina autoridad de protección de datos (en adelante, APD) y se entiende

[25] Art.16.2 del TFUE: ¨El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes¨.

[26] Art.41.2 de la Carta: ¨Este derecho incluye en particular: el derecho de toda persona a ser oída antes de que se tome en contra suya una medida individual que le afecte desfavorablemente, el derecho de toda persona a acceder al expediente que le afecte, dentro del respeto de los intereses legítimos de la confidencialidad y del secreto profesional y comercial, la obligación que incumbe a la administración de motivar sus decisiones¨.

como el organismo público que supervisa la aplicación de la legislación sobre protección de datos, así, existe una en cada Estado de la Unión Europea (Comisión Europea, 2023).

Así, según el Art.52.1 de la Carta[27], únicamente se podrán imponer restricciones al ejercicio de los derechos y libertades consagrado en la Carta cuando sea indispensable, respetando el principio de proporcionalidad, a efectos del interés general o para proteger los derechos y las libertades de los demás, siempre y cuando dichas limitaciones estén fijadas en la ley y satisfagan el contenido esencial de la Carta.

2.2.1.2. Reglamento (UE) 2016/679, de 27 de abril de 2016 relativo con la protección de las personas físicas respecta con el tratamiento de datos personales y la libre circulación de estos datos.

En las conclusiones de la presidencia del Consejo de la Unión Europea 11481/20, se afirma que, con el paso del tiempo, las empresas y los Gobiernos han utilizado los datos personales y la IA cada vez con mayor frecuencia por diferentes motivos, entre ellos, el estudio del comportamiento de los grupos y acercarse a personas integrantes de un grupo determinado. Del mismo modo, sostiene que deben determinarse salvaguardias para garantizar que la aplicación de estos sistemas estén conformes con la legislación en materia de privacidad y protección de datos, en concreto, el RGPD, la legislación nacional y los derechos fundamentales (Consejo de la UE, 2020, p.9).

En mayo de 2018 entró en vigor lo anterior, con la finalidad de resguardar a todos los ciudadanos de la Unión Europea "frente a las violaciones de la privacidad y de los datos personales en un mundo cada vez más basado en los datos, creando al mismo tiempo un marco más claro y coherente para las empresas" (Parlamento Europeo, 2023, p.3). Esto se ha expuesto en el apartado de Conceptos Primordiales, donde se ampara la identificación biométrica como una categoría especial de datos personales siempre y cuando estos revelen lo siguiente:

> El origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos

[27]Art.52.1 de la Carta: ¨Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando 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¨.

biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física (Art.9.1, RGPD).

Por ello, se establece la prohibición genérica a su tratamiento[28], prohibición que se desarrolla en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, así como en el Art.10 de la Directiva 2016/680 sobre protección de datos en el ámbito penal de 27 de abril de 2016. Salvo que concurran algunas circunstancias indicadas en los apartados 2, 3 y 4 del mismo Art. del RGOD, los que son la base normativa de que los Estados miembros puedan desarrollar sus propios mecanismos de identificación biométrica (AEPD, 2020b).

La exoneración de dicha protección se basa, en su mayoría, en el consentimiento, como el supuesto 9.2.a) que lo permite en aquellos escenarios donde el interesado diera su autorización explícita con uno o múltiples fines específicos, así como que sean imprescindibles para proteger intereses vitales del interesado (Art.9.2.c, RGPD), asimismo, cuando es necesario para el cumplimiento de obligaciones y el ejercicios de derechos del responsable del tratamiento en el ámbito laboral (Art.9.2.b, RGPD).

Sin embargo, la excepción que ha creado más discusión y la que va a la par de este estudio es aquella que se encuentra en manos del Estado y no del individuo, esta dicta que se permitirá el tratamiento de datos personales de naturaleza especial cuando sea requerido por lo siguiente:

> 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 (Art.9.2. g, RGPD)[29].

[28] El Art.4.2 del RGPD lo define como: ¨Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción¨ (Art.4.2, RGPD).

[29] Análogamente se encuentra regulado en el Art.6.1. e del RGPD, el que lo expone como uno de los supuestos de la licitud del tratamiento, a efectos de que el ¨el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento¨ (Art.6.1. e, RGPD).

A propósito de lo que se debe entender como interés público esencial, deben tomarse en consideración la Jurisprudencia del Tribunal Europeo de Derecho Humanos (en adelante, TEDH) que, al tenor del Art.8 del Convenio Europeo de Derecho Humanos[30], señala que el tratamiento de la información personal puede afectar el derecho a la privacidad, pero es permisible mientras esté en conformidad con la ley, tenga una finalidad legítima, respete los derechos fundamentales, y sea necesario y proporcionado en una sociedad democrática para alcanzar un objetivo válido.

Algunos de los precedentes destacables, conforme con la guía sobre el Art.8 del Convenio Europeo de Derechos Humanos, en el sector de protección de datos, son el Caso Rotary contra Rumania nº28341/91 del 4 de mayo de 2000[31], S. y Marper contra Reino Unido, N.º 305627/04 del 4 de diciembre de 2008[32], en especial, el Caso Leander contra Suecia, N.º 9248/81 del 26 de marzo de 1987[33], lo que asegura que debe existir un equilibrio entre el interés público esencial y el derecho a la privacidad, aparte de que el concepto de necesidad corresponde con una necesidad social imperiosa, por ello, recae en las autoridades nacionales valorar, en primer lugar, la necesidad de una injerencia determinada. Según el Tribunal, "las autoridades nacionales disponen de un «margen de apreciación» al proceder a dicha evaluación, pero las decisiones de las autoridades nacionales se someten al control de los órganos del Convenio" (TEDH 9248/81, de 26 de marzo, párrafo[34] 67º).

En la misma medida, se tiene la doctrina del Tribunal Constitucional Español, como la Sentencia 292/2000 del 30 de noviembre de 2000, dictada por el Pleno del TC núm. 4 sobre el recurso inconstitucional núm. 1463-2000, y la Sentencia 76/2019 de 22 de mayo de 2019, dictada por el Pleno del TC núm. 4 sobre el recurso inconstitucional núm. 1405-2019, la que proyecta la incertidumbre respecto con la falta de precisión sobre

[30] Art.8.2 del Convenio Europeo de Derechos Humanos: ¨no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás¨ (Art.8.2, TEDH).
[31] TEDH. Caso Rotary contra Rumania nº28341/91. Sentencia de 4 de mayo de 2000.
[32] TEDH. Caso S. y Marper contra Reino Unido, N°305627/04, Sentencia del 4 de diciembre de 2008.
[33] TEDH. Caso Leander contra Suecia N°9248/81, Sentencia del 26 de marzo de 1987.
[34] en adelante, párr.

el concepto de interés público esencial y las garantías que suponen esta práctica. Se concluye que la legitimidad constitucional de la restricción del derecho fundamental a la protección de datos personales no se puede justificar con la afirmación genérica de un interés que no está definido claramente, "tampoco puede aceptarse, por igualmente imprecisa, que se refiere al funcionamiento del sistema democrático, pues también encierra un grado elevado de incertidumbre y puede suponer un razonamiento circular" (STC 76/2019, de 22 de mayo, Fundamento Jurídico[35] 7º).

Concretamente, como lo expresa el informe 0098/2022 de la AEPD, se ha declarado que el derecho a la protección de datos no es ilimitado, aun cuando la Constitución Española (CE) no fije límites específicos ni remita a los Poderes Públicos para su determinación como en otros derechos fundamentales, de este modo, es evidente que estos límites deben ser determinados de manera coherente, respetando los demás derechos fundamentales y los bienes jurídicos protegidos por la misma Constitución, como exige el principio de unidad constitucional (AEPD, 2022, p. 8).

Ahora bien, el RGPD establece principios de la protección de datos de carácter personal, los que deben aplicarse a toda información relativa con una persona física identificable durante el ejercicio de la actividad de una persona jurídica, como la de un Estado. De forma sintetizada, se desarrollan seis pilares en el Capítulo II, algunos de estos se han estudiado posteriormente y son la licitud, la lealtad y la transparencia, la limitación de la finalidad, la minimización de datos, la exactitud, la limitación del plazo de conservación, la integridad y la confidencialidad.

A esto se debe sumar que, en el Capítulo III, se establece un conjunto de derechos para los ciudadanos respecto con sus datos, por lo que se determina la obligación de protegerlos mediante la implementación de mecanismos efectivos para ejercerlos. Estos derechos incluyen transparencia, información, acceso, rectificación, supresión, limitación, oposición, portabilidad, y derechos específicos para la toma de decisiones automatizadas respecto con la elaboración de perfiles (AEPD, 2020b, p.15).

[35] en adelante FJ.

2.2.1.3. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de IA.

Esta es su denominación oficial, así, la Propuesta de Reglamento del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas en materia de IA (en adelante, Ley de IA) fue propuesta, originalmente, por la Comisión Europea en abril de 2021, así, actualmente se encuentra en uno de sus últimos trámites, luego de ser aprobada por la Comisión Europea (World Economic Forum, 2023).

Únicamente se plantea esta directiva, lo que supone exponer el "carácter estratégico y prioritario que entraña la IA para la UE ha quedado de manifiesto en la celeridad con la que se ha presentado por la Comisión Europea un proyecto normativo en la materia" (Gamero, 2021, p.7). Así, se cuenta con la primera legislación europea dirigida, exclusivamente, a la IA, la que aspira a "reforzar la posición de Europa como centro mundial de excelencia en IA desde el laboratorio hasta el mercado, garantizar que la IA en Europa respete nuestros valores y normas, y aprovechar el potencial de la IA para uso industrial" (World Economic Forum, 2023). Sin perjuicio que se encuentre en trámite, se puede encontrar citada en la legislación nacional, como en el Decreto-ley 2/2023, del 8 de marzo, de medidas urgentes de impulso a la IA en Extremadura[36], lo que confirma su finalidad, para reforzar la seguridad y los derechos fundamentales de los individuos y las empresas en el campo de la IA.

La columna vertebral de esta normativa parte de un *risk-based approach,* es decir, es un sistema de clasificación compuesto por niveles de riesgo creados, específicamente, por las aplicaciones de IA[37] (Anexo A) hacia la salud, la seguridad y los derechos fundamentales; el marco abarca los siguientes niveles de riesgo: inaceptables, alto, limitado y mínimo o ningún riesgo. Luego del estudio de múltiples cuerpos normativos y supuestos jurisprudenciales, esta es la primera normativa que regulará los sistemas de identificación biométrica a efectos de sus altos niveles de peligrosidad. La realidad es que sería posible estudiar todos los puntos expuestos en este futuro reglamento, no obstante,

[36] España. Real Decreto-ley 2/2023, de 8 de marzo, de medidas urgentes de impulso a la inteligencia artificial en Extremadura. Boletín Oficial del Estado, 8 de abril de 2023, núm.84, exposición de motivos.
[37] Véase la información facilitada por la Comisión Europea en su publicación, *Regulatory framework proposal on artificial intelligence*. Las citas que se hacen en este trabajo de este texto son de elaboración/traducción propia, dado que la única versión oficial del documento es en inglés.

no se busca una síntesis de esta, sino una respuesta a una actividad que ha traído consecuencias a la sociedad y se encuentra regulada, débilmente, a través de analogías.

El primer detalle que llamó la atención es cómo, desde el Considerando núm.18, se afirma que el uso de sistemas de IA para la identificación biométrica remota en tiempo real[38] en espacios de acceso público, con el objetivo de aplicar la ley, a efectos de la naturaleza de la práctica, infringe particularmente los derechos y las libertades de las personas. Por ende, puede "afectar a la vida privada de una gran parte de la población, provocar la sensación de estar bajo una vigilancia constante y disuadir indirectamente a los ciudadanos de ejercer su libertad de reunión y otros derechos fundamentales" (Considerando 18, Ley de IA). Lo anterior agrava aún más la situación, pues es la celeridad en la manifestación de las implicaciones y la limitada capacidad para efectuar verificaciones o rectificaciones adicionales respecto con estos sistemas en concreto, los que incrementan el riesgo para los derechos y las libertades de los individuos[39].

El aprovechamiento de estos sistemas en espacios de acceso público implica, inevitablemente, el tratamiento de datos biométricos, por lo que las normas de la Ley de IA que prohíben, con algunas excepciones, el empleo dichos sistemas, con base en el Art.16 del TFUE, deben emplearse como *lex specialis*[40] en cuanto las normas sobre el tratamiento de datos biométricos que se plasman en el Art.10[41] de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa con la protección de las personas físicas, esto respecto con el 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 (Considerando 23, Ley de IA).

[38] Este tipo de tratamiento de datos biométrico fue explicado, posteriormente, en el apartado de Conceptos primordiales.
[39] Considerando 18, Ley de IA
[40] Conforme el Diccionario panhispánico del español jurídico (en adelante, DPEJ) significa que es una norma específica con respecto a una más general (DPEJ, s.f.).
[41] Este va de la par con el Art.9 de la RGPD expuesto, el que expone algunas excepciones respecto con la prohibición del tratamiento de categorías especiales de datos biométricos, en este caso, el Art.10 de la Directiva (UE) 2016/680 no afirma que se podrá realizar dicha práctica cuando: a) lo autorice el Derecho de la Unión o del Estado miembro; b) sea necesario para proteger los intereses vitales del interesado o de otra persona física, o c) dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos (Art.10, Directiva 2016/680).

El listado de prácticas prohibidas se indica en el título II y se alude a todos los sistemas de IA que se consideran inapropiados debido a su antinomia irreductible con los valores de la Unión Europea, como aquellos que violan los derechos fundamentales. Las prohibiciones abarcan las prácticas que encierran un enorme potencial para manipular a individuos a través de técnicas subliminales que actúan por debajo del umbral de su conciencia, además del uso de técnicas que explotan las debilidades de colectivos específicos, como menores o personas con discapacidad, con el fin de modificar su comportamiento de manera sustancial, lo que probablemente resultará en deterioración física o psicológica para ellos o terceros[42].

Por lo tanto, el supuesto de este estudio se encuentra especialmente protegido en dos apartados, por un lado, en el Art.5.1.d) que hace referencia a la prohibición del uso de sistemas de identificación biométrica remota, en tiempo real, en espacios de acceso público a efectos de adoptar la ley, a excepción de que sea absolutamente necesario para lograr uno o varios de los siguientes objetivos: i) la búsqueda selectiva de posibles víctimas concretas de un delito[43]; ii) 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; iii) la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido un delito en concreto (art.5.1.d, Ley de IA).

Estos delitos son expuestos por el mismo apartado, iniciando por aquellos exhibidos en el Art.2.2 de la Decisión Marco 2002/584/JAI del Consejo, del 13 de junio de 2002, relativa con la orden de detención europea y los procedimientos de entrega entre Estados miembros. Algunos de los 32 delitos regulados son la pertenencia a una organización delictiva, el terrorismo, la trata de seres humanos, la explotación sexual de los niños y la pornografía infantil, el tráfico ilícito de armas, municiones y explosivos, la corrupción, el blanqueo del producto del delito, entre otros[44] (Art.2.2, Decisión Marco 2002/584/JAI). Además, se podrá exonerar esta prohibición cuando el delito cometido,

[42] Véase de forma más detallada en la Exposición de motivos de la Ley de IA, en su apartado 5.2 respecto con la explicación detallada de las disposiciones específicas de la propuesta.
[43] Incluidos menores desaparecidos, conforme el art.5.1. d) de la Ley de IA
[44] Para observar todos los supuestos observe el art.2.2 de la Decisión Marco 2002/584/JAI

para el que la normativa está en vigor en el Estado implicado, suponga imponer una pena o medida de seguridad privativas de libertad, cuya duración mínima sea de tres años.

Para el uso de estos sistemas de identificación biométrica en los supuestos presentados, se deberán tomar en cuenta los aspectos del Art.5.2, los que se traducen al hecho de que se deberá analizar cada caso en concreto. Por un lado, se determinará la naturaleza de la situación en cuestión, incluyendo la gravedad, la probabilidad y la magnitud del perjuicio que pudiera resultar en caso de no recurrir a dicho sistema, del mismo modo, se deberán evaluar las consecuencias del uso del sistema sobre los derechos y las libertades de las personas afectadas, incluyendo la naturaleza de las posibles consecuencias, y la probabilidad y la magnitud de su ocurrencia (art.5.2, Ley de IA). Además de ello, las autoridades públicas estarán obligadas a cumplir las salvaguardias, especialmente, en cuanto a las restricciones en el tiempo, lugar e individuo perjudicado.

Cobra una importancia particular el fondo del apartado tres, pues, gracias a este, el uso de sistemas de identificación biométrico en el ámbito remoto y en tiempo real se verá supeditado al otorgamiento de una autorización previa "por parte de una autoridad judicial o una autoridad administrativa independiente del Estado miembro donde vaya a utilizarse dicho sistema, que la otorgarán previa solicitud motivada y de conformidad con las normas detalladas del Derecho interno" (art.5.3, Ley de IA). Dicha autoridad judicial o administrativa concederá únicamente la autorización si se demuestra, mediante pruebas objetivas o indicios claros, que el uso del sistema de identificación biométrica es necesario y proporcional para lograr uno de los objetivos indicados en la solicitud.

En tal marco, el derecho interno al que se refiere se desarrolla en el apartado cuatro que vincula a los Estados miembros respecto con la posibilidad de autorizar, sea total o parcialmente, el uso de esta IA. A tal efecto, se tendrán que establecer normas internas que detallarán todo el cuerpo de la solicitud, la concesión y el ejercicio de las autorizaciones, juntamente con los mecanismos de supervisión pertinentes. Por consiguiente, especificarán cuáles de los escenarios enumerados en el apartado 1, letra d), se podrán autorizar y, si procede, cuáles delitos indicados en su inciso iii) se perseguirán (art.5.4, Ley de IA).

Los puntos mencionados han suscitado una intensa controversia centrada en las críticas de esta futura legislación, así, durante el XIX Congreso de la Asociación de Constitucionalistas de España (en adelante, ACOES) celebrado en Madrid el 24 y 25 de marzo del 2022, se tocaron estos temas de conflicto, tales como el reducido nivel de control, la falta de medidas específicas que vayan de la mano con la velocidad de la tecnología, sobre todo, que las protecciones planteadas por la Ley de IA no están exentas de riesgos respecto con la vulneración de los derechos fundamentales (Gallego, 2022).

En su publicación titulada "Seguridad e igualdad en la utilización de los sistemas de identificación biométrica en remoto por parte de los cuerpos y fuerzas de seguridad del Estado en tiempos de pandemia", se argumenta que la propuesta de reglamento sea más prolija/pulcra, pues existe un riesgo de sufrir inconvenientes "en cuanto a su aprobación en el desarrollo del apartado 4 en el que se establece que los Estados miembros podrán decidir contemplar la posibilidad de autorizar… que a tal fin, tendrán que establecer en sus respectivos Derechos internos¨ (Gallego, 2022, p.18).

Un hecho alarmante, desde el punto de vista de este estudio, es la autonomía que se le otorga al Estado: por un lado, este será el responsable de crear la ley interna que permitirá la autorización o la prohibición de dichos sistemas de identificación biométrica, lo que podría traducirse, con el paso del tiempo, en un alto de nivel de incoherencia entre la legislación interna y comunitaria. Sin embargo, aún más inquietante resultan aquellos supuestos que no van a necesitar la autorización previa para poner en práctica sus servicios, con base en una urgencia debidamente justificada, hasta tal punto que podrá solicitar la autorización después de su utilidad (art.5.3, Ley de IA)[45], lo que podría suponer la vulneración de los derechos fundamentales, a efectos de que ninguna autoridad realizara la revisión conveniente.

Esta exclusión de la norma general resulta particular, pues el CEPD y el Supervisor Europeo de Protección de Datos (en adelante, SEPD) han adoptado una postura más rigurosa en cuanto a la regulación de los sistemas biométricos, conforme con

[45] El Considerando 21 es el único apartado que profundiza este supuesto excepcional describe dicha situación de urgencia debidamente justificada con ¨aquellas en las que la necesidad de utilizar los sistemas en cuestión sea tan imperiosa que imposibilite, de manera efectiva y objetiva, obtener una autorización antes de iniciar el uso¨ (Considerando 21, Ley de IA).

el Dict. conjunto 5/2021 sobre la propuesta. En este, se analiza la propuesta en detalle, sin embargo, conviene resaltar su perspectiva respecto con la identificación biométrica remota de individuos en espacios de acceso público, debido a que lo describe como una actividad de alto riesgo de intromisión en la vida privada de las personas, por lo que se exhorta un enfoque estricto y detallado (CEPD, 2021b).

De acuerdo con la fuente citada[46], se indica que la situación podría ser más preocupante de lo inicialmente estimado y se presentan problemas de proporcionalidad, discriminación y una base normativa frágil, lo que conlleva una consecuencia irreversible "sobre la expectativa (razonable) de la población de anónima en los espacios públicos, lo que se traduce en un efecto negativo directo sobre el ejercicio de la libertad de expresión, de reunión, de asociación y de circulación" (CEPD, 2021b, p.11)

Al tiempo, cabe cuestionarse ¿qué ocurre con los sistemas de identificación biométrica que no buscan la aplicación de la ley? El resto simplemente tienen otras finalidades, como el estudio del comportamiento de las personas o la creación de perfiles sociológicos. En este caso, se está ante la protección otorgada a las actividades de alto riesgo localizadas en el Art.6 del Título III de la misma Ley de IA; esta dicta que se considerará un sistema de IA de alto riesgo cuando reúna las siguientes condiciones: a) está orientado a ser utilizado como componente de seguridad de uno de los productos contemplados en la legislación de armonización de la Unión que se indica en el Anexo II ; b) conforme con la legislación de armonización de la Unión que se indica en el Anexo II, deberán ser objeto de una evaluación de conformidad efectuada por un organismo independiente para la introducción en el mercado o la entrada en servicio (art.6.1, Ley de IA).

Como se puede evidenciar en el Anexo II, la identificación biométrica y la categorización de personas físicas, concretamente, los sistemas de IA destinados a utilizarse en la identificación biométrica remota «en tiempo real» o «en diferido» de personas físicas son considerados de alto riesgo[47]. Desde un enfoque utilitario, el

[46] Las citas textuales que se hacen en este trabajo de este texto son de elaboración/traducción propia, dado que la versión oficial del documento es en inglés.
[47] Podrá observar en el Anexo B, a través de una tabla, la protección de los sistemas biométricos en la propuesta de reglamento de formar sintetizada.

Considerando 54 garantiza que, en estas condiciones, las autoridades públicas que habiliten IA de alto riesgo "para su propio uso pueden aprobar y aplicar las normas que regulen el sistema de gestión de la calidad en el marco del sistema de gestión de la calidad adoptado a escala nacional o regional, según proceda" (Consideración 54, Ley de IA).

2.2.2. Derecho interno

El Gobierno de España, dirigido por la Secretaría de Estado de Digitalización e IA perteneciente al Ministerio de Asuntos Económicos y Transformación Digital (en adelante, MINECO), y la Comisión Europea presentaron, el 27 de junio de 2022, el proyecto piloto para poner la marcha el primer *sandbox*[48] regulatorio de la Unión Europea sobre IA (MINECO, 2022). En este acto, se coloca a España como un Estado miembro pionero y colaborativo respecto con el procedimiento de digitalización de la regulación de la IA. Durante la partición, Thierry Breton, el Comisario europeo de Mercado Interior y Servicios, ha deseado "felicitar a España por ser el primer país que ha decidido invertir parte de su Fondo de Recuperación y Resiliencia para poner en marcha este ambicioso primer piloto de un recinto de seguridad para la IA en Europa" (Gobierno de España, 2022b, p.1).

Asimismo, se puede apreciar este interés en la España Digital 2026, donde se restaura el compromiso por parte del Estado; en esta agenda, se afirma que la IA es una herramienta de gran potencial para la sociedad y la economía. Se debe destacar la Estrategia Nacional de IA (en adelante, ENIA), pues su puesta en marcha ha sido la responsable de iniciativas de gran importancia para el tratamiento de datos. En materia de un marco normativo ético, se ha emitido la Carta de Derechos Digitales[49] y se ha creado el Consejo Asesor de la IA (Gobierno de España, 2022a).

La Carta de Derechos Digitales no es de naturaleza normativa, sino que busca reconocer los nuevos desafíos en la aplicación e interpretación de los derechos en el

[48] El MINECO lo define como ¨un espacio controlado de pruebas que permite la realización controlada y delimitada de pruebas dentro de un proyecto que puede aportar una innovación financiera de base tecnológica aplicable en el sistema financiero, de forma que pueda dar lugar a nuevos modelos de negocio, aplicaciones, procesos o productos, y contribuir a la mejor comprensión de la transformación digital¨ (MINECO, s.f).

[49] Está compuesta por una estructura de 27 derechos, agrupados en seis categorías: 1) Derechos y libertades en el entorno digital; 2) Derecho de igualdad; 3) Derechos de participación y de conformación de espacios públicos; 3) Derechos del entorno laboral y empresarial; 4) Derechos del entorno laboral y empresarial; 5) Derechos digitales en entornos específicos; 6) Garantías y Eficacia (Gobierno de España, 2021).

entorno digital, además de plantear principios[50] y políticas relacionadas con ellos en ese contexto (Gobierno de España, 2021). No obstante, se presenta una exposición detallada de los derechos que se encuentran íntimamente vinculados con los sistemas de identificación biométrica en áreas públicas, el respeto a la privacidad, y la proliferación de tecnologías emergentes en espacios públicos que son adoptadas por las autoridades gubernamentales.

Uno de ellos es el derecho de la persona a no ser localizada y perfilada, este afirma que la localización, los sistemas de análisis de personalidad o conducta que consistan en la toma de decisiones automatizadas[51] o el perfilado de individuos o grupos de individuos "únicamente podrán realizarse en los casos permitidos por la normativa vigente y con las garantías adecuadas en ella dispuestas" (Gobierno de España, 2021, p.9).

Además, se le dedica un apartado a la función de las autoridades, este es llamado "Derechos digitales de la ciudadanía en sus relaciones con la Administración Pública" (Gobierno de España, 2021, p.19). En este, se sostiene que sobre el Estado recae la obligación de garantizar la capacidad de comprobar la identidad legal en el contexto digital, lo que conlleva una administración pública basada en tecnologías de reconocimiento biométrico sofisticadas y confiables (Veridas, 2022).

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

La CE es pionera de la protección de las personas físicas en este campo, así, el tratamiento de datos personales es considerado un derecho fundamental por el Art.18.4 que dispone que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" (art. 18.4 CE).

[50] Asimismo, se han incluido muchas de estas cuestiones, en términos generales para los sistemas de IT, en la Recomendación sobre la ética de la IA adoptada en París del 9 al 24 de noviembre de 2021 por UNESCO (UNESCO, 2021).

[51] Esta es una de las características clave de los sistemas de identificación biométrica, con base en una IA completamente automatizada, al igual que el perfilado de un individuo en concreto, en especial, en el ámbito penal.

Por otro lado, la Sentencia 94/1998, del 4 de mayo, hace referencia a la Sentencia 254/1993 que asume la declaración de que el Art.18.4 de la Constitución Española añade una protección adicional a los derechos y las libertades fundamentales, en particular, en relación con el derecho al honor y la intimidad; la interpretación jurisprudencial señala lo siguiente:

> La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático, *habeas data*[52], y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (STC 94/1998, de 4 de mayo, FJ. 4º).

A continuación, la sentencia hace referencia a la normativa que desarrolla lo establecido en el Art.18.4 de la Constitución Española y destaca, como un principio cardinal de la protección de datos, la necesidad de que su uso sea congruente y racional, con una protección reforzada de los datos sensibles. Además, la sentencia prohíbe taxativamente, de manera explícita, el uso de estos datos para fines distintos a los que motivaron su obtención legítima y reconoce una tutela especial para los datos sensibles (STC 94/1998, de 4 de mayo, FJ. 4º).

Estos puntos se adaptan al ordenamiento jurídico en la Ley Orgánica 3/2018, del 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales[53] (en adelante, LOPDGDD), al igual que el RGPD. Conforme con dicha ley, el derecho fundamental recogido en el Art.18.4 se ejercerá con arreglo al RGPD y garantizará los derechos digitales de la ciudadanía que nacen de dicha protección (Art.1, LOPDGDD).

Por lo tanto, se encuentran las mismas protecciones que el RGPD y no se busca ser reiterativos, no obstante, es significativo señalar los artículos (en adelante, Arts.) que protegen los puntos de mayor relevancia, como el Art.9 que hace referencia a las

[52] La misma jurisprudencia lo define, en otras palabras, se puede comprender como el ¨Derecho a la propia intimidad informática, que confiere a su titular un derecho de control sobre los datos (acceso, rectificación y cancelación de los mismos), interviniendo el Estado en su protección y tutela con agencias o comisarios para la protección de los datos (DPEJ, s.f.).

[53] El Boletín Oficial del Estado ha publicado el 9 de mayo de 2023 una modificación de esta Ley Orgánica titulada Ley 11/2023, de 8 de mayo, de trasposición de Directivas de la Unión Europea en materia de accesibilidad de determinados productos y servicios, migración de personas altamente cualificadas, tributaria y digitalización de actuaciones notariales y registrales, no obstante, las cuestiones modificadas no son objeto de estudio (AEPD, 2023).

categorías especiales de datos, como los biométricos. En este apartado, a efectos del Art.9.2.a) del RGPD, se refuerza la protección al objeto de evitar situaciones discriminatorias, "el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico" (Art.9.1, LOPDGDD).

Por ello, el tratamiento de dichos datos quedará bajo el amparo de los restantes supuestos contemplados en el Art.9.2 del RGPD (Art.9.1, LOPDGDD) de estos; es relevante mencionar el apartado g) por razones de un interés público esencial y el i) por razones de interés público en el ámbito de la salud pública.

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

Otra disposición legal de fecha reciente y la primera regulación positiva del uso de la IA por las administraciones públicas y las empresas en España (Guervóz, 2022, p.49) es la Ley 15/2022 del 12 de julio, integral esta para la igualdad de trato y la no discriminación (Ley 15/2022). Según María Ángeles Guervós, en su libro "Fiscalidad de las *smart cities*"[54], se está ante una regulación programática y voluntarista que elabora las líneas de actuación de las administraciones públicas, para poder favorecer, promover y priorizar aquellas políticas y prácticas ligadas con el uso de algoritmos involucrados en la toma de decisiones (Guervós, 2022, p.49).

En el marco de esta normativa, cabe resaltar el Art.23, este se refiere específicamente a la IA y los sistemas de toma de decisiones automatizadas, asimismo, se menciona que, dentro de la perspectiva del marco de la Estrategia Nacional de IA de la Carta de Derechos Digitales y las iniciativas europeas en torno a la IA, la Administración Pública española deberá fomentar la implementación de medidas que permitan que los algoritmos utilizados en la toma de decisiones en las instituciones públicas consideren criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea viable desde una perspectiva técnica (art.23.1, Ley 15/2022).

[54] También llamadas ciudades inteligentes, son aquellas ¨en las que se aplican las tecnologías de la información y de la comunicación con el objetivo de proveerlas de infraestructuras que garanticen: un desarrollo sostenible, un incremento de la calidad de vida de los ciudadanos, una mayor eficacia de los recursos disponibles y una participación ciudadana activa¨ (Fundación Endesa, s.f.).

Dichas medidas incluirán el diseño[55] de los algoritmos y los datos utilizados para entrenarlos, así, deberán abordar su probable repercusión discriminatoria. Para alcanzar este último objetivo, se llevarán a cabo evaluaciones de impacto que identifiquen cualquier sesgo discriminatorio potencial (art.23.1, Ley 15/2022), de igual modo, se exige a las administraciones públicas y a las empresas promover el empleo de una IA "ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido" (art.23.2, Ley 15/2022), lo que se verificará a través de un sello de calidad de los algoritmos (art.23.4, Ley 15/2022).

2.3. JURISPRUDENCIA DESTACABLE

La jurisprudencia consolidada hace referencia a conflictos de esta índole en todos los aspectos, por las actuaciones de las entidades privadas y el de las autoridades públicas, por ello, se consideran relevantes aquellas en el ámbito comunitario que tratan sobre dicha cuestión, para comprender el nivel de sensibilidad de la utilidad/recopilación de datos biométricos. Algunas a destacar son aquellas del Tribunal de Justicia de la Unión Europea (en adelante, TJUE), como la Sentencia de 13 de mayo de 2014, *Google Spain,* S.L. y Google Inc. contra AEPD y Mario Costeja González[56], y la Sentencia de 6 de octubre de 2015, *Data Protection Commissioner* contra *Facebook Ireland Limited* y Maximillian Schrems[57].

A su vez, el TEDH ha creado un valioso apoyo jurisprudencial para la data biométrica, en especial, respecto con la obtención de muestras celulares, perfiles del ADN, huellas dactilares, huellas palmares y muestras de voz, lo que se encuentra desarrollado en la *Guide to the Case-Law of the European Court of Human Rights, Data protection, Genetic and biometric data* (TEDH, 2022, pp.12-14). Analizar el papel que cumple el Estado para la protección de estos derechos es primordial, de este modo, gracias a la jurisprudencia, se evidencia desde en la *praxis* cuáles son las exigencias y los

[55] Respecto con el diseño, el apartado segundo dicta que ¨las administraciones públicas, en el marco de sus competencias en el ámbito de los algoritmos involucrados en procesos de toma de decisiones, priorizarán la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos¨ (art.23.2, Ley 15/2022).
[56] TJUE. *Google Spain,* S.L. y Google Inc. contra AEPD y Mario Costeja González (C-131/12). Sentencia de 13 de mayo de 2014.
[57] TJUE. *Data Protection Commissioner* contra *Facebook Ireland Limited* y Maximillian Schrems (C-311/18). Sentencia de 16 de julio de 2020.

resultados de los proyectos que se han puesto como meta el tratamiento masivo de datos biométricos en espacios de acceso público.

2.3.1. Esfera nacional

La jurisprudencia española ha sido firme respecto con el derecho fundamental a la protección de datos, en especial, al derecho de autodeterminación informativa, el que, en esencia, se trata de la capacidad de una persona para ejercer su control sobre los datos personales que posee y decidir qué información compartir con terceros, sea con el Estado o con individuos privados, así como determinar qué datos pueden ser recopilados por dicho tercero, además de saber, con exactitud, quién posee dichos datos y cuál será su uso, con el fin de oponerse a dicha posesión o uso (STC 292/2000, de 4 de enero, FJ. 7º).

Por lo tanto, estos poderes de control y disposición sobre los datos personales, que forman parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la capacidad de dar consentimiento a "la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular" (STC 292/2000, de 4 de enero, FJ. 7º) .

En el siguiente supuesto, la jurisprudencia fija una serie de estándares sobre el tratamiento de datos biométricos, concretamente, los adquiridos de la huella fácil de los perjudicados. Indiferentemente de que este tratamiento se realice por una entidad privada, el lugar de su aplicación es considerado un espacio de acceso público conforme con la Ley de IA, por lo que requieren las mismas prohibiciones si fuera realizado por las autoridades públicas.

2.3.1.1. Auto de la Audiencia Provincial de Barcelona 1448/2021, Sección 9ª, Auto 72/2021 de 15 Feb. 2021, Rec. 840/2021

La reconocida sociedad mercantil, Mercadona S.A., presenta el 6 de mayo de 2019 un escrito que manifestaba la intención de implementar un sistema de vigilancia en sus supermercados, para poder realizar el reconocimiento facial de aquellas personas con sentencias firmes y órdenes de alejamiento en vigor contra Mercadona o sus empleados. Dicha solicitud fue denegada por el Juzgado de lo penal núm. 24 Barcelona en el auto en

fecha 27 de septiembre de 2019, a efectos de su desproporcionalidad, razón por la cual en fecha 25 de noviembre de 2020, la mercantil presenta recurso de apelación resuelta en la Sentencia de la Audiencia Provincial (en adelante, SSAP) de Barcelona 1448/2021[58].

No obstante, a causa del aprovechamiento de este sistema piloto de reconocimiento facial en múltiples sucursales, el cual inició el 1 de julio de 2020 y se practicó durante varios meses, se presentaron dos reclamaciones, una el día 15 de julio de 2020, número de registro 025103/2020, de la Asociación de Consumidores y Usuarios en Acción-Facua, otra el 27 de julio de 2020, número de registro 026511/2020, procedente de Apedanica, por lo que inició el procedimiento sancionador de AEPD PS/00120/2021.

Tanto en la revisión del tribunal como en el procedimiento sancionador, se afirma que la aplicación de esta IA es un tratamiento desproporcionado. A simple vista, resulta un tratamiento excesivo, debido a que para hacer eficaz una medida de seguridad para un número limitado de personas, en este caso solo dos personas, por un periodo limitado y establecido en sentencia, que no podrá exceder de seis meses al tratarse de un delito leve (art. 57.3 del Código Penal), se podrían monitorear a un colectivo de más de 100.000 trabajadores y 1.624 establecimientos para la fecha (AEPD, 2021, p.84).

El Mercadona argumenta que no existe un tratamiento de datos, ya que, lleva a cabo la identificación en tiempo real y elimina en 0,3 segundos toda la información, solo utilizando resultados positivos para contactar a las autoridades en caso de detección. Esto dentro del análisis es insignificante, en palabras del tribunal, “resulta, no obstante, cuanto menos sorprendente que se amparen en la "rapidez". Por muy rápido que sea, existe una violación de la privacidad. Tanto el argumento de la rapidez como el no tratamiento de datos caen por su propio peso” (SSAP 1448/2021, de 15 de febrero, FJ. 2º).

A efectos de su alta complejidad, la sentencia realiza un acercamiento doctrinal a la AEPD en su informe 36/2020. Gracias a su interpretación, se reafirma que el uso de tecnologías de reconocimiento facial en sistemas de videovigilancia implica el tratamiento de datos biométricos que tienen como objetivo identificar de forma única a una persona física, este tipo de tratamiento de datos constituye una categoría especial que,

[58] La fuente de este apartado será exclusivamente la jurisprudencia en cuestión y el proceso sancionador por parte de la AEPD, en el caso de que no, será indicado adecuadamente en el texto.

en principio, está prohibido por el art. 9.1 del RGPD. Se establece de manera explícita que "para tratar categorías especiales de datos con estos fines, la normativa requiere que exista un interés público esencial recogido en una norma con rango de ley que no existe actualmente en el ordenamiento jurídico" (SSAP 1448/2021, de 15 de febrero, FJ. 2º). En otras palabras, para que el reconocimiento facial tenga las mínimas garantías, debe existir una protección legal específica, la cual no existe en nuestro ordenamiento jurídico.

Conforme a lo anteriormente expuesto, se establece que el Mercadona a través de este proyecto piloto ha infringido un número significativo de normas, como el art.6 del RGPD relativo a la licitud del tratamiento de datos personales, el art.5.1.c) referente del principio de minimización de datos y el art.9 anteriormente expuesto. Por consiguiente, se desestima el recurso de apelación, se confirma íntegramente el Auto de fecha 27 de septiembre de 2019, dictado por el Juzgado de lo Penal N.º 24 de Barcelona y se le sanciona con el pago de 3,15 millones de euros, los cuales luego fueron reducidos a 2.520.00 € por pago voluntario.

2.3.2. Esfera Internacional

En diversos países democráticos, se observa que la implementación de sistemas biométricos de identificación está dirigida, en gran medida, a aplicaciones relacionadas con la seguridad pública (Lorenzo, 2022). A partir de la observación de la práctica, se desprende que el rendimiento de dichas tecnologías ha sido limitado y perjudicial para los derechos fundamentales.

Algunos ejemplos implican el uso del *software* Videmo 360 por parte de la policía de Hamburgo, Alemania. Para ejemplificar la amplitud de las intromisiones en la privacidad que estos "programas piloto" pueden abarcar, durante la reunión del G20 en 2018, la Agencia de Protección de Datos de Hamburgo (en adelante, HmbBfDI) descubrió que la policía de Hamburgo había recolectado, aproximadamente, 17 terabytes[59] de imágenes y videos que se procesaron a través de tecnología de reconocimiento facial automatizado (European Digital Rights, 2021).

[59] Por lo general, un terabyte equivale a unos 1.000 GB o un billón de bytes.

Preocupantemente, a través de la utilización de este *software* adquirido, se procedió a procesar, de manera biométrica, la totalidad de los rostros de las personas que aparecían en el vasto material de videos e imágenes, sin excepción alguna. Dicho *software*, mediante la lectura de las características destacadas del rostro humano, generó y almacenó modelos matemáticos en forma de plantillas de rostros que podían ser consultados y comparados (HmbBfDI, 2018a).

A través de la Orden de acuerdo con el Art.6 de la Ley de Hamburgo sobre la supervisión de la aplicación de la regulación emitida para la implementación de la Directiva 2016/680 (HmbRI (EU)2016/680UmsAAG), se detectó que esto se había llevado a cabo sin una base legal adecuada[60], lo que violentó el derecho a la autodeterminación informativa y la protección de datos personales (HmbBfDI, 2018b).

Otras iniciativas fracasadas fueron puestas en funcionamiento en el año 2017, cuando las autoridades federales alemanas anunciaron un proyecto piloto para probar la tecnología de vigilancia de reconocimiento facial en la estación de tren de Südkreuz en Berlín, la que es ampliamente utilizada (Ministerio Federal del Interior, Construcción y Patria de Alemania, 2018). Dicho proyecto se extendió lo suficiente, por lo que, para noviembre del 2020, aproximadamente 79 cámaras fijas de la policía estatal estaban en funcionamiento en el espacio público del centro de Colonia, Alemania, utilizando sistemas de identificación biométrica facial (Kameras stoppen, 2020).

Esto creó un gran revuelo dentro de la sociedad y un rechazo significativo por parte de la misma, por ende, el 18 de enero de 2021 se dictó la Sentencia 20 L 2340/19 del Tribunal Administrativo de Colonia, esta exigió detener inmediatamente la videovigilancia de la Plaza Breslauer y sus calles laterales en Colonia, siendo esta una de las más observadas por la policía (Tribunal Administrativo de Colonia, 20 L 2340/19), a efecto del quebrantamiento del derecho a la autodeterminación informática y la vida privada. Así, dejó en manifiesto que “debe interpretarse, de manera restrictiva, a la luz de la justificación de la ley y debido a las importantes violaciones de los derechos

[60] Tanto las citas textuales como las parafraseadas que se hacen en este trabajo respecto con la jurisprudencia alemana son de elaboración/traducción propia, dado que la versión oficial se encuentra en alemán.

fundamentales que van de la mano con el monitoreo y la grabación de vídeo" (Tribunal Administrativo de Colonia, 20 L 2340/19, FJ. 20º).

La situación es altamente inquietante, de este modo, el 16 de abril de 2021, el Garante italiano de la protección de datos (en adelante, GPDP) determinó que el *Sistema Automatico di Riconoscimento Immagini*, utilizado desde 2019 por la Policía Científica italiana, era inadmisible, debido a la escasez de transparencia y su característico proceso de alimentación de imágenes que ronda los 16.000.000 (Rita, 2021). Sumado con esto, el GPDP publicó la Orden judicial contra Clearview AI del 10 de febrero de 2022 (9751362), imponiendo una multa de 20.000.000 de euros a la empresa estadounidense, por haber implementado un seguimiento biométrico de personas en el territorio italiano, violado los principios que conciernen con la transparencia, debido a la falta de información adecuada proporcionada a los usuarios, las restricciones en cuanto a la finalidad del tratamiento de datos, el uso de los datos de los usuarios para propósitos diferentes a los que fueron publicados originalmente en línea y las limitaciones en cuanto a la retención de dichos datos (GPDP, 2022).

2.3.2.1. Sentencia de la Corte de Apelaciones de Inglaterra y Gales sobre tecnología de reconocimiento facial. *R (Bridges) v-Chief Constable of South Wales Police & Others.* Caso N° C1/2019/2670

Este recurso de gran trascendencia[61] estudia la legalidad del uso de la tecnología de reconocimiento facial automatizado, concretamente el sistema denominado *AFR Locate,* parte de la Policía de Gales[62]. El funcionamiento de la tecnología es simple, gracias al despliegue de cámaras de vigilancia, se captan imágenes digitales de los ciudadanos de Reino Unido en espacios públicos, que luego son procesadas y comparadas con la base de datos.

El mismo se caracteriza por su extracción de data biométrica de manera automatizada, utilizando el *software* NeoFace Watch, lo cual implica la recogida, el tratamiento y el almacenamiento de una amplia variedad de información delicada, tales

[61] La importancia de este caso reside en que se trata del primer caso de éxito en la lucha en contra de la tecnología de reconocimiento facial en el Reino Unido (Consejo para la Transparencia, 2022).
[62] La fuente de este apartado será exclusivamente la jurisprudencia en cuestión, en el caso de que no, será indicado adecuadamente en el texto. Sentencia de la Corte de Apelaciones de Inglaterra y Gales sobre tecnología de reconocimiento facial. *R (Bridges) v-Chief Constable of South Wales Police & Others,* de 11 de agosto del 2020. Caso N°C1/2019/2670.

como 1) Imágenes faciales; 2) Rasgos faciales; 3) Metadatos biométrico incluyendo la hora y ubicación asociados; 4) Información sobre coincidencias con la lista de vigilancia[63], para la fecha la lista contenía la imagen de 400-500 personas, que estaban siendo buscadas por diferentes razones, por orden judicial, por encontrarse ilegalmente en libertad, personas desaparecidas o vulnerables.

En septiembre del 2019, Edward Bridges, con el apoyo de Liberty, conocida organización independiente de defensa de las libertades civiles, se interpone una acción de *judicial review proceeding*[64], por el uso de esta tecnología en dos oraciones en concreto y su continuidad por parte de las autoridades. Los motivos son la incompatibilidad con el derecho a la vida privada, la legislación nacional sobre protección de datos y la Ley de Igualdad del Sector Público.

Uno de los puntos claves para la comprensión del caso, es la recopilación excesiva de datos, en estas dos ocasiones, 21 de diciembre del 2017 y 27 de marzo del 2018, alrededor de 500.000 rostros fueron escaneados y "la inmensa mayoría de las personas cuyos datos biométricos son capturados y procesados por la policía de gales mediante *AFR Locate* no son sospechosas de ningún delito ni presentan ningún otro interés para la policía" (Tribunal Administrativo, 2020, párr. 16). A esto se le debe sumar el preocupante número de falsos positivos por parte del programador, durante estos despliegues se produjeron 290 alertas, de las cuales 82 fueron verdaderos positivos y 208 falsos positivos, siendo estas las cifras de únicamente las alarmas, por lo que el resto de las personas que fueron analizadas biométricamente es un número desconocido (Tribunal Administrativo, 2020, párr. 187).

En primera instancia se estableció que, a pesar de que la tecnología de *AFR Locate* amenazaba los derechos a la privacidad y a la protección de datos de las personas escaneadas, el Estado contaba con un marco legal lo suficientemente capacitado para el aprovechamiento de esta tecnología, se determinó que la utilización de esta tecnología con el objetivo de recopilar información biométrica de la población se realizaba dentro

[63] Tómese en consideración que el escrito original viene únicamente en inglés, por lo que, las citas textuales y parafraseadas son de elaboración/traducción propia.
[64] Revisión Judicial

de las competencias asignadas a la policía para prevenir y descubrir actividades delictivas (Consejo para la Transparencia, 2022).

No obstante, luego de un exhaustivo análisis por parte de la Corte de Apelaciones en la división administrativa, se anula el fallo a primera instancia, dictando que el uso de esta tecnología en espacios públicos si conlleva la vulneración de la normativa. Por un lado, se aprecia la transgresión hacia el Art.8 del Convenio Europea de Derecho Humanos, el cual hace referencia del derecho a la vida privada y familiar, ya que se incumple uno de los principios respecto la protección de datos, que el tratamiento de datos personales para cualquiera de los fines policiales sólo se considerará lícito si se ataña a la ley y a) el interesado ha dado su consentimiento o b) el tratamiento es necesario para el cumplimiento de una misión en concreto (Tribunal Administrativo, 2020, párr. 101).

Del mismo modo, se señala el incumplimiento del *Data Protection Act 2018*[65], pues que no se evaluaron adecuadamente los riesgos que estarían enfrentando los derechos y libertades de los individuos, además de no fijar medidas para los supuestos de deficiencias, como los grandes errores que se han encontrado en el *software* en cuestión (Tribunal Administrativo, 2020, párr. 153). Asimismo, los cuerpos policiales incumplieron las exigencias respecto a la igualdad, conforme el *Equality Act 2010*[66], ya que, no se tomó en consideración, ni antes ni durante su aplicación, la posibilidad de que *AFR Locate* pudiera generar resultados que indirectamente produjeran discriminación por motivos de género y/o raza, a causa de producir resultados con un mayor número de coincidencias positivas para rostros de mujeres y/o de personas negras y pertenecientes a minorías étnicas (Tribunal Administrativo, 2020, párr. 52).

2.4. LOS DESAFÍOS EN EL USO DE LA IDENTIFICACIÓN BIOMÉTRICA REMOTA EN ESPACIOS PÚBLICOS

La evaluación del impacto de la Propuesta de Reglamento es uno de los estudios de mayor importancia para comprender en su totalidad el papel que podría cumplir esta normativa si esta entrara en vigor. Dentro de este, se estudian todos los aspectos que

[65] La Ley de Protección de Datos de 2018 es la aplicación en el Reino Unido del RGPD.
[66] Este requerimiento establece que los organismos públicos deben considerar adecuadamente la importancia de erradicar la discriminación, impulsar la equidad de oportunidades y fomentar la convivencia pacífica entre todas las personas, mientras llevan a cabo sus actividades (Gobierno de Reino Unido, 2010).

pudieran verse afectados como consecuencia de la aplicación de la IA, al igual que los mayores obstáculos, los cuales podrán observar en la siguiente tabla:

Principales problemas	Interesados afectados
1. El uso de la IA aumenta los riesgos para la seguridad de los ciudadanos.	● Ciudadanos, consumidores y otras víctimas ● Empresas afectadas.
2. El uso de la IA aumenta el riesgo de violación de los derechos fundamentales de los ciudadanos y de los valores de la UE.	● Ciudadanos, consumidores y otras víctimas. ● Grupos enteros de la sociedad. ● Usuarios de sistemas de IA responsables de violaciones de derechos fundamentales.
3. Las autoridades carecen de competencias, marcos procedimentales y recursos para garantizar y supervisar el cumplimiento de las normas aplicables al desarrollo y uso de la IA.	● Autoridades nacionales responsables del cumplimiento de las normas de seguridad y derechos fundamentales.
4. La seguridad jurídica y la complejidad de la aplicación de las normas existentes a los sistemas de IA disuaden a las empresas de desarrollar y utilizar estos sistemas.	● Empresas y otros proveedores que desarrollan sistemas de IA. ● Empresas y otros usuarios que utilizan sistemas de IA.
5. La desconfianza en la IA frenaría su desarrollo en Europa y reduciría la competitividad global de la economía de la Unión Europea.	● Empresas y otros usuarios que utilizan sistemas de IA. ● Ciudadanos que utilizan sistemas de IA o se ven afectados por ellos.
6. La fragmentación de las medidas obstaculiza el mercado único transfronterizo de IA y amenaza la soberanía digital de la Unión Europea.	● Empresas que desarrollan IA, principalmente pymes[67] afectadas. ● Usuarios del sistema de IA, incluidos consumidores, empresas y autoridades públicas. [68]

[67] Acorde al Reglamento (UE) N°651/2014 de la Comisión, de 17 de junio de 2014, por el que se declaran determinadas categorías de ayudas compatibles con el mercado interior en aplicación de los Arts.107 y 108 del Tratado, es aquella empresa que con al menos de 250 personas y cuyo volumen de negocios anual no excede de 50.000.000 de euros o su balance general anual no excede de 43.000.000 de euros (Anexo I, Reglamento nº 651/2014).

[68] La fuente oficial de esta tabla está exclusivamente en inglés, por lo tanto, en el Anexo C se podrá ver la versión original y la que se puede observar en el texto es de elaboración/traducción propia.

2.4.1. Los Derechos Fundamentales en riesgo de vulneración

El "Libro Blanco sobre la IA, un enfoque europeo orientado a la excelencia y la confianza" de la Comisión Europea proporciona alternativas políticas que faciliten un desarrollo seguro y fiable de la IA en la región, por lo que un componente esencial del escrito es el análisis de los derechos fundamentales afectados, para diseñar un ecosistema de confianza respecto con el marco regulatorio de la IA (Comisión Europea, 2020).

El uso de estas nuevas tecnologías puede afectar significativamente los valores de la Unión Europea y provocar la conculcación de un número significativo de sus derechos, como los siguientes:

> La libertad de expresión, la libertad de reunión, la dignidad humana, la ausencia de discriminación por razón de sexo, raza u origen étnico, religión o credo, discapacidad, edad u orientación sexual, y, en su aplicación en determinados ámbitos, la protección de los datos personales y de la vida privada[69], el derecho a una tutela judicial efectiva y a un juicio justo, o la protección de los consumidores (Comisión Europea, 2020, p.13).

Esta vulneración puede ser la respuesta de defectos en el diseño general de los sistemas de IA, en especial, cuando se refieren a la supervisión humana o por utilizar datos potencialmente sesgados si no se obtiene la corrección correspondiente; un ejemplo de esto último es la filtración de algoritmos que utilizan, exclusiva o principalmente, los datos de hombres, lo que significaba resultados perjudiciales para las mujeres (Comisión Europea, 2020). Sin menoscabar los derechos fundamentales expuestos, hay tres derechos que se destacan dentro de la práctica de los sistemas de identificación biométrica: el derecho a la vida privada, la protección de los datos personales y la no discriminación.

En el caso de los sistemas de identificación biométrica, en concreto, aquellos relacionados con el tratamiento de datos fáciles, el respeto a la vida privada y la protección de datos personales juegan un papel primordial. Aunque ambos están estrechamente relacionados, son derechos distintos y autónomos; se han descrito como el

[69] La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa con el tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas, estudió los riesgos a la vida privada, comprendiendo que los sistemas de IA pueden suponer más de lo que se han estudiado (Considerando 26, Directiva 2002/58).

derecho "clásico" a la protección de la intimidad o vida privada y un derecho más "moderno", el derecho a la protección de datos[70]. De acuerdo con la FRA, en su informe, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*[71], ambas garantías "se esfuerzan por proteger valores similares, es decir, la autonomía y la dignidad humana de los individuos, concediéndose una esfera personal en la que puedan desarrollar libremente su personalidad" (FRA, 2019, p.23).

El respeto a la vida privada[72] en espacios de acceso público puede ser un aspecto complejo de delimitar, pero el TEDH utiliza el concepto de una expectativa razonable de intimidad, es decir, encontrar el punto en el que dicha persona no se siente observada en espacios públicos (FRA, 2019, p.23). En la Sentencia del TEDH López Ribalda y otros contra España, C-1874/13 y C-8567/13 del 17 de octubre de 2019, se asegura que no existe punto de comparación entre la videovigilancia en el lugar de trabajo o supermercado, donde se realizan actividades cotidianas, asimismo, que en dichos lugares públicos se realice una grabación sistemática o permanente de imágenes de personas físicas identificadas y el posterior procesamiento de estas (TEDH 1874/13 y 8567/13, de 17 de octubre, párr. 93º).

Igualmente, es necesario dar prioridad a la igualdad, la no discriminación y la solidaridad, incluyendo los derechos de las personas en riesgo de exclusión; estos, conforme con las Directrices Éticas para una IA Fiable de la Comisión Europea, son un requisito crucial para tener IA moralmente correcta. En este campo, la igualdad implica que el funcionamiento de los sistemas de identificación no genere resultados injustamente sesgados, además de contar con la protección adecuada para los grupos potencialmente vulnerables, como pueden ser los "trabajadores, las mujeres, las personas con discapacidad, las minorías étnicas, los niños, los consumidores u otras personas en riesgo de exclusión" (Comisión Europea, 2019, p.13).

[70] TJUE. *Volker und Markus Schecke GbR y Hartmut Eifert* contra Land Hessen, asuntos acumulados C-92/09 y C-93/09. Sentencia de 9 de noviembre de 2010.
[71] Las citas que se hacen en este trabajo de este texto son de elaboración/traducción propia, dado que la única versión oficial del documento es en inglés.
[72] De acuerdo con el pie de página núm.57 respecto con la dignidad humana, ¨son parte primordial de la preocupación en torno a los derechos fundamentales cuando se utiliza la tecnología de reconocimiento facial¨ (Comisión Europea, 2020, p.26).

De igual manera, es relevante destacar los beneficios de utilizar datos biométricos para fines de identificación, en concreto, aquellos sistemas que evalúan el rostro de las personas y el ADN. Ambas tecnologías pueden contribuir, de forma eficaz, a la lucha contra la delincuencia y la revelación efectiva de la identidad de una persona desconocida sospechosa de haber cometido un delito grave (Dict. 3/2012 Consejo de la UE, de 27 de abril 2012, p.9). No obstante, cuando se busca la recopilación masiva de datos, tal y como se practica en espacios públicos, pueden ocurrir efectos colaterales graves.

Un ejemplo es el caso de la identificación facial, donde hay facilidad de la obtención, debido a que puede ocurrir con o sin el consentimiento del individuo, así, el uso generalizado podría poner fin al anonimato en los espacios públicos y permitir el monitoreo continuo de la persona. En el contexto de los datos de ADN, la utilización de esta tecnología podría divulgar datos sensibles relativos con la salud de una persona (Dict. 3/2012 Consejo de la UE, de 27 de abril 2012, p.9).

Un supuesto a destacar es la elaboración de perfiles étnicos por la policía española, de este modo, en Cataluña se han detectado faltas de proporcionalidad llamativas y, en 2018, un grupo de expertos de la ONU calificó de "endémica" la elaboración de perfiles de afrodescendientes en España, lo que trae como resultado el aprendizaje de los algoritmos y la identificación, en mayor cantidad, de las personas con rasgos afrodescendientes, número que aumenta si se es hombre, pues se tiene tres veces más probabilidad de ser detenido en comparación con las mujeres (State Watch Organization, 2022).

2.4.2. Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2023/C 23/01).

En la Comunicación de la Comisión al Parlamento Europeo, el Consejo, el Comité Económico y Social Europeo, y el Comité de las Regiones, Brújula Digital 2030: el enfoque de Europa para el Decenio Digital, se plantea la necesidad de crear un solo cuerpo que unifique, en una declaración interinstitucional solemne, el conjunto de principios y derechos digitales, para tener un marco solo en materia de digitalización (Comisión Europea, 2021). Por ello, nace la iniciativa de la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital.

Esta se conoce por ser la responsable de presentar "el compromiso de la UE con una transformación digital protegida, segura y sostenible que sitúe a las personas en el centro, en consonancia con los valores fundamentales de la UE y los derechos fundamentales" (Comisión Europea, 2023). Lo anterior se puede observar desde su primer capítulo, donde se afirma que el núcleo de la transformación digital de la Unión Europea son las personas, por lo que la tecnología debe servir como una herramienta para que todos los individuos en el territorio comunitario se sientan beneficiados por su uso. Esto hace referencia a las interacciones con algoritmos y los sistemas de IA, la que ha de ser un instrumento al servicio de las personas y su objetivo último es aumentar el bienestar humano, al igual que compromete a los órganos de la Unión Europea a fomentar sistemas de IA humanitarios, fiables y éticos a lo largo de su desarrollo, con el despliegue y la utilización, a la par de los valores de la misma institución.

Uno de los puntos que presenta mayor dificultad se expone en el Capítulo III que sostiene que se debe velar por que la IA no sea utilizada para anticipar o predecir las decisiones que las personas puedan tomar en áreas como la salud, la educación, el empleo o la privacidad (Comisión Europea, 2023). Lo anterior se ve evidentemente retado por los sistemas de identificación biométrica en espacios de acceso público, así, la privacidad es sustancialmente afectada gracias a estas prácticas. Por ello, se hallan contradicciones a la hora de la práctica de dos cuerpos modernos: la declaración europea sobre los Derechos y Principios Digitales para la Década Digital, y la Ley de IA.

Pese a que la Declaración no es una norma jurídica, desde el punto de vista de este estudio, no es un simple propósito político. De igual manera lo plantea Moisés Barrio[73], pues forma parte de toda una campaña de la digitalización europea, además de señalar los mayores obstáculos para la región. Por lo tanto, se está ante una expresión del fortalecimiento del constitucionalismo en la era digital "subrayando así que el futuro digital de la UE se apoya en un programa digital presidido por los valores constitucionales europeos" (Barrio, 2023). Esta idea fue materializada en la Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, por la que se establece el programa estratégico de la Década Digital para 2030, lo que se encarga de instaurar un

[73] Fundador de IDESOFT, empresa productora de *software*, de soluciones tecnológicas y de ciberseguridad, además de letrado del Consejo de Estado y Profesor de Derecho Digital en las Universidades Carlos III de Madrid, ICADE, San Pablo CEU y Complutense de Madrid (Consejo General, 2023).

mecanismo de vigilancia y cooperación durante esta etapa de transformación (Parlamento Europeo, 2022).

Igualmente, se busca reforzar las iniciativas desarrolladas por los Estados miembros, una de ellas implica la Carta de Derechos digitales española y la Ley N°2016-1321 de 7 de octubre de 2016 por una República digital en Francia, titulada *Loi* N°*2016-1321, du 7 octobre 2016, pour une République numérique,* compuesta por 113 Arts., en concreto, el Título II dedicado a la protección de datos y la privacidad de sus ciudadanos (República Francesa, 2016).

2.4.3. Las restricciones para el tratamiento de datos biométricos

A la luz de la normativa expuesta a lo largo del trabajo, la protección de los derechos fundamentales y la jurisprudencia, los datos biométricos solo podrían ser comprometidos legalmente, y en el caso de que sea imprescindible, para preservar un interés público significativo en una sociedad democrática. No obstante, el uso de aplicaciones de IA para la identificación biométrica remota, al igual que otras tecnologías de vigilancia altamente intrusivas, entraña riesgos específicos para los derechos fundamentales, por ende, siempre deben clasificarse de riesgo elevado y utilizarse con fines debidamente justificados, proporcionados y sujetos a garantías adecuadas (Comisión Europea, 2020).

Por un lado, se encuentran los límites formales[74] de la reserva de ley y el interés público, este último desde un punto de vista formal, por lo que se entiende como el uso público de bases de datos, con la finalidad de un interés general previsto en la ley, es decir, "no cualquier utilización de la información merecerá este calificativo, sino aquella que obedece a una necesidad, utilidad, beneficio o provecho de la sociedad y, además, esté contemplado en una norma con rango de ley" (Simón y Dorado, 2021, p.8). En este aspecto, la reserva de ley se encuentra en el Art.8 de la LOPDGDD y el Art.6.1.c) del RGPD. Sobre el uso público que le corresponde a dicho interés general, este se halla en la CE en múltiples preceptos, tales como el Art.76.1 y 124.1 que hacen referencia al interés público.

[74] Respecto con los límites subjetivos en relación con el responsable del tratamiento, en este caso, el Estado, se ha debatido a lo largo del estudio que se fija el posicionamiento jurisprudencial conforme con la definición del interés público.

De igual forma, se analiza en el Considerando 46 del RGPD, pues señala que cuando se hace referencia al tratamiento de datos personales, el interés vital puede basarse en motivos importantes de interés público y en los intereses vitales del interesado, así, un supuesto es "cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo, en caso de catástrofes naturales o de origen humano" (Considerando 46, RGPD). Un aspecto favorable es que la propuesta de Ley IA fija, con exactitud, los supuestos en los que se va a poder implementar la identificación biométrica remota y/o tiempo real para aplicar la ley, donde se tiene en cuenta el principio de una actividad prohibida.

Sin embargo, dichos límites pueden perder su eficacia cuando no se acompañan de las restricciones materiales adecuadas, como el principio de proporcionalidad y contenido mínimo[75], ambos altamente amenazados por las técnicas de identificación biométrica, en especial, cuando esta se practica en espacios públicos.

Según la doctrina reiterada del Tribunal Constitucional, el principio de proporcionalidad es una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, como la intimidad. En este sentido, para determinar si una medida que restringe un derecho fundamental cumple con el requisito de proporcionalidad, debe superar tres controles:

- El juicio de idoneidad: Si tal medida es susceptible de conseguir el objetivo propuesto.
- El juicio de necesidad: Si es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia.
- El juicio de proporcionalidad en sentido estricto: Si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (STC 207/1996, de 22 de enero, FJ. 4º).

[75] Uno de los principios relativos con el tratamiento expuesto en el Art.5 del RGPD, también conocido como minimización de datos, entiende que los datos personales deberán ser ¨adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados¨ (Art.5.1.c, RGPD).

De estos tres puntos, uno de los más conflictivos, respecto con la identificación biométrica en espacios públicos, es la justificación de la necesidad, pues es difícil, si no es imposible en algunos supuestos, por la inexistencia de otros medios menos gravosos que puedan obtener los mismos resultados (Simón y Dorado, 2021). De conformidad con la publicación "Límites y garantías constitucionales frente a la identificación biométrica", el uso de estas tecnologías no supera este juicio de proporcionalidad, un ejemplo es el supuesto de que se busque una persona en condena, de igual forma, se estarán recopilando los datos de los individuos transitando en el espacio público: "el interés privado en juego, disfrazado de interés público, no puede prosperar para justificar el tratamiento masivo de datos sensibles" (Simón y Dorado, 2021, p.10).

Del mismo modo, la jurisprudencia entiende que, en consideración con los riesgos que conlleva el tratamiento de datos personales sensibles, este debe estar supeditado a las garantías adecuadas de protección de los derechos y libertades del interesado, salvaguardias que todavía no forman parte de los Estados. De acuerdo con las conclusiones del abogado general de la Sentencia del TJUE Hristo Gaydarov contra *Direktor na Glavna direktsia «Ohranitelna politsia» pri Ministerstvo na vatres hnite raboti,* asunto C-205/21[76], para determinar la existencia de estas salvaguardias, "es necesario tener una visión de conjunto de todas las condiciones para poder determinar el alcance exacto del tratamiento de que se trate y garantizar una protección eficaz contra los tratamientos inapropiados o abusivos" (Pitruzzella, 2022, párr. 57).

En tal marco, este es un procedimiento similar al que ha asumido el SEPD en lo relativo con el reconocimiento automatizado en los espacios públicos de los rasgos humanos, el que incluye los rostros, la andadura, las huellas dactilares, el ADN, la voz, las pulsaciones de teclado y otras señales biométricas o de comportamiento; esta autoridad supervisora apoya la siguiente idea:

> Una moratoria sobre el despliegue, en la UE, para que pueda tener lugar un debate con conocimiento de causa y democrático y hasta el momento en que la UE y los Estados miembros dispongan de todas las garantías adecuadas, incluido un marco

[76] TJUE. Hristo Gaydarov contra *Direktor na Glavna direktsia «Ohranitelna politsia» pri Ministerstvo na vatres hnite raboti*, (C-430/10). Sentencia de 17 de noviembre de 2011.

jurídico completo para garantizar la proporcionalidad de las respectivas tecnologías y sistemas para el caso de uso específico (SEPD, 2020, p.1).

2.5. UN FUTURO INCIERTO

La IA se ha incorporado a la vida de las personas de manera acelerada, lo que ha superado el marco regulatorio existente, además de dejar a las empresas líderes en esta tecnología un campo de ejecución preocupante, sin una adecuada supervisión legal y en un vacío normativo; este es el posicionamiento de expertos en la materia (Organización Otras Voces en Educación, 2023). Luego de la propuesta de la Comisión Europea de la Ley de IA, y ante el paso gigantesco de votar a favor del Parlamento Europeo el 11 de mayo de 2023, luego de dos años de debate y la aparición de tecnologías arrasadoras como el ChatGPT[77], se puede observar que su regulación está en marcha (Ayuso y Pascual, 2023). Se estima que para este 2023 entre en vigor y se inicie con el periodo transitorio, donde se deberá exigir el desarrollo de estándares por parte de los Gobiernos de la Unión Europea, para que, en la segunda mitad de 2024, se apliquen los operadores de IA con los salvaguardias normativos y se realicen las primeras evaluaciones (Comisión Europea, 2022).

En este orden de ideas, Mher Hakobyan, asesor de la organización no gubernamental Amnistía Internacional, entiende que, si bien el texto no proscribe la vigilancia masiva, sí limita su uso a las fuerzas de seguridad solo y dentro de límites legales estrictos (Amnistía Internacional, 2023). De igual forma, hace hincapié en las garantías respecto con la transparencia y la responsabilidad en el uso de la IA en espacios públicos y su impacto a los derechos humanos, por ello, se debe facultar a los individuos perjudicados, asegurando la igualdad de oportunidades para acceder a la tecnología y el derecho a imponer recurso cuando sea lo pertinente (Amnistía Internacional, 2023).

En concreto, las voces en Europa no son unánimes, puesto que, de acuerdo con los hallazgos del informe *National strategies on Artificial Intelligence: A European perspective*, en su edición del 2022, cada país tiene un nivel de rechazo a la identificación

[77] De acuerdo con EDEM, escuela de empresas, negocios y *management,* Chat GPT es un modelo de lenguaje desarrollado por OpenAI, que tiene la fidelidad de desarrollar tecnologías de IA de alta calidad y de libre acceso para la sociedad (Ortiz, s.f.).

biométrica, en especial, aquella que se base en el reconocimiento fácil, no obstante, sí reconoce que "la UE y los Estados miembros van por buen camino para aprovechar los beneficios y promover el desarrollo de una IA centrada en el ser humano, sostenible, segura, integradora y digna de confianza en Europa" (Ricart et al., 2022, p.91).

Es positivo que, hasta el momento, se pudiera llegar a un consenso, en virtud de que es un punto clave para enfrentar esta ola de avances tecnológicos, no obstante, mientras pasa el tiempo, más se ponen en marcha los proyectos que tienen la finalidad de procesar datos masivamente. A nivel europeo, es preciso recordar la Resolución del Parlamento Europeo, del 6 de octubre de 2021, sobre la IA en el derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (Parlamento Europeo, 2021a), sin importar que esta no sea vinculante, por lo tanto, se entiende que esta práctica, que se realiza en todo Europea, debe ceñirse a una supervisión humana y poderes legales sólidos, para prevenir la discriminación por parte de la IA, particularmente, en las circunstancias fronterizas (Parlamento Europeo, 2021b).

3. CONCLUSIONES

A continuación, se exponen las conclusiones del presente estudio, en cuya elaboración se han tenido en cuenta los objetivos y metodología establecidas en la introducción. Respecto al planteamiento inicial del trabajo, se ha podido realizar una evaluación acertada de la normativa vigente, la jurisprudencia y la doctrina especializada relacionados con la repercusión de los derechos fundamentales en el contexto de la identificación biométrica remota por parte de autoridades en lugares de acceso público, lo cual ha puesto en evidencia que:

1. La materia objeto de esta investigación, los sistemas de identificación biométrica, carece de una regulación normativa vigente que permita su puesta en práctica conforme el respeto y protección de los derechos fundamentales. La regulación del procesamiento masivo de datos personales de categoría especial, tanto a nivel nacional como comunitario, es inexistente y de urgente creación, como se pudo identificar en la jurisprudencia. Por consiguiente, es imperativo proseguir con una revisión rigurosa y exhaustiva de esta IA en espacios de acceso público, para así favorecer al desarrollo de futuras disposiciones legales que resguarden la salvaguarda de los derechos y principios implicados en el campo de aplicación.

2. La propuesta de Reglamento del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas en materia de IA, la cual representaría la primera normativa de ámbito comunitario y nacional que recoja esta tecnología, pasa por alto la precisión y eficiencia que requiere los sistemas de IA los cuales siempre pondrán en riesgos un número significativo de derechos fundamentales. Siendo especialmente alarmante la falta de claridad respecto a la posibilidad de no presentar la autorización previa para poner en marcha proyectos de verificación/identificación biométrica, siempre y cuando esta se base en una urgencia debidamente justificada, excepción que no se encuentra debidamente desarrollada en el escrito en cuestión.

3. La *praxis* ha demostrado la existencia de lagunas por parte de las autoridades, en especial de los cuerpos de seguridad, del tratamiento de datos personales de naturaleza especial, el cual puede realizarse por razones de un interés público esencial, siempre y cuando se respeten los límites materiales. En virtud de las características intrínsecas de la tecnología en cuestión, se ha demostrado que resulta extremadamente complejo garantizar la observancia del principio de proporcionalidad, así como la minimización y

protección de los datos personales, incluyendo el derecho de *habeas data*. Por consiguiente, se puede establecer que las autoridades públicas no cuentan con las competencias técnicas necesarias y los recursos suficientes para el despliegue de esta tecnología y hacer frente a los riesgos imprevistos asociados con el procesamiento masivo de datos biométricos.

4. En términos comparativos jurisprudenciales, se observa que el rendimiento a nivel europeo de los sistemas biométricos ha sido restringido y desfavorable para los derechos fundamentales, como se analiza en los casos de Alemania, Italia y Reino Unido, mientras que, en España, se detectan faltas graves de proporcionalidad y discriminación arraigada a los algoritmos de identificación biométrica. El análisis en paralelo de los resultados obtenidos en Europa y en España ha llevado a la deducción de que el derecho a la vida privada, la protección de los datos personales y la no discriminación, se están viendo diariamente afectados por proyectos tanto gubernamentales como privados aplicados en espacios de acceso público.

5. Considerando que la IA, en todas sus vertientes, es una realidad cada vez más presente en nuestra vida y, a la vista de los resultados obtenidos, se recomienda priorizar el diseño de sistemas de verificación e identificación de identidad basados en rasgos fisiológicos o conductuales, en línea con los principios éticos y de transparencia, con el fin de evitar cualquier tipo de defecto en el *software*, especialmente en lo que se refiere a la recopilación excesiva de su base de datos personales. Además, se insta a enfatizar la investigación normativa, a fin de reducir las desventajas derivadas de la rapidez con la que evoluciona este sector tecnológico y la demora característica de su regulación.

A pesar de la complejidad que entraña el objeto de estudio, los frutos alcanzados sobrepasan las expectativas originales, ofreciendo evidencia significativa e imprevista que abren nuevas vías de investigación normativa. Esta oportunidad unida con mis prácticas universitarias me ha permitido desarrollarme como estudiante y como futura profesional, Además, al tener la oportunidad de presenciar directamente la dinámica del derecho como un organismo en constante evolución, que demanda niveles elevados de adaptabilidad y precisión, no puedo más que expresar mi más sincero agradecimiento por darnos este espacio a los estudiantes.

4. FUENTES NORMATIVAS

4.1. Legislación comunitaria

4.1.1. Tratados

Unión Europea. Carta de los Derechos Fundamentales de la Unión Europea, firmado en Niza el 7 de diciembre de 200. [Internet]. Diario Oficial de la Unión Europea, 18 de diciembre de 2000. [Consultado 1 de marzo de 2023]. Disponible en: https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Unión Europea. Tratado de Funcionamiento de la Unión Europea, firmado en Roma el 25 de marzo de 1957. [Internet]. Diario Oficial de la Unión Europea, 01 de enero de 1958. [Consultado 1 de marzo de 2023]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A12012E%2FTXT

4.1.2. Reglamentos

Unión Europea. 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) y se modifican determinados actos legislativos de la Unión. [Internet]. Diario Oficial de la Unión Europea, 21 de abril de 2021. [Consultado 1 de marzo de 2023]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52021PC0206

Unión Europea. 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. [Internet]. Diario Oficial de la Unión Europea L 119/1, 27 de abril de 2016. [Consultado 1 de marzo de 2023]. Disponible en: https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A32016R0679

Unión Europea. Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se

derogan el Reglamento (CE) N°45/2001 y la Decisión N°1247/2002/CE. [Internet]. Diario Oficial de la Unión Europea L 295/39, 21 de noviembre de 2018. [Consultado 1 de marzo de 2023]. Disponible en: https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A32016R0679

Unión Europea. Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) N°45/2001 y la Decisión N°1247/2002/CE. [Internet]. Diario Oficial de la Unión Europea L 295/39, 21 de noviembre de 2018. [Consultado 1 de marzo de 2023]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32018R1725

4.1.3. Directivas

Unión Europea. 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. [Internet]. Diario Oficial de la Unión Europea L 119/89, 4 de mayo de 2016. [Consultado 15 de marzo de 2023] Disponible en: https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A32016L0680

Unión Europea. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. [Internet]. Diario Oficial de la Unión Europea L 201, 31 de julio de 2002. [Consultado 15 de marzo de 2023] Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32002L0058

4.1.4. Decisión

Unión Europea. Decisión Marco del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros. [Internet]. Diario Oficial de la Unión Europea L 190, 18 de julio de 2002. [Consultado 15 de marzo de 2023] Disponible en: https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A32002F0584

Unión Europea. Decisión UE) 2022/2481 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 por la que se establece el programa estratégico de la Década Digital para 2030. [Internet]. Diario Oficial de la Unión Europea L 323/4, 19 de diciembre de 2022. [Consultado 15 de marzo de 2023] Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022D2481

4.1.5. Dictamen

Unión Europea. Dictamen 3/2012 sobre la evolución de las tecnologías biométricas. [Internet]. Diario Oficial de la Unión Europea WP193, 27 de abril de 2012. [Consultado 15 de marzo de 2023] Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

Unión Europea. Dictamen conjunto 5/2021 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre la inteligencia artificial (Ley de Inteligencia Artificial). [Internet].Comité Europeo de Protección de Datos, 28 de junio de 2021. [Consultado 17 de marzo de 2023] Disponible en: https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

4.2. Normativa nacional

Constitución Española. [Internet]. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 311. [Consultado 22 de abril de 2023]. Disponible en: https://www.boe.es/buscar/pdf/1978/BOE-A-1978-31229-consolidado.pdf

España. Decreto-ley 2/2023, de 8 de marzo, de medidas urgentes de impulso a la inteligencia artificial en Extremadura. [Internet]. Boletín Oficial del Estado, 10 de

marzo de 2023, núm. 48. [Consultado 22 de abril de 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

España. Ley 11/2023, de 8 de mayo, de trasposición de Directivas de la Unión Europea en materia de accesibilidad de determinados productos y servicios, migración de personas altamente cualificadas, tributaria y digitalización de actuaciones notariales y registrales; y por la que se modifica la Ley 12/2011, de 27 de mayo, sobre responsabilidad civil por daños nucleares o producidos por materiales radiactivos. [Internet]. Boletín Oficial del Estado, 9 de mayo de 2023, núm. 110. [Consultado 22 de abril de 2023]. Disponible en: https://www.boe.es/boe/dias/2023/05/09/pdfs/BOE-A-2023-11022.pdf

España. Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación. [Internet]. Boletín Oficial del Estado, 13 de julio de 2022, núm. 167. [Consultado 22 de abril de 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2022-11589

España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Internet]. Boletín Oficial del Estado, 24 de noviembre de 1995, núm. 281. [Consultado 22 de abril de 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. [Internet]. Boletín Oficial del Estado, 06 de diciembre de 2018, núm. 294. [Consultado 23 de abril de 2023]. Disponible en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

4.3. Normativa internacional

Francia. LEY N°2016-1321 de 7 de octubre de 2016 por una República digital. [Internet]. Diario Oficial del Estado, 8 de octubre de 2016, núm.1. [Consultado 22 de abril de 2023]. Disponible en: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746

Reino Unido. Data Protection Act 2018. [Internet]. Base de datos de leyes estatutarias del Reino Unido, 23 de mayo de 2018 [Consultado 23 de abril de 2023]. Disponible en: https://www.legislation.gov.uk/ukpga/2018/12/contents

Reino Unido. The Equality Act 2010 (Specific Duties) Regulations 2011. [Internet]. Base de datos de leyes estatutarias del Reino Unido, 9 de septiembre de 2011 [Consultado 24 de abril de 2023]. Disponible en: https://www.legislation.gov.uk/uksi/2011/2260/contents/made

5. BIBLIOGRAFÍA

5.1. Bibliografía jurisprudencial

5.1.1. Comunitaria

Tribunal de Justicia de la Unión Europea. Caso *Google Spain,* S.L. y Google Inc. contra AEPD y Mario Costeja González (C-131/12) [Internet]. Sentencia de 13 de mayo de 2014. [Consultado el 24 de abril de 2023]. Disponible en: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:62012CJ0131

Tribunal de Justicia de la Unión Europea. Caso Hristo Gaydarov contra *Direktor na Glavna direktsia «Ohranitelna politsia» pri Ministerstvo na vatres hnite raboti*, (C-430/10) [Internet]. Sentencia de 17 de noviembre de 2011. [Consultado el 25 de abril de 2023]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62010CJ0430&from=HR

Tribunal de Justicia de la Unión Europea. Caso *Volker und Markus Schecke GbR y Hartmut Eifert* contra Land Hessen, asuntos acumulados C-92/09 y C-93/09 [Internet]. Sentencia de 9 de noviembre de 2010. [Consultado el 25 de abril de 2023]. Disponible en: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:62009CJ0092

Tribunal de Justicia de la Unión Europea. *Data Protection Commissioner* contra *Facebook Ireland Limited* y Maximillian Schrems (C-311/18) [Internet]. Sentencia de 16 de julio de 2020. [Consultado el 24 de abril de 2023]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62018CJ0311&qid=1680905698198

Tribunal Europeo de Derecho Humanos. Caso Leander contra Suecia N°9248/81 [Internet]. Sentencia del 26 de marzo de 1987. [Consultado el 25 de abril de 2023]. Disponible en: https://hudoc.echr.coe.int/spa#{%22fulltext%22:[%22Leander%22],%22docume

ntcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-57519%22]}

Tribunal Europeo de Derecho Humanos. Caso Rotary contra Rumania nº28341/91 [Internet]. Sentencia de 4 de mayo de 2000. [Consultado el 25 de abril de 2023]. Disponible en: https://hudoc.echr.coe.int/app/conversion/docx/?library=ECHR&id=001-162581&filename=CASE%20OF%20ROTARU%20v.%20ROMANIA%20-%20%5BSpanish%20Translation%5D%20summary%20by%20the%20Spanish%20Cortes%20Generales.docx&logEvent=False

Tribunal Europeo de Derecho Humanos. Caso S. y Marper contra Reino Unido, N°305627/04 y 305666/04 [Internet]. Sentencia del 4 de diciembre de 2008. [Consultado el 25 de abril de 2023]. Disponible en: https://hudoc.echr.coe.int/spa#{%22fulltext%22:[%22Marper%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-90051%22]}

Tribunal Europeo de Derecho Humanos. López Ribalda y otros contra España, nº1874/13 y 8567/13 [Internet]. Sentencia del 26 de marzo de 1987. [Consultado el 25 de abril de 2023]. Disponible en: https://hudoc.echr.coe.int/spa#{%22fulltext%22:[%22L%C3%B3pez%20Ribalda%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-197098%22]}

5.1.2. Nacional

España. Audiencia Provincial de Barcelona (Sala Segunda). [Internet]. Auto 1448/2021, de 15 de febrero de 2020. Recurso de apelación 840/2020. [Consultado el 28 de abril de 2023]. Disponible en: https://www.poderjudicial.es/search/AN/openDocument/e8e8bb906a961365/20210518

España. Tribunal Constitucional (Pleno). [Internet]. Sentencia 254/1993, de 22 de julio de 1993. Recurso de inconstitucionalidad 1827/90. [Consultado el 26 de abril de 2023]. Disponible en: https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2383

España. Tribunal Constitucional (Pleno). [Internet]. Sentencia 76/2019, de 22 de mayo de 2019. Recurso de inconstitucionalidad 1405-2019. [Consultado el 25 de abril de 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2019-9548

España. Tribunal Constitucional (Pleno). [Internet]. Sentencia núm. 292/2000 de 30 de noviembre de 2001. Recurso de inconstitucionalidad 1463-2000. [Consultado el 25 de abril de 2023]. Disponible en: https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276

España. Tribunal Constitucional (Sala Segunda). [Internet]. Sentencia 207/1996, de 16 de mayo de 1996. Recurso de amparo 1789/96. [Consultado el 27 de abril de 2023]. Disponible en: https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/3259

España. Tribunal Constitucional (Sala Segunda). [Internet]. Sentencia 94/1998, de 4 de mayo de 1998. Recurso de amparo 840/1995. [Consultado el 26 de abril de 2023]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-T-1998-13334

5.1.3. Internacional

Alemania. Tribunal Administrativo de Colonia (Cámara 20). [Internet]. Sentencia 20 L 2340/19, de 18 de enero de 2021. Procedimiento principal 20 K 6706/20. [Consultado el 29 de abril de 2023]. Disponible en: http://www.justiz.nrw.de/nrwe/ovgs/vg_koeln/j2021/20_L_2340_19_Beschluss_20210118.html

Reino Unido. Corte de Apelaciones de Inglaterra y Gales (División Civil). [Internet]. Sentencia Caso N°C1/2019/2670 sobre tecnología de reconocimiento facial. *R (Bridges) v-Chief Constable of South Wales Police & Others.* [Consultado el 29 de abril de 2023]. Disponible en: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

5.2. Bibliografía doctrinal

5.2.1. Libro

Guervós, M. (2022). *Fiscalidad de las Smart Cities* (1.ª ed.). ARANZADI. Recuperado de https://www.google.com/url?q=https://acortar.link/uszUge&sa=D&source=docs&ust=1684267845451229&usg=AOvVaw1TFJVCeS4zySw_3qb0L6gb

Rouhianen, L. (2018). *Inteligencia Artificial 101 cosas que debes saber hoy nuestro futuro* (1.ª ed.). Barcelona , España: Alienta editorial. Recuperado de https://www.planetadelibros.com/libros_contenido_extra/40/39307_Inteligencia_artificial.pdf

5.2.2. Revista científica

Cotino, L. (2022). Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal. *Revista El Cronista del Estado Social y Democrático de Derecho*, *100*, 68-79. Recuperado de https://www.uv.es/cotino/publicaciones/cronistacotinopublicado.pdf

Drnas de Clément, Z. (2022). Inteligencia artificial en el Derecho Internacional, Naciones Unidas y Unión Europea. *Revista Estudios Jurídicos. Segunda Época*, (22). Recuperado de https://doi.org/10.17561/rej.n22.7524

Gamero, E. (2021). El Enfoque Europeo de Inteligencia Artificial. *Revista de Derecho Administrativa*, *20*, 268-289. Recuperado de https://revistas.pucp.edu.pe/index.php/derechoadministrativo/article/view/25212/23802

García, S. (2022). Una aproximación a la futura regulación de la inteligencia artificial en la Unión Europea. *Revista de Estudios Europeos*, *79*, 304-323. Recuperado de https://revistas.uva.es/index.php/ree/article/view/5728/4204

McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, Agosto 31, 1955. *AI Magazine*, *27*(4), 12. Recuperado de https://doi.org/10.1609/aimag.v27i4.1904

O'Callaghan Muñoz, Xavier. (1996). Los derechos de la personalidad. (1996). *La Ley. Revista jurídica española de doctrina, jurisprudencia y bibliografía*, (4), 1247-1251. Recuperado de https://vlex.es/vid/derechos-personalidad-214783

Rodríguez, V. (2023). Sistemas biométricos en materia criminal: un estudio comparado. *Revista del Instituto de Ciencias Jurídicas de Puebla*, *31*, 28-47. Recuperado de https://www.revistaius.com/index.php/ius/article/view/19/14

Simón Castellano, P., D. F. Xavi. «Límites Y garantías Constitucionales Frente a La identificación biométrica». *IDP. Revista De Internet, Derecho Y Política*, n.º 35, marzo de 2022, pp. 1-13. Recuperado de https://raco.cat/index.php/IDP/article/view/n35-simon/491134

Turing, A. M. (1950). Computing machinery and intelligence. *Oxford Academic*, *LIX*, 433-460. Recuperado de https://academic.oup.com/mind/article/LIX/236/433/986238

5.2.3. Doctrina Administrativa

Ministerio Federal del Interior, Construcción y Patria de Alemania. (2018, agosto). Pequeña pregunta de Niema Movassat y otros del grupo parlamentario DIE LINKE.: Biometría y protección de datos en el marco del Reglamento general de protección de datos de la UE BT impreso 19/3726. Recuperado 16 de abril de 2023, de https://www.linksfraktion.de/fileadmin/user_upload/PDF_Dokumente/KA_19_3726__1_.pdf

5.2.3.1. Agencia de Protección de Datos española

AEPD. (2020b). Procedimiento Sancionador Nº: E/03925/2020. Recuperado 16 de marzo de 2023, de https://www.uv.es/ceconomiacol/Resoluci%C3%B3nAEPDhuella.pdf

AEPD. (2020a, 8 mayo). Informe jurídico N/REF: 0036/2020. Recuperado 16 de abril de 2023, de https://www.aepd.es/es/documento/2020-0036.pdf

AEPD. (2023, 20 enero). Informe jurídico N/REF: 0098/2022. Recuperado 16 de abril de 2023, de https://www.aepd.es/es/documento/2022-0098.pdf

AEPD. (2021, 2 julio). Procedimiento Sancionador Nº: PS/00120/2021. Recuperado 16 de marzo de 2023, de https://www.aepd.es/es/documento/ps-00120-2021.pdf

5.2.3.2. Garante de Protección de Datos internacional

GPDP. (2022, 10 febrero). Orden de restricción contra Clearview AI. Recuperado 16 de marzo de 2023, de https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9751362

HmbBfDI. (2018a, 31 agosto). Objeción a la introducción del reconocimiento facial automatizado: No hay base legal para la creación de huellas faciales biométricas por la policía de Hamburgo aparente. Recuperado 16 de abril de 2023, de https://datenschutz-hamburg.de/pressemitteilungen/2018/08/2018-09-31-polhh-g20-videmo360

HmbBfDI. (2018b, diciembre 18). Utilización del software de reconocimiento facial «Videmo 360» por la policía de Hamburgo para la en relación con la cumbre del G20 que tuvo lugar en Hamburgo. Cumbre. Recuperado 16 de abril de 2023, de https://datenschutz-hamburg.de/assets/pdf/Anordnung_HmbBfDI_2018-12-18.pdf

5.3. Otros recursos empleados

Consejo General. (2023). Sobre los autores. Recuperado 16 de marzo de 2023, de https://www.abogacia.es/publicaciones/blogs/blog-de-innovacion-legal/sobre-los-autores-innovacion-legal/#moises_barrio

DPEJ. (s. f.-a). habeas data. Recuperado 4 de marzo de 2023, de https://dpej.rae.es/lema/habeas-data

DPEJ. (s. f.-b). lex specialis. Recuperado 16 de febrero de 2023, de https://dpej.rae.es/lema/lex-specialis#:~:text=Gral.,respecto%20a%20una%20m%C3%A1s%20general

Fernández, R. (2021, 7 diciembre). Asistentes virtuales en uso en el mundo 2019-2024. Recuperado 5 de enero de 2023, de https://es.statista.com/estadisticas/972995/asistentes-virtuales-en-uso-en-el-mundo/

Gallego, P. (2022). Seguridad e igualdad en la utilización de los sistemas de identificación biométrica en remoto por parte de los cuerpos y fuerzas de seguridad del Estado en tiempos de pandemia. Recuperado 8 de febrero de 2023, de https://www.acoes.es/wp-content/uploads/2022/03/ComunicacionPabloGallego.pdf

MINECO. (s. f.). SANDBOX REGULATORIO. Recuperado 16 de marzo de 2023, de https://dgsfp.mineco.gob.es/es/Sandbox/Paginas/default.aspx

Ortiz, P. (s. f.). Chat gpt: qué es, para qué sirve y su aplicación en la economía [explicado por chat gpt]. Recuperado 5 de marzo de 2023, de https://edem.eu/chat-gpt-que-es-para-que-sirve-y-su-aplicacion-en-la-economia-explicado-por-chat-gpt/

5.3.1. Unión Europea

CEPD. (2021, 7 julio). Directrices 2/2021 sobre los asistentes de voz virtuales. Recuperado 16 de febrero de 2023, de https://edpb.europa.eu/system/files/2022-02/edpb_guidelines_202102_on_vva_v2.0_adopted_es.pdf

Comisión Europea. (2019). Directrices éticas para una IA fiable. Recuperado 16 de febrero de 2023, de https://op.europa.eu/es/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1

Comisión Europea. (2020, 19 febrero). Libro Blanco: sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza. Recuperado 16 de febrero de 2023, de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0065

Consejo de Europa. (1981, 28 enero). Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Recuperado 16 de febrero de 2023, de https://rm.coe.int/16806c1abd

FRA. (2019). Facial recognition technology: fundamental rights considerations in the context of law enforcement. Recuperado 16 de febrero de 2023, de https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

FRA. (2021). Construir correctamente el futuro. La inteligencia artificial y los derechos fundamentales. *European union agency for fundamental rights*, 1-17. https://doi.org/10.2811/818206

Parlamento Europeo. (2019). La inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales: Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI)). Recuperado 16 de febrero de 2023, de https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.pdf

Parlamento Europeo. (2023). La protección de los datos personales. Recuperado 16 de febrero de 2023, de https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/es/FTU_4.2.8.pdf

SEPD. (2020, 17 noviembre). Resumen del dictamen del Supervisor Europeo de Protección de Datos sobre el Libro Blanco de la Comisión Europea sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza. Recuperado 16 de febrero de 2023, de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XX1117(01)&from=EN

TEDH. (1950, 4 noviembre). Convenio de Derecho Humanos. Recuperado 16 de marzo de 2023, de https://www.echr.coe.int/documents/convention_spa.pdf

5.3.1.1. Comunicación de Comisión Europea

Comisión Europea. (2018a, 25 abril). Comunicación De La Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité De Las Regiones: Inteligencia artificial para Europa. Recuperado 16 de marzo de 2023, de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0237&from=ES

Comisión Europea. (2021, 9 marzo). Comunicación De La Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité De Brújula Digital 2030: el enfoque de Europa para el Decenio Digital. Recuperado 16 de marzo de 2023, de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021DC0118

Comisión Europea. (2021, 9 marzo). Comunicación De La Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité De Brújula Digital 2030: el enfoque de Europa para el Decenio Digital. Recuperado 16 de marzo de 2023, de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021DC0118

5.3.2. Artículo de noticias en línea

AEPD. (2023, 9 mayo). Modificación de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. Recuperado 16 de marzo de 2023, de https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/modificacion-ley-organica-proteccion-datos-personales-y-garantia-derechos-digitales

Ayuso, S., & Pascual, M. (2023, 11 mayo). Europa quiere poner más obligaciones a la inteligencia artificial generativa como la de ChatGPT. Recuperado 11 de marzo de 2023, de https://elpais.com/tecnologia/2023-05-11/europa-quiere-poner-mas-obligaciones-a-la-inteligencia-artificial-generativa-como-la-de-chatgpt.html

Comisión Europea. (2018b, 9 marzo). Artificial intelligence: Commission kicks off work on marrying cutting-edge technology and ethical standards. Recuperado 12 de enero de 2023, de https://ec.europa.eu/commission/presscorner/detail/es/IP_18_1381

Otras Voces en Educación. (2023). La Unión Europea se encamina a su primera ley de inteligencia artificial. Recuperado 8 de marzo de 2023, de https://otrasvoceseneducacion.org/archivos/404630

Parlamento Europeo. (2021b, 6 octubre). Use of artificial intelligence by the police: MEPs oppose mass surveillance. Recuperado 6 de marzo de 2023, de https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance

Rita, M. (2021, 23 marzo). SARI, il riconoscimento facciale nella pubblica sicurezza: servono regole e trasparenza. Recuperado 9 de febrero de 2023, de https://www.agendadigitale.eu/sicurezza/privacy/sari-vantaggi-e-rischi-del-riconoscimento-facciale-nella-pubblica-sicurezza/

Subarroca, M. (2019, 11 noviembre). Las cuatro brechas de seguridad del lector de huellas y el reconocimiento facial. Recuperado 13 de enero de 2023, de https://www.uoc.edu/portal/es/news/actualitat/2019/310-seguridad-huella-reconocimiento-facial.html

Tucker, J. (2014, 23 noviembre). How facial recognition technology came to be: The FBI's astonishing new identification system is the product of 175 years of innovation—and paranoia. A visual history. *GLOBE CORRESPONDENT*. Recuperado 16 de abril de 2023, de https://www.wesleyan.edu/allbritton/cspl/scholarship/jennifertucker.pdf

5.3.3. Informe/Guía

AEPD. (2020b, febrero). Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. Recuperado 8 de mayo de 2023, de https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

Consejo para la Transparencia. (2022). La protección de datos personales en contextos de avanzado desarrollo tecnológico, con énfasis en videovigilancia y tecnología de reconocimiento facial empleada por el sector público. Recuperado 16 de enero de 2023, de https://www.consejotransparencia.cl/wp-content/uploads/2022/01/La-proteccio%CC%81n-de-datos-personales-en-contextos-de-avanzado-desarrollo-tecnolo%CC%81gico-con-e%CC%81nfasis-en-videovigilancia-y-tecnologi%CC%81a-de-reconocimiento-facial-empleada-por-el-sector-pu%CC%81blico-1.pdf

European Digital Rights. (2021). The rise and rose of biometric mass surveillance in the EU: A legal analysis of biometric mass surveillance practices in Germany, the Netherlands, and Poland. Recuperado 8 de febrero de 2023, de https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf

INCIBE. (2016). Tecnologías biométricas aplicadas a la ciberseguridad : Una guía de aproximación para el empresario. Recuperado 16 de febrero de 2023, de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

Ricard, J., Van Roy, R., Rossetti, F., & Tangi, L. (2022). National strategies on Artificial Intelligence: A European perspective. Recuperado 16 de febrero de 2023, de https://publications.jrc.ec.europa.eu/repository/handle/JRC129123

TEDH. (2018, 31 diciembre). Guía sobre el artículo 8 del Convenio Europeo de Derechos Humanos. Recuperado 16 de febrero de 2023, de https://www.echr.coe.int/Documents/Guide_Art_8_SPA.pdf

TEDH. (2022). Guide to the Case-Law of the of the European Court of Human Rights. Recuperado 16 de febrero de 2023, de https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf

UNESCO. (2022). Recomendación sobre la ética de la inteligencia artificial. Recuperado 16 de febrero de 2023, de https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa

World Wide Web Foundation. (2017, julio). Algorithmic Accountability, Applying the concept to different country contexts. Recuperado 7 de marzo de 2023, de http://webfoundation.org/docs/2017/07/WF_Algorithms.pdf

5.3.3. Organizaciones no gubernamentales

Amnistía Internacional. (2023, 11 mayo). Unión Europea: La prohibición del uso más perjudicial de la IA da un paso más. Recuperado 13 de marzo de 2023, de https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/la-ue-da-un-paso-adelante-para-regular-el-uso-de-la-inteligencia-artificial/

Fundación Endesa. (s. f.). Smart Cities. Recuperado 12 de marzo de 2023, de https://www.fundacionendesa.org/es/educacion/endesa-educa/recursos/smart-city

Kameras stoppen. (2020). Estado de los lugares de videovigilancia en colonia. Recuperado 10 de febrero de 2023, de https://kameras-stoppen.org/videobeobachtung-in-koeln/

State Watch Organization. (2022). La construcción del Estado biométrico: poderes policiales y discriminación. Recuperado 6 de febrero de 2023, de https://www.statewatch.org/media/3170/building-the-biometric-state-es.pdf

World Economic Forum. (2023, 5 abril). La confianza es la piedra angular de la Ley de Inteligencia Artificial de la UE - De esto se trata. Recuperado 16 de febrero de 2023, de https://es.weforum.org/agenda/2023/04/esto-es-lo-que-dice-la-nueva-ley-de-inteligencia-artificial-de-la-union-europea/#:~:text=La%20Ley%20de%20Inteligencia%20Artificial%20fue%20propuesta%20originalmente%20por%20la,debatiendo%20en%20el%20Parlamento%20Europeo

5.3.3. Páginas oficiales gubernamentales

Gobierno de España. (2021). Carta de Derechos Digitales. Recuperado 7 de abril de 2023, de https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

Gobierno de Reino Unido. (2010). Review of public sector equality duty. Recuperado 21 de enero de 2023, de https://www.gov.uk/government/groups/review-of-public-sector-equality-duty-steering-group

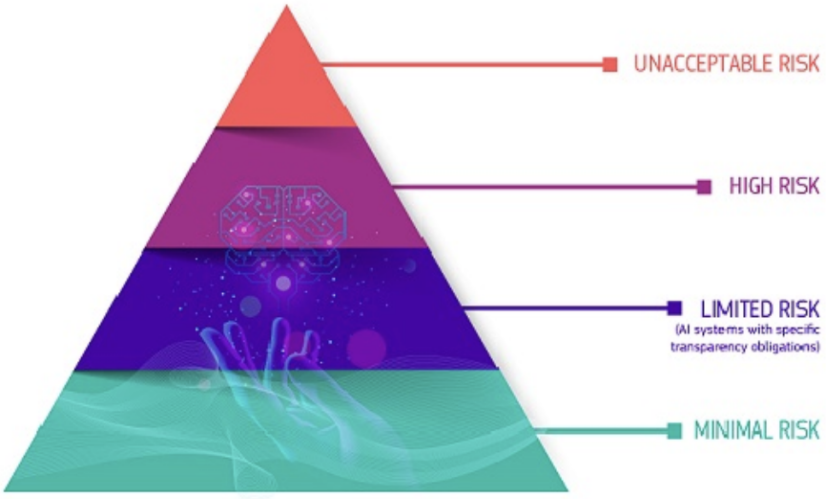
Gobierno de España. (2022b, junio 27). El Gobierno de España presenta, en colaboración con la Comisión Europea, el primer piloto del sandbox de regulación de Inteligencia Artificial en la UE. Recuperado 8 de marzo de 2023, de https://planderecuperacion.gob.es/noticias/el-gobierno-de-espana-presenta-en-colaboracion-con-la-comision-europea-el-primer-piloto

MINECO. (2022, 27 junio). El Gobierno de España presenta, en colaboración con la Comisión Europea, el primer piloto del sandbox de regulación de Inteligencia Artificial en la UE. Recuperado 7 de marzo de 2023, de https://portal.mineco.gob.es/es-es/comunicacion/Paginas/20220627-PR_AI_Sandbox.aspx

Gobierno de España. (2022a). España Digital 2023. Recuperado 14 de marzo de 2023, de https://espanadigital.gob.es/sites/espanadigital/files/2022-07/Espa%C3%B1aDigital_2026.pdf

6. ANEXOS

Anexo A. Un enfoque basado en el riesgo



Fuente: Comisión Europea. (2023). Regulatory framework proposal on artificial intelligence. Recuperado 12 de enero de 2023, de https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Anexo B. Los sistemas biométricos en la propuesta de reglamento de Inteligencia Artificial de la Comisión Europea

CLASIFICACIÓN DE LOS DATOS BIOMÉTRICOS EN PROPUESTA DE REGLAMENTO DE IA

SUPUESTOS	DATOS SENSIBLES	RIESGO ASOCIADO
Verificación o autenticación biométrica [1:1]	NO	Bajo o inexistente
Identificación biométrica [1:N]	SÍ	Bajo o inexistente
Identificación biométrica [1:N] remota "en tiempo real" o "en diferido" de personas físicas, y sin que el usuario del sistema de IA sepa de antemano si la persona en cuestión se encontrará en dicha base de datos y podría ser identificada	SÍ	Alto
Identificación biométrica [1:N] remota "en tiempo real" de personas físicas en espacios de acceso público y sin que el usuario del sistema de IA sepa de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada, con fines de aplicación de la ley	SÍ	Prohibido, salvo excepciones
	RGPD	Propuesta de reglamento de IA de Comisión Europea

Fuente: Veridas. (2022, 7 febrero). Los sistemas biométricos en la propuesta de reglamento de Inteligencia Artificial de la Comisión Europea. Recuperado 6 de febrero

de 2023, de https://veridas.com/docs/Veridas-Datos-biometricos-sistemas-biometricos.pdf

Anexo C. El análisis de las pruebas disponibles sugiere que existen seis problemas principales relacionados entre sí y desencadenados por el desarrollo y el uso de sistemas de IA que la iniciativa actual pretende abordar.

Table 2: Main problems

MAIN PROBLEMS	STAKEHOLDERS CONCERNED
1. Use of AI poses increased risks to safety and security of citizens	Citizens, consumers and other victims Affected businesses
2. Use of AI poses increased risk of violations of citizens' fundamental rights and Union values	Citizens, consumers and other victims Whole groups of the society, Users of AI systems liable for fundamental rights violations
3. Authorities do not have powers, procedural frameworks and resources to ensure and monitor compliance of AI development and use with applicable rules	National authorities responsible for compliance with safety and fundamental rights rules
4. Legal uncertainty and complexity on how existing rules apply to AI systems dissuade businesses from developing and using AI systems	Businesses and other providers developing AI systems Businesses and other users using AI systems
5. Mistrust in AI would slow down AI development in Europe and reduce the global competitiveness of the EU economy	Businesses and other users using AI systems Citizens using AI systems or being affected by them
6. Fragmented measures create obstacles for cross-border AI single market and threaten Union's digital sovereignty	Businesses developing AI, mainly SMEs affected Users of AI system, including consumers, businesses and public authorities

Fuente: Comisión Europea. (2021, 21 abril). EVALUACIÓN DE IMPACTO que acompaña a la Propuesta de Reglamento del Parlamento Europeo y del Consejo. Recuperado 14 de marzo de 2023, de https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021SC0084