Universidad de Oviedo
FACULTAD DE DERECHO

GRADO EN DERECHO

TRABAJO FIN DE GRADO

EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL: ANÁLISIS JURÍDICO DEL USO DE LA BIOMETRÍA

Estudiante: Alba Sanz Prendes

Convocatoria: Extraordinaria primer semestre

DECLARACIÓN DE ACUERDO CON EL ARTÍCULO 8.3 DEL REGLAMENTO SOBRE LA ASIGNATURA TRABAJO FIN DE GRADO

Yo ALBA SANZ PRENDES,

DECLARO

que el TFG titulado (El Reglamento Europeo de Inteligencia Artificial: análisis jurídico del uso de la biometría) es una obra original, de mi propia autoría y que he referenciado debidamente todas las fuentes utilizadas, no habiendo recurrido al plagio, a la realización del trabajo por persona distinta del propio estudiante ni a ningún otro medio fraudulento de elaboración, incluidos los basados en sistemas de inteligencia artificial.

(17/01/2025)

RESUMEN

La adopción del Reglamento Europeo de Inteligencia Artificial ha supuesto el culmen de un proceso social y normativo que lleva gestándose durante décadas a escala global. Este texto europeo se erige como el primer marco normativo integral en el mundo dedicado a regular este tipo de tecnologías. El presente trabajo analiza el contenido del RIA y sus rasgos más importantes, poniendo especial atención en las disposiciones respectivas al uso de la biometría. El análisis examina las implicaciones éticas y legales del empleo de estos sistemas, resaltando los riesgos inherentes a su utilización y que inciden en los derechos fundamentales de la ciudadanía.

El enfoque del estudio emplea una metodología multidisciplinar que deriva en un análisis normativo, jurisprudencial y doctrinal que permite obtener una visión global de los antecedentes al RIA y del propio contenido de este, en concreto en lo respectivo a las prohibiciones impuestas por la norma y las excepciones a las mismas. En definitiva, este análisis busca explicar cómo el Reglamento supone un esfuerzo para equilibrar la innovación tecnológica y la salvaguarda de los derechos fundamentales, creando un marco normativo pionero que servirá como precedente para posteriores regulaciones de estas tecnologías fuera del ámbito de la Unión Europea.

ABSTRACT

The adoption of the Artificial Intelligence Act has been the culmination of a social and regulatory process that has been brewing over decades on a global scale. This text is the first comprehensive regulative framework for this type of technology in the world. The paper analyses the contents of the AI Act and its most important features, paying particular attention to the provisions concerning the use of biometry. The analysis examines the ethical and legal implications of the use of these systems, highlighting the risks inherent in their use that have an impact on the fundamental rights of citizens.

The approach of the study employs a multidisciplinary methodology that encompasses a legal, jurisprudential and doctrinal analysis that provides a global vision of the background to the AI Act and its contents, specifically regarding the prohibitions imposed by the regulation and the exceptions to them. In essence, this paper seeks to explain how the European regulation represents an effort to balance technological innovation and the safeguarding of fundamental rights, creating a pioneering framework that will serve as a precedent for subsequent regulations of these technologies outside the scope of the European Union.

ABREVIATURAS Y ACRÓNIMOS

AEPD.....Agencia Española de Protección de Datos

AESIA.....Agencia Española de Supervisión de la Inteligencia Artificial

AI HLEG ..... Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial

CE ..... Constitución Española de 1978

CNECT .....Dirección General de Redes de Comunicación, Contenido y Tecnologías

DGPN .... Director de la Dirección General de Policía Nacional del Ministerio del Interior

GPAI.....Asociación Global sobre Inteligencia Artificial

IA.....Inteligencia Artificial

IRA ..... Ejército Republicano Irlandés

LOPDD ..... Ley Orgánica de Protección de Datos y de Derechos Digitales

RIA .....Reglamento de Inteligencia Artificial

RGPD .....Reglamento General de Protección de Datos

TEDH.....Tribunal Europeo de Derechos Humanos

TJUE .....Tribunal de Justicia de la Unión Europea

UE .....Unión Europea

ÍNDICE

1. INTRODUCCIÓN

1.1. CONTEXTUALIZACIÓN Y OBJETIVOS DEL TRABAJO

Este trabajo es una síntesis de los procesos sociales y jurídicos que se han observado durante los últimos años en el seno de la Unión Europea, y que son la explicación de la adopción el pasado día 21 de mayo del Reglamento de Inteligencia Artificial por parte del Consejo de la UE[1]. Este acontecimiento ha recibido una amplia cobertura mediática porque supone la primera vez en la que esta tecnología ha sido regulada en el mundo. Tal y como afirmó Mathieu Michel, secretario de Estado de Digitalización de Bélgica:

> "La adopción del Reglamento de Inteligencia Artificial es un hito de gran importancia para la Unión Europea. Este acto legislativo histórico —el primero de este tipo en el mundo— aborda un reto tecnológico mundial que, al mismo tiempo, crea oportunidades para nuestras sociedades y nuestras economías. Con el Reglamento de Inteligencia Artificial, Europa hace hincapié en la importancia de la confianza, la transparencia y la rendición de cuentas a la hora de abordar las nuevas tecnologías y, al mismo tiempo, garantiza que esta tecnología en rápida evolución pueda prosperar e impulsar la innovación europea"[2].

Por otro lado, la adopción de la norma se engloba en un contexto mucho más amplio: las autoridades están empezando a regular las aplicaciones de la Inteligencia Artificial debido al "boom" que han tenido estas tecnologías recientemente. Esta situación genera nuevas posibilidades para los agentes del mercado, pero también grandes riesgos para la sociedad civil, que puede ver afectados sus derechos fundamentales. Según las palabras de Barkane, I.[3], el Reglamento trata de lograr dos objetivos diferenciados, pero no opuestos taxativamente: por un lado, busca favorecer el desarrollo y uso de la IA en el mercado interno europeo; por el otro, crea un ecosistema de confianza al asegurar la seguridad y protección de derechos fundamentales y valores de la UE.

---

[1] Consejo de la Unión Europea. (2024, 21 de mayo). *Artificial Intelligence Act: Council gives final green light to the first worldwide rules on AI*. https://www.consilium.europa.eu/es/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/.

[2] Consejo de la Unión Europea, 2024, ya citado. https://www.consilium.europa.eu/es/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/.

[3] Barkane, I. (2022). "Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance". *Information Polity*, 27(2), pág. 149.

Este no es un análisis en profundidad de todos los elementos este Reglamento, ya que su extensión y complejidad supone el principal límite al estudio: para realizar un examen de todo su contenido, sería conveniente que éste fuera objeto de un análisis pormenorizado e individualizado de sus secciones y preceptos. Pese a ello, este trabajo se consagra como un resumen sistemático de los rasgos diferenciadores del texto y de las principales innovaciones que supone en materia legislativa. Además, se expone un estudio más extenso del artículo 5 del Reglamento de IA, donde se recogen las prácticas prohibidas relacionadas con esta materia. En concreto, se estudiará la prohibición del uso de sistemas de identificación biométrica remota "en tiempo real", y las correspondientes excepciones a este veto.

1.2. EVOLUCIÓN EN EL TIEMPO DE LOS ESFUERZOS DE PRODUCCIÓN NORMATIVA

Cuando escuchamos el término "Inteligencia Artificial" nos da la sensación de que estamos ante una tecnología novedosa, pero en realidad, esta disciplina de investigación apareció en la Conferencia de Dartmouth en el año 1956[4]. Como expone Antonov, A. (2022), la Inteligencia Artificial ha experimentado desde ese momento periodos de rápido desarrollo y otros donde la evolución de esta tecnología se ha estancado, los denominados "inviernos de la IA". No obstante, durante los últimos años se ha venido produciendo una adopción a gran escala de esta tecnología, catalizada por el incremento de la cantidad de datos legibles y procesables, y el aumento de la capacidad computacional de los ordenadores modernos. Este autor afirma que el proceso de innovación relativamente reciente ha tenido una motivación fundamentalmente orientada a fines comerciales, y se ha llevado a cabo en clústeres de investigación privados.

La cronología de los esfuerzos de producción normativa europea se remonta al 21 de abril de 2021, fecha en la que la Comisión publicó su propuesta de regulación de la IA en la UE[5]. No obstante, esta no fue la primera vez donde se abordó esta materia en el marco de la Unión Europea: en 2019 se publicaron las *Directrices éticas para una IA fiable* y las *Recomendaciones de políticas e inversión para una IA fiable*; y en el año 2020 la Comisión presentó el *Libro Blanco sobre la inteligencia artificial*.

[4] Antonov, Alexander. (2022). "Gestionar la complejidad: la contribución de la UE a la gobernanza de la inteligencia artificial". *Revista CIDOB d'Afers Internacionals*, n.º 131 (septiembre de 2022), pág. 46.

[5] Artificial Intelligence Act. (s.f.). *Avances en la regulación de la Inteligencia Artificial*. https://artificialintelligenceact.eu/es/avances/

Los dos primeros documentos fueron elaborados por el Grupo de expertos de Alto Nivel sobre Inteligencia Artificial, en adelante AI HLEG, creado por la Comisión en 2018. En las *Directrices éticas para una IA fiable*[6] se establecen una serie de directrices que buscan crear un marco para tener una IA fiable en la Unión Europea. En resumen, el AI HLEG estableció que la fiabilidad se debe apoyar en tres componentes: la IA debe ser lícita, ética, y robusta. En el capítulo II del documento se enumeran siete requisitos que deben cumplir los sistemas de IA para ser fiables:

1) Acción y supervisión humanas
2) Solidez técnica y seguridad
3) Gestión de privacidad y de los datos
4) Transparencia
5) Diversidad, no discriminación y equidad
6) Bienestar ambiental y social
7) Rendición de cuentas

Mientras que este primer documento subraya la importancia de desarrollar un enfoque respecto la IA centrado en el propio ser humano, las *Recomendaciones de políticas de inversión para una IA fiable*[7] tratan de actuar como una guía para lograr la sostenibilidad, crecimiento, competitividad e inclusión en el uso de estas tecnologías[8]. Por otro lado, el AI HLEG no ha llevado a cabo un trabajo autónomo, sino que ha actuado a través del marco de AI Alliance[9], un foro *online* integrado por representantes del sector académico, empresarial, político, así como miembros de la sociedad civil y ciudadanos de la UE. El mandato del AI HLEG generó resultados de gran utilidad para delimitar el enfoque de la Comisión respecto a la Inteligencia Artificial, siendo fundamental en el posterior desarrollo legislativo.

En 2020 Bruselas publicó el *Libro Blanco sobre la inteligencia artificial*[10], donde se asienta el enfoque europeo basado en dos conceptos fundamentales: la excelencia y la

---

[6] AI HLEG – High-level Expert Group on Artificial Intelligence. (Abril de 2019). *Ethics guidelines for trustworthy AI*. Comisión Europea. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[7] AI HLEG – High-level Expert Group on Artificial Intelligence. (abril de 2019). *Policy and investment recommendations for trustworthy Artificial Intelligence*. Comisión Europea. https://digitalstrategy.ec.europa.eu/en/library/policyandinvestmentrecommendationstrustworthy-artificial-intelligence

[8] European Commission. (s.f.). *High-Level Expert Group on Artificial Intelligence (AI HLEG)*. https://digital-strategy.ec.europa.eu/es/policies/expert-group-ai

[9] The Global Partnership on Artificial Intelligence (GPAI). (s.f.). *Home*. https://thealliance.ai/

[10] Comisión Europea**.** (2020). *Libro Blanco sobre la inteligencia artificial: Un enfoque europeo orientado a la excelencia y la confianza*. https://ec.europa.eu/

confianza. En su contenido, la Comisión introduce el doble enfoque que caracteriza el desarrollo legislativo posterior, tratando de promover la innovación y el desarrollo de esta tecnología, pero defendiendo que esto se produzca de forma ética y segura. La Comisión afirma en este documento que el uso de la Inteligencia Artificial puede incrementar la calidad de vida de los ciudadanos, mejorando la actuación en sectores como la sanidad, la industria y la agricultura. No obstante, también reconoce la existencia de los riesgos vinculados a esta tecnología, como la opacidad en su funcionamiento, la vulneración del derecho de privacidad de las personas, o la discriminación que se puede generar por su uso. Estos documentos fueron una fuente de inspiración para la primera propuesta por parte de la Comisión en el año 2021, que fue evolucionando y enmendándose durante los últimos años hasta alcanzar un texto que fue objeto de acuerdo entre Parlamento y Consejo el pasado mes de diciembre de 2023. Finalmente, el Consejo Europeo adoptó el Reglamento de IA el 21 de mayo de 2024[11].

Por otro lado, la materia está relacionada en muchos ámbitos relativos al tratamiento de datos personales con el contenido del Reglamento General de Protección de Datos. En concreto, la identificación biométrica está sujeta a las disposiciones contenidas en la Directiva 2016/680 y en la propia RGDP 2016/679[12]. Además, su contenido también se vincula con las disposiciones de la Carta de Derechos Fundamentales de la Unión Europea[13]. En clave nacional, el tratamiento de datos de carácter personal también está regulada por la Ley Orgánica de Protección de Datos Personales. Más adelante se estudiarán las incidencias que tiene el nuevo Reglamento de Inteligencia Artificial como norma armonizadora de la actual regulación nacional y europea.

1.3. METODOLOGÍA

En este trabajo la metodología seleccionada es multidisciplinar, tal y como defienden Felländer, A., Rebane, J., Larsson, S., Wiggberg, M., & Heintz, F. (2022). Estos autores afirman que el enfoque organizacional de la IA debe combinar aspectos tecnológicos y científicos, así como visiones desde un punto de vista humanístico y ético sobre la

[11] Artificial Intelligence Act. (s.f.). *Avances*. https://artificialintelligenceact.eu/es/avances/

[12] Ministerio de Asuntos Económicos y Transformación Digital. (noviembre de 2023). *Resumen del Reglamento Europeo de Inteligencia Artificial*. https://portal.mineco.gob.es/es-es/digitalizacionIA/sandbox-IA/Documents/20220919_Resumen_detallado_Reglamento_IA.pdf

[13] Barkane, I. (2022). “Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance” 1. *Information Polity*, 27(2), pag. 149.

gobernanza de estas tecnologías. Así, esta aproximación debe ser "desarrollada desde una perspectiva holística y multidisciplinar, que incorpore puntos de vista técnicos, legales y sociales; con el objetivo de detectar externalidades negativas por parte de las organizaciones, que de otra forma podrían infringir derechos y libertades, así como principios organizativos".[14] Por un lado, es necesario definir los criterios de análisis respecto a una materia englobada dentro del derecho de la UE. Por otro, también es importante clarificar los esquemas de actuación para llevar a cabo un estudio de este tipo de tecnologías.

En primer lugar, siguiendo la línea de pensamiento de Bastos, F. B. (2023), este análisis trata de distanciarse de las "preconcepciones nacionales"[15], que pueden llegar a producir sesgos cuando se examina la legislación europea. Por tanto, el trabajo se enfoca desde un punto de vista endógeno a la Unión Europea, por lo que las referencias a la normativa española serán superficiales y a modo de comparativa. No obstante, como recalca este autor: "no se pretende negar la importancia de la profunda interdependencia que existe entre el derecho nacional y el derecho de la UE"[16]. Por otro lado, Hervey, T., Cryer, R., Sokhi-Bulley, B., & Bohm, A. (2011) explican las consideraciones que han de tomarse respecto a un objeto de estudio caracterizado por la intersección de derecho y tecnología. Es necesario estudiar la regulación tecnológica, y en concreto la destinada a ordenar la Inteligencia Artificial, que plantea desafíos particulares al englobar problemáticas como la privacidad de los datos tratados, la justificación de las decisiones tomadas a partir de logaritmos, o como se pueden encajar cuestiones éticas en su uso.

Para el análisis se ha realizado una revisión bibliográfica extensa, donde en primer lugar se ha utilizado el propio texto del Reglamento de Inteligencia Artificial, así como las diferentes versiones que han existido de este antes de la adopción del documento final. Además, una gran parte del estudio se ha realizado a través del análisis de fuentes académicas secundarias, estudiando los trabajos de autores españoles y extranjeros que han publicado sus propios textos acerca de los diferentes elementos del Reglamento, así como de la propia disciplina de estudio de la Inteligencia Artificial, y específicamente de las tecnologías de identificación mediante el uso de biometría. Un

[14] . Felländer, A., Rebane, J., Larsson, S., Wiggberg, M., & Heintz, F. (2022). Achieving a data-driven risk assessment methodology for ethical AI. *Digital Society*, *1*(2), 13. Pág. 3.

[15] Bastos, F. B. (2023). Metodología doctrinal en el derecho administrativo de la UE: reaccionar frente a la "impronta estatal*". Revista de Derecho Público: teoría y método*, 8, pág. 53.

[16] Ibid., pág. 54.

límite al estudio en este sentido es la escasez de fuentes secundarias que versen sobre el texto final del RIA, debido a su novedad en el momento de realizar este análisis.

Por otro lado, también son muy relevantes los textos no normativos emitidos por las diferentes instituciones de la UE, así como de las autoridades competentes en nuestro territorio nacional. Estos documentos muchas veces son la inspiración de los posteriores frutos legales, y para entender los resultados finales de los procesos normativos es importante analizar sus antecedentes y estos textos informativos publicados por comités de expertos en la materia.

1.4. BÚSQUEDA DE FUENTES

Para hallar las fuentes sobre las que se sustenta este estudio, se ha recurrido a motores de búsqueda académicos, como Google Académico, Dialnet, o desde la propia Biblioteca de la Universidad de Oviedo. En relación al análisis jurisprudencial, las principales fuentes empleadas fueron fruto del uso de herramientas como Aranzadi Instituciones, CENDOJ, o, en el caso de las sentencias europeas, CURIA.

Además, han sido de gran utilidad los materiales publicados por los propios órganos de la Unión Europea, como puede ser el texto final del Reglamento, las propuestas previas a él, o la emisión de informes de expertos por parte de la Comisión. Por otro lado, páginas web como https://www.consilium.europa.eu/es/ o https://artificialintelligenceact.eu/es/ también han sido de gran ayuda para consultar de forma simplificada las distintas fuentes y para estar al tanto de los avances que se han producido en esta materia durante los últimos meses en el seno de la UE.

2. JURISPRUDENCIA RELACIONADA

2.1. SENTENCIAS EUROPEAS

Wendehorst, C., & Duller, Y. (2021) en su estudio solicitado por los comités JURI y PETI en el seno del Parlamento Europeo enumeran varias sentencias tanto del TEDH como del TJUE relacionadas con la recogida y el uso de datos biométricos.

2.1.2. SENTENCIAS DEL TEDH

Existe jurisprudencia de este Tribunal de relativa antigüedad acerca de la recogida y almacenamiento de fotografías personales, y de cómo estas situaciones pueden afectar al derecho de privacidad de los ciudadanos. En concreto, la sentencia Murray v. Reino

Unido[17], del año 1994, resuelve un caso en el que se produjo la detención de una persona por presuntos vínculos con la financiación de la compra de armas por parte del IRA. Durante esa detención, se procedió a recolectar fotografías de la persona sin su consentimiento, imágenes que después fueron conservadas en los archivos del cuerpo policial. La Gran Cámara resolvió afirmando que la toma de datos biométricos básicos, como puede ser una fotografía, no excede los límites procedimentales en la investigación de delitos de terrorismo. En la resolución se establece que "la toma y retención de una fotografía de la parte afectada sin su consentimiento, aunque no se asentó sobre una base normativa, […] fue lícita bajo los principios del *common law*".[18]

En otra instancia, la sentencia S. and Harper v. Reino Unido[19] se refiere a la recolección y almacenamiento de otros datos biométricos, como pueden ser muestras de ADN o huellas dactilares. En este caso, los demandantes consideraban que se había vulnerado el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, ya que las fuerzas de la autoridad tomaron sus muestras biométricas en el marco de detenciones policiales, y esta información se almacenó de forma indefinida a pesar de que finalmente ambos sujetos fueron absueltos y no se presentaron cargos contra ellos.

El contenido del artículo 8 es el siguiente:

3. Artículo 8.

> 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
>
> 2. 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 del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

El Tribunal procedió en primer lugar a examinar si realmente se produjo una inferencia en su vida privada a causa de la conservación de las huellas dactilares, los perfiles de

[17] Tribunal Europeo de Derechos Humanos (TEDH). (1994, 28 de octubre). *Murray v. United Kingdom* (Solicitud núm. 14310/88).

[18] Tribunal Europeo de Derechos Humanos (TEDH). (1994, 28 de octubre). *Murray v. United Kingdom* (Solicitud núm. 14310/88). Pág.29.

[19] Tribunal Europeo de Derechos Humanos (TEDH). (2008, 4 de diciembre). *S. and Marper v. the United Kingdom* (Solicitudes núm. 30562/04 y 30566/04).

ADN y las muestras celulares por parte de las autoridades policiales. El órgano judicial resolvió que las tres prácticas de recolección de datos suponen efectivamente una intromisión en la privacidad de los ciudadanos, tal y como comentan Wendehorst, C., & Duller, Y. (2021), siendo menos importante la interferencia en el caso de las huellas dactilares, ya que el ADN contiene más información y de carácter más sensible sobre los sujetos. El Tribunal también tuvo en cuenta en su postura el "posible uso que se le puede dar al material celular en el futuro, donde la retención sistemática de dicho material es suficientemente intrusiva para ser considerada como una interferencia al derecho al respeto de la vida privada"[20].

Respecto a la justificación de la intromisión en la vida privada, el órgano juzgador afirma que, para estar fundada, la interferencia debe ser considerada como "necesaria en la sociedad democrática, y para ello, debe ser proporcionada al objetivo perseguido, y las razones para justificarla debe ser relevantes y suficientes""[21]. En este supuesto, el Tribunal reconoció que la lucha contra el crimen es un objetivo primordial en la sociedad contemporánea; pero también recuerda que las autoridades deben respetar los principios relativos a la protección de datos, ya que "la retención de datos debe ser proporcional al propósito de su recogida y debe basarse en periodos temporales limitados respecto a su almacenamiento"[22].

Así, el Tribunal también analiza el hecho de que Reino Unido es uno de los países pioneros en el uso de la información contenida en el ADN para fines relacionados con la prevención y detención del crimen, empleando tecnologías vanguardistas y complejas en su funcionamiento. En su resolución, el órgano establece que estos Estados que están en primera posición en la carrera tecnológica también deben encontrar un balance frente a las posibles consecuencias que puede desencadenar la utilización de estas tecnologías. En concreto, el Tribunal consideró que el almacenamiento indefinido de la información biométrica en los archivos policiales suponía una vulneración a la presunción de inocencia de estas personas, ya que sus datos eran tratados de la misma manera que los de sujetos condenados por crímenes, cuando los primeros habían sido absueltos. En conclusión, el órgano afirmó que "no se alcanzó un balance justo entre los intereses públicos y privados en juego, y que el Estado se había excedido en su actuación. Asimismo, la retención supuso una interferencia desproporcionada en el

[20] Tribunal Europeo de Derechos Humanos (TEDH). (2008, 4 de diciembre). *S. and Marper v. the United Kingdom* (Solicitudes núm. 30562/04 y 30566/04), párrafo 70, pág. 22.

[21] Ibid., párrafo 101, pág.29.

[22] Ibid., párrafo 107, pág. 31.

derecho de los demandantes al respecto de su vida privada, que no se puede considerar necesaria en la sociedad democrática".[23] Por todo esto, el órgano resolvió que el almacenamiento indefinido suponía una violación del artículo 8 del Convenio.

En último lugar, en la reciente sentencia Glukhin c. Rusia[24] el Tribunal examinó la condena de un sujeto que viajó en el metro de Moscú con una figura de cartón de Konstantin Kotov, otro individuo que fue arrestado y condenado por vulnerar repetidamente el artículo 212.1 del Código Criminal Ruso, relativo a las reglas sobre eventos públicos. El día 23 de agosto de 2019 el demandante fue grabado llevando dicha pancarta, donde aparecía un texto que decía ""You must be f**king kidding me. I'm Konstantin Kotov. I'm facing up to five years [in prison] under [Article] 212.1 for peaceful protests."[25] Posteriormente, la policía lo detuvo, alegando que había sido identificado a través de cámaras de seguridad ubicadas en el metro que empleaban un sistema de reconocimiento facial. El demandante alegó que se vulneró en la actuación el artículo 10 del Convenio, relativo a la libertad de expresión, así como el artículo 8, relativo al derecho a la privacidad.

El artículo 10 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales se lee:

> Artículo 10.
>
> 1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa.
>
> 2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos,

[23] Ibid., párrafo 125, pág. 35.

[24]Tribunal Europeo de Derechos Humanos (TEDH). (2023, 4 de julio). *Glukhin c. Rusia* (Solicitud núm. 11519/20).

[25]Tribunal Europeo de Derechos Humanos (TEDH). (2023, 4 de julio). *Glukhin c. Rusia* (Solicitud núm. 11519/20), párrafo 7, pág.2.

para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial.

El Tribunal resolvió que el arresto del demandante y su condena por la vía administrativa constituyeron una inferencia en su derecho a la libertad de expresión, ya que los actos objeto de estudio están protegidos por el artículo 10.

Por su parte, el Gobierno ruso alegó que la condena fue lícita -estando amparada por el Derecho ruso- ya que es necesario notificar a las autoridades antes de organizar eventos públicos y el demandante no había satisfecho este requisito. No obstante, el Tribunal afirmó que estas acciones fueron indiscutiblemente pacíficas y no interrumpieron de forma alguna la vida de los transeúntes ni supusieron ningún peligro al orden público o a la seguridad del transporte. Bajo la perspectiva del órgano judicial, "las autoridades no mostraron el grado requerido de tolerancia"[26], y, por tanto, se constató una vulneración al artículo 10.

Respeto a la violación del artículo 8, el demandante afirmaba en autos que su detención se basó en una identificación realizada mediante la tecnología de reconocimiento facial. No hubo ninguna decisión judicial autorizando la recogida de esta información biométrica, ni tampoco su almacenamiento o posterior utilización en el procedimiento. El Tribunal, en línea con su jurisprudencia, afirmó que "la recogida y el almacenamiento de datos por las autoridades respecto a individuos particulares constituyen una interferencia con la vida privada de las personas, hasta cuando esa información se basa exclusivamente en las actividades públicas del individuo, como puede ser su participación en protestas contra el Gobierno"[27].

Por otro lado, siguiendo el artículo 8.2., el órgano consideró que sí que existía una habilitación legal permitiendo dicha intromisión, pero se planteó si esta cumplía los requisitos de legalidad necesarios. El Tribunal declaró que "es esencial en el contexto de implementación de tecnologías de reconocimiento facial la existencia de reglas específicas que rijan el alcance y aplicación de medidas, así como salvaguardias contra el riesgo de abuso y arbitrariedad"[28]. La ley nacional no contenía ninguna limitación en su uso, y establecía que podía emplearse esta tecnología en cualquier procedimiento judicial. El Tribunal consideró estas medidas "particularmente intrusivas"[29], indicando

[26] Ibid., párrafo 56, pág.20.

[27] Ibid., párrafo 67, pág. 22.

[28] Ibid., párrafo 82, pág. 26.

[29] Ibid., párrafo 86, pág. 27.

que no se correspondían con una urgente necesidad que las justificase. Por tanto, estas actuaciones no se pueden considerar necesarias en una sociedad democrática, y suponen una vulneración al artículo 8 del Convenio.

2.1.2. SENTENCIAS DEL TJUE

En el marco de la Unión Europea no existe tanta jurisprudencia respecto al uso de la identificación a partir de datos biométricos como la examinada anteriormente procedente del TEDH. No obstante, existen algunos pronunciamientos del Tribunal de Justicia de la Unión Europea respecto a la recolección y almacenamiento de datos de carácter personal y biométrico.

La primera sentencia analizada es Schwarz c. Stadt Bochum[30] del año 2013. En este caso, el Sr. Schwarz solicitó la expedición de un pasaporte, negándose a que se tomaran sus huellas digitales para ello. El Reglamento 2252/2004 establece la obligación de recolectar dos huellas dactilares completas y una imagen facial a la hora de expedir un pasaporte para los nacionales europeos. El demandante impugnó la validez de esta norma considerando que vulneraba los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea, relativos al derecho a la vida privada y al derecho a la protección de datos de carácter personal, respectivamente.

El Tribunal comienza analizando si existe dicha vulneración, y establece que ésta puede llegar a existir cuando hay un tratamiento de datos personales por un tercero. El órgano afirma que "las impresiones dactilares están comprendidas en este concepto [como datos personales] por contener objetivamente información única sobre personas físicas y permitir su identificación precisa"[31]. A colación de esto, el artículo 1 del Reglamento 2252/2004 habilita a las autoridades nacionales para que recojan las huellas dactilares de los interesados en el pasaporte, conservando las mismas en el propio documento identificativo. Esto supone un tratamiento de datos personales, por lo que existe una afectación de los derechos recogidos en los artículos 7 y 8 de la Carta.

El Tribunal procede a analizar si dicha inferencia es justificada. El órgano judicial recuerda que estos derechos no son unas prerrogativas absolutas, sino que "deben ser considerados en relación con su función en la sociedad"[32]. Este criterio se materializa en el apartado 1 del artículo 52 de la Carta, donde se permiten las limitaciones en el

[30] Tribunal de Justicia de la Unión Europea (TJUE). (2013, 17 de octubre). *Schwarz c. Stadt Bochum* (Asunto C-291/12)

[31] Tribunal de Justicia de la Unión Europea (TJUE). (2013, 17 de octubre). *Schwarz c. Stadt Bochum* (Asunto C-291/12), párrafo. 27.

[32] Ibid., párrafo 33.

ejercicio de los derechos que en ella se contienen siempre que se respete su contenido esencial, el principio de proporcionalidad, y el requisito de que las limitaciones respondan a objetivos de interés general dentro de la Unión Europea o a la necesidad de protección de derechos y libertades.

Respecto al contenido del Reglamento 2252/2004, podemos afirmar que en él se persiguen claramente dos objetivos: evitar la falsificación de pasaportes e impedir su uso fraudulento por personas que no son sus titulares legítimos. Su meta común es prevenir la entrada ilegal de individuos no autorizados en la Unión Europea. Por tanto, el Tribunal declara que el instrumento normativo sí que busca un objetivo de interés general para la UE; y que no hay nada que indique que dichas previsiones no respetan el contenido esencial de los derechos de los artículos 7 y 8. En lo relativo al principio de proporcionalidad, el órgano afirma que el método de verificación de la identidad mediante el uso de las huellas dactilares es el idóneo para alcanzar los objetivos planteados en el Reglamento. Respecto a la existencia de medidas menos lesivas para alcanzar este propósito, el Tribunal admite la existencia de otro método: la captación de imágenes del iris del ojo. No obstante, esta tecnología no estaba tan desarrollada en ese momento como la de identificación de huellas dactilares, y además era más costosa que la primera, haciéndola "menos apta para su uso generalizado"[33].

El Tribunal continúa citando la sentencia del TEDH S. y Marper c. Reino Unido, antes comentada, respecto a la que se declara que "el legislador debe asegurarse de que existen garantías específicas destinadas a proteger eficazmente tales datos contra los tratamientos inapropiados y abusivos"[34]. El Reglamento 2252/2004 establece que las huellas solo serán empleadas con un único fin: verificar la autenticidad del pasaporte y la identidad del titular de éste. Por tanto, el órgano judicial declara que la vulneración de los derechos recogidos en la Carta está justificada por "el objetivo de proteger los pasaportes contra su uso fraudulento"[35], y, por tanto, el Reglamento 2252/2004 no adolece de motivos de invalidez.

El TJUE se reafirmó en su jurisprudencia en la reciente sentencia RL c. Landeshauptstadt Wiesbaden[36], en la que se alega la invalidez del Reglamento 2019/1157 (que establece que los documentos de identidad expedidos por los EEMM

[33] Ibid., párrafo 52.

[34] Ibid., párrafo 55.

[35] Ibid., párrafo 64.

[36] Tribunal de Justicia de la Unión Europea (TJUE). (2024, 21 de marzo). *RL c. Landeshauptstadt Wiesbaden* (Asunto C-61/22).

deben contener dos impresiones dactilares completas), por haber infringido los artículos 7 y 8 de la Carta. El Tribunal considera que "tales datos personales permiten la identificación precisa de las personas físicas de que se trate y son particularmente sensibles debido a los importantes riesgos para los derechos y las libertades fundamentales que su utilización puede presentar"[37]. Además, esta obligación lleva aparejadas dos operaciones de tratamiento de datos personales: la recogida de las huellas dactilares y, posteriormente, su almacenamiento provisional. Todo ello constituye una vulneración a los derechos contenidos en los artículos 7 y 8 de la Carta. El órgano judicial reitera la existencia de una justificación a esta intromisión: las limitaciones garantizan el principio de legalidad al estar recogidas y desarrolladas con claridad y precisión en el Reglamento 2019/1157, y en ellas se respeta el contenido esencial de estos derechos, salvaguardando de igual manera el principio de proporcionalidad.

En palabras del Tribunal:

> "En el caso de autos, la integración de dos impresiones dactilares completas en el medio de almacenamiento de los documentos de identidad es idónea para alcanzar los objetivos de interés general de lucha contra la producción de documentos de identidad falsos y la suplantación de identidad, así como de interoperabilidad de los sistemas de verificación, invocados por el legislador de la Unión para justificar dicha medida."[38]

Por otro lado, las huellas dactilares, por su condición de datos biométricos y particularmente sensibles, tienen una protección específica en el Derecho de la UE. Ello se ve reflejado en que las impresiones dactilares solo están autorizadas en el marco del Reglamento 2019/1157 con el objetivo de ser almacenadas en el propio documento de identidad, que está en poder del interesado en su expedición. Además, esta norma también se opone a que se realice una conservación de forma centralizada de estos datos que busque ir más allá de su almacenamiento provisional para gestionar la expedición del documento de identidad. Por tanto, a ojos del Tribunal, la limitación de los derechos contenidos en la Carta no viola tampoco el principio de proporcionalidad, por lo que esta afectación no es motivo de invalidez del Reglamento 2019/1157.

En último lugar, el TJUE dictó una sentencia con gran relevancia en 2024, relativa al tratamiento de datos personales por parte de las autoridades en supuestos relacionados

---

[37] Tribunal de Justicia de la Unión Europea (TJUE). (2024, 21 de marzo). *RL c. Landeshauptstadt Wiesbaden* (Asunto C-61/22).), párrafo 72.

[38] Ibid., párrafo 89.

con la jurisdicción penal. En la sentencia NG v. DGPN[39] se analiza la denegación de la autoridad estatal de la solicitud de cancelar un asiento en el registro policial donde se inscriben los delitos públicos dolosos en Bulgaria. Esta petición se fundó en que el sujeto solicitante fue beneficiario de una rehabilitación tras haber sido condenado por una sentencia penal firme. La persona condenada y posteriormente objeto de la rehabilitación alegó que los datos relativos a su historial penal seguían conservándose dentro del registro policial, y que las autoridades podían seguir tratando dicha información. La única limitación temporal que supondría la salida de sus datos personales del registro sería el fallecimiento del sujeto en cuestión. Esto supone una vulneración al artículo 8 de la Carta, relativo al derecho de protección de los datos personales. Este tipo de datos biométricos se encuentra dentro de la categoría especial de datos personales a la que se dedica el artículo 10 de la Directiva 2016/680. La norma de transposición búlgara prevé la conservación de este tipo de información de forma indefinida hasta el fallecimiento del sujeto. Por otro lado, tampoco se reconoce al interesado ninguna potestad para que pueda suprimir esos datos ni limitar su tratamiento.

En primer lugar, el Tribunal recuerda que "los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales, garantizados en los artículos 7 y 8 de la Carta, no constituyen prerrogativas absolutas, sino que deben considerarse según su función en la sociedad y ponderarse con otros derechos fundamentales"[40]. En virtud de la Directiva 2016/680, la conservación de los datos supone una intromisión en estos derechos fundamentales, aunque los datos almacenados no sean empleados posteriormente. Por otro lado, el artículo 4, apartado 1, letra e) del instrumento normativo establece que el periodo de conservación de la información no debe ser superior al que sea estrictamente necesario para cumplir con los fines fijados. Los propios EEMM son los competentes para fijar los plazos apropiados para cumplir la normativa europea.

La Directiva 2016/680 recoge el derecho de los interesados de solicitar la supresión de los datos cuando el almacenamiento de estos haya perdido su utilidad. El Tribunal considera que:

> "Las disposiciones de la Directiva establecen un marco general que permite garantizar […] que la conservación de datos personales y, más concretamente, su duración, se limiten a lo que resulte necesario para los fines para los que se

[39] Tribunal de Justicia de la Unión Europea (TJUE) (2024, 30 de enero) *NG y Direktor na Glavna direktsia Natsionalna politsia pri Ministerstvo na vatreshnite raboti — Sofia* (Asunto C-118/22).

[40] Tribunal de Justicia de la Unión Europea (TJUE) (2024, 30 de enero) *NG y Direktor na Glavna direktsia Natsionalna politsia pri Ministerstvo na vatreshnite raboti — Sofia* (Asunto C-118/22), párrafo 39.

> conserva tales datos al tiempo que dejan a los Estados miembros la tarea de determinar, respetando ese marco, las situaciones concretas en las que la protección de los derechos fundamentales del interesado requiere la supresión de tales datos y el momento en el que esta debe producirse. […] Estas disposiciones no exigen que los Estados miembros establezcan límites temporales absolutos para la conservación de los datos personales, más allá de los cuales deban suprimirse automáticamente".[41]

Respecto a la utilidad de los datos personales contenidos en los registros, el órgano judicial admite que esta información puede resultar conveniente para investigar otros delitos diferentes que hayan podido cometer los mismos sujetos; o, en caso contrario, pueden favorecer a la exculpación de delitos que no han cometido mediante la comparación de los datos biométricos contenidos en los registros.

El Tribunal analiza la proporcionalidad de la conservación, así como la adecuación de las medidas tomadas en virtud del Derecho nacional para asegurar la confidencialidad y seguridad de la información almacenada. Respecto al plazo de almacenamiento, destaca que solamente es indefinido y hasta el fallecimiento del sujeto cuando se trata de individuos condenados por sentencias firmes en casos de delitos públicos dolosos. El órgano señala que el término "delito público doloso" no es específico, y por tanto es aplicable a una amplia categoría de delitos. Esto provoca que no todos los individuos condenados firmemente tengan el mismo riesgo de reincidir en otras infracciones a ley, por lo que no se justifica que haya un plazo uniforme de conservación que no esté modulado en atención a las características de cada caso. En los supuestos en los que el riesgo de reincidencia sea mínimo, no está justificada la limitación de los derechos fundamentales por el fin perseguido.

Por tanto, el Tribunal declara que el Derecho doméstico, que regula la recogida y conservación de datos personales en todos los casos donde existe una condena firme por delitos públicos dolosos, no cumple el requisito contenido en el artículo 10 de la Directiva 2016/680, relativo a la estricta necesidad. El órgano afirmó respecto a la obligación de los EEMM de fijar plazos apropiados para dicho almacenamiento, que estos deben incluir una valoración de las circunstancias que justifican la conservación. Así, esto no ocurre cuando "es aplicable de manera general e indiferenciada a toda persona condenada mediante sentencia firme"[42]. El órgano decisor falla en que la normativa nacional se opone al contenido del Derecho de la UE, ya que establece la

[41] Ibid., párrafo 52.

[42] Ibid., párrafo 68.

conservación de datos biométricos hasta el fallecimiento de los sujetos. Además, en el Derecho nacional no se prevé la revisión periódica acerca de la utilidad de dicho almacenamiento, ni el derecho de los interesados de solicitar la supresión de los datos personales cuando estos ya no sean necesarios para los objetivos para los que se recabaron.

2.2. SENTENCIAS NACIONALES

En relación con la jurisprudencia nacional, existen dos sentencias esenciales para este estudio, que se refieren al uso de tecnología de reconocimiento facial automático por parte de las autoridades policiales, y al reconocimiento facial en el contexto laboral.

En el caso de Inglaterra, la sentencia R (Bridges) c. CCSWP y SSHD constituye un importante exponente jurisprudencial[43]. La problemática legal se basa en el uso de un sistema de reconocimiento facial automático (AFR, por sus siglas en inglés) en eventos públicos por parte de los cuerpos de seguridad ingleses. En el asunto se cuestiona si esta utilización vulnera el artículo 8 del Convenio Europeo de Derechos Humanos, la normativa relativa a la protección de datos personales, o el principio de igualdad al generar discriminación a través de sesgos.

El contenido del artículo 8 es el siguiente:

3. Artículo 8.

> 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
>
> 2. 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 del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

El Alto Tribunal analiza el empleo del sistema "*AFR Locate"*, en el que el cuerpo policial colocó en una serie de eventos cámaras de videovigilancia que tomaban imágenes de los asistentes. Estas fotografías eran procesadas en tiempo real y se comparaban con otras imágenes de personas dentro de listas de interés elaboradas por la Policía del Sur de Gales (SWP). El demandante, Edward Bridges, alegó que esta tecnología era

[43] High Court of Justice (Divisional Court of Cardiff) (2019, 4 de septiembre) *Case No: CO/4085/2018, EWCH 2341.*

contraria a los dispuesto en el artículo 8 del Convenio al no respetar la vida privada de las personas; y que, además, infringía el deber de igualdad al que deben de someterse los cuerpos estatales en el ejercicio de su autoridad.

En la sentencia, el Alto Tribunal examina tres elementos relativos a la vulneración del artículo 8: si el uso del AFR suponía verdaderamente una intromisión al derecho recogido en el precepto, si en el caso de que se hubiera producido una interferencia esta estaba prevista en el apartado 2 de dicho artículo; y finalmente, si la injerencia respeta el principio de proporcionalidad.

Respecto al primer análisis, el Alto Tribunal replica fielmente la jurisprudencia del TEDH, refiriéndose a la "vida privada como un concepto amplio que no es susceptible de una definición exhaustiva, pero que, en cualquier caso, no se puede restringir a los ámbitos más propios de la esfera íntima de la persona".[44] No obstante, el órgano recalca que este no es un derecho sin limitaciones, y que la simple toma de una fotografía en la pública, si no va acompañada de otras circunstancias agravantes, no supone por si sola una intromisión en la vida privada de los ciudadanos. El Alto Tribunal se basa en la jurisprudencia del TEDH y afirma que la injerencia se produce porque existe un almacenamiento posterior de estas imágenes. La toma de datos biométricos es una fuente de información sobre las personas, no solamente las que son grabadas por las cámaras en eventos públicos, sino también de las que están en las listas de interés creadas por la policía inglesa. Carrasco, I. M (2020) argumenta que esta justificación no es la ideal ya que la vulneración de la vida privada no tiene su origen en el almacenamiento, que es instantáneo porque las imágenes se procesan en tiempo real, sino que una argumentación más sólida tendría que basarse en "el contexto en el que la información es recogida, el carácter de los datos consignados, la manera en la que son utilizados y tratados y los resultados que pueden extraerse de ellos".[45]

Una vez constada la vulneración al artículo 8, el órgano judicial examina si esta limitación está amparada por el segundo apartado del precepto. El primer elemento de estudio es si la intromisión está habilitada por la legislación: el Alto Tribunal considera que los miembros de las fuerzas de la autoridad tienen el deber de proteger el orden público y luchar contra la actividad delictiva. Este deber está vinculado a la potestad de tomar medidas que tengan como objetivo detectar y prevenir delitos. El órgano afirma

[44] Carrasco, M. I. (2020). La utilización policial de los sistemas de reconocimiento facial automático. *Ius et Veritas,* (60), Pág. 90.

[45] Carrasco, M. I. (2020). La utilización policial de los sistemas de reconocimiento facial automático*. Ius et Veritas*, (60), Pág. 95.

que la policía no necesita una habilitación legal específica para poner en funcionamiento una tecnología como la del *AFR Locate*. En segundo lugar, la sentencia establece que existe un marco normativo que cumple los requisitos de claridad, suficiencia, accesibilidad y previsibilidad, y que regula correctamente el uso del reconocimiento facial automático. Por último, el Alto Tribunal realiza un juicio proporcionalidad, donde se descartó que la utilización del sistema fuera desproporcionada principalmente porque la intromisión al derecho de los ciudadanos era mínima y solo limitada a un procesamiento momentáneo, después del cual se eliminaban automáticamente los datos biométricos de los afectados.

Respecto al tratamiento de datos de carácter personal, es notable que los datos biométricos constituyen este tipo de información a la luz del artículo 4 del RGPD. Por tanto, las autoridades policiales están obligadas a procesarlos en conformidad con esta normativa, particularmente cumpliendo los dispuesto en el artículo 6 del Reglamento, relativo a la necesidad de licitud.

A ojos del Alto Tribunal, el supuesto de hecho queda recogido dentro del contenido del artículo 6 f):

> "6.f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño".

Además, el órgano juzgador también sostiene que se cumple lo dispuesto por la Directiva 2016/680, que en su artículo 10 se refiere al tratamiento de datos biométricos.

Por último, la parte demandante también alegó que el uso del *AFR Locate* tenía consecuencias discriminatorias entre los ciudadanos. El órgano judicial, en cambio, sostuvo que no había evidencias reales de que este sistema produjera resultados discriminatorios ni sesgos notables entre las distintas personas. La sentencia también reitera que el procesamiento automático no se traduce en la toma de decisiones automatizadas, sino que las actuaciones se llevan a cabo por miembros de la policía, que revisan la información y toman decisiones de forma autónoma.

La segunda resolución está en clave nacional: se trata de la Sentencia nº190/23[46], resuelta por el Juzgado de lo Social de Alicante en septiembre de 2023. La parte actora

[46] Juzgado de lo Social N°. 2 de Alicante/Alacant (2023, 15 de septiembre) *Sentencia 190/2023, Rec. 489/2023.*

alega que no prestó su consentimiento para que la empresa de la que era empleado usara su imagen para controlar su entrada y salida del centro de trabajo. El trabajador firmó una hoja dando su consentimiento para la recogida y tratamiento de sus datos personales con fines dedicados a la difusión y promoción de la entidad, como pueden ser publicaciones en redes sociales, folletos o publicidad corporativa. No obstante, la fotografía del demandante fue usada en el marco del programa de control *Ocean*, creado para la supervisión de la presencia de los empleados. La sociedad demandada alegó que para el control no se utilizaban técnicas de elaboración de perfiles automatizadas, y que los datos se conservaban temporalmente durante un mes para posteriormente ser borrados.

El empleado reclamó frente la Agencia Española de Protección de Datos, declarando que en ningún caso había prestado consentimiento para que se les diera ese uso a sus datos biométricos. La AEPD resolvió requiriendo a la empresa para que cesara en su uso de dicho sistema de reconocimiento, en tanto no hubiera realizado la preceptiva evaluación de impacto de protección de datos necesaria para evaluar los riesgos potenciales para los derechos y libertades de los trabajadores, así como para establecer las garantías adecuadas para el tratamiento.

El Juzgado examina también la vulneración al derecho a la intimidad y la propia imagen del demandante. Admite que, en el marco de las relaciones laborales, este derecho puede ser limitado en virtud del poder de vigilancia y supervisión del empresario, pero afirma que:

> "Toda medida restrictiva debe superar un test de proporcionalidad […]. Se vulnera el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto no sea adecuada con la ley, no sea eficazmente consentida o, aun autorizada, trastorne los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida".[47]

El demandante alega que, además de no prestar su consentimiento para que los datos fueran procesados con un fin de control de presencia, la empresa no llevó a cabo la evaluación de impacto previa requerida legalmente, y además la relación entre la necesidad real de uso de los datos respecto a la sensibilidad de su naturaleza es claramente desproporcionada. El Tribunal ratifica que efectivamente no hubo un consentimiento por parte del trabajador, y que el uso del sistema basado en datos

[47] Juzgado de lo Social N°. 2 de Alicante/Alacant (2023, 15 de septiembre) *Sentencia 190/2023, Rec. 489/2023*, párrafo 2.

biométricos no era esencial para llevar a cabo esta tarea de control, que podría haberse desarrollado mediante el uso métodos menos intrusivos, como la posibilidad de fichar con una tarjeta. Por tanto, el Juzgado entiende que se ha vulnerado el derecho a la intimidad y la propia imagen del empleado, y procede a condenar a la empresa al cese de uso de este *software* y al pago de una indemnización.

3. NORMATIVA

3.1. EL REGLAMENTO EUROPEO DE IA

3.1.1. DEFINICIÓN Y ESTRUCTURA

En el texto definitivo del Reglamento 2024/1689, el artículo 3 se destina a enumerar las definiciones de elementos clave dentro del instrumento normativo. Según Plaza Penadés, J. (2024), uno de los hitos de la Ley de Inteligencia artificial es definir por vez primera el concepto de sistema de IA. En sus palabras, no obstante, "el concepto de sistema de inteligencia artificial en su artículo 3, […] es oscuro y críptico, […], pues es evidente que existe una deficiente e incorrecta traducción que aboca a una falta de entendimiento y comprensión de dicho concepto"[48].

> Artículo 3
>
> 1) "Sistema de IA": un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

La primera parte de la descripción es una traducción literal de la palabra *"machine"* en la versión oficial en lengua inglesa. Para Plaza, una correcta interpretación sería la de "sistema de aprendizaje automático o autónomo"[49], ya que, a diferencia de los sistemas de programación convencionales (en los que las personas son las que definen el funcionamiento y las pautas), las reglas se generan automáticamente en el seno del propio sistema. Respecto a este concepto, el considerando 12 del Reglamento establece lo siguiente:

[48] Plaza Penadés, J. (2024)**.** Claves del futuro Reglamento (Ley) de inteligencia artificial de la UE. *Aranzadi digital num. 1/2024.* Pág. 2.

[49] Plaza Penadés, J. (2024)**.** Claves del futuro Reglamento (Ley) de inteligencia artificial de la UE. *Aranzadi digital num. 1/2024.* P.3.

(12)

> […] La definición debe basarse en las principales características de los sistemas de IA que los distinguen de los sistemas de software o los planteamientos de programación tradicionales y más sencillos, y no debe incluir los sistemas basados en las normas definidas únicamente por personas físicas para ejecutar automáticamente operaciones. […] Las técnicas que permiten la inferencia al construir un sistema de IA incluyen estrategias de aprendizaje automático que aprenden de los datos cómo alcanzar determinados objetivos y estrategias basadas en la lógica y el conocimiento que infieren a partir de conocimientos codificados o de una representación simbólica de la tarea que debe resolverse. La capacidad de inferencia de un sistema de IA trasciende el tratamiento básico de datos, al permitir el aprendizaje, el razonamiento o la modelización. El término «basado en una máquina» se refiere al hecho de que los sistemas de IA se ejecutan en máquinas.

La combinación de estos dos preceptos esclarece que la característica diferenciadora de los sistemas informáticos basados en inteligencia artificial radica en que su desarrollo no se basa en un proceso de programación por parte de un individuo, sino que gracias a los datos con los que se las “alimenta”, los programas generan la capacidad autónoma de realizar deducciones e inferencias.

Por otro lado, el Reglamento realiza una clasificación de los distintos sistemas mediante una evaluación del riesgo que conllevan. Esta categorización lleva aparejados importantes efectos jurídicos respecto a su legalidad, control y funcionamiento dentro del seno de la Unión Europea. El término “riesgo” del artículo 3, apartado 2, hace referencia a “la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio”[50]. Ya en sus primeras fases, el instrumento normativo usaba un enfoque basado en el riesgo que dividía los sistemas de inteligencia artificial en cuatro niveles, enumerados por I. Barkane (2022). Esta clasificación tiene su origen en lo dispuesto en el *Libro Blanco sobre inteligencia artificial*, que ya distribuía las diversas aplicaciones en función de que fueran de riesgo alto o de riesgo bajo, como afirma Antonov, A. (2022).

[50] Parlamento Europeo y Consejo de la Unión Europea. (2024). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial)*. Diario Oficial de la Unión Europea, L 1689, 14 de junio de 2024, artículo 3, apartado 2.

En el Capítulo II aparecen las aplicaciones de riesgo inaceptable, donde se recogen los usos prohibidos de los sistemas de inteligencia artificial. Su apartado primero se destina a detallar las distintas prácticas que podrían causar estragos de importante magnitud en los ciudadanos y sus derechos fundamentales. Así, se prohíben los sistemas que empleen métodos subliminales o engañosos para manipular el comportamiento de los sujetos, los que exploten las vulnerabilidades en razón de su edad, discapacidad o situación económica, y los que clasifiquen a las personas por su comportamiento o rasgos personales (esta última siempre y cuando se traduzca en un trato injusto o perjudicial). También se suprime la posibilidad de creación de bases de datos de reconocimiento facial a partir de imágenes obtenidas sin consentimiento, la evaluación de riesgo de comisión de delitos basado únicamente en perfiles de personalidad, y el uso de sistemas de reconocimiento de emociones en lugares de trabajo o educativos (salvo por razones de salud o seguridad). González, M.R. (2023) afirma que estos usos no están regulados en el instrumento normativo porque directamente no están permitidos en el territorio de la Unión Europea. Las letras h) y g) de este apartado, así como los apartados 2, 3, 4, 5, 6, y 7 se refieren a los sistemas basados en identificación biométrica, que serán analizados más adelante.

En el tercer Capítulo aparecen los usos de alto riesgo, permitidos siempre y cuando se cumplan los requisitos y exigencias previstos. Estos sistemas se caracterizan por "crear un impacto adverso en la seguridad o en los derechos fundamentales"[51]. La sección primera establece las reglas de calificación de los sistemas de alto riesgo; en concreto, su artículo sexto dispone lo siguiente:

> Artículo 6
>
> 1. Con independencia de si se ha introducido en el mercado o se ha puesto en servicio sin estar integrado en los productos que se mencionan en las letras a) y b), un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican a continuación:
>
> a) que el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I, o que el propio sistema de IA sea uno de dichos productos, y
>
> b) que el producto del que el sistema de IA sea componente de seguridad con arreglo a la letra a), o el propio sistema de IA como producto, deba someterse a

[51] Barkane, I. (2022). "Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance". *Information Polity*, 27(2), pág.152.

> una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I.
>
> 2. Además de los sistemas de IA de alto riesgo a que se refiere el apartado 1, también se considerarán de alto riesgo los sistemas de IA contemplados en el anexo III.

En el anexo III se recoge una lista de sistema de IA de alto riesgo estructurada en los distintos ámbitos de su operatividad. Destaca su apartado 1, en el que se clasifican como sistemas de alto riesgo los relacionados con la biometría, en concreto los sistemas de identificación biométrica remota, los de categorización biométrica y los destinados al reconocimiento de emociones. El apartado 3 del artículo 6, no obstante, establece que la enumeración del anexo III no se considerará de alto riesgo si no supone un peligro importante para la salud, seguridad o derechos fundamentales de las personas físicas, y también cuando no influyan en la toma de decisiones de los individuos; siempre que se den los supuestos enumerados en las letras a), b), c) y d). Sin embargo, el precepto establece se considerarán aplicaciones de alto riesgo en todo caso si efectúan procesos de elaboración de perfiles de personas físicas.

Tras definir las pautas que permiten clasificar a un sistema de IA como de alto riesgo, el Reglamento detalla en la Sección 2 del Capítulo los requisitos que deben cumplir estos sistemas. Estas condiciones se basan en la existencia de sistemas de identificación y gestión del riesgo, la creación de bases de datos de alta calidad, conservación de un registro automático de eventos, transparencia en su funcionamiento, y la necesidad imperiosa de supervisión humana de la aplicación. Por otro lado, la Sección 3 se encarga de enumerar las diversas obligaciones reforzadas para los proveedores, importadores, y responsables de despliegue de los sistemas de IA de alto riesgo. Estos agentes deben asegurar el cumplimiento de las imposiciones que aparecen en los artículos 16 a 27, entre los que destacan la existencia de sistemas de gestión de calidad, de evaluación de conformidad, procesos de notificación, publicación de la información técnica… Por último, el instrumento normativo regula los modelos de IA de uso general en el Capítulo V, procediendo a establecer reglas de calificación y normas que ordenen el funcionamiento este tipo de aplicaciones en el mercado. Esta categoría, así como los sistemas de riesgo mínimo, no serán objeto de análisis en el presente trabajo.

3.1.2. APLICABILIDAD TEMPORAL, ESPACIAL Y MATERIAL

El RIA fue publicado en el Diario Oficial de la Unión Europea el día 12 de julio de 2024, entrando en vigor el 1 de agosto de este mismo año. En su artículo 113 se establece que sus disposiciones son aplicables desde el día 2 de agosto de 2026. No obstante, en el contenido del instrumento normativo se establecen una serie de capítulos y disposiciones que serán aplicables antes de esta fecha. De esta manera, y en orden cronológico:

1) El artículo 77, apartado 2 establece el día 2 de noviembre de 2024 como límite para que los Estados designen y hagan públicas las autoridades u organismos encargados de la protección de los derechos fundamentales, tal y como expresa el apartado 1 de este artículo.
2) La letra a) del artículo 113 indica que el día 2 de febrero de 2025 serán aplicables los capítulos I y II, referidos a las prohibiciones sobre determinados sistemas de Inteligencia Artificial.
3) La letra b) de este mismo precepto establece el 2 de agosto de 2025 como fecha en la que se empezarán a aplicar las normas referidas a organismos notificados, modelos GPAI, gobernanza, confidencialidad y sanciones[52].
4) Para el 2 de febrero de 2026, la comisión deberá haber hecho públicas las directrices relativas a la aplicación del artículo 6: Normas de clasificación de los sistemas de IA de alto riesgo, incluyendo una lista de ejemplos prácticos que permitan diferenciar usos de alto riesgo de los que no lo son, tal y como se expresa en el apartado 5 del precepto. Esta fecha también marca el comienzo de la aplicación del resto del RAI, a excepción del citado artículo 6, apartado 1.
5) El artículo 113, en su letra c) establece que tanto el artículo 6, apartado 1, como las obligaciones que se derivan del Reglamento empezarán a ser aplicables a partir del 2 de agosto de 2027.
6) Un año más tarde, el 2 de agosto de 2028, la Comisión se encargará de evaluar el funcionamiento de la Oficina de IA, asegurándose de que posee las competencias y recursos necesarios para llevar a cabo sus encomendaciones. También se examinarán los códigos de conducta voluntarios relativos a los sistemas de IA distintos a los de alto riesgo. Esto aparece recogido en el artículo 112 del Reglamento.

[52]Artificial Intelligence Act. (s.f.). *Implementation timeline*. https://artificialintelligenceact.eu/es/implementation-timeline/

7) El 1 de agosto de 2029 se producirá la expiración del poder de la Comisión para adoptar actos delegados respecto a los artículos 6, 7, 11, 43, 47, 51, 52 y 53; a menos que dicha delegación se prorrogue de acuerdo con el artículo 97. La prórroga se extenderá en periodos de 5 años, salvo que o bien el Consejo o el Parlamento se opongan. El día siguiente (2 de agosto de 2029), la Comisión debe publicar un informe relativo a la revisión y evaluación del instrumento normativo.
8) En último lugar, el artículo 112 establece que el día 2 de agosto de 2031 se debe producir una evaluación de aplicación del RIA por parte de la Comisión, que deberá presentar un informe refiriéndose al desempeño del instrumento durante los primeros años desde su implantación. Dicho informe será presentado ante el Consejo, Parlamento Europeo y Comité Económico y Social Europeo.

El ámbito de aplicación subjetivo, espacial y material aparece regulado en el artículo 2 del RIA. Este precepto sirve para garantizar la protección de derechos, asentar los deberes de los distintos individuos nombrados, y proporcionar coherencia regulatoria tanto dentro como fuera de la Unión Europea. Así pues, según el artículo 2.1, el contenido del Reglamento es aplicable a:

1) Proveedores de sistemas de IA que los introduzcan o los pongan en funcionamiento en el seno de la UE, independientemente de si estos sujetos residen en el territorio de la Unión o en un país tercero.
2) Responsables de despliegue de estos sistemas que estén establecidos en el seno de la Unión, así como los importadores, distribuidores y fabricantes.
3) Proveedores y responsables de despliegue con residencia en un tercer país, en el caso de que los resultados de la implementación del sistema de IA se usen dentro de la UE. También a los representantes autorizados de estos proveedores que no estén establecidos dentro de la Unión.
4) A las personas afectadas que estén ubicadas dentro de la UE.

Por otro lado, el artículo 2 también enumera las exclusiones a la aplicabilidad del Reglamento, como comenta Rincón, M. A. (2024). Respecto a las omisiones de carácter material, en su apartado 2 se dispone que a los sistemas de IA de alto riesgo solo se les aplicará el artículo 6.1, los artículos 102 a 109, y el artículo 112, relativos a la gobernanza, vigilancia del mercado y sanciones relacionadas con estos programas. El artículo 57 también será aplicable cuando los requisitos para estos sistemas estén integrados en actos legislativos de armonización de la Unión. El apartado 3 expresa que los sistemas con fines exclusivamente militares, de defensa o seguridad nacional no se

incluyen en ningún caso en el ámbito de aplicación. Los apartados 6 y 8, por su parte, establecen que los programas enfocados a la investigación y desarrollo científicos también están excluidos en el caso de que no se pongan en servicio ni se introduzcan en el mercado europeo. El apartado 10 recoge la omisión de la aplicabilidad para los usos personales y no profesionales, y el apartado 12 también excluye las licencias libres y los sistemas “de código abierto” (siempre que no se introduzcan en el mercado, se consideren de alto riesgo, o se hallen sujetos a prohibiciones específicas). La entrada en vigor del RIA no afectará tampoco al régimen regulatorio de la responsabilidad de los prestadores de servicios intermediarios, ni a la relación normativa relativa a consumidores y seguridad de productos.

En materia de exclusiones de naturaleza espacial, quedarán fuera del alcance territorial del instrumento en virtud del apartado 4 las autoridades de terceros países y organizaciones internacionales si el uso de estos sistemas de IA se produce en el marco de acuerdos internacionales que tengan el propósito de facilitar la cooperación con la Unión o sus miembros, o cuyo fin sea garantizar el cumplimiento del Derecho, y siempre que se pueda certificar la protección de derechos y libertades fundamentales. El apartado 3 dispone en este ámbito que tampoco formarán parte del alcance de aplicación los programas usados exclusivamente fuera del territorio de la UE con fines militares o de seguridad nacional.

3.1.3. REFERENCIA A LA GOBERNANZA

La gobernanza aparece regulada en el Capítulo VII del instrumento normativo. Se divide en dos secciones, diferenciando la competencia a escala europea (artículos 64 a 69), y nacional (artículo 70). En primer lugar, el texto del Reglamento recoge la existencia y funciones de la Oficina de IA, establecida por la Comisión e integrada dentro de su propia estructura administrativa. Este órgano está destinado principalmente a garantizar la implementación del RIA y a desarrollar actividades de coordinación y soporte, asumiendo también funciones de secretaría del Consejo de IA. Novelli, C. et al. (2024) afirman que la Oficina contará con parte de la infraestructura y recursos de la Dirección General de Redes de Comunicación, Contenido y Tecnologías (CNECT). Según los autores, esto podría ser perjudicial para su autonomía operativa debido a que podría generar una dependencia en el plan estructural y estratégico que tenga la CNECT. La capacidad de autogobierno de este órgano también se podría ver afectada por la ambigüedad respecto a la gestión de conflictos o la superposición de competencias con otros organismos como puede ser el Consejo Europeo de Protección de Datos. Esta

vulnerabilidad también se ve reforzada por el hecho de que la Oficina de IA carece de personalidad jurídica y sus decisiones no son vinculantes.

Un elemento de mucha relevancia dentro de está sección está en los artículos 65 y 66, donde se encuentra regulado el Consejo de IA. Destaca la composición de este, formado por un representante de cada Estado Miembro, así como el Supervisor Europeo de Protección de Datos (en calidad de observador) y la Oficina de IA. Sus funciones se detallan en garantizar la aplicación uniforme del Reglamento, resolver discusiones técnicas y operativas, emitir recomendaciones a solicitud de la Comisión o por iniciativa propia, y contribuir a la cooperación con autoridades de terceros países y organizaciones internacionales, entre otros.

Además, en esta sección también aparecen las figuras del foro consultivo (artículo 67) y del grupo de expertos independientes (artículo 68). El primero está compuesto por representantes de la industria, sociedad civil y académicos o expertos en la materia designados por la Comisión. Sus funciones se definen en labores de asesoramiento al Consejo de IA, y también a la propia Comisión. El panel científico independiente, por otra parte, se compone de individuos con dominio en la materia, seleccionados también por la Comisión y encomendados con brindar apoyo técnico y asesoramiento a la Oficina de IA, así como a los Estados Miembros que lo soliciten.

Por otro lado, en relación con la gobernanza desde la perspectiva nacional, el artículo 70 establece que cada Estado Miembro debe designar al menos a una autoridad notificante y a una autoridad de vigilancia del mercado. La actividad de estas autoridades debe desarrollarse de manera independiente e imparcial para garantizar la objetividad en su funcionamiento, y los Estados deben asegurarse de que estos organismos tengan los suficientes recursos y estén equipados para el desempeño de sus funciones.

3.2. EL USO DE LA BIOMETRÍA EN EL REGLAMENTO DE IA

3.2.1. CONCEPTOS FUNDAMENTALES

No es la primera vez que el concepto de biometría o de datos biométricos se emplea por parte del legislador europeo. Así, el Reglamento 2252/2004 ya obligaba a los Estados miembros a incluir identificadores biométricos en la expedición de pasaportes; otro ejemplo sería la Decisión 2008/633/JAI, que introdujo el uso de este tipo de datos dentro del Sistema de Información de Visados. No obstante, la definición formal del concepto “datos biométricos” se recogería por primera vez en el articulado del RGPD, en concreto en su artículo 4.14:

> Artículo 4
>
> A efectos del presente Reglamento se entenderá por:
>
> 14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

Santisteban Galarza, M. (2021) sostiene que para determinar si un dato puede considerarse de naturaleza biométrica, es necesario analizar una trifecta de factores: la naturaleza de los datos (que debe tener relación con un abanico de características físicas, fisiológicas o conductuales de una persona física), los métodos y técnicas de tratamiento (es necesario un proceso técnico específico para su obtención), y la finalidad de dicho tratamiento (cuyo fin debe ser identificar de forma inequívoca a esa persona física). Este tipo de datos, cuando son dirigidos a la identificación unívoca de la persona física, forman parte de la "categoría especial de datos" de la que se ocupan los artículos 9 y 10 de esta misma norma. En estos preceptos se establecen una serie de restricciones y garantías para su tratamiento.

Dentro del Reglamento de IA, podemos ver que el considerando (14) hace referencia a los datos biométricos, disponiendo lo siguiente:

> (14) El concepto de «datos biométricos» empleado en el presente Reglamento debe interpretarse a la luz del concepto de «datos biométricos» tal como se define en el artículo 4, punto 14, del Reglamento (UE) 2016/679, en el artículo 3, punto 18, del Reglamento (UE) 2018/1725, y en el artículo 3, punto 13, de la Directiva (UE) 2016/680. Los datos biométricos pueden permitir la autenticación, la identificación o la categorización de las personas físicas y el reconocimiento de las emociones de las personas físicas.

Así pues, la definición que nos compete está en consonancia con la legislación europea previa, aunque no se hace una referencia directa a la capacidad de identificación unívoca que sí que se menciona en el RGPD. Etxeberria, J.F. (2024) afirma que en este marco conceptual destaca el componente innovador que aportó el Parlamento Europeo en el texto enmendado del Reglamento, introduciendo el concepto de "datos de base biométrica", que se separan de los datos biométricos en un sentido estricto por la falta de este elemento de identificación única. Según el autor, está ampliación de la definición para recoger un abanico más amplio de datos sirve para garantizar que no queden excluidas aplicaciones de sistemas de IA que operen sobre datos con fundamento biométrico que no se engloben dentro de los datos biométricos en sentido estricto. Este

tipo de información de forma aislada parece no tener la capacidad de identificar con precisión a individuos concretos, pero su uso y procesamiento combinados por tecnologías de IA podría contribuir significativamente a estos procesos de identificación, por lo que se hace necesario incluirlos.

3.2.2. CLASES DE BIOMETRÍA

El Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE en su Dictamen 3/2012 analizó las implicaciones del uso de sistemas biométricos en el ámbito de la protección de datos. En este ámbito hizo importantes avances en la clasificación de estas tecnologías, distinguiendo tres usos separados:

1) Autenticación/verificación biométrica ("*one-to-one comparison")*. Estos sistemas comparan dos plantillas biométricas con el fin de comprobar que las dos pertenecen al mismo individuo. Este proceso se puede llevar a cabo de distintas maneras, aunque la más habitual es que una de las plantillas esté almacenada en la memoria del sistema, mientras que la segunda se obtiene en tiempo real.
2) Identificación biométrica (*"one-to-many comparison"*). Dentro de esta categoría, la plantilla biométrica se compara con una multitud de otras plantillas, previamente almacenadas en bases de datos o ficheros. Este proceso de identificación a la vez se divide o bien en un conjunto cerrado -donde se conoce la existencia de la plantilla de la persona que se está buscando- o bien en un conjunto abierto, en el que la búsqueda se produce sin la garantía de que exista dicha plantilla.
3) Categorización biométrica (*"matching general characteristics")*. En esta última clasificación, el objetivo del sistema biométrico es clasificar a las personas físicas dentro de grupos con características predefinidas. Para llevar a cabo esta tarea, se emplean rasgos del individuo como su etnia, edad o género.

Este encasillado fue fuente de inspiración para posteriores textos normativos como el del RGPD o, en el caso de que nos compete, el Reglamento de IA. Así los considerandos (15), (16), y (17) profundizan al respecto de esta clasificación, esencial para entender el contenido de esta norma.

> (15) El concepto de «identificación biométrica» a que hace referencia el presente Reglamento debe definirse como el reconocimiento automatizado de características humanas de tipo físico, fisiológico o conductual, como la cara, el movimiento ocular, la forma del cuerpo, la voz, la entonación, el modo de andar, la postura, la frecuencia cardíaca, la presión arterial, el olor o las características de las pulsaciones de tecla, a fin de determinar la identidad de una persona

> comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos de referencia, independientemente de que la persona haya dado o no su consentimiento. Quedan excluidos los sistemas de IA destinados a la verificación biométrica, que comprende la autenticación, cuyo único propósito es confirmar que una persona física concreta es la persona que dice ser, así como la identidad de una persona física con la finalidad exclusiva de que tenga acceso a un servicio, desbloquee un dispositivo o tenga acceso de seguridad a un local.

En la segunda parte del precepto podemos observar como el legislador europeo se encarga de separar claramente el concepto de “identificación” con el de “verificación”, diferencia previamente comentada.

> (16) El concepto de «categorización biométrica» a que hace referencia el presente Reglamento debe definirse como la inclusión de personas físicas en categorías específicas en función de sus datos biométricos. Estas categorías específicas pueden referirse a aspectos como el sexo, la edad, el color del pelo, el color de los ojos, los tatuajes, los rasgos conductuales o de la personalidad, la lengua, la religión, la pertenencia a una minoría nacional o la orientación sexual o política. No se incluyen los sistemas de categorización biométrica que sean una característica meramente accesoria intrínsecamente vinculada a otro servicio comercial, lo que significa que la característica no puede utilizarse, por razones técnicas objetivas, sin el servicio principal y que la integración de dicha característica o funcionalidad no es un medio para eludir la aplicabilidad de las normas del presente Reglamento. […].

En esta definición el legislador excluye conscientemente las tecnologías de categorización biométrica accesorias a servicios comerciales por considerarlas de bajo impacto. Ejemplos de estos casos son los filtros para mercados en línea, o los filtros en redes sociales por considerar la actividad principal la creación del contenido subyacente.

> (17) El concepto de «sistema de identificación biométrica remota» a que hace referencia el presente Reglamento debe definirse de manera funcional como un sistema de IA destinado a identificar a personas físicas sin su participación activa, generalmente a distancia, comparando sus datos biométricos con los que figuren en una base de datos de referencia, con independencia de la tecnología, los procesos o los tipos de datos biométricos concretos que se usen. Estos sistemas de identificación biométrica remota suelen utilizarse para detectar a varias personas o su comportamiento de forma simultánea, a fin de simplificar considerablemente la identificación de personas sin su participación activa. […]. En el caso de los sistemas «en tiempo real», la recogida de los datos biométricos, la comparación y la identificación se producen de manera

> instantánea, casi instantánea o, en cualquier caso, sin una importante demora. En este sentido, no debe existir la posibilidad de eludir las normas contempladas en el presente Reglamento en relación con el uso «en tiempo real» de los sistemas de IA de que se trate generando demoras mínimas. Los sistemas «en tiempo real» implican el uso de materiales «en directo» o «casi en directo», como grabaciones de vídeo, generados por una cámara u otro dispositivo con funciones similares. En cambio, en los sistemas «en diferido» ya se han recabado los datos biométricos y la comparación e identificación se producen con una importante demora. A tal fin se utilizan materiales, como imágenes o grabaciones de vídeo captadas por cámaras de televisión en circuito cerrado o dispositivos privados, generados con anterioridad a la utilización del sistema en relación con las personas físicas afectadas.

Esta detallada definición será de utilidad para acotar el alcance de las prohibiciones ubicadas en el artículo 5 de la norma. Así pues, el concepto empleado "nos induce a pensar que la identificación biométrica "remota" se reducirá en la mayoría de los casos al tratamiento de la imagen facial mediante las tecnologías de reconocimiento facial, considerando la facilidad en la captura de dichas imágenes"[53]. Por otro lado, la detallada referencia al concepto de "en tiempo real" parece tratar de evitar elusiones originadas en demoras mínimas en el tratamiento de la información, es decir, cuando la identificación sea realmente "en diferido".

Además de esta clasificación general, el Reglamento hace referencia a un subtipo específico de sistemas, los sistemas de identificación biométricas remota en tiempo real y en espacio de acceso público con fines de cumplimiento del Derecho, contenidos dentro del artículo 5.h) dentro de las prácticas de IA prohibidas, como examinaremos detenidamente en el próximo epígrafe.

3.2.3. PROHIBICIONES DE USO Y EXCEPCIONES

La aproximación del Reglamento de IA es claramente un enfoque de riesgos, y esto no es distinto para el artículo 5 del mismo, que versa sobre las prácticas de IA prohibidas. Desde una primera lectura del precepto es claro que el uso de sistemas biométricos se encuentra altamente restringido. Como apunta Garriga, A. (2024), debido a los riesgos inaceptables que el uso de estos sistemas puede suponer para la protección de los derechos humanos y los valores inherentemente democráticos, se produce la prohibición del uso de sistemas de identificación biométrica en tiempo real en espacios

[53] Etxeberria Guridi, J. F. (2024). El uso de sistemas de inteligencia artificial (IA) de identificación biométrica remota en espacios públicos en la Ley Europea de IA. *Actualidad Jurídica Iberoamericana, 21*, 528-565. Pág.544.

públicos con fines de aplicación de la ley. La autora destaca, no obstante, que la prohibición no tiene carácter absoluto: se permite su empleo en situaciones específicas en las que concurren claramente determinados objetivos.

Otras de las prohibiciones del artículo 5 relativas a este tipo de tecnologías es el veto a sistemas biométricos que impliquen la categorización biométrica basada en características sensibles (apartado 1, letra c).), los sistemas de vigilancia predictiva (apartado 1, letra d).), la extracción indiscriminada de imágenes faciales, ya sea a través de circuitos cerrados de videovigilancia o de Internet (apartado 1, letra e.)), y los sistemas de reconocimiento emocional en ámbitos laborales y educativos si su uso no es por fines médicos o de seguridad (apartado 1, letra f).).

El apartado más interesante de cara al estudio de este precepto es el apartado 1, letra h), donde se recoge la primera prohibición abordada. Este precepto dispone lo siguiente:

> Artículo 5
>
> 1. Quedan prohibidas las siguientes prácticas de IA:
>
> (h) el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:
>
> i) la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas,
>
> ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista,
>
> iii) la localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

El contenido del artículo está muy influenciado por la existencia de un desequilibrio de poder relativo a las actuaciones de las autoridades encargadas de la aplicación del Reglamento para la identificación biométrica remota, tal como se expresa en el considerando (59). Según este, el uso de estos sistemas puede llevar a la vigilancia, detención o incluso privación de la libertad de las personas físicas, pudiendo generar

también otras consecuencias que amenazan a los derechos fundamentales. En esta línea, el considerando (32) subraya que concretamente esta tecnología afecta desproporcionadamente a la vida privada, y podría causar estragos a la hora de que los ciudadanos ejerzan sus derechos fundamentales al provocar una sensación de vigilancia constante. Santisteban Galarza, M. (2021) recuerda además la posición del Grupo de Trabajo del artículo 29 respecto a estos sistemas, donde identifican sus potenciales riesgos: la suplantación, la violación de datos y la desviación de la finalidad. Este autor destaca este último punto como la principal contingencia con relación al uso de esta tecnología, en especial en el campo del reconocimiento facial. Los riesgos que supone son alarmantes ya que, debido a la sensible naturaleza de los datos biométricos, su uso sin supervisión o control puede derivar en consecuencias graves para los derechos fundamentales de los individuos. Este problema se ve exacerbado por la falta de transparencia en los procesos de recolección y tratamiento, y por la inmediatez de estos, lo que dificulta su control. Por tanto, parece natural que el legislador europeo haya querido limitar su utilización a un puñado de casos, y siempre con una serie de garantías.

El uso de sistemas de identificación biométrica “en tiempo real” en espacios de acceso público con fines de garantía del cumplimiento del Derecho está prohibido en virtud de esta norma, salvo que se den las situaciones enumeradas en el articulado del precepto. Etxeberria, J.F. (2024) insiste en que la posibilidad de empleo no solo se encuentra supeditada a la consecución de estos objetivos, sino que también debe respetar los principios de necesidad y proporcionalidad. Así, el artículo 52.1 CDFUE[54] establece la estricta necesidad para llevar a cabo una limitación de los derechos fundamentales, así como la prueba de que no existen medios menos restrictivos para garantizar el mismo resultado. Este precepto ha sido empleado múltiples veces por parte del TJUE en su jurisprudencia, como examinamos anteriormente, y es observable en sentencias como la STJUE de 30 de enero de 2024 (asunto C-118/22)[55]. Todo ello remarca verdaderamente el carácter extraordinario de la permisión del empleo de estas tecnologías.

El primero de los supuestos excepcionales enumerados se basa en la búsqueda selectiva de personas físicas, concepto contrapuesto al de una vigilancia indiscriminada. La busca debe estar dirigida a una colectividad de personas determinada (inclusive en caso de personas desaparecidas), y solo se permite en relación a una serie de delitos

[54] Carta de los Derechos Fundamentales de la Unión Europea (CDFUE). (2000). Diario Oficial de la Unión Europea, C 364, 18 de diciembre de 2000.

[55] Tribunal de Justicia de la Unión Europea (TJUE). (2024). *Sentencia de 30 de enero de 2024 en el asunto C-118/22*.

tasados y no para cualquier infracción penal. La lista de delitos que se enumeran tiene la particularidad común de que la víctima se encuentra bajo una restricción de su libertad ambulatoria, como señala Etxeberria, J.F. (2024).

El segundo de los objetivos establecidos por el RIA versa sobre la prevención de una amenaza para la vida o seguridad física de las personas, o la amenaza de un atentado terrorista. La naturaleza de la amenaza debe ser específica, importante e inminente: este requisito de proximidad temporal también sirve para delimitar la duración del uso de estos sistemas. Por otro lado, los bienes que busca proteger (la vida e integridad física de las personas) son intereses de máxima relevancia dentro del ordenamiento jurídico, lo que también sirve para justificar el uso de estas tecnologías. Por tanto, parece que este artículo establece un marco de equilibrio entre la seguridad en los espacios públicos y las libertades individuales.

El tercer y último supuesto se basa en la identificación o localización de una persona sospechosa de la comisión de un delito de los recogidos en el Anexo II de la normativa. Un requisito que aparece en este apartado es que dicho delito debe estar tipificado en el Estado miembro correspondiente con una pena (o medida privativa de libertad) con una duración de, por lo menos, cuatro años. La enumeración de delitos a los que se puede aplicar el precepto es amplia, y engloba el terrorismo, el tráfico de seres humanos, explotación sexual infantil, y otros. Todos destacan por la gravedad de los bienes jurídicos a los que afectan, como la vida, la libertad y la dignidad humana.

Una vez esclarecidos los objetivos, el artículo 5.2 establece una serie de criterios de ponderación que están estrechamente relacionados con el mencionado artículo 52.1 CDFUE y el principio de proporcionalidad en el ordenamiento europeo.

> Artículo 5
>
> 2. El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho para cualquiera de los objetivos mencionados en el apartado 1, párrafo primero, letra h), debe desplegarse para los fines establecidos en dicha letra, únicamente para confirmar la identidad de la persona que constituya el objetivo específico y tendrá en cuenta los siguientes aspectos:
>
> a) la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema;

> b) las consecuencias que tendría el uso del sistema en los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias.

Este artículo refleja la excepcionalidad del uso de estos sistemas, destacando la necesidad de considerar la naturaleza de la situación y las consecuencias de la utilización -o, en su caso, la omisión del uso- de estas tecnologías. Para atender a estas necesidades, es vital un análisis de factores temporales, geográficos y personales, para que estos sistemas se empleen únicamente en escenarios donde exista un vínculo inescindible y directo con los objetivos enumerados y los bienes jurídicos protegidos, como defiende Etxeberria, J.F. (2024). La redacción de esté último párrafo también menciona la necesidad de una previa evaluación de impacto a los derechos fundamentales (artículo 27), y el registro de estos sistemas en la base de datos de la UE (artículo 49). No obstante, también en el texto se introduce una excepción a estos requisitos para situaciones de urgencia, en virtud de la cual se permite el uso de estas tecnologías sin su registro inicial, indicando que no obstante que este debe ser completado sin demora indebida. De esta forma se palian los efectos perjudiciales consecuencia de supuestos en los que se debe actuar con rapidez en contextos críticos para cumplir los objetivos antes enumerados.

El apartado tercero de este artículo 5 establece una serie de garantías adicionales a la par que otorga un importante nivel de discrecionalidad a los Estados Miembros al definir que “normas detalladas del Derecho nacional”[56] sean las que regulen los procedimientos para la autorización de estas tecnologías. Esta potestad también queda reflejada en el contenido del apartado 5, en el que se dispone que los Estados podrán autorizar parcial o totalmente el uso de estos sistemas. En este sentido, el considerando (37) permite la elección autónoma sobre la incorporación esta posible utilización:

> (37) Por otro lado, conviene disponer, en el marco exhaustivo que establece este Reglamento, que dicho uso en el territorio de un Estado miembro conforme a lo dispuesto en el presente Reglamento solo debe ser posible cuando el Estado miembro de que se trate haya decidido contemplar expresamente la posibilidad de autorizarlo en las normas detalladas de su Derecho nacional, y en la medida en que lo haya contemplado. En consecuencia, con arreglo al presente Reglamento los Estados miembros siguen teniendo la libertad de no ofrecer esta posibilidad en absoluto o de ofrecerla únicamente en relación con algunos de los

[56] Parlamento Europeo y Consejo de la Unión Europea. (2024). *Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial)*. Diario Oficial de la Unión Europea, L 1689, 14 de junio de 2024, artículo 5, apartado 3.

> objetivos que pueden justificar un uso autorizado conforme al presente Reglamento. Dichas normas nacionales deben notificarse a la Comisión en un plazo de treinta días a partir de su adopción.

Así, queda dentro de la competencia nacional la elección de la autoridad a la que se hace referencia, pudiendo ser esta o bien judicial; o bien una autoridad administrativa independiente. Asimismo, son los Estados los que elaborarán las reglas específicas respecto a la solicitud, tramitación y expedición de esta autorización previa. La discrecionalidad nacional se ve limitada por el propio articulado del Reglamento: en este apartado se indica que la valoración sobre su concesión debe de tener siempre en cuenta que el empleo de estos sistemas es necesario y proporcionado para alcanzar alguno de los objetivos que aparecen en el apartado 1, letra h).

Ahora bien, de la misma forma que vimos en el apartado 2, en el caso de la gestión de situaciones urgentes, el Reglamento prevé un marco en virtud del cual se podrán empezar a utilizar estos sistemas sin la autorización previa, siempre que esta se solicite en menos de 24 horas desde el comienzo de dicha utilización. En esta situación, si se deniega la autorización necesaria, el uso del sistema debe detenerse inmediatamente, eliminándose los resultados y la información de salida fruto de su empleo. Queda en duda cuál será la autoridad española a la que se encomiende esta tarea, y si será de naturaleza administrativa o judicial. El Reglamento establece como fecha límite para la designación de autoridades el 2 de agosto de 2025, pero autores como Etxeberria, J.F. (2024) afirman que podría tratarse de un órgano jurisdiccional -como el Juez de Instrucción del orden penal o los Juzgados de lo Contencioso-administrativo- o, en el caso de ser una autoridad administrativa independiente, esta podría ser la Agencia Española de Protección de Datos (AEPD) o las Comisiones de Videovigilancia a las que se refiere la LO 4/1997[57]. Por otro lado, el apartado 4 de este artículo indica que cualquier uso de estas tecnologías debe ser notificado a la autoridad de vigilancia del mercado y a la autoridad nacional de protección de datos. Esta primera parece que será la Agencia Española de la IA (AESIA)[58].

Por su parte, el apartado 6 y 7 del artículo contiene la obligación para estas autoridades y para la Comisión de publicar informes anuales sobre el uso de los sistemas de

[57] Gobierno de España. (1997). Artículo 5, *Comisiones de videovigilancia*, en *Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos*. Boletín Oficial del Estado, núm. 186, de 5 de agosto de 1997.

[58] Cinco Días. (2024, 19 de diciembre). *La AESIA planea ya la futura implementación de sus certificaciones*. https://cincodias.elpais.com/legal/2024-12-19/la-aesia-planea-ya-la-futura-implementacion-de-sus-certificaciones.html

identificación biométrica “en tiempo real” en espacios de acceso público con fines de garantía del cumplimiento del Derecho. En último lugar, el apartado 8 establece este artículo no será limitante de la aplicación de las prohibiciones que correspondan cuando alguna de las prácticas de IA contravenga otras disposiciones del Derecho de la UE.

Para el caso de los sistemas biométricos que no pertenezcan a la tipología de prácticas prohibidas de IA -como los sistemas de identificación biométrica “en diferido”- el tratamiento jurídico por parte del Reglamento es su clasificación como sistemas “de alto riesgo”. Como establece el Anexo III del instrumento normativo, su uso está en primer lugar condicionado a la existencia de una habilitación por parte del Derecho de la UE o por la legislación nacional aplicable. Por tanto, la regulación de la biometría en el texto no implica una automática autorización para su uso dentro de la Unión Europea, como también recuerda el considerando (54). En el caso de que su utilización esté habilitada en este aspecto, Garriga, A. (2024) comenta que los sistemas biométricos de “de alto riesgo” deben cumplir una serie de requisitos específicos contenidos en el artículo 9 del RIA y relacionados con los principios de seguridad, transparencia y protección de los derechos fundamentales. Algunas de estas medidas consisten en la implantación de un sistema de gestión de riesgos, la garantía de la calidad de datos, o la implementación de registros que permitan la trazabilidad del funcionamiento, entre otros.

4. CONCLUSIONES

Primero – El Reglamento Europeo de Inteligencia Artificial constituye el culmen de un proceso social y normativo que empieza en 1956, cuando se acuña por primera vez el término “Inteligencia Artificial” durante la Conferencia de Dartmouth. Este texto regula por vez primera en el mundo el uso de estas tecnologías, creando un marco regulatorio que prima el respeto a los derechos fundamentales a la par que permite su introducción en la vida cotidiana y sus usos de mercado. La estructura del RIA se basa en un enfoque de riesgos que permite la clasificación de los distintos sistemas de IA dependiendo de su potencial impacto en los sujetos. Esta regulación fomenta la proporcionalidad, la protección de los derechos y libertades fundamentales, y la competitividad y liderazgo tecnológico en la UE.

Segundo – A día de hoy, las tecnologías de naturaleza biométrica se consideran como unos de los sistemas más disruptivos de nuestro siglo: sus aplicaciones van desde la verificación de la identidad de personas físicas en circuitos cerrados hasta la posibilidad de realizar una captación y tratamiento de datos masivo e inmediato con el objetivo de identificar a sujetos “en tiempo real” cuando están en espacios públicos y concurridos. Esta capacidad para procesar características de tipo físico y conductual en cuestión de segundos y de forma automatizada hace que se conviertan en útiles herramientas para prevenir delitos y mejorar la eficiencia de sistemas ya existentes. Es innegable que la biometría tiene un importante papel dentro de la transición a una sociedad digital, pero su despliegue debe responder a los principios que caracterizan la convivencia dentro de la Unión Europea, pilares como la legalidad, la igualdad o la seguridad jurídica.

Tercero – A pesar de este claro potencial, los sistemas biométricos plantean riesgos importantes que pueden afectar a la privacidad, libertad y equidad entre ciudadanos. La naturaleza tan sensible de este tipo de datos abre la puerta a que se lleven a cabo usos indebidos de los mismos; como puede ser la vigilancia masiva, el control de la ciudadanía, y la introducción de sesgos discriminatorios, entre otros. Hemos observado que existe un peligro de que se genere una sensación de vigilancia constante que pueda llegar a disuadir a los ciudadanos del ejercicio de derechos básicos como la libertad de expresión o asociación. Además, estas tecnologías presentan importantes riesgos para las minorías más vulnerables ya que la introducción de sesgos se ve amplificada por el tratamiento automatizado y por la opacidad de diseño y funcionamiento de estos sistemas. En este contexto, la identificación y depuración de responsabilidades y reparación de daños devienen tareas complejas.

Cuarto – El Reglamento de IA prohíbe en su artículo 5 las prácticas de riesgo inaceptable, entre que las que se encuentra el uso de sistemas de identificación biométrica remota “en tiempo real” en espacios públicos con fines de cumplimiento del Derecho. Seguidamente, se exponen una serie de supuestos en el que se exceptúa el veto a estas tecnologías, siempre que se cumplan los requisitos y garantías para ello. Por otro lado, estos objetivos están sujetos a los principios de necesidad y proporcionalidad, además de requerirse una autorización previa a su uso. El texto normativo también reitera las obligaciones de transparencia y supervisión humana, subrayando la importancia de la trazabilidad de uso de los sistemas biométricos para que las decisiones que se basen en ellos puedan ser justificadas y recurridas.

Quinto – En un contexto global en el que la tecnología avanza más rápido que el desarrollo normativo, el RIA supone un esfuerzo integral para regular la amplitud de los usos de la Inteligencia Artificial, así como elementos específicos como los sistemas biométricos. Aunque el legislador europeo ha establecido un marco sólido con esta normativa, es innegable que aparecen nuevos desafíos como la gestión de la cooperación entre Estados miembros, la implementación práctica del contenido de la normal y la vigilancia respecto a su cumplimiento. En este sentido, el impacto de la biometría dependerá mucho del uso que se le dé y de que las disposiciones del Reglamento sean verdaderamente respetadas en su despliegue. Esta nueva norma europea crea un precedente para su regulación en otras partes del mundo gracias a su enfoque protector de los derechos fundamentales y fomentador de la innovación. El RIA se erige como un ejemplo de cómo equilibrar normativamente estos intereses, estableciendo un innovador modelo normativo que servirá de inspiración para crear un marco jurídico y ético robusto.

5. BIBLIOGRAFÍA Y DOCUMENTACIÓN

ANTONOV, A. (2022). "Gestionar la complejidad: la contribución de la UE a la gobernanza de la inteligencia artificial". *Revista CIDOB d'Afers Internacionals*, n.º 131, p. 41-68.

AYUDA, F.G., & CALLEJA, M. P. L. (1995). "Metodología para el desarrollo de sistemas jurídicos de inteligencia artificial: el prototipo ARPO-2 como ejemplo"*. Scire: Representación y Organización del conocimiento*, 73-103.

BASTOS, F. B. (2023). "Metodología doctrinal en el derecho administrativo de la UE: reaccionar frente a la "impronta estatal"". *Revista de Derecho Público: teoría y método*, 8, 7-69.

BARKANE, I. (2022). "Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance". *Information Polity*, 27(2), 147-162.

CARRASCO, M. I. (2020). "La utilización policial de los sistemas de reconocimiento facial automático"*. IUS ET VERITAS*, (60), 86-103.

ETXEBERRIA GURIDI, J. F. (2024), "El uso de sistemas de inteligencia artificial (IA) de identificación biométrica remota en espacios públicos en la Ley Europea de IA", *Actualidad Jurídica Iberoamericana*, nº 21, págs. 528-565.

FELLÄNDER, A., REBANE, J., LARSSON, S., WIGGBERG, M., & HEINTZ, F. (2022). "Achieving a data-driven risk assessment methodology for ethical AI". *Digital Society*, 1(2), 13.

GARRIGA DOMÍNGUEZ, A. (2024), "Los derechos ante los sistemas biométricos que incorporan inteligencia artificial"*. Universidad de Vigo*.

HERVEY, T., CRYER, R., SOKHI-BULLEY, B., & BOHM, A. (2011). "Research methodologies in EU and international law"*. Bloomsbury Publishing*.

NOVELLI, C., HACKER, P., MORLEY, J., TRONDAL, J., & FLORIDI, L. (2024). "A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities"*. AI Board, Scientific Panel, and National Authorities*.

PLAZA PENADÉS, J. (2024). "Claves del futuro Reglamento (Ley) de inteligencia artificial de la UE". *Aranzadi digital*, nº 1/2024.

RINCÓN, M. A. (2024). "Aproximación a la propuesta legislativa europea sobre inteligencia artificial", *Quaderns IEE: Revista de l'Institut d'Estudis Europeus*, vol. 3, nº 1, págs. 110-124.

SANTISTEBAN GALARZA, M. (2021). "Reconocimiento facial y protección de datos: Una respuesta provisional a un problema pendiente", *Revista de Derecho UNED*, nº 28, págs. 499-526.

WENDERHORST C., & DULLER, Y. (2021*).* "Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces". *Policy Department for Citizens´ Rights and Constitutional Affairs. Directorate-General for Internal Policies*.

DOCUMENTACIÓN

AI HLEG – High-level Expert Group on Artificial Intelligence. (abril de 2019). *Ethics guidelines for trustworthy AI*. Comisión Europea.

https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

AI HLEG – High-level Expert Group on Artificial Intelligence. (abril de 2019). *Policy and investment recommendations for trustworthy Artificial Intelligence*. Comisión Europea.

https://digitalstrategy.ec.europa.eu/en/library/policyandinvestmentrecommendationstrustworthy-artificial-intelligence

Ministerio de Asuntos Económicos y Transformación Digital. (noviembre de 2023). Resumen del Reglamento Europeo de Inteligencia Artificial.

https://portal.mineco.gob.es/es-es/digitalizacionIA/sandbox-IA/Documents/20220919_Resumen_detallado_Reglamento_IA.pdf

PÁGINAS WEB

Cinco Días. (2024, 19 de diciembre). *La AESIA planea ya la futura implementación de sus certificaciones*. Recuperado de https://cincodias.elpais.com/legal/2024-12-19/la-aesia-planea-ya-la-futura-implementacion-de-sus-certificaciones.html

Consejo de la Unión Europea. (2024, 21 de mayo). *Artificial Intelligence Act: Council gives final green light to the first worldwide rules on AI*. Recuperado de https://www.consilium.europa.eu/es/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/.

Artificial Intelligence Act. (s.f.). *Avances en la regulación de la Inteligencia Artificial*. Recuperado de https://artificialintelligenceact.eu/es/avances/

European Commission. (s.f.). *High-Level Expert Group on Artificial Intelligence (AI HLEG)*. Recuperado de https://digital-strategy.ec.europa.eu/es/policies/expert-group-ai

The Global Partnership on Artificial Intelligence (GPAI). (s.f.). *Home*. Recuperado de https://thealliance.ai/

Artificial Intelligence Act. (s.f.). *Avances*. Recuperado de https://artificialintelligenceact.eu/es/avances/

Artificial Intelligence Act. (s.f.). *Implementation timeline*. Recuperado de https://artificialintelligenceact.eu/es/implementation-timeline/

6. NORMATIVA CITADA

NORMATIVA EUROPEA

Comisión Europea. (2020). Libro Blanco sobre la inteligencia artificial: Un enfoque europeo orientado a la excelencia y la confianza*.*

Consejo de Europa. (1950). Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CETS No. 005*).* Roma, 4 de noviembre de 1950.

Consejo de la Unión Europea. (2008). Decisión 2008/633/JAI del Consejo, de 23 de junio de 2008, por la que se regula el acceso para consulta, con fines de prevención, investigación, detección y enjuiciamiento de delitos penales, incluidos los actos de terrorismo, a los datos del Sistema de Información de Visados (VIS). *Diario Oficial de la Unión Europea*, L 218, 13 de agosto de 2008.

Consejo de la Unión Europea. (2008). Decisión 2008/633/JAI del Consejo, de 23 de junio de 2008, por la que se regula el acceso para consulta, con fines de prevención, investigación, detección y enjuiciamiento de delitos penales, incluidos los actos de terrorismo, a los datos del Sistema de Información de Visados (VIS). *Diario Oficial de la Unión Europea*, L 218, 13 de agosto de 2008.

Gobierno de España. (1997). Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos*. Boletín Oficial del Estado*, núm. 186, de 5 de agosto de 1997.

Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. (2012). Dictamen 3/2012 sobre la evolución de las tecnologías biométricas*.*

Parlamento Europeo y Consejo de la Unión Europea. (1995). Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario Oficial de las Comunidades Europeas*, L 281, 23 de noviembre de 1995.

Parlamento Europeo y Consejo de la Unión Europea. (2004). Reglamento (CE) n.º 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las características de seguridad y los elementos biométricos de los pasaportes y documentos de viaje expedidos por los Estados miembros. *Diario Oficial de la Unión Europea*, L 385, 29 de diciembre de 2004.

Parlamento Europeo y Consejo de la Unión Europea. (2016). Directiva (UE) 2016/680, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por 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. *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016.

Parlamento Europeo y Consejo de la Unión Europea. (2016). 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 (Reglamento General de Protección de Datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016.

Parlamento Europeo y Consejo de la Unión Europea. (2019). Reglamento (UE) 2019/1157, de 20 de junio de 2019, sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y de los documentos de residencia expedidos a los ciudadanos de la Unión y a sus familiares. *Diario Oficial de la Unión Europea*, L 188, 12 de julio de 2019.

Parlamento Europeo y Consejo de la Unión Europea. (2024). Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial). *Diario Oficial de la Unión Europea*, L 1689, 14 de junio de 2024.

Unión Europea. (2000*).* Carta de Derechos Fundamentales de la Unión Europea. Diario Oficial de la Unión Europea, C 364, 18 de diciembre de 2000.

NORMATIVA NACIONAL

Gobierno de España. (1997). Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos*. Boletín Oficial del Estado*, núm. 186, de 5 de agosto de 1997.

7. JURISPRUDENCIA Y DOCTRINA JUDICIAL

High Court of Justice (Divisional Court of Cardiff) (2019, 4 de septiembre). *Case No: CO/4085/2018, EWCH 2341.*

Juzgado de lo Social Nº 2 de Alicante/Alacant (2023, 15 de septiembre). *Sentencia 190/2023, Rec. 489/2023.*

Tribunal de Justicia de la Unión Europea (TJUE) (2013, 17 de octubre). *Schwarz c. Stadt Bochum (Asunto C-291/12).*

Tribunal de Justicia de la Unión Europea (TJUE) (2024, 30 de enero). *NG y Direktor na Glavna direktsia Natsionalna politsia pri Ministerstvo na vatreshnite raboti — Sofia (Asunto C-118/22).*

Tribunal de Justicia de la Unión Europea (TJUE) (2024, 21 de marzo). *RL c. Landeshauptstadt Wiesbaden (Asunto C-61/22).*

Tribunal Europeo de Derechos Humanos (TEDH) (1994, 28 de octubre). *Murray v. United Kingdom (Solicitud núm. 14310/88).*

Tribunal Europeo de Derechos Humanos (TEDH) (2008, 4 de diciembre). *S. and Marper v. the United Kingdom (Solicitudes núm. 30562/04 y 30566/04).*

Tribunal Europeo de Derechos Humanos (TEDH) (2023, 4 de julio). *Glukhin c. Rusia (Solicitud núm. 11519/20).*