Oñati Socio-Legal Series (ISSN: 2079-5971)
Oñati International Institute for the Sociology of Law
Avenida Universidad, 8 – Apdo. 28
20560 Oñati – Gipuzkoa – Spain
Tel. (+34) 943 783064 / opo@iisj.net / https://opo.iisj.net

El uso de inteligencia artificial y los tratamientos de datos biométricos realizados por las autoridades policiales

(The Use of Artificial Intelligence and the Processing of Biometric Data by Law Enforcement Authorities)

OÑATI SOCIO-LEGAL SERIES FORTHCOMING
DOI LINK: HTTPS://DOI.ORG/10.35295/OSLS.IISL.2398
RECEIVED 21 JUNE 2025, ACCEPTED 2 SEPTEMBER 2025, FIRST-ONLINE PUBLISHED 23 SEPTEMBER 2025

LORENA PÉREZ CAMPILLO[1]

Resumen

Este trabajo de investigación analiza el uso creciente de la Inteligencia Artificial (IA) y la biometría por parte de la administración pública y las autoridades policiales, destacando sus implicaciones éticas y jurídicas. Se expone la necesidad de reconfigurar las garantías legales actuales, ya que el marco normativo vigente resulta insuficiente para afrontar los retos de estas tecnologías. Asimismo, se estudian los distintos tratamientos de datos biométricos y sus fundamentos legales, prestando especial atención al complejo concepto de «interés público» como base legitimadora. El análisis aborda la urgencia de una regulación armonizada que establezca límites, requisitos y garantías claras, junto con principios de transparencia y seguridad. Igualmente, se diferencia entre los usos destinados a vigilancia y los aplicados a la autenticación.Finalmente, el estudio concluye subrayando la necesidad de regulación específica y de garantías reforzadas que aseguren un uso responsable de la IA y la biometría, protegiendo los derechos fundamentales en la era digital.

Palabras clave

Inteligencia artificial; datos biométricos, protección de datos; seguridad pública; reglamento inteligencia artificial; armonización

Abstract

This research paper explores the increasing use of Artificial Intelligence (AI) and biometric technologies by public administration and law enforcement authorities, and the complex ethical and legal implications that this entails. Initially, it examines the need to reconfigure legal safeguards in the face of the emergence of AI in public

[1] Lorena Pérez Campillo, Profesora Universidad Tecnológica Atlántico-Mediterráneo (UTAMED) (Málaga, España). Área de Ciencias Jurídicas y RRHH. Directora del Área de CCJJ y RRHH. Email: lorena.perez@utamed.es ORCID: https://orcid.org/0000-0002-8047-0293

administration, recognising the inadequacy of the current regulatory framework and the need to adopt proactive policies to ensure the ethical and respectful use of AI. It then explores the path towards a responsible use of AI and biometrics, considering the different types of biometric data processing and their lawfulness bases, with a particular focus on the complexity of the 'public interest' justification. The study addresses the need for regulation and regulatory harmonisation to establish clear limits, requirements and safeguards for the processing of biometric data, as well as the importance of transparency, security and guidelines for data protection authorities. The necessary differentiation of the types of biometric data processing is further explored, analysing whether surveillance control activities are well differentiated from biometric authentication and verification. Finally, final reflections are presented on the need for specific regulation and the reconfiguration of legal safeguards to ensure a responsible use of biometric data.

Key words

Artificial intelligence; biometric data, data protection; public security; artificial intelligence regulation; harmonisation

Table of contents

1. Introducción 4
2. La IA en la administración pública: ¿es necesaria una reconfiguración de garantías jurídicas? 5
3. Hacia un uso responsable de la IA y la tecnología biométrica por la administración pública y autoridades policiales 6
3.1. Los tipos de tratamiento de datos biométricos y su base legitimadora 6
3.2. El interés público como base legitimadora en el tratamiento de datos: Un equilibrio complejo 7
3.3. Necesidad de regulación y armonización: Límites, requisitos y garantías 7
3.4. Transparencia, seguridad y guías de las autoridades de protección de datos: Hacia un uso responsable de la biometría 10
4. La interpretación en la necesaria diferenciación de los tipos de tratamiento de datos biométricos 11
4.1. ¿Se encuentran correctamente diferenciadas las actividades de control de vigilancia de autenticación y verificación biométrica? 12
4.2. La necesidad de una clara diferenciación o categorización de tipos de tratamientos de datos biométricos. 13
4.3. Análisis de interpretación regulatoria de los tipos de tratamientos de datos biométricos antes del AIA 14
4.4. Análisis de interpretación regulatoria en los tratamientos de datos biométricos a partir del AIA 16
5. Reflexiones finales hacia la necesidad de una regulación específica y a la reconfiguración de las garantías jurídicas 17
6. Conclusiones 20
Referencias 21
Fuentes jurídicas 24
Jurisprudencia 25

1. Introducción

En los últimos años, se ha observado un creciente uso de la Inteligencia Artificial (IA, en adelante) por parte de los Cuerpos y Fuerzas de Seguridad, con el objetivo de mejorar la eficiencia y eficacia de la aplicación de la ley. Diversas tecnologías basadas en IA se han implementado en diferentes ámbitos, como el análisis predictivo, el reconocimiento facial, el procesamiento de datos y la automatización de tareas (Gimeno 2023). Estas herramientas prometen optimizar el despliegue de recursos, facilitar las investigaciones y aumentar la productividad. Sin embargo, el empleo de la IA en el contexto policial también ha generado preocupaciones y debates en torno a cuestiones éticas, legales y de derechos humanos. Por ello, se deben abordar cuidadosamente aspectos como la transparencia de los algoritmos, los sesgos potenciales, la privacidad de los ciudadanos y el riesgo de discriminación para garantizar que estas tecnologías se implementen responsable y respetuosamente con los principios del Estado de Derecho.

La función de las autoridades policiales se concibe como un servicio público orientado a la protección de la comunidad y la defensa del orden democrático a quienes les corresponde la tarea de proteger el libre ejercicio de los derechos y libertades, así como garantizar la seguridad ciudadana. De modo que, desempeñan, una misión de servicio público y son garantes de los derechos de los ciudadanos, a la vez que están vinculados por estos mismos derechos. Por ende, la actuación de la policía debe respetar y garantizar dichas libertades y derechos fundamentales de los ciudadanos (Cfr. Art. 104 CE).

La labor policial, como servicio público, busca proteger los derechos y libertades de la ciudadanía y garantizar la seguridad, pero debe equilibrarse con el respeto a los derechos fundamentales, incluyendo la protección de datos personales. Este derecho, reconocido como fundamental en el artículo 18.4 de la Constitución Española y a nivel europeo en el Convenio 108+ (Martínez 2021) y la Carta de Derechos Fundamentales de la UE, también se considera un derecho humano según la Declaración Universal de los Derechos Humanos. La evolución tecnológica ha intensificado la necesidad de proteger la privacidad frente al uso indebido de datos personales, como señaló el TEDH en casos clave. En España, alguna jurisprudencia como la STC 254/1993 y desarrollos normativos han definido marcos específicos para el tratamiento de datos por las fuerzas policiales, estableciendo límites y garantías para evitar abusos y proteger tanto la seguridad pública como los derechos individuales.

El desarrollo y uso de IA por autoridades debe estar plenamente alineado con el respeto a los derechos humanos, evitando prejuicios y situando a las personas en el centro. El uso de esos sistemas de IA por parte de los Cuerpos y Fuerzas de la Seguridad ha generado crecientes preocupaciones sobre sus implicaciones éticas y legales. Casos como *COMPAS, Clearview AI, iBorderCtrl, VioGen y VeriPol* ilustran los desafíos que surgen cuando existen algoritmos opacos y potencialmente sesgados que pueden plantear amenazas a los derechos fundamentales, como la privacidad, el debido proceso y la no discriminación, si no se cumple la normativa.

Si bien la IA puede ser valiosa para investigar delitos y cubrir déficits de recursos humanos y puede ser una herramienta muy útil para las Fuerzas y Cuerpos de Seguridad y los organismos encargados de la aplicación de la ley en la investigación de delitos. La IA puede procesar y analizar rápidamente grandes cantidades de

información, como registros de comunicaciones, transacciones financieras e imágenes de vigilancia, esto permite identificar patrones y conexiones que podrían pasar desapercibidos para los investigadores humanos, incluso hasta los datos públicos recopilados de redes sociales o plataformas digitales (Dhar 2013). Los algoritmos de IA pueden detectar patrones de comportamiento criminal y predecir posibles actividades delictivas futuras, ayudando a las autoridades a anticiparse y prevenir delitos (Jordan y Mitchel 2015). Además, el reconocimiento facial, de huellas dactilares, de voz y otras tecnologías biométricas basados en IA pueden ayudar a identificar sospechosos y víctimas durante las investigaciones y son muy útiles para investigar actividades ilícitas, controlar fronteras y flujos migratorios, criminalística, analítica forense, gestión, etc.

Este trabajo de investigación orbita en torno a tres conglomerados normativos) como son el Reglamento Europeo de Inteligencia Artificial o *AI Act*, (en adelante, AIA, la Directiva europea 680/2016 (en adelante, Directiva Policial) y el Reglamento (UE) 2016/679 (en adelante, RGPD). A lo largo del mismo, examinaremos críticamente la interrelación entre los tres, analizando su coherencia y posibles divergencias, lo que nos permitirá evaluar la eficacia del marco regulatorio actual en su conjunto, identificar potenciales lagunas o contradicciones, y reflexionar sobre la necesidad de ajustes o desarrollos adicionales para asegurar una protección integral de los derechos fundamentales en la era de la IA.

2. La IA en la administración pública: ¿es necesaria una reconfiguración de garantías jurídicas?

Sin perjuicio de todas las funciones y ventajas citadas al inicio con la llegada de la IA, (…) cabe preguntarnos en qué situación se encuentran las instituciones, las administraciones públicas y autoridades y si es necesario reconfigurar las garantías jurídicas actuales.

Aunque en la actualidad no se está desafiando fundamentalmente los cimientos del Derecho administrativo ni requiriendo una reestructuración significativa de sus instituciones, sí que se percibe la necesidad inmediata de formular «nuevos conceptos jurídicos» para abordar la implementación de la IA en la administración pública.

El marco normativo del 2007 presenta limitaciones para abordar los desafíos que plantea la IA en la administración pública , especialmente en áreas como la automatización cognitiva, el análisis predictivo y el aprendizaje automático (Valero 2019).

Ante esta brecha legal, este autor enfatiza la responsabilidad de las Administraciones públicas de adoptar proactivamente políticas y prácticas que garanticen un uso ético y respetuoso de la IA, alineado con los principios de buena administración y la defensa del interés general.

Para hacer frente a estos desafíos, Valero propone una «reconfiguración de las garantías jurídicas » existentes, adaptándolas al contexto de la IA. Esto implica no solo la adopción de políticas provisionales mientras se desarrolla un marco normativo específico, sino también un esfuerzo por justificar cómo las garantías actuales pueden aplicarse a la IA. Aunque este enfoque proactivo puede influir positivamente en el desarrollo de futuras normativas, también conlleva riesgos, como la posible variación de políticas entre administraciones y el potencial obstáculo al desarrollo de aplicaciones de IA en el sector público si las políticas resultan excesivamente cautelosas.

En este contexto, Valero subraya acertadamente la importancia de asumir las consecuencias de un «funcionamiento anormal» de los servicios públicos, de acuerdo con el artículo 32 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, RJSP), refiriéndose a la obligación de la Administración de indemnizar a los particulares por los daños causados por sus actividades. Esto implica una responsabilidad objetiva, donde la Administración debe compensar a los ciudadanos por lesiones a sus bienes y derechos sin necesidad de demostrar culpa o negligencia. La indemnización se basa en criterios legales y requiere un nexo causal directo entre el servicio público y el perjuicio. Este principio busca proteger a los ciudadanos frente a daños administrativos, asegurando que la Administración asuma la responsabilidad por el funcionamiento inadecuado de sus servicios.

No sólo serán necesarios «nuevos conceptos jurídicos», sino que también será necesaria una armonización en el marco jurídico-constitucional que minimice los perjuicios tanto a los bienes jurídicos protegidos por la Constitución con mecanismos jurídicos eficaces para la resolución de conflictos que puedan surgir de la aplicación de la IA. Además, este marco tendrá que resolver los desafíos constitucionales planteados por la IA, pero con una visión altamente supranacional donde las respuestas trascienden las fronteras físicas y la jurisdicción tradicional de los Estados, tal y como ocurrió en su momento con la llegada de internet.

Para garantizar un uso ético y legal de la IA y la tecnología biométrica por parte de las administraciones públicas y las autoridades policiales, se requiere el establecimiento de nuevas garantías jurídicas. Estas salvaguardias deberán promover la responsabilidad, la transparencia y la protección de los derechos fundamentales en el despliegue de estas tecnologías sensibles.

3. Hacia un uso responsable de la IA y la tecnología biométrica por la administración pública y autoridades policiales

Este apartado analiza el uso responsable de la IA y la biometría por parte de la administración pública y autoridades policiales, considerando los tipos de tratamiento de datos biométricos y su base legitimadora. Se explorará la complejidad del «interés público» como base legitimadora, así como las insuficiencias regulatorias y la necesidad de armonización normativa en la materia. Finalmente, se aborda la importancia de la transparencia, seguridad y las guías de las autoridades de protección de datos para un uso responsable de la biometría.

3.1. Los tipos de tratamiento de datos biométricos y su base legitimadora

Existen algunos autores como Martínez Boada (2024) que catalogan los datos biométricos como especiales, sin embargo, en casos de autenticación, los datos biométricos podrían no considerarse de categoría especial.[2] Esto tiene implicaciones importantes, como la posibilidad de aplicar la base jurídica de obligación legal (art. 6.1. c)) o consentimiento (art. 6.1.a) para el tratamiento de datos, simplificando así el cumplimiento normativo. Por el contrario, para la identificación biométrica debería

[2] Véase Informe Jurídico 36/2020 de la AEPD; CEPD, Directrices 05/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley; y GT29, Dictamen 3/2012.

soportar el levantamiento de la prohibición del art. 9.2. g), haciendo más complejo el proceso de implementación práctica de las tecnologías para las autoridades. En ambos casos se desaconseja el uso del consentimiento como base jurídica debido a la dificultad que puede derivarse ante cualquier influencia o presión inadecuada ejercida sobre el interesado manifestada de diferentes formas.

En el primer caso, con tratamiento de datos biométricos sin ser categoría especial, se apuesta por poner luz sobre la base jurídica de obligación legal que, dependiendo de la finalidad del tratamiento y de los usuarios, por ejemplo, si pensamos en un sistema de autenticación o verificación de personal en instalaciones críticas reiterado con QR.

En el segundo escenario, -más complejo-, se recomienda el levantamiento de la prohibición del artículo 9.2. g) a través del «interés público esencial» con una norma de rango de ley -conforme el art.8.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en adelante, «LOPDGDD».

donde se regule la ponderación previa de los intereses atendiendo al «principio de proporcionalidad, todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías técnicas, organizativas y procedimentales adecuadas, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos» (AEPD 2020).

3.2. El interés público como base legitimadora en el tratamiento de datos: Un equilibrio complejo

No obstante, lo anterior, debemos estar atentos a la vaguedad de la noción de «interés público» el cual podría ser motivo de control de constitucionalidad debido a la indeterminación del precitado concepto (Simón y Dorado 2022). Aunque la preocupación de estos autores sobre la vaguedad del concepto de «interés público», en mi opinión, es comprensible, su crítica puede considerarse excesivamente cautelosa.

El marco legal existente, incluyendo el AIA y la LOPDGDD, establece salvaguardas significativas contra el uso indebido de este concepto. La flexibilidad inherente al término «interés público» es necesaria para adaptarse a un entorno tecnológico en rápida evolución. Además, la jurisprudencia establecida, la aplicación del principio de proporcionalidad y las garantías procedimentales requeridas proporcionan contrapesos importantes. En el contexto dinámico de la protección de datos, esta flexibilidad, combinada con los mecanismos de control existentes, puede considerarse más una fortaleza que una debilidad, permitiendo una aplicación adaptativa de la ley sin comprometer los derechos fundamentales.

3.3. Necesidad de regulación y armonización: Límites, requisitos y garantías

Partimos de la premisa fundamental de armonizar las diversas fuentes jurídicas que regulan el tratamiento de datos biométricos y genéticos en el ámbito policial y de seguridad. Esta armonización debe abarcar las líneas jurisprudenciales establecidas por los tribunales europeos, el marco normativo de la Unión Europea (que incluye el Reglamento General de Protección de Datos, la Directiva Policial y el futuro Reglamento

de IA), las legislaciones nacionales de los Estados miembros, y las normativas específicas aplicables a los cuerpos y fuerzas de seguridad.

A continuación, examinaremos la evolución de la jurisprudencia en esta materia, y las más recientes sentencias del Tribunal de Justicia de la Unión Europea. Este análisis nos permitirá comprender cómo los tribunales han ido refinando su interpretación sobre el equilibrio entre la seguridad pública y los derechos individuales en el contexto del tratamiento de datos biométricos. Finalmente, evidenciamos la necesidad de una regulación más específica y armonizada para garantizar una protección uniforme de los derechos fundamentales en toda la Unión Europea, facilitar la cooperación transfronteriza y evitar disparidades regulatorias entre los Estados miembros.

El Tribunal Europeo de Derechos Humanos (STEDH, 2008) en el caso *S. y Marper c. Reino Unido*, años antes, en 2008, involucró a dos personas absueltas de delitos cuyas huellas dactilares y muestras de ADN fueron conservadas por las autoridades británicas. A pesar de solicitar su eliminación, las autoridades se negaron a hacerlo, basándose en la legislación que permitía la conservación indefinida de estos datos para la prevención y detección de delitos. El TEDH consideró que esta práctica constituía una injerencia en el derecho a la vida privada (artículo 8 del CEDH). Aunque existía una base legal para la conservación de los datos, la regulación sobre su uso y conservación era imprecisa.

El Tribunal destacó que la conservación indiscriminada y sin límite temporal de datos de personas no condenadas era desproporcionada y no necesaria en una sociedad democrática. La sentencia del TEDH concluyó que se violó el artículo 8 del CEDH, al considerar que la conservación de estos datos en las condiciones descritas era una injerencia desproporcionada. Se subrayó la necesidad de equilibrar la seguridad pública con los derechos individuales, especialmente en el caso de personas no condenadas. Además, se enfatizó la importancia de contar con garantías claras y precisas en la legislación sobre conservación y uso de datos personales, así como la necesidad de mecanismos de revisión independientes para evaluar la necesidad de conservar los datos.

A pesar del avance en dicho reconocimiento, quien suscribe, critica que el TEDH no abordarse en profundidad las implicaciones de las diferencias tecnológicas entre los distintos tipos de datos biométricos, como las huellas dactilares y el ADN, que pueden tener distintos niveles de sensibilidad y potencial de uso. Tampoco exploró exhaustivamente las posibles excepciones en las que la conservación de datos de personas no condenadas podría ser justificable en casos particulares de seguridad nacional o prevención del crimen.

Por otro lado, la sentencia más reciente del Tribunal de Justicia de la Unión Europea (STJUE, 2022, asunto C-118/22), establece –marcando la misma línea- que la conservación general e indiferenciada de datos biométricos y genéticos hasta el fallecimiento de personas condenadas por delitos dolosos es contraria al Derecho de la Unión. El TJUE enfatiza la necesidad de límites temporales y justificaciones claras para la conservación de estos datos, obligando a revisar periódicamente si su mantenimiento sigue siendo necesario. Además, reconoce el «derecho del interesado a solicitar la supresión» de sus datos cuando la finalidad de conservación desaparezca. Esta decisión busca equilibrar la seguridad pública con la protección de la privacidad individual, rechazando la conservación indefinida de datos sensibles.

No obstante, en opinión de quien suscribe, se podría decir que no se han proporcionado directrices detalladas sobre los plazos concretos de conservación de datos biométricos en diferentes contextos ni se han abordado en profundidad los estándares técnicos para la protección y seguridad de los datos biométricos almacenados. El rápido avance tecnológico en este campo va a plantear desafíos continuos que requerirán una revisión y actualización constante de la jurisprudencia.

En relación con las garantías, a pesar del citado abanico de legislaciones, pronunciamientos y guías, aún existen críticas por su insuficiencia. Se acusa la falta de una ley reguladora específica y con garantías concretas para el uso de sistemas de identificación biométrica (Cotino 2022, p. 39), quedando un ámbito muy importante que requiere la intervención del legislador estatal en el ámbito criminal y policial. En este sentido, existe coincidencia en que faltan determinadas salvaguardias en la Directiva (Caruana 2017, Jasserand 2018), donde se podría haber proporcionado un nivel más alto de protección de datos.

La doctrina acierta al señalar la necesidad de una regulación más específica y garantías concretas para el uso de sistemas de identificación biométrica, especialmente en el ámbito criminal y policial. Además, la falta de una ley específica puede llevar a interpretaciones divergentes entre estados miembros, socavando la protección uniforme de los derechos de los ciudadanos en la UE.

El AIA parece ignorar –y desaprovecha la ocasión- en gran medida el régimen de protección de datos existente en lo relativo a datos biométricos. Podrían ser necesarias medidas adicionales tal y como señala el Comité Europeo de Protección de Datos, «CEPD», en adelante. Estas incluirían la creación de mecanismos de supervisión independientes para monitorear el uso de estos sistemas, así como la implementación de requisitos más estrictos para el consentimiento informado en la recolección y uso de datos biométricos. Es crucial establecer límites claros sobre la duración del almacenamiento de estos datos sensibles y fortalecer las sanciones por uso indebido o no autorizado.

La jurisprudencia, en la sentencia del 26 de enero de 2023 (STJUE, 2023, C-205/21), el Tribunal de Justicia de la Unión Europea estableció límites importantes a la recogida y conservación de datos biométricos y genéticos por parte de las autoridades policiales. El TJUE dictamina que la Directiva 2016/680 («Directiva policial») se opone a una normativa nacional que permita la recogida sistemática de estos datos de cualquier persona investigada por un delito público doloso sin una justificación adecuada. La sentencia enfatiza que dicha recogida debe ser estrictamente necesaria para objetivos concretos y precisos, y que no se puedan lograr por medios menos intrusivos. Además, el Tribunal subraya la necesidad de una base jurídica nacional clara y precisa, la obligación de revisar periódicamente la necesidad de conservación de los datos, y el derecho del interesado a solicitar su supresión cuando la finalidad de conservación desaparezca. Se destaca también que la conservación no puede ser indefinida hasta el fallecimiento del interesado, sino que debe estar sujeta a límites temporales y revisiones periódicas.

Quien suscribe considera crucial la coherencia entre el AIA, el RGPD y la Directiva Policial para evitar contradicciones y lagunas legales, asegurando un enfoque integral y transparente en el uso de sistemas biométricos. La armonización entre Estados es

igualmente esencial para garantizar una protección uniforme de los derechos fundamentales, facilitar la cooperación transfronteriza en seguridad y justicia. Focalizarse y abogar por establecer salvaguardias y una regulación específica proponiendo medidas concretas como certificaciones y códigos de conducta puede ser lo más acertado.

3.4. Transparencia, seguridad y guías de las autoridades de protección de datos: Hacia un uso responsable de la biometría

Es indiscutible la necesidad de avanzar hacia un uso responsable de las tecnologías biométricas que respete plenamente el «principio de transparencia». Para ello, resulta imperativo examinar críticamente el camino a seguir y analizar cómo las autoridades de control e instituciones europeas en materia de protección de datos están delineando este recorrido. Este análisis nos permitirá comprender las directrices actuales y anticipar los desafíos futuros en la regulación y aplicación de estas tecnologías, asegurando un equilibrio entre la innovación y la salvaguarda de los derechos fundamentales de los ciudadanos.

En relación con este principio, se recomienda que los resultados de estas evaluaciones de impacto, o al menos sus principales conclusiones, se hagan «públicos» para aumentar la confianza y la transparencia (CEPD 2022, párr. 57).

Ahora bien, ¿cuál debe ser el cauce para ello? La transparencia debería lograrse a través del derecho de acceso a la información pública, la obligación de motivar las decisiones, la prohibición de la arbitrariedad, el derecho a una buena administración y las garantías del debido proceso (Vestri 2021). En opinión de quien suscribe, este cauce podría tener limitaciones tales como exponer vulnerabilidades de seguridad, comprometer información confidencial y resultar demasiado técnica para el público general, además de suponer una carga administrativa considerable.

Limitaciones que sí han sido contempladas por las instituciones comunitarias quienes han destacado la necesidad de compartimentar y separar los datos, plantillas y datos brutos, cifrar los datos y plantillas biométricas, definir una política de cifrado y gestión de claves criptográficas, asociar firma o hash a la integridad de los datos y prohibir cualquier acceso externo a los datos biométricos y recuerda que la seguridad es aún más relevante si se utiliza un proveedor de servicios externo, y menciona la norma ISO 24745 sobre protección de información biométrica. Estas garantías deben exigirse con especial intensidad en el caso de sistemas biométricos.

Todo ello se refleja en las orientaciones y guías que la Agencia Española de Protección de Datos (AEPD, en adelante) ha publicado. Estas directrices establecen requisitos y principios que las organizaciones debían cumplir en el uso de datos, incluso antes de aprobarse el AIA, aunque no fueran vinculantes. No hace mucho tiempo, la AEPD emitió una nueva guía (2023) que se prevé será referenciada en futuros informes jurídicos, resoluciones y procedimientos sancionadores, utilizándose como criterio interpretativo de la normativa vigente. Alternativamente, estas guías podrían incorporarse a códigos de conducta aprobados según el artículo 40 del RGPD, lo que les conferirá un carácter más vinculante para las entidades adheridas.

El desarrollo de esquemas de certificación basados en estas guías también podría incentivar su cumplimiento. Las administraciones públicas podrían incluir el cumplimiento de estas guías como requisito en los pliegos de contratación pública para proyectos relacionados con IA. Aunque estas medidas pueden aumentar la relevancia práctica de las guías, su carácter vinculante en sentido estricto sólo puede provenir de su incorporación a normas jurídicas formales.

Además, se deberían requerir auditorías regulares y transparentes de los sistemas de IA de alto riesgo, mejorar los mecanismos de recurso y reparación para individuos afectados por decisiones basadas en estos sistemas, y establecer estándares más rigurosos para garantizar la precisión y fiabilidad de los sistemas de reconocimiento facial y biométrico.

4. La interpretación en la necesaria diferenciación de los tipos de tratamiento de datos biométricos

La identificación biométrica puede ser un método de reconocimiento automático basado en características físicas o de comportamiento únicas de las personas por los Cuerpos y Fuerzas de Seguridad. Los datos personales biométricos son obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona, que permiten o confirman su identificación única como las huellas dactilares, reconocimiento facial, iris y voz, geometría de la mano, patrones de venas o ADN, entre otros. En este sentido, el aprendizaje profundo y el aprendizaje automático son ampliamente utilizados en el análisis facial, facilitando una identificación más precisa y sencilla.

Ahora bien, las tecnologías biométricas plantean importantes desafíos interpretativos y jurídicos porque podrían ser considerados «datos de categoría especial» según el RGPD (vid. art. 4.14 y 9.1). Esta normativa europea no parece considerar a todo tratamiento de datos biométricos como tratamiento de categorías especiales de datos ya que los datos biométricos sólo constituyen una categoría especial de datos en el caso de que se sometan a un tratamiento técnico específico dirigido a identificar de manera unívoca a una persona física. Así, el Considerando 51 aclara que no todas las fotografías requieren ese nivel elevado de protección, sino solo aquellas utilizadas con fines biométricos específicos. De hecho, en el Convenio 108+ se incluye únicamente como categorías especiales de datos, en su artículo 6.1 a los datos biométricos dirigidos a la identificación unívoca de una persona «*biometric data uniquely identifying a person*», sin incluir la referencia a la autenticación.

Además, éstas necesitan medidas de seguridad robustas para proteger la confidencialidad e integridad de los datos, una Evaluación de Impacto en la Protección de Datos antes de su implementación y cumplir con los principios de minimización de datos y limitación de la finalidad.

De forma específica, los Cuerpos y Fuerzas de Seguridad pueden usar diversas formas para el control de acceso a áreas sensibles, para la autenticación de personal para acceso a sistemas e información clasificada, la prevención de suplantación de identidad de agentes de seguridad, la identificación de sospechosos comparando datos biométricos con bases de datos, vigilancia en espacios públicos usando reconocimiento facial, control

fronterizo para verificar la identidad de viajeros o la gestión de detenidos para registro y verificación de identidad.

La importancia de las salvaguardias en los sistemas de «vigilancia masiva electrónica» ha sido subrayada por el Tribunal Europeo de Derechos Humanos en casos como *Big Brother Watch y otros c. Reino Unido* en 2021 donde se ha señalado que para que sea compatible con el derecho al respeto a la vida privada y familiar, deben cumplirse ciertas condiciones; deben contar con garantías adecuadas, supervisión efectiva, protección de datos personales, base legal clara y proporcionalidad en su aplicación.

Aunque se determinó que el régimen de vigilancia masiva del Reino Unido viola los derechos a la privacidad y la libertad de expresión debido a varias deficiencias críticas en su diseño y ejecución, el TEDH reconoció que los Estados pueden operar sistemas de interceptación electrónica masiva y compartir información con otros Estados, siempre que se cumplan las mencionadas garantías (Paúl 2019).

Por otro lado, y de forma más alarmante, la proliferación de cámaras de vigilancia se ha justificado por las autoridades como una medida para aumentar la seguridad y prevenir delitos. Sin embargo, organizaciones de derechos humanos advierten que más cámaras no se traducen necesariamente en menos crímenes, además, existe el riesgo de que los gobiernos utilicen estas tecnologías para vulnerar la privacidad de los ciudadanos y perseguir a opositores políticos, especialmente en países con regímenes autoritarios, siendo peligroso su uso extensivo (Fussey y Murray 2019).

El consentimiento por parte de los ciudadanos fue a menudo inexistente o forzado especialmente cuando se trataba de vigilancia o de la recopilación de datos a través de tecnologías como el reconocimiento facial o las cámaras corporales (Mittelstadt *et al.* 2016, Laux *et al.* 2024). Esto desafiaba las normas convencionales sobre el consentimiento informado y plantea preguntas sobre cuánto control deberían tener las personas sobre sus propios datos cuando interactúan con las fuerzas del orden (Hernández y Baquero 2023). Además, hay que tener en cuenta que la IA puede contribuir a la creación de una «huella digital policial» muy detallada de los individuos dañando la privacidad civil (Cohen 2012).

En conclusión, el uso de las tecnologías biométricas puede dirigirse desde actividades de control de vigilancia de autenticación o verificación biométrica hasta la más polémica vigilancia biométrica en espacios públicos; todas ellas tienen diferentes implicaciones jurídicas. Las primeras tecnologías biométricas son las que están explorando las autoridades y administraciones públicas.

4.1. ¿Se encuentran correctamente diferenciadas las actividades de control de vigilancia de autenticación y verificación biométrica?

La distinción entre identificación y autenticación biométrica es fundamental en el contexto de la regulación de IA. La identificación biométrica busca reconocer a una persona específica dentro de un grupo amplio, realizando una comparación uno a varios. En contraste, la autenticación biométrica verifica la identidad declarada por un individuo, comparando sus datos con una plantilla preexistente en una comparación uno a uno. Esta diferenciación es crucial en el Reglamento europeo de IA, que clasifica los sistemas de autenticación biométrica que requieren participación activa del usuario

como de bajo riesgo, mientras que la Identificación Biométrica Remota o RBI, especialmente en tiempo real y en espacios públicos, se considera de alto riesgo o incluso prohibida, excepto en situaciones excepcionales. Esta categorización refleja las diferentes implicaciones éticas y de privacidad de cada tipo de sistema biométrico.

Los sistemas de reconocimiento biométrico, especialmente aquellos que utilizan tecnología algorítmica para reconocer individuos previamente registrados en una base de datos, se consideran como procesamiento de información personal altamente sensible. En consecuencia, estos sistemas deben ser evaluados minuciosamente para garantizar su conformidad con los principios constitucionales.

En casos de «autenticación», los datos biométricos podrían no considerarse de categoría especial (CEPD 2022, AEPD 2023). Esto tiene implicaciones importantes, como la posibilidad de aplicar la base jurídica de obligación legal para el tratamiento de datos, simplificando así el cumplimiento normativo para las autoridades policiales. Por el contrario, para la «identificación biométrica» debería soportar el levantamiento de la prohibición del 9.2. g).

La Audiencia Provincial de Barcelona, Sección Novena (2021), en su Auto 72/2021, de 15 de febrero, abordó efectivamente la distinción entre identificación y autenticación biométrica en el contexto de una solicitud de una cadena de supermercados para utilizar reconocimiento facial. El tribunal denegó la autorización para el uso de medios automatizados de captación de datos biométricos de personas condenadas por robo, con el fin de detectar su entrada en los establecimientos de la cadena. El tribunal señaló que el uso de tecnologías de reconocimiento facial en sistemas de video vigilancia constituye un tratamiento de datos biométricos que va más allá de una simple autenticación, tratándose en realidad de un proceso de identificación. La Audiencia -acertadamente- desestimó el argumento de Mercadona sobre la rapidez del procesamiento (0,3 segundos), reconociendo que incluso un procesamiento rápido puede constituir una violación de la privacidad. En mi opinión, los tribunales y juzgados españoles podrían estar bien capacitados para establecer diferencia entre identificación y autenticación biométrica, reconociendo que el sistema propuesto constituía un proceso de identificación más invasivo por lo que lo que quedaría es armonizar la regulación a nivel comunitario europeo.

4.2. La necesidad de una clara diferenciación o categorización de tipos de tratamientos de datos biométricos

Partimos de la idea de que el tratamiento de datos biométricos constituye una «interferencia grave», -incluso si dura milisegundos-, en la privacidad y puede tratar a todos los individuos como «potenciales sospechosos» afectando la presunción de inocencia. Podrían no ser suficientes para prevenir abusos donde su efectividad en la práctica preocupa. Los principios de transparencia, explicabilidad y no discriminación son esenciales, pero su implementación puede ser compleja. Se necesita una evaluación rigurosa de idoneidad, necesidad y proporcionalidad antes de implementar sistemas biométricos donde urge implementar garantías organizativas, técnicas y jurídicas más fuertes en el uso de tecnologías biométricas.

Los Cuerpos y Fuerzas de Seguridad podrían utilizar este tipo de tratamientos, más delicados, normalmente utilizados por expertos de la policía científica, para la identificación de culpables y sospechosos como es el sistema ABIS o *Automated Biometric Identification System,* que se utiliza para comparar imágenes con una base de datos de aproximadamente de cinco millones de fotografías faciales de personas detenidas o sospechosas, para operaciones de localización e identificación por comisión de delitos graves, especialmente aquellos mencionados en la Decisión Marco del Consejo Europeo de 2002 con penas de al menos tres años, para la prevención de amenazas contra la vida e integridad de los ciudadanos, la prevención de riesgos de ataques terroristas o la búsqueda de víctimas de delitos. Dichos sistemas tal y como señalan fuentes del Ministerio de Interior no se utilizarían para la identificación de personas captadas por cámaras de seguridad ni para reconocimiento en vivo en espacios públicos. Existen otros sistemas como SAID para la identificación utilizado por el Cuerpo Nacional de Policía en España para la identificación mediante huellas dactilares o EURODAC para solicitantes de asilo o migrantes irregulares.

Existen actividades de menor complejidad que utilizan datos biométricos, como el control de acceso a eventos específicos o la autenticación de personal reiterado en instalaciones críticas. El principal desafío radica en el tratamiento de datos biométricos como categoría especial (art. 9.2 RGPD), especialmente en la identificación biométrica. Para levantar la prohibición de su uso, se desaconseja el consentimiento (Art. 9.2.a), siendo más viable la opción de «**i**nterés público esencial» respaldada por leyes (Art. 8.2. LOPDGDD). Es obligatoria una Evaluación de Impacto en la Protección de Datos (EIPD) que documente el cumplimiento del triple examen de idoneidad, necesidad y proporcionalidad en el tratamiento de datos biométricos. Este proceso debe demostrar también la observancia de normativas como la Directiva Policial y el Reglamento sobre Inteligencia Artificial (AIA).

4.3. Análisis de interpretación regulatoria de los tipos de tratamientos de datos biométricos antes del AIA

Era tal la preocupación que despertó la situación que el Parlamento Europeo, a través de su Resolución en octubre de 2021, instó a la Agencia de Derechos Fundamentales de la UE a elaborar directrices, recomendaciones y buenas prácticas integrales sobre el uso de IA por parte de las autoridades.

Este documento establece límites al uso policial de herramientas de IA: se exigía supervisión humana, controles legales y la posibilidad de apelar decisiones tomadas por sistemas de IA; se reconocía y alertaba del riesgo de errores y perfilados discriminatorios de colectivos vulnerables; se prohibía el uso de bases de datos privadas de reconocimiento facial y técnicas predictivas de comportamiento; no se permitía el reconocimiento automático en fronteras ni espacios públicos, salvo excepciones y se hacía hincapié en que los algoritmos deben ser transparentes, trazables y preferiblemente de código abierto. Sin duda, esta resolución sentó las bases para el desarrollo de la futura IA. No obstante, al no ser vinculante será insuficiente para regular efectivamente el uso de IA por autoridades en comparación con el AIA, el cual ofreció una respuesta algo más completa, aunque con limitaciones como veremos.

En casos de autenticación, tal y como señala la autoridad de control española y las instituciones comunitarias ya citadas previamente (GT29 2012, CEPD 2022, AEPD 2023) los datos biométricos podrían no considerarse de categoría especial. Esto tiene implicaciones importantes, como la posibilidad de aplicar la base jurídica de obligación legal (art. 6.1. c)) o consentimiento (art. 6.1.a) para el tratamiento de datos, simplificando así el cumplimiento normativo. Por el contrario, para la identificación biométrica debería soportar el levantamiento de la prohibición del art. 9.2. g), haciendo más complejo el proceso de implementación práctica de las tecnologías para las autoridades. En ambos casos se desaconseja el uso del consentimiento como base jurídica debido a la dificultad que puede derivarse ante cualquier influencia o presión inadecuada ejercida sobre el interesado manifestada de diferentes formas.

En el primer caso, con tratamiento de datos biométricos sin ser categoría especial, se apuesta por poner luz sobre la base jurídica de obligación legal que, dependiendo de la finalidad del tratamiento y de los usuarios, por ejemplo, si pensamos en un sistema de autenticación o verificación de personal en instalaciones críticas reiterado con QR.

En el segundo escenario, -más complejo-, se recomienda el levantamiento de la prohibición del artículo 9.2. g) a través del interés público esencial con una norma de rango de ley (Art.8.2 LOPDGDD) donde se regule la ponderación previa de los intereses atendiendo al «principio de proporcionalidad, todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías técnicas, organizativas y procedimentales adecuadas, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos» (AEPD 2020).

No obstante, debemos estar atentos a la vaguedad de la noción de «interés público» el cual podría ser motivo de control de constitucionalidad debido a la indeterminación del precitado concepto (Simón y Dorado 2022).

Aunque la preocupación de estos autores sobre la vaguedad del concepto de interés público, en mi humilde opinión, es comprensible, su crítica puede considerarse excesivamente cautelosa. El interés público es reconocido como un concepto jurídico indeterminado, lo que no implica arbitrariedad en su aplicación y su inclusión en la Constitución proporciona una base sólida para su interpretación y aplicación. No es un concepto totalmente abierto o arbitrario.

En relación, con las garantías, a pesar del citado abanico de legislaciones, pronunciamientos y guías existen aún críticas por su insuficiencia como hemos señalado anteriormente, existen claras críticas (Caruana 2017, Jasserand 2018, Cotino 2022) en torno a la necesidad de una regulación más específica y garantías concretas para el uso de sistemas de identificación biométrica, especialmente en el ámbito criminal y policial. Además, es necesario afirmar que la falta de una ley específica puede llevar a interpretaciones divergentes entre estados miembros, socavando la protección uniforme de los derechos de los ciudadanos en la UE.

4.4. Análisis de interpretación regulatoria en los tratamientos de datos biométricos a partir del AIA

El marco legal existente, incluyendo el AIA y la LOPDGDD, establece salvaguardas significativas contra el uso indebido de este concepto. La flexibilidad inherente al término interés público es necesaria para adaptarse a un entorno tecnológico en rápida evolución respetando las salvaguardas de un Estado de Derecho. Además, la jurisprudencia establecida, la aplicación del principio de proporcionalidad y las garantías procedimentales requeridas proporcionan contrapesos importantes. En el contexto dinámico de la protección de datos, esta flexibilidad, combinada con los mecanismos de control existentes, puede considerarse más una fortaleza que una debilidad, permitiendo una aplicación adaptativa de la ley sin comprometer los derechos fundamentales.

No obstante, quien suscribe añadiría que resulta crucial la coherencia entre el AIA, el RGPD y la Directiva Policial para evitar contradicciones y lagunas legales, asegurando un enfoque integral y transparente en el uso de sistemas biométricos.

El AIA parece ignorar –y desaprovecha la ocasión– en gran medida el régimen de protección de datos existente en lo relativo a datos biométricos. Podrían ser necesarias medidas adicionales tal y como señala el CEPD. Estas incluirían la creación de mecanismos de supervisión independientes para monitorear el uso de estos sistemas, así como la implementación de requisitos más estrictos para el consentimiento informado en la recolección y uso de datos biométricos. Es crucial establecer límites claros sobre la duración del almacenamiento de estos datos sensibles y fortalecer las sanciones por uso indebido o no autorizado. Además, se deberían requerir auditorías regulares y transparentes de los sistemas de IA de alto riesgo, mejorar los mecanismos de recurso y reparación para individuos afectados por decisiones basadas en estos sistemas, y establecer estándares más rigurosos para garantizar la precisión y fiabilidad de los sistemas de reconocimiento facial y biométrico.

La preocupación de la vigilancia masiva llegó a instituciones como el CEPD, el SEPD y el Parlamento Europeo quienes se mostraron bastante preocupados con la propuesta inicial del AIA. No era suficiente para regular adecuadamente la identificación biométrica con IA y se opusieron a la «identificación biométrica remota» en espacios públicos y su alto riesgo de invasión de la privacidad con consecuencias para la expectativa de anonimato de la población, así que solicitaron prohibir el uso de IA para reconocer automatizado de rasgos humanos en «espacios públicos», como rostros, huellas dactilares, ADN, voz y otros datos biométricos o de comportamiento que clasifican a las personas en grupos por motivos étnicos, sexo, orientación política o sexual u otros motivos de discriminación. Finalmente, se prohibió el uso de la vigilancia biométrica en tiempo real: se conocen como «riesgo inaceptable». Solo los sistemas de identificación biométrica a distancia podrán usarse si se aplica la ley para perseguir delitos graves y sólo tras una autorización judicial.

La «regulación de algoritmos policiales» en España es actualmente escasa (Rivero 2023).

El principal marco legal español es el artículo 23 de la Ley 15/2022, de 12 de julio, para la igualdad de trato y la no discriminación, sin embargo, esta regulación es general y no

aborda específicamente los algoritmos policiales planteando desafíos significativos en términos de garantías legales y protección de derechos fundamentales.

Por lo tanto, con la llegada del AIA –definitivo- se reforzó la protección a los individuos en relación con las tecnologías biométricas suponiendo mejoras respecto de su regulación. Se escucharon las demandas del SEPD y el CEPD, así como de otras organizaciones internacionales y europeas. La exigencia de evaluaciones de impacto en los derechos de los individuos y las obligaciones de transparencia durante todo el ciclo de vida del sistema permiten generar una mayor confianza social. Esto incluye conocer quién diseña las categorías, su significado y quién decide bajo qué circunstancias serán decisivas. Sin duda, fue un gran paso y empuje por parte de las instituciones para fortalecer la protección de los derechos y libertades de las personas en el ámbito de las tecnologías biométricas, aunque no será suficiente.

El AIA clasificó como «alto riesgo» a los sistemas de reconocimiento facial y biométrico. El AIA exige la implementación de *mecanismos de supervisión humana, auditorías periódicas y medidas* para mitigar riesgos. Por ende, en el caso de que se opte por adoptar concretos sistemas de identificación biométricos, además de la obligatoria regulación legal y legitimación de estos, de su necesidad y proporcionalidad, habrá que cumplirse toda una batería de garantías y exigencias de *estudios de impacto*, responsabilidad activa y en el diseño (Cotino 2020).

Además de los análisis y evaluaciones de impacto, la normativa de protección de datos impone otras obligaciones para el uso de sistemas biométricos llevar un *registro de actividades* (vid. Art. 25 Directiva Policial), realizar análisis de riesgos, aplicar medidas de seudonimización y anonimización de datos, gestionar adecuadamente la calidad de los datos, documentar cualquier violación de datos, problemas de ciberseguridad, e implementar medidas de seguridad apropiadas.

5. Reflexiones finales hacia la necesidad de una regulación específica y a la reconfiguración de las garantías jurídicas

El Reglamento europeo de IA analizado es incompleto sin una mayor regulación o normalización sectorial. La fusión conceptual en la Ley de IA oculta la necesidad de instituciones confiables para fomentar la confianza ciudadana en la IA donde las asimetrías de conocimiento entre expertos en IA y ciudadanos comunes plantean desafíos adicionales.

Se plantean interrogantes sobre la necesidad de reconfigurar las garantías jurídicas existentes. El marco normativo actual, basado en gran medida en la legislación de 2007, resulta insuficiente para abordar las complejidades de la IA, especialmente en áreas como la automatización cognitiva y el análisis predictivo. Es necesario formular nuevos conceptos jurídicos y armonizar el marco jurídico-constitucional para minimizar los perjuicios a los bienes jurídicos protegidos por la Constitución. Además, es fundamental que la administración pública asuma la responsabilidad por los daños causados por el funcionamiento anormal de los servicios públicos impulsados por la IA. Se deben adaptar las garantías jurídicas existentes al contexto de la IA, garantizando que se respeten los principios de buena administración y la defensa del interés general, y adoptar una visión supranacional para abordar los desafíos constitucionales planteados por la IA.

Considerando que el derecho actúa como garante fundamental para la correcta ordenación de las relaciones entre las personas y que, en un sistema democrático, resulta indispensable asegurar las garantías que protegen los derechos fundamentales de los ciudadanos (Castellanos 2023), se impone una reflexión crítica respecto a la integración de nuevas tecnologías en la administración pública.

En este sentido, ante la posible y creciente implementación de sistemas de IA en los procesos administrativos, y dada la especial relevancia que reviste el grado de automatización en la actuación administrativa (Cotino 2023), surge la imperiosa necesidad de establecer una «salvaguardia constitucional». Esta medida debe responder a la incidencia directa que dicha tecnología ejerce sobre el derecho fundamental al «debido proceso», previsto en el artículo 24.2 de la Constitución Española, garantizando así la protección efectiva de las garantías procesales ante la transformación digital del ámbito público.

Esta medida se fundamenta en que la adopción masiva de IA en la administración pública, si bien orientada a mejorar la eficiencia y reducir la burocracia, puede comprometer principios constitucionales esenciales como el debido proceso y la tutela judicial efectiva. La automatización y el análisis algorítmico, sin la debida supervisión, tienen el potencial de afectar la transparencia de las decisiones, limitar el derecho a la defensa y debilitar los mecanismos de control efectivo, elementos imprescindibles para garantizar la legitimidad y equidad en las actuaciones administrativas.

La regulación de la IA en los procedimientos administrativos debe centrarse en la protección de los derechos fundamentales, asegurando que el principio de debido proceso incluye no sólo la formalidad procesal, sino también el acceso real a la información, la posibilidad de impugnar y revisar racionalmente las decisiones emitidas por sistemas automatizados. La doctrina destaca que, sin controles adecuados, las decisiones algorítmicas pueden devenir opacas y sesgadas, vulnerando el derecho a la tutela judicial efectiva (STC 76/2018, FJ 3). La jurisprudencia constitucional española ha establecido la importancia de que cualquier innovación tecnológica respete el marco constitucional, especialmente en la función pública, garantizando mecanismos de supervisión humana, auditorías transparentes y recursos accesibles para impugnar decisiones automatizadas.

La base legal debe contemplar expresamente los requisitos y condiciones para la utilización de IA, evitando improvisaciones y lagunas normativas y exigiendo un control riguroso de su aplicación. Debe establecerse que toda decisión asistida o tomada por IA esté sujeta a una supervisión humana real, competente e independiente, que permita revisar, modificar o anular las decisiones automatizadas cuando se detecten errores, sesgos o afectación de derechos, asegurando así el control de legalidad y la eficacia de los recursos judiciales y administrativos.la salvaguardia constitucional debe exigir la realización de auditorías periódicas, técnicas, independientes y sistemáticas sobre los sistemas de IA, para detectar, corregir y prevenir posibles sesgos, errores o discriminaciones que puedan surgir en los algoritmos, garantizando la igualdad y el principio de no discriminación en la administración pública. Así, se preserva el imperio de la ley, la justicia material y el respeto a la dignidad humana, fundamentales en el derecho procesal constitucional. Este enfoque se fundamenta en la doctrina actual (Cotino 2024, Carlón 2024) y en la interpretación jurisprudencial española, como expone

el análisis del Real Decreto-ley 6/2023 y la posición de órganos como el Consejo General del Poder Judicial, que destaca la necesidad de una supervisión independiente y especializada para sistemas de IA jurisdiccionales de alto riesgo, acorde con la separación de poderes y la protección de derechos procesales efectivos

Asimismo, la Comisión Europea (Medaglia *et al.* 2024) resalta la necesidad de competencias técnicas y éticas que permitan adecuar la gobernanza pública ante la irrupción de la IA, enfatizando la importancia de un equilibrio entre innovación tecnológica y garantías jurídicas para preservar los derechos fundamentales y la legitimidad democrática. Por ello, la «salvaguardia constitucional» propuesta no solo es un requerimiento doctrinal, sino un mandato práctico indispensable para una administración pública cada vez más automatizada y dependiente de sistemas inteligentes.

Por último, es imprescindible destacar la carencia actual en España de una regulación específica y coherente sobre los algoritmos utilizados por las fuerzas policiales aunque exista un Anteproyecto de Ley para el buen uso y la gobernanza de la IA (2025) del Ministerio para la Transformación Digital y de la Función Pública. El marco normativo vigente, principalmente el artículo 23 de la Ley 15/2022 para la igualdad de trato y no discriminación, resulta insuficiente para abordar los retos jurídicos y éticos que plantea el uso de algoritmos policiales. Esta laguna normativa suscita importantes desafíos en materia de garantías legales y protección de derechos fundamentales, que requieren una respuesta regulatoria urgente y precisa para evitar vulneraciones en el ejercicio del poder público mediante tecnologías algorítmicas

Es indiscutible que el respeto a los derechos fundamentales debe ser un principio rector en todo el ciclo de vida de los sistemas de IA utilizados por las autoridades. La concepción del derecho a la protección de datos y a la privacidad como derecho humano se refleja en la tríada normativa formada por; el AIA, la Directiva policial y el RGPD, que servirá de guía para desarrolladores y usuarios de sistemas IA. En este artículo, aunque se aplaude los avances de los legisladores, se aseveran aspectos que podrían haber mejorado.

Sin embargo, el AIA parece no alinearse completamente con estas normas, especialmente en lo referente a datos biométricos, revelando una falta de armonización entre la regulación de la IA y las leyes de protección de datos existentes.

Además, es innegable que el Supervisor Europeo de Protección de Datos (SEPD 2024) y el CEPD (2021) han sido fundamentales en la definición del Reglamento de Inteligencia Artificial (AIA), estableciendo restricciones más rigurosas en el uso de tecnologías de IA, particularmente en el ámbito de la identificación biométrica. Sin embargo, el enfoque actual de las autoridades parece centrarse más en el uso de estas tecnologías para fines de autenticación o verificación, en lugar de la vigilancia biométrica generalizada. Un ejemplo de esto sería el control de acceso recurrente del personal a instalaciones de alta seguridad.

En el Reglamento de IA se pierde la oportunidad de profundizar en los procedimientos que podrían demostrar la tan mencionada transparencia. Esta transparencia podría lograrse mediante el acceso a la información pública, la obligación de motivar las decisiones, la prohibición de la arbitrariedad, el derecho a una buena administración y

las garantías del debido proceso. Sin embargo, esta perspectiva se debilita al sugerir que la confianza en la IA puede basarse más en factores emocionales o heurísticos que en una comprensión técnica profunda.

Finalmente, con objeto de conseguir cierta «armonización normativa», la Agencia de Derechos Fundamentales de la UE debería elaborar más directrices, recomendaciones y buenas prácticas integrales sobre el uso de IA por parte de las autoridades. La Oficina de IA y el Comité Europeo de Inteligencia Artificial deberán liderar iniciativas de directrices detalladas, creación de códigos de conductas y establecimiento de estándares armonizados en materia de seguridad pública y penal. Auguramos que lograr el equilibrio adecuado entre los beneficios del uso de IA y los riesgos para los derechos individuales será cada vez más complejo. La IA es una tecnología muy amplia que se aplica en diferentes sectores lo que dificulta la creación de normas armonizadas.

Un enfoque equilibrado y éticamente informado es esencial para garantizar el máximo beneficio de los sistemas IA y minimizar sus riesgos y desafíos éticos donde la necesidad del diálogo constante entre los actores (Fuerzas y Cuerpos de Seguridad, reguladores, juristas, jueces, desarrolladores y tecnólogos, ciudadanía, AEPD, Agencia Española de Supervisión de IA o AESIA, etc.) donde la labor de las diferentes áreas de estas autoridades y administraciones públicas son relevantes (oficina técnica, asesoría jurídica, etc.) unido a la colaboración de expertos en IA y privacidad para asegurar el uso de la tecnología maximizando la utilidad pública sin erosionar los derechos y libertades de las personas. La creación de sellos de calidad de IA responsable y ética para las autoridades policiales y judiciales, la inclusión de proyectos biométricos o de perfilado en el *Sandbox* español de IA, crear una Carta de Derechos para establecer estándares sobre el uso de la IA en seguridad pública y penal alineándose con los objetivos de la ley para beneficiar a los usuarios y ciudadanos son posibles soluciones -paralelas- por construir.

6. Conclusiones

1. Urge una regulación específica y coherente para la IA y los algoritmos utilizados por la policía, ya que la actual legislación es limitada y no aborda los desafíos éticos y jurídicos particulares de este ámbito. Aunque se reconocen los avances en la protección de derechos fundamentales en el uso de IA, existe una falta de armonización entre el AIA, el RGPD y la Directiva Policial, especialmente en el tratamiento de datos biométricos. Es esencial alinear estas normativas para garantizar una protección integral de los derechos individuales, a través de directrices integrales de la Agencia de Derechos Fundamentales de la UE.
2. Se propone una salvaguarda constitucional para proteger el debido proceso ante la creciente integración de la IA en procesos administrativos y judiciales. Esta salvaguardia garantizaría la transparencia, la rendición de cuentas y la no discriminación, priorizando una interpretación evolutiva por parte del Tribunal Constitucional como mecanismo más viable.
3. Las autoridades parecen enfocarse en la autenticación biométrica (uno a uno) en lugar de la identificación (uno a varios). El AIA clasifica estos usos de manera diferente, con la autenticación considerada de menor riesgo. Es fundamental comprender esta distinción para una aplicación correcta de la

regulación, la cual ha sido bien comprendida por los tribunales españoles al entender la graduación de invasión en el proceso de identificación.

4. Los sistemas de reconocimiento biométrico deben someterse a una evaluación rigurosa para asegurar su conformidad con los principios constitucionales, ya que implican el procesamiento de información personal altamente sensible.
5. La clasificación de los datos biométricos como « de categoría especial» varía según su uso (autenticación o. identificación), lo que afecta la base jurídica aplicable para su tratamiento por parte de las autoridades policiales.
6. El uso de la IA por parte de la Administración Pública conlleva una serie de límites, riesgos y responsabilidades que deben ser abordados de manera integral. Aunque la preocupación sobre la vaguedad del concepto de interés público es comprensible, el marco legal existente, incluyendo el AIA y la LOPDGDD, establece salvaguardias significativas contra el uso indebido de este concepto. A pesar del abanico de legislaciones, pronunciamientos y guías existentes, aún se consideran insuficientes, siendo necesaria una regulación más específica y garantías concretas para el uso de sistemas de identificación biométrica, especialmente en el ámbito criminal y policial.
7. El enfoque de algunos autores de asegurar la transparencia a través del derecho de acceso a la información pública tiene limitaciones como la exposición de vulnerabilidades de seguridad y de información confidencial, y de ineficiencia administrativa.
8. Es fundamental compartimentar y separar los datos, plantillas y datos brutos, cifrar los datos y plantillas biométricas, definir una política de cifrado y gestión de claves criptográficas, asociar firma o hash a la integridad de los datos y prohibir cualquier acceso externo a los datos biométricos.
9. La Oficina de IA y el Comité Europeo de Inteligencia Artificial podrían liderar la creación de códigos de conducta y estándares armonizados en seguridad pública y penal. Lograr un equilibrio entre los beneficios y riesgos de la IA será un desafío constante.
10. Se deben desarrollar guías y códigos de conducta que establezcan criterios interpretativos de la normativa vigente y otorguen un carácter más vinculante a las obligaciones de las organizaciones, así como el desarrollo de esquemas de certificación que permitan generar confianza. Un enfoque ético e informado, junto con un diálogo constante entre las partes interesadas (autoridades, reguladores, expertos, ciudadanos), es esencial para maximizar los beneficios de la IA y minimizar sus riesgos. Se proponen la creación de sellos de calidad, la inclusión de proyectos en «sandboxes» regulatorios, y una Carta de Derechos para el uso de la IA en seguridad pública.

Referencias

Agencia Española de Protección de Datos (AEPD), 2020. *Informe Jurídico 36/2020* [en línea]. Disponible en: https://www.aepd.es/documento/2020-0036.pdf

Agencia Española de Protección de Datos (AEPD), 2023. *Guía sobre tratamiento de control de presencia mediante sistemas biométricos* [en línea]. Noviembre. Disponible en: https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf

Carlón Ruiz, M., 2024. *Utilización de sistemas de inteligencia artificial por administraciones públicas: un sistema propio de garantías como requisito imprescindible para su viabilidad* [en línea]. Ponencia presentada en el Congreso AEPDA 2024. Disponible en: https://congresoaepdavigo2024.es/wp-content/uploads/2023/12/Ponencia-M-Carlon-LA-ADMINISTRACION-PUBLICA-ANTE-LA-INTELIGENCIA-ARTIFICIAL.pdf

Caruana, M., 2017. The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement. *International Review of Law, Computers and Technology* [en línea], 33(3). Disponible en: https://doi.org/10.1080/13600869.2017.1370224

Castellanos Claramunt, J., 2023. Sobre los desafíos constitucionales ante el avance de la Inteligencia Artificial. *Revista de Derecho Político* [en línea], 118. Disponible en: https://doi.org/10.5944/rdp.118.2023.39105

Cohen, J.E., 2012. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice***.** Yale University Press.

Comité Europeo de Protección de Datos (CEPD), 2022. *Directrices 05/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley* [en línea]. Disponible en: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en

Comité y Supervisor Europeo de Protección de Datos (CEPD), 2021. *Dictamen conjunto 5/2021 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial)* [en línea]. 18 de junio. Disponible en: https://www.edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_es.pdf

Cotino Hueso, L, 2022. Transparencia y explicabilidad de la inteligencia artificial y «compañía» (comunicación, interpretabilidad, inteligibilidad, auditabilidad, testabilidad, comprobabilidad, simulabilidad…). Para qué, para quién y cuánta. *En:* L. Cotino Hueso y J. Castellanos Claramunt, eds., *Transparencia y explicabilidad de la inteligencia artificial.* Valencia: Tirant lo Blanch.

Cotino Hueso, L., 2023. Los usos de la inteligencia artificial en el sector público, su variable impacto y categorización jurídica. *Revista Canaria de Administración Pública* [en línea], 1. Disponible en: https://revistacanarias.tirant.com/index.php/revista-canaria/article/view/7

Cotino Hueso, L., 2024. El uso jurisdiccional de la inteligencia artificial: habilitación legal, garantías necesarias y supervisión. *Revista Actualidad Jurídica Iberoamericana* [en línea], 21. Disponible en: https://producciocientifica.uv.es/documentos/66c38db00bd02a6216608507

Dhar, V., 2013. Data science and prediction. *Communications of the ACM*, 56(12), 2013, 64-73.

Fussey, P., y Murray, D., 2019. *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology* [en línea]. Julio. University of

Essex Human Rights Centre. Disponible en: https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf

Gimeno, J., 2023. Instrumentos actuales de policía y justicia predictiva en el proceso penal español: análisis crítico y reflexiones de lege ferenda ante aplicaciones futuras. *Estudios Penales y Criminológicos* [en línea], 44(Ext.), 1-22. Disponible en: https://doi.org/10.15304/epc.44.9027

Grupo de Trabajo del Art. 29 (GT29). *Dictamen 3/2012* [en línea]. Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp193_es.pdf

Hernández, M.T., y Baquero, P.J., 2023. Datos policiales e inteligencia artificial. Un equilibrio delicado entre la privacidad, la utilidad y la ética. *Revista RCAP* [en línea], nº extraordinario, pp. 143-173. Disponible en: https://doi.org/10.36151/RCAP.ext.6

Jasserand, C., 2018. Subsequent use of GDPR data for a law enforcement purpose: the forgotten principle of purpose limitation?. *European Data Protection Law Review* [en línea], 4(2), 152-167. Disponible en: https://doi.org/10.21552/edpl/2018/2/6

Jordan, M.I., y Mitchell, T.M., 2015. Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245), 255-260.

Laux, J., Wachter, S., y Mittelstad, B., 2024. Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk. *Regulation & Governance* [en línea], (2024)18, 3-32. Disponible en: https://doi.org/10.1111/rego.12512

Martínez Boada, J., 2024. Blockchain como sistema para cumplir con la obligación de control y registro de la jornada laboral de los trabajadores. *IDP. Revista de Internet, Derecho y Política* [en línea], n.º 41. Disponible en: https://doi.org/10.7238/idp.v0i41.430846

Martínez López-Saéz, M., 2021. La ratificación española del Convenio 108+: consideraciones jurídicas básicas del nuevo marco paneuropeo de protección de datos. *Revista General de Derecho Europeo,* 54.

Medaglia, R., Mikalef, P., y Tangi, L., 2024. *Competences and governance practices for artificial intelligence in the public sector* [en línea]. Comisión Europea, Centro Común de Investigación. Luxemburgo: Oficina de Publicaciones de la Unión Europea. Disponible en: https://publications.jrc.ec.europa.eu/repository/handle/JRC138702

Ministerio para la Transformación Digital y de la Función Pública, 2025. *Ley para el buen uso y la gobernanza de la inteligencia artificial (Anteproyecto)* [en línea]. Madrid: Gobierno de España. Disponible en: https://avance.digital.gob.es/_layouts/15/HttpHandlerParticipacionPublicaAnexos.ashx?k=19128

Mittelstadt, B., *et al.*, 2016. The ethics of algorithms: Mapping the debate. *Big Data & Society* [en línea]. Disponible en: https://doi.org/10.1177/2053951716679679

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 parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. *Diario Oficial de la Unión Europea* [en línea], L 119, 4 de mayo de 2016. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L0680

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. *Diario Oficial de la Unión Europea* [en línea], L 119, 4 de mayo de 2016. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Paúl, A., 2019. El 'Gran Hermano': Un caso de vigilancia masiva en Europa ('Big Brother': A Case of Mass Surveillance in Europe). *Revista de Derecho Universidad San Sebastián* [en línea], 25, 140-152. Disponible en: https://ssrn.com/abstract=3385821

Rivero Ortega, R., 2023. Algoritmos, inteligencia artificial y policía predictiva del Estado vigilante. *Revista General de Derecho Administrativo* [en línea]. Disponible en: https://www.iustel.com/v2/revistas/detalle_revista.asp?id_noticia=425794

Simón Castellano, P., y Dorado Ferrer, X., 2022. Límites y garantías constitucionales frente a la identificación biométrica. *IDP. Revista de Internet, Derecho y Política* [en línea], núm. 35. Disponible en: http://dx.doi.org/10.7238/idp.v0i35.392324

Supervisor Europeo de Protección de Datos (SEPD), 2024. *Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems* [en línea]. 3 de junio. Disponible en: https://www.edps.europa.eu/system/files/2024-05/24-05-29_genai_orientations_en_0.pdf

Valero Torrijos, J., 2019. Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración. *Revista Catalana de Dret Públic* [en línea], núm. 58, p. 82. Disponible en: https://doi.org/10.2436/rcdp.i58.2019.3307

Vestri, G., 2021. La inteligencia artificial ante el desafío de la transparencia algorítmica: Una aproximación desde la perspectiva jurídico-administrativa. *Revista Aragonesa de Administración Pública* [en línea], (56), 368-398. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7971161

Fuentes jurídicas

Ley 15/2022, de 12 de julio, para la igualdad de trato y la no discriminación. *Boletín Oficial del Estado* [en línea], núm. 167, 13 de julio de 2022. Disponible en: https://www.boe.es/eli/es/l/2022/07/12/15

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. *BOE* [en línea], núm. 236, 2 de octubre de 2015. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado* [en línea], núm. 294, 6 de diciembre de 2018. Disponible en: https://www.boe.es/eli/es/lo/2018/12/05/3/con

Jurisprudencia

Audiencia Provincial de Barcelona, Sección Novena. Auto nº 72/2021, de 15 de febrero de 2021 (Recurso nº 840/2021). *Diario La Ley*, nº 52.

Tribunal Constitucional, 1993. Sentencia núm. 254/1993, de 20 de julio. *BOE* [en línea], núm. 186, de 6 de agosto de 1993, pp. 23591-23604. Disponible en: https://www.congreso.es/constitucion/ficheros/sentencias/stc_254_1993.pdf

Tribunal Constitucional, 2018. Sentencia 76/2018, de 5 de julio de 2018. *BOE* [en línea], núm. 189, 6 de agosto de 2018. ECLI:ES:TC:2018:76. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-11274

Tribunal de Justicia de la Unión Europea. *NG contra Direktor na Glavna direktsia Natsionalna politsia pri MVR — Sofia, Asunto C-118/22* [en línea]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62022CA0118

Tribunal Europeo de Derechos Humanos. *Big Brother Watch y otros c. Reino Unido (Demandas núms. 58170/13, 62322/14 y 24960/15)*. Sentencia de la Gran Sala de 25 de mayo de 2021.

Tribunal Europeo de Derechos Humanos. *S. y Marper c. Reino Unido, n.º 30562/04 y 30566/04, 4 de diciembre de 2008* [en línea]. Disponible en: https://hudoc.echr.coe.int/eng?i=002-1784

Tribunal Justicia Unión Europea. *Asunto C-205/21, de 26 de enero de 2023* [en línea]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62022CA0118