XVII
2024

Anuario de la Facultad de Derecho

UAH

UNIVERSIDAD DE ALCALÁ

ANUARIO DE LA FACULTAD DE DERECHO DE LA UNIVERSIDAD DE ALCALÁ
VOL. XVII-2024

Monográfico dedicado a las implicaciones legales de la Inteligencia Artificial

ANUARIO DE LA FACULTAD DE DERECHO DE LA UNIVERSIDAD DE ALCALA

CONSEJO DE REDACCIÓN

COMITÉ ASESOR

---

* Hasta octubre de 2023, el Director de la revista fue el Prof. Dr. Miguel Rodríguez Blanco.

** Hasta octubre de 2023, el Secretario de la revista fue el Prof. Dr. José Antonio del Olmo.

SUSCRIPCIÓN

Facultad de Derecho.
C/ Libreros 27. 28801 Alcalá de Henares (Madrid)

Para la suscripción, adquisición de ejemplares o colaboración con el Anuario, consultar las Instrucciones para los autores y la Hoja de pedido/suscripción.

ISSN: 1888-3214
Depósito legal: M-3.445-1992
DOI: https://doi.org/10.14679/3896

El Anuario de la Facultad de Derecho de la Universidad de Alcalá es una publicación de periodicidad anual que se publica en el primer trimestre de cada año. El Anuario se encuentra indexado en las bases de datos ACNP, CIRC, COPAC, CSIC, DIALNET, DICE, DULCINEA, EBSCO, IN-RECJ, ISOC, JSTOR, Directorio y Catálogo LATINDEX, MIAR, OCLC WorldCat, RESH, SUDOC, vLEX y ZDB.

ÍNDICE

I. ESTUDIOS

II. NOTAS

III. TRABAJOS PREMIADOS

LA UTILIZACIÓN DE LA IDENTIFICACIÓN BIOMÉTRICA EN ESPACIOS DE ACCESO PÚBLICO: EXCEPCIONES, PRINCIPIOS Y LÍMITES [1]

THE USE OF BIOMETRIC IDENTIFICATION IN PUBLIC ACCESS AREAS: EXCEPTIONS, PRINCIPLES AND LIMITS

CRISTINA SAN MIGUEL CASO
Universidad de Cantabria

Recibido: 08/10/2024
Aceptado: 25/11/2024

DOI: https://doi.org/10.14679/3900

Resumen: La utilización de sistemas de identificación biométrica en espacios de acceso público como medio de investigación en un proceso penal, no está exenta de controversia debido a los riesgos inherentes que entraña la implementación de estas prácticas altamente invasivas, tanto en los derechos de los sujetos investigados como, también, en los de la sociedad en su conjunto. Por esta razón, el presente estudio pretende ilustrar al lector en torno a los procedimientos, principios y límites que deben ser observados por la autoridad judicial a tenor de lo dispuesto, recientemente, en el Reglamento Europeo de Inteligencia Artificial. Para ello, será preciso elaborar una construcción teórica en torno al concepto, desgranando cómo, dónde, cuándo y para qué puede llevarse a cabo la práctica de la medida, no sin antes realizar una reflexión somera y generalista respecto al carácter sensible de los datos biométricos objeto de tratamiento. Desde una perspectiva garantista, se examinarán los procedimientos previos que deben acompañar a la solicitud de autorización analizando, posteriormente, el conjunto de principios que deben ponderarse en la toma de decisión que permitirá su utilización. Finalmente, el estudio concluye con una serie de conclusiones críticas dirigidas a solventar aquellas vicisitudes no resueltas por el reglamento y manifestadas en el trabajo.

Palabras clave: inteligencia artificial, identificación biométrica, datos biométricos, espacios de acceso público, remoto.

Abstract: *The use of biometric identification systems in publicly accessible spaces as a means of investigation in criminal proceedings is not without controversy due to the inherent risks involved in the implementation of these highly invasive practices, both in terms of the rights of the subjects under investigation and those of society as a whole. For this reason, this study aims to enlighten the reader on the procedures, principles and limits that must be observed by the judicial authority in accordance with the recent*

[1] Esta publicación es parte del proyecto de I+D+i "Inteligencia artificial jurídica y Estado de Derecho" [PID 2022 – 139773OB-100], financiado por MICIU/AEI/10.13039/501100011033 y por FEDER, UE.

provisions of the European Regulation on Artificial Intelligence. In order to do so, it will be necessary to develop a theoretical construction around the concept, unpacking how, where, when and for what purpose the measure can be carried out, not without first making a brief and general reflection on the sensitive nature of the biometric data that are the object of the processing. From a safeguarding perspective, the prior procedures that must accompany the application for authorisation will be examined, followed by an analysis of the set of principles that must be weighed up in the decision making process that will allow its use. Finally, the study concludes with a series of critical conclusions aimed at resolving those vicissitudes not resolved by the regulation and expressed in the work.

Keywords: *artificial intelligence, biometric identification, biometric data, public access spaces, remote.*

1. INTRODUCCIÓN

El debate sobre la utilización de sistemas de identificación biométrica en espacios públicos ha colmado la actividad parlamentaria a nivel europeo con el objetivo de mitigar los efectos negativos que su implementación puede tener en los derechos fundamentales de los ciudadanos. No obstante, y tras alcanzar un acuerdo general que prohíbe su utilización de forma masiva, el Reglamento de Inteligencia Artificial permite, de manera excepcional, su utilización para la consecución de unos objetivos previamente definidos.

Así, la búsqueda de víctimas, la prevención de ataques terroristas y la identificación del sospechoso de determinados delitos serán los ejes centrales sobre los que pivotarán el conjunto de requisitos, principios y límites que, necesariamente deben observarse para poder acordar la medida.

En base a este presupuesto, el presente estudio pretende analizar, en primer lugar, el concepto adoptado en el reglamento relativo a los sistemas de identificación biométrica remota en tiempo real en espacios de acceso público para el cumplimiento de la aplicación de la ley, no sin antes explorar someramente la relevancia de los datos biométricos en dicha identificación.

En segundo lugar, abordaremos los límites intrínsecos y generales a la utilización de estos sistemas de identificación, examinando aquellos presupuestos, como la evaluación de impacto en los derechos fundamentales y el registro del sistema en la base de datos de la Unión Europea, que deben darse necesariamente para poder solicitar la autorización del sistema de identificación en los términos descritos. Además, se pondrá de manifiesto en torno a esta cuestión, ciertos extremos que a nuestro parecer no han quedado resueltos, permitiendo llevar a cabo una interpretación subjetiva que, en función de las circunstancias, puede suponer una merma de garantías y cierta inseguridad jurídica.

Por último, el estudio finaliza con una conclusión proyectada en la responsabilidad del legislador respecto al rumbo que, en nuestra opinión, sería conveniente adoptar desde una perspectiva garantista y eficaz. No hay duda de que la identificación biométrica puede ser un instrumento sumamente eficiente en la investigación y persecución de determinados delitos. Sin embargo, su utilización debe ir precedida de una exhaustiva regulación legal que conjugue, equilibre y atempere todos los intereses en juego. Por esta razón, esta contribución pretende colmar varios de los interrogantes surgidos al albor de la propuesta de la nueva regulación europea y poner el énfasis en aquellos límites y principios que deben regir en la toma de decisión para permitir su implementación en el ámbito del proceso.

2. APROXIMACIÓN CONCEPTUAL: LA IDENTIFICACIÓN A TRAVÉS DE LOS DATOS BIOMÉTRICOS

El estudio de la identificación biométrica en espacios de acceso público implica, con carácter previo, llevar a cabo una aproximación conceptual que nos permita poner de manifiesto aquellos aspectos terminológicos más importantes que, sin duda, tendrán una repercusión determinante desde el punto de vista ético, jurídico y social.

Esta triple dimensión supone, como veremos más adelante, una obligación tanto para el legislador como para los desarrolladores de estos sistemas de identificación, de establecer un conjunto de directrices básicas de obligado cumplimiento en las que, por un lado, se minimicen los riesgos intrínsecos al desarrollo de esta tecnología y, por otro, se conjuguen los derechos individuales con los intereses públicos y generales en casos determinados y previamente establecidos pues, el devenir tecnológico en el que nos encontramos inmersos nos obligará, en términos generales, a situarnos en un nuevo escenario en el que la utilización de la tecnología marcará la hoja de ruta en relación al desarrollo normativo a nivel nacional y europeo, tal y como ya estamos presenciando.

Al respecto es interesante observar cómo la inteligencia artificial está poniendo de relieve la aparición de nuevos desafíos[2] con una clara incidencia en los derechos individuales y colectivos de las personas. Sin embargo, desde un punto de vista eficientista, global y pragmático, parece que, de forma colectiva, se ha optado por apostar por la utilización de la tecnología, en numerosos ámbitos, llevando a cabo una concesión parcial y, en ocasiones, involuntaria de datos, derechos e incluso garantías en un proceso judicial.

[2] En relación con los desafíos que plantea la inteligencia artificial puede consultarse AYLLÓN GARCÍA, Jesús Daniel, "La inteligencia artificial como un medio para administrar justicia", BUENO DE MATA, Federico y GONZÁLEZ PULIDO, Irene (dir.), *Fodertics 8: estudios sobre tecnologías disruptivas y justicia*, Comares, Madrid, 2020, pp. 3-14. Así, como el original planteamiento que realiza en otro estudio AYLLÓN GARCÍA, Jesús Daniel, "La inteligencia artificial como medio de difusión y control de las fake news", VILLEGAS DELGADO, César y MARTÍN RÍOS, Pilar (coord.), *El derecho en la encrucijada tecnológica: Estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial,* Tirant lo Blanch, Valencia, 2022, pp. 231 y ss.

Por lo tanto, no podemos afirmar que nos encontremos ante una relación simétrica en el uso de la inteligencia artificial ya que, quien dispone del algoritmo y tiene la capacidad de aplicarlo en un ámbito concreto, ejerce sobre los demás una situación de poder llegando incluso a generar situaciones de desigualdad y efectos nocivos sobre el libre ejercicio de determinados derechos fundamentales. Al respecto, compartimos el planteamiento realizado por RIDAURA MARTÍNEZ sobre el *chilling effect,* es decir, el efecto intimidatorio sobre el comportamiento humano que trae causa de un estado de sobrevigilancia mediante el empleo de técnicas de reconocimiento facial[3].

En estos términos, todo parece indicar que, a pesar de que las personas deben situarse en el centro del desarrollo tecnológico y convertirse la tecnología en una herramienta impulsora de la sociedad[4], en ocasiones nos encontramos en una situación inversa que ha generado una gran preocupación a nivel internacional en relación con el abuso de poder que puede cometerse a través de estos sistemas.

Por ello, es muy común que la utilización de determinadas tecnologías se encuentre prohibida como regla general y permitida, únicamente, en casos sumamente excepcionales como lo es la identificación biométrica que será objeto de tratamiento en este trabajo.

En el ámbito de los sistemas de identificación biométrica definidos por COTINO HUESO como "aquellos procesos automatizados utilizados para reconocer a un individuo a partir de medir, almacenar y comparar sus datos biométricos relativos a sus características físicas, fisiológicas o de comportamiento"[5], el desarrollo tecnológico ha propiciado avances significativos en la precisión y velocidad de los sistemas, permitiendo su integración en numerosos sectores como la seguridad o el acceso a servicios públicos y privados.

Indudablemente, estos avances dependen en gran medida de la recopilación y procesamiento de los datos biométricos, es decir, aquellas características únicas de cada individuo que permiten identificar a una persona a través de su huella dactilar, del iris, de la voz o incluso de sus movimientos corporales, entre otros.

En este sentido, debemos clarificar que, al hablar de los datos biométricos nos estamos refiriendo a una categoría especial de datos personales, siendo considerados tras la publicación del Reglamento Europeo de Protección de Datos, como datos

---

[3] RIDAURA MARTÍNEZ, María Josefa, "El reconocimiento facial como herramienta para garantizar la seguridad: de la incertidumbre ¿a un escenario de certeza?", CAAMAÑO, Francisco y JOVE VILLARES, Daniel (dir.), *Tecnologías abusivas y derecho,* Tirant lo Blanch, Valencia, 2024, p.154.

[4] SÁNCHEZ MARTÍNEZ, María Olga, "El impacto de la sociedad digital en los derechos humanos", SOLAR CAYÓN, José Ignacio y SÁNCHEZ MARTÍNEZ, María Olga. (coord.), *El impacto de la inteligencia artificial en la teoría y práctica jurídica,* La Ley, Madrid, 2022, p. 120.

[5] COTINO HUESO, Lorenzo, "Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos", BALAGUER CALLEJÓN, Francisco y COTINO HUESO, Lorenzo (coord.) *Derecho público de la inteligencia artificial*, Fundación Manuel Giménez Abad, Zaragoza, 2023, pp. 352 y 353.

sensibles[6]. Al respecto, consideramos oportuna esta clasificación ya que los datos biométricos suponen la identificación directa e inequívoca de la persona debido al carácter personalísimo e inmutable de los mismos.

Por lo tanto, nos encontramos ante datos que poseen unas características extremadamente sensibles y únicas implicando un mayor riesgo en caso de un uso indebido o una cesión no autorizada. En consecuencia, ante las graves injerencias que pueden producirse tanto en los derechos fundamentales como en la privacidad de los individuos se exige que estos datos estén sujetos a mayores restricciones en cuanto a su tratamiento y a mayores medidas de protección en aras a evitar un uso indebido de los mismos.

Al respecto, TOMÁS MALLÉN sostiene de forma acertada que los datos biométricos adquirirán tal condición "cuando se usen específicamente para identificar de manera única a la persona en cuestión"[7]. De esta forma, cuando el tratamiento de imágenes tenga como finalidad revelar información sensible de una persona, se considerará tratamiento de datos confidenciales mientras que, por el contrario, el realizado por un sistema de videovigilancia por motivos de seguridad, no tendrá tal consideración[8]. Por ello, siguiendo el argumento expuesto por la citada autora, podemos sostener que en función de la finalidad para la cual se realice el tratamiento, los datos objeto del mismo, deberán tener una u otra condición.

La utilización de los datos biométricos nos invita, desde una perspectiva conceptual, a realizar una distinción entre la identificación, la verificación y la categorización biométrica[9] pues, como tendrá ocasión de observar el lector, este trabajo de investigación se centrará, principalmente, en la identificación biométrica llevada a cabo en los espacios públicos.

Dicha identificación biométrica implica el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los de otras personas que se encuentran almacenados en una base de datos. En este supuesto, la persona no lleva a cabo una cesión previa de sus datos, como si ocurrirá en el caso de la verificación pues, el objetivo principal de la identificación consiste en determinar quién es una persona a través de la coincidencia existente entre los datos recogidos y los almacenados en la base de datos, sin que sea necesario que el sujeto sobre el cual esté recayendo la identificación realice ninguna acción o aportación adicional.

---

[6] BARONA VILAR, Silvia, "Tecnología biométrica y datos biométricos. Bondades y peligros. No todo vale", *Actualidad Jurídica Iberoamericana,* núm. 21, 2024, p. 319.

[7] TOMÁS MALLÉN, Beatriz, "Las sinergias entre el Reglamento General de Protección de Datos de la Unión Europea y el Convenio 108+ del Consejo de Europa", GARCÍA MAHAMUT, Rosario y TOMÁS MALLÉN, Beatriz (Eds.), *El Reglamento General del Protección de Datos. Un enfoque nacional y comparado,* Tirant lo Blanch, Valencia, 2019, p. 74.

[8] Ibidem.

[9] Esta cuestión es desarrollada conceptualmente en los considerandos 15 y 16 del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024, sobre Inteligencia Artificial.

Por su parte, la verificación biométrica consiste en el cotejo automatizado, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con aquellos que han sido facilitados con carácter previo. En este caso, el objetivo de la verificación es contrastar que una persona es quien dice ser y, por lo tanto, el proceso es diferente de la identificación porque, en este supuesto, la persona ha facilitado de forma voluntaria sus datos biométricos siendo consciente de que su cesión va a ser empleada para el fin que es conocido y aceptado por el usuario.

Finalmente, la categorización biométrica es una funcionalidad de los sistemas de IA ciertamente controvertido ya que se encuentra destinado a incluir a las personas físicas en categorías específicas en función de sus datos biométricos. En este caso, la categorización biométrica está resultando sumamente perjudicial para aquellos colectivos o personas más vulnerables o, incluso, históricamente infrarrepresentadas ya que la categorización se lleva a cabo a través de sistemas inteligentes cuyos algoritmos vienen precedidos por una serie de sesgos que, a menudo, perpetúan problemas de discriminación en numerosos ámbitos[10].

2.1. La identificación biométrica en el nuevo Reglamento de Inteligencia Artificial

El 12 de julio de 2024 se publicó en el Diario Oficial de la Unión Europea (DOUE) el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen las normas armonizadas en materia de inteligencia artificial, dando paso, así, al comúnmente conocido Reglamento de inteligencia artificial, en adelante RIA.

Sin ánimo de ser exhaustivos respecto a los antecedentes relativos a elaboración del presente reglamento[11], lo cierto es que todos los esfuerzos se dirigieron de forma unánime a establecer unas reglas básicas que permitieran la aplicación de la inteligencia artificial en la Unión Europea sin que ello implicase la eventual quiebra de los derechos fundamentales de los ciudadanos europeos.

A diferencia de otros ordenamientos jurídicos que, de forma consciente, han invertido la balanza hacia la plena aplicación de la inteligencia artificial sin tener en cuenta el coste, en materia de derechos y libertades, que esto puede suponer para la sociedad en su conjunto, la Unión Europea, a través del citado Reglamento ha priorizado los derechos fundamentales frente a la utilización indiscriminada de tecnología ciertamente invasiva en determinados ámbitos sociales, laborales o jurídicos[12].

---

[10] Sobre esta cuestión resulta sumamente interesante el documental "Sesgo Codificado" disponible en la plataforma Netflix en el que la Doctora Joy Buolamwini pone de relieve los riesgos de la Inteligencia Artificial, especialmente en el ámbito de la identificación biométrica.

[11] Sobre el proceso de elaboración del Reglamento de Inteligencia Artificial puede consultarse BARRIO ANDRÉS, Moisés, "Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia Artificial", BARRIO ANDRÉS, Moisés (Dir.) *El Reglamento Europeo de Inteligencia Artificial,* Tirant lo Blanch, Valencia, 2024, pp. 27 y ss.

[12] Como muestra de ello, el considerando número 31 alude, de forma explícita, a los riesgos que pueden generarse a través de la utilización del puntaje social; práctica prohibida en

Por esta razón, el RIA ha profundizado en la producción del riesgo que implica la inteligencia artificial en diversas prácticas estableciendo una enumeración de aquellas que, siendo catalogadas como prohibidas o de alto riesgo, supondrán una grave amenaza para la seguridad y la promoción y salvaguarda de nuestros derechos.

Sin embargo, hay que tener en cuenta que, a pesar de que la entrada en vigor del RIA se llevó a cabo a los 20 días de su publicación en el DOUE y se contempla que sea aplicable a partir del 2 de agosto de 2026, determinados capítulos del mismo se encuentran sujetos a un llamativo calendario previsto en su artículo 113. Así, la aplicación del citado reglamento se producirá de la siguiente forma:

1) los capítulos I y II serán aplicables a partir del 2 de febrero de 2025;
2) el capítulo III, sección 4, el capítulo V, el capítulo VII y el capítulo XII y el artículo 78 serán aplicables a partir del 2 de agosto de 2025, a excepción del artículo 101;
3) el artículo 6, apartado 1, y las obligaciones correspondientes del presente Reglamento serán aplicables a partir del 2 de agosto de 2027.

La elaboración de una normativa común en la Unión Europea, a través de un reglamento de aplicación directa a los estados miembros supone, en opinión de quien suscribe, un importante hito a nivel internacional por diversas razones:

a) En primer lugar, nos encontramos ante una armonización normativa sumamente garantista relativa a una temática compleja y no exenta de controversia debido, por un lado, al conjunto de intereses divergentes que existen en relación con su aplicación y efectos sobre el conjunto de la sociedad y, por otro, al desarrollo tecnológico y evolución constante que caracteriza el fenómeno de la inteligencia artificial.

   Al hilo de lo indicado, el RIA aporta, una visión actualizada del uso de la inteligencia artificial en el momento de su entrada en vigor. No obstante, y con el firme propósito de lograr una normativa actualizada en virtud de la dinámica tecnológica estará sujeto, a una revisión anual que, entre otros extremos, permita actualizar el listado de prácticas prohibidas contenidas en el artículo 5 del reglamento. A ello debe añadirse, a su vez, una serie de revisiones que se realizarán cada tres o cuatro años, respectivamente, y que favorecerán una actualización permanente y necesaria en relación con una temática dinámica y en constante cambio.

b) En segundo lugar, nos encontramos ante una regulación que, de forma consensuada y debatida, ha logrado, desde una perspectiva conceptual, unificar terminológicamente los diversos conceptos relacionados con la inteligencia artificial, ofreciendo un acervo de definiciones que son la

Europa, pero utilizada a diario en otros países. Al respecto indica que llevar a cabo una puntuación ciudadana de las personas físicas "puede tener resultados discriminatorios y abocar a la exclusión a determinados colectivos. Puede menoscabar el derecho a la dignidad y a la no discriminación y los valores de igualdad y justicia".

base fundamental para albergar, con posterioridad, el conjunto de normas y previsiones en relación con la materia.

Este aspecto, de suma importancia desde el punto de vista teórico, ha sido óbice de numerosos debates conceptuales que conjugaban distintas posiciones doctrinales en relación con la terminología con la que debía referirse a determinados conceptos. Por ello, no es de extrañar, que algunos autores aludieran a la amplitud de los conceptos como una garantía adicional que evitara la propia obsolescencia del término[13].

Como indicó ETXEBERRIA GURIDI la unificación de los conceptos tiene una importancia singular en el ámbito europeo "donde conviven ordenamientos jurídicos diversos y con particularidades propias significativas"[14]. Por esta razón, el establecimiento de elementos conceptuales comunes aporta en el conjunto de los países miembros una mayor seguridad jurídica al encontrarnos ante un conjunto armonizado de normas que conjugan tanto los objetivos comunes como las particularidades propias de cada estado.

c) Finalmente, y con independencia de las someras menciones que hemos realizado con anterioridad respecto al impacto que puede tener en nuestros derechos fundamentales la aplicación de la inteligencia artificial, debemos poner en valor el enfoque garantista que se observa de forma constante a lo largo de todo el reglamento al establecer un marco normativo que garantice un uso proporcionado y respetuoso con los derechos fundamentales. Situar a las personas en el centro del desarrollo tecnológico y, no al revés, ha sido uno de los pilares esenciales que han guiado la elaboración del conjunto de directrices contenidas en la norma. No obstante, y a pesar del espíritu plausible plasmado en el RIA, debemos ser conscientes del carácter no absoluto de los derechos fundamentales que nos asisten y, en consecuencia, de la flexibilización a la que, irremediablemente, estaremos sujetos en aquellas circunstancias que, con carácter extraordinario, se encuentran recogidas en el texto a analizar.

   Esto no implica, de modo alguno, una cesión permanente o una renuncia implícita en determinadas circunstancias, sino que, como veremos a continuación, partiendo de una prohibición general se prevé la utilización de la inteligencia artificial para casos concretos y determinados, aunque ello conlleve una flexibilización puntual de un derecho concreto en aras a resolver una cuestión de interés público.

En este sentido, el objeto de este estudio basado en el uso de sistemas de identificación biométrica en tiempo real en espacios de acceso público, parte de una pre-

---

[13] SAN MIGUEL CASO, Cristina, "La aplicación de la Inteligencia Artificial en el proceso: ¿un nuevo reto para las garantías procesales?", *Revista Ius et Scientia: Revista electrónica de Derecho y Ciencia,* vol. 7, núm. 1, 2021, p. 288.

[14] ETXEBERRÍA GURIDI, José Francisco, "El uso de sistemas de inteligencia artificial (IA) de identificación biométrica remota en espacios públicos en la ley europea de IA", *Actualidad Jurídica Iberoamericana,* núm. 21, 2024, p. 536.

misa general que consiste en la prohibición de esta práctica al encontrarse contemplada en la enumeración del artículo 5 del reglamento. Su ubicación trae causa de los riesgos que genera el uso de la biometría en la práctica y los efectos nocivos que ello puede tener en la sociedad en su conjunto[15]. De esta forma, el considerando número 54 alude a las imprecisiones técnicas de estos sistemas como aquellos que *pueden dar lugar a resultados sesgados y tener efectos discriminatorios. El riesgo de dichos resultados sesgados y efectos discriminatorios es especialmente pertinente por lo que respecta a la edad, la etnia, la raza, el sexo o la discapacidad. Por lo tanto, los sistemas de identificación biométrica remota deben clasificarse como de alto riesgo debido a los riesgos que entrañan*.

No obstante, esta medida podrá implementarse en determinados casos cuando su utilización sea estrictamente necesaria para lograr los siguientes objetivos:

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 penal 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.

Estas excepciones, cuyo examen se realizará con detalle en epígrafes posteriores, estarán sujetas a una serie de requisitos de obligado cumplimiento que dotarán a estas de las garantías óptimas requeridas para llevarlas a cabo en un marco jurídico sumamente garantista para todos los afectados.

Sin embargo, antes de abordar esta cuestión, es fundamental explicar de manera previa cómo se puede realizar la identificación biométrica a través de sistemas de inteligencia artificial. Por ello, en las próximas líneas, analizaremos cómo, cuándo, dónde, y para qué de la práctica de esta medida en el nuevo marco normativo establecido por el reglamento de inteligencia artificial.

2.1.1. Cómo: de forma remota

El reglamento de inteligencia artificial define en su artículo 3 apartado 41 al sistema de identificación biométrica remota como aquel "sistema de IA destinado a identificar a las personas físicas sin su participación activa y generalmente a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia". De esta definición, podemos extraer tres notas características:

[15] Aspecto puesto de manifiesto por COTINO HUESO, Lorenzo, "Reconocimiento facial automatizado…" cit., p. 359.

En primer lugar, el adjetivo *remota* nos indica el modo o la forma en que se llevará a cabo la identificación, implicando esto la ausencia de inmediatez física entre el sujeto que pretende ser identificado y el medio empleado para su identificación. En consecuencia, la identificación de personas físicas se realizará a distancia generando esta circunstancia una doble limitación tanto de los datos que se obtengan como de la técnica que se utilice.

Al respecto, no debemos olvidar que la biometría es una disciplina caracterizada por el empleo de una amplia tipología de técnicas biométricas[16] como pueden ser las huellas dactilares, el reconocimiento del iris o la geometría del árbol de venas del dedo, entre otras. Sin embargo, al practicarse a distancia todo parece indicar que determinadas técnicas biométricas quedan excluidas, de forma directa, ya que su empleo implicaría necesariamente una presencialidad física respecto del sujeto objeto de identificación.

De igual modo, la obtención de datos biométricos a distancia restringe notablemente el tipo de datos que pueden ser objeto de tratamiento pues, frecuentemente, la adquisición de estos depende tanto de su presencialidad como de la participación del sujeto en cuestión.

No obstante, acudiendo al tenor literal del citado reglamento la obtención remota se caracterizará, a su vez, por la no participación activa de la persona objeto de identificación y, por lo tanto, esto implicará un sometimiento no voluntario y, en ocasiones, inconsciente a participar en la identificación a través de un sistema inteligente.

Si conjugamos ambas características de forma simultánea, es decir, tanto la ausencia de participación activa, como la distancia requerida, podemos intuir que el texto objeto de estudio se refiere, indirectamente, al reconocimiento facial[17] pues su práctica permite llevarse a cabo a distancia y, tampoco se necesitaría la participación activa del individuo para poder realizar el cotejo de los datos requeridos para la identificación al consistir, únicamente, en el análisis de los rasgos faciales del individuo a través del tratamiento automatizado de las imágenes que han sido captadas previamente[18].

2.1.2. Cuándo: en tiempo real

La identificación biométrica llevada a cabo de forma remota permite, a su vez, que la recogida de los datos, la comparación y la identificación se produzca en tiempo real, de forma casi instantánea, sin que ello produzca retrasos importantes.

Esto implica que los medios utilizados para lograr la realización de la identificación se empleen en directo o, en su caso, haya transcurrido un tiempo mínimo entre la captación de la imagen y el cotejo de los datos obtenidos.

---

[16] Más extensamente sobre la tipología de las técnicas biométricas puede consultarse BARONA VILAR, Silvia, "Tecnología biométrica…", cit., p. 319.

[17] Aspecto indicado por ETXEBERRÍA GURIDI, José Francisco, "El uso de sistemas de inteligencia artificial…", cit., p. 544.

[18] FREIRE MONTERO, Antón Fructuoso, "El reconocimiento facial como instrumento de investigación y prevención del delito", *Anuario da Facultade de Dereito da Universidade da Coruña*, Vol. 26, 2022, pp. 70 y ss.

En caso contrario, es decir, cuando concurra un periodo de tiempo significativo entre ambas acciones –la obtención de los datos biométricos y la comparación con la base de datos– nos encontraremos ante sistemas en diferido que, en el propio reglamento, son definidos en el artículo 3 apartado 43 como aquellos sistemas de identificación biométrica remota que no se producen en tiempo real[19].

En relación con esta cuestión, la diferencia entre la identificación que se produce en tiempo real y aquella que se realice en diferido es sumamente relevante, pues la primera de ellas se recoge en el RIA como una práctica prohibida mientras que la segunda se concibe en una sistematización distinta como una práctica de alto riesgo sometida a los controles y requisitos comunes para todas aquellas prácticas que tengan la misma entidad.

Sin embargo, como se ha puesto de manifiesto anteriormente, la diferencia entre ambas radica en el momento en el que se produce la comprobación o el cotejo tras la obtención de los datos biométricos. Y ello, puede generar ciertas vicisitudes en relación con la propia terminología utilizada en la redacción de ambos conceptos pues, a pesar de que la identificación en diferido implica, por exclusión, la asunción de todo lo que no es en directo, al definir este último término el reglamento utiliza una concepción ambigua al aludir "a la identificación que se produce sin una demora significativa" o en todo caso a la "demora mínima limitada".

En estos términos, podríamos entender que la demora a la que alude el artículo 3.42 sería equivalente a un lapso de tiempo mínimo e insignificante que pueda provenir del propio proceso de autorización que, salvo razones de urgencia, precisa la medida o, incluso, desde una perspectiva más restrictiva, podríamos llegar a considerar que aquella que se practica en tiempo real es, únicamente, aquella que tiene lugar por razones de urgencia. No obstante, esta interpretación estaría sujeta a ciertas matizaciones debido a la imprecisión que, en torno a esta cuestión, se desprende del tenor literal de la norma.

Por esta razón, consideramos oportuno y conveniente que, en las futuras actualizaciones del reglamento en cuestión se realice una matización severa sobre este extremo en aras a solventar las posibles incertidumbres que pueda generar esta imprecisión en los agentes implicados tanto en la adopción de la medida como en aquellos encargados de su ejecución.

2.1.3. Dónde: en un espacio de acceso público

La prohibición general relativa a la implementación de sistemas de inteligencia artificial de identificación biométrica trae causa de la multitud de riesgos que su utilización podría entrañar cuando aquella tenga lugar en espacios de acceso público.

[19] RAMÓN FERNÁNDEZ, Francisca, "La aplicación de la inteligencia artificial y su desarrollo en el ámbito de la videovigilancia y los drones", RAMÓN FERNÁNDEZ, Francisca (coord.), *Ciencia de datos y perspectiva de la inteligencia artificial,* Tirant lo Blanch, Valencia, 2024, p. 224.

Concretamente, el considerando número 32 hace alusión a la afectación a la vida privada de la colectividad y, en consecuencia, a la sensación de encontrarse en estado de vigilancia constante que disuada a los ciudadanos de ejercer su libertad de reunión, así como de otros derechos fundamentales que les son propios.

Sin duda, el lugar en el que la medida puede llevarse a cabo es uno de los extremos más importantes pues, atendiendo a las excepciones que permiten la utilización de la identificación biométrica esta debe llevarse a cabo en los denominados espacios de acceso público.

Siguiendo el tenor literal del RIA dichos espacios han sido definidos en el artículo 3.44 como "cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas físicas, con independencia de que deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad".

Como puede observarse, nos encontramos ante una interpretación extensiva del concepto más aún si acudimos al considerando 19 en donde la aproximación conceptual de lo que puede entenderse por espacio de acceso público adquiere un desarrollo mayor permitiéndonos, así, extraer unas notas esenciales en torno al mismo:

En primer lugar, la amplia conceptualización del término recae, indubitadamente, sobre la propiedad pública o privada del espacio pues, dicha naturaleza, resulta irrelevante si al mismo puede acceder un número indeterminado de personas. Ello invita a reflexionar sobre el propio concepto adoptado en el reglamento pues, como podrá observar el lector, no se hace alusión a los lugares públicos sino a aquellos espacios de acceso público con los matices que ello implica en la acepción terminológica del mismo.

Así, la diferencia principal existente entre ambos términos es que el lugar público hace alusión a un espacio de titularidad pública mientras que, por el contrario, el espacio de acceso público engloba cualquier lugar al que el público pueda acceder con independencia de la titularidad pública o privada que ostente el mismo. En consecuencia, este pequeño matiz implica un mayor margen de actuación en relación con el lugar en el que puede llevarse a cabo la medida, lo que supondrá, por un lado, una mayor efectividad de la misma y, por otro, una afectación generalizada a los derechos fundamentales de los ciudadanos.

En segundo lugar, no debemos obviar que, en la práctica, podemos encontrarnos con espacios que adquieran, de forma simultánea, una naturaleza tanto pública como privada, incluyendo zonas de acceso público y espacios que no ostentan esta categoría. Para estos casos y otros tantos que puedan resultar controvertidos el RIA incluye una previsión final en la que apuesta por determinar caso por caso, de forma singular, si un espacio es de acceso público o no, teniendo en cuenta las particularidades de la situación concreta.

Finalmente, y con ánimo aclaratorio, encontramos en el considerando 19 una previsión en la que se enuncian en sentido negativo que lugares no pueden ser considerados espacios de acceso público. Concretamente, los locales de las empresas y fábricas, así como las oficinas y lugares de trabajo a los que solo se pretende que

accedan los empleados y proveedores de servicios y, las prisiones ni las zonas en las que se realizan inspecciones transfronterizas.

2.1.4. Para qué: para el cumplimiento de la aplicación de la ley

La utilización de la identificación biométrica en espacios de acceso público como instrumento en la investigación de un proceso penal es la excepción a la regla general de prohibición que, en base a los riesgos que su uso podría entrañar tanto a nivel colectivo como individual, desaconseja a todas luces su viabilidad en una sociedad democrática.

No obstante, en determinados supuestos, el RIA permite la utilización de estos sistemas siempre y cuando su utilización se conciba como una *garantía en cumplimiento del derecho*. Este concepto ha sido definido en el artículo 3.46 como aquellas actividades realizadas por las autoridades garantes del cumplimiento del Derecho, o en su nombre, para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de las mismas.

En el escenario descrito, debemos conectar dicha definición con los delitos concretos para los cuales, está previsto el empleo de esta tecnología ya que, sin la enumeración de estos, nos encontraríamos ante el uso invasivo de medidas de investigación o represión penal que no cumplirían el estándar necesario de la especialización. Sobre esta cuestión, se pronunció de forma acertada, RODRÍGUEZ DEL BLANCO al aludir no sólo al riesgo que ello comportaría respecto a las investigaciones prospectivas que, en forma alguna, pueden tener lugar en nuestro ordenamiento jurídico, sino también al principio de especialidad en el que, a través de la idoneidad, estos sistemas sean implementados cuando otras medidas menos invasivas no hayan arrojado unos resultados óptimos en torno a la investigación[20].

De esta forma, la investigación llevada a cabo a través de la identificación biométrica se encuentra sujeta a una serie de previsiones y garantías cuya repercusión o incidencia en los derechos fundamentales de las partes y de los terceros sometidos de forma indirecta a dicha identificación debe ser absolutamente proporcional en relación con el objeto de la investigación y la idoneidad y necesidad de la medida.

La balanza entre la protección de los derechos individuales y los sistemas de identificación biométrica ha logrado hallar su punto justo de equilibrio a través de la taxatividad de los supuestos en los que su utilización se concibe, además, con carácter supletorio respecto de otras medidas de investigación que siendo menos invasivas pueden albergar unos resultados altamente satisfactorios respecto del objeto del proceso. Así, podemos afirmar que la excepcionalidad y la subsidiariedad en la utilización de estos sistemas han sido los ejes claves sobre los que ha pivotado la regulación en torno a los mismos.

[20] RODRÍGUEZ DEL BLANCO, Alfredo, "Detectando los riesgos de la inteligencia artificial en la instrucción penal", *Revista General de Derecho Procesal,* núm. 64, 2024, pp. 26 y 27.

3. SUPUESTOS DE APLICACIÓN

Amén de los riesgos que entraña la utilización de los sistemas de identificación biométrica, su implementación como medida de investigación en un proceso penal se permite en determinados supuestos y bajo el cumplimiento estricto de una serie de requisitos que analizaremos posteriormente.

No obstante, y como ya se adelantó en el epígrafe anterior, su uso debe concebirse, atendiendo a los riesgos que entraña, como una medida supletoria cuando el empleo de otras diligencias de investigación no resulten idóneas o, aun siéndolo, el resultado obtenido no satisfaga los fines de la investigación.

Esta premisa se deduce de los extremos que, invocados por el RIA, deben ser observados a la hora de evaluar la práctica de la medida pues, adoptando un enfoque de carácter preventivo, el análisis valorativo del riesgo que implicarían estos sistemas pivotaría sobre tres elementos clave: la gravedad, la probabilidad y la magnitud. No obstante, estos criterios se evaluarían por partida doble; en primer lugar, respecto de la naturaleza de la situación y, en segundo lugar, en relación con los derechos fundamentales de las personas implicadas.

Como se puede observar, se trata de llevar a cabo una utilización responsable de estos sistemas, evitándoles cuando puedan generar, de forma innecesaria, mayor perjuicio que beneficio sobre los derechos fundamentales[21] o la seguridad de los ciudadanos.

Atendiendo al doble control que se desprende de la normativa europea, la naturaleza de la situación se encuentra íntimamente relacionada con aquellos supuestos de aplicación en los que, de forma explícita, el RIA permite su utilización en el ámbito de la investigación en aras a la consecución de los siguientes objetivos:

En primer lugar, para 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.

En segundo lugar, para la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista.

En tercer y último lugar, para la localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penal 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

[21] Sobre esta cuestión, resulta ilustrativa la expresión realizada por GÓMEZ COLOMER, Juan Luis, "Los actos de investigación garantizados basados en las nuevas tecnologías", GÓMEZ COLOMER, Juan Luis, y BARONA VILAR, Silvia (coord.), *Proceso Penal. Derecho Procesal III,* 4ª edición, Valencia, 2024, p. 249, al señalar que "No debemos exagerar, pero tampoco dejar de estar atentos, pues el garantismo procesal en España ha alcanzado una cota una vez restablecida la democracia, tras décadas de ausencia, que vale la pena mantener en favor del juicio «justo» o con todas las garantías, siendo admisibles matices en donde ese nivel presente fisuras, justificadas bajo estrictos requisitos, que puedan afectar a derechos de la ciudadanía honesta".

pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

En relación con lo indicado, el citado reglamento no opta por realizar una enumeración taxativa de delitos, sino que apuesta por enunciar los objetivos cuya consecución se hará depender, en mayor o menor medida, del empleo de sistemas de identificación biométrica y no del manejo de otro tipo de medidas pues, indudablemente, el reconocimiento facial[22] será determinante para la localización e identificación de los sospechosos y de las víctimas.

Sin embargo, su afectación a derechos tales como la intimidad, la libertad, la no discriminación y la igualdad son algunos de los que, indudablemente, se pueden ver comprometidos cuando la utilización de esta medida se emplea en el escenario procesal. A ello debe añadirse, además, la dudable fiabilidad[23] que, en la actualidad, presentan los sistemas de identificación biométrica por lo que, además de una afectación a derechos fundamentales también nos podremos encontrar con una pérdida de garantías procesales que afecten a nuestro derecho a la tutela judicial efectiva[24].

Este último aspecto resulta esencial para poner de manifiesto la excepcionalidad en el empleo diligente de esta medida, así como asegurar el firme cumplimiento de una serie de principios y límites que deben observarse tanto en la adopción de la misma como en su empleo posterior con el propósito de que esta, se lleve a cabo en unas condiciones óptimas y garantistas.

4. ASPECTOS ESENCIALES PARA LA ADOPCIÓN DE LA MEDIDA

El empleo de los sistemas de identificación biométrica durante la fase de instrucción debe someterse a un riguroso análisis desde la perspectiva de los derechos fundamentales[25] y las garantías procesales.

En este contexto, la observancia de una serie de principios y límites resulta primordial no solo por los riesgos inherentes que conlleva su utilización, sino también

---

[22] Un estudio sobre la cuestión puede consultarse en IGLESIAS CANLE, Inés Celia, "Reconocimiento facial y proceso penal", CASTILLEJO MANZANARES, Raquel y NOYA FERREIRO, Lourdes (coord.) *Inteligencia artificial y proceso penal: un reto para la justicia,* Aranzadi, Cizur Menor, 2023, pp. 190 y ss.

[23] Los errores en la fiabilidad de los sistemas de reconocimiento facial han sido puestos de manifiesto por BARONA VILAR, Silvia, *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice,* Tirant lo Blanch, Valencia, 2021, p. 494; BORGES BLÁZQUEZ, Raquel, *Inteligencia artificial y proceso penal,* Aranzadi, Cizur Menor, 2021, p. 60.

[24] Sobre la cuestión SAN MIGUEL CASO, Cristina, "Inteligencia artificial y algoritmos: La controvertida evolución de la tutela judicial efectiva en el proceso penal" en *Estudios Penales y Criminológicos,* núm. extra-44, 2023, pp. 10 y ss.

[25] GÓMEZ COLOMER, Juan Luis "Derechos fundamentales, proceso e inteligencia artificial: una reflexión", CALAZA LÓPEZ, Sonia y LLORENTE SÁNCHEZ-ARJONA, Mercedes (dir.), *Inteligencia Artificial legal y administración de justicia,* Aranzadi, Cizur Menor, 2022, pp. 264 y ss.

por la seguridad jurídica que otorga a las partes el cumplimiento de unos estándares previamente definidos a nivel europeo[26].

El equilibrio entre la efectividad de la investigación y la protección de los derechos fundamentales debe ser el elemento clave sobre el que pivoten todas las previsiones que, en torno a esta materia, establecen la existencia de unos criterios proteccionistas. En este sentido, la utilización de los sistemas inteligentes no puede llevarse a cabo sin un marco normativo que limite su aplicación y evite posibles excesos o abusos por parte de las autoridades. Estos límites son esenciales para evitar que el afán de modernización y eficiencia en la investigación derive en prácticas que puedan comprometer los derechos fundamentales de las partes.

En aras a la consecución de estos objetivos, analizaremos los procedimientos previos que, en atención al RIA deben llevarse a cabo, examinando su oportunidad y pertinencia. A su vez, se pondrán de manifiesto algunas propuestas en relación con ciertas cuestiones no resueltas por el reglamento que, a juicio de quien escribe, deben clarificarse para aportar mayor fiabilidad al procedimiento.

4.1. La evaluación de impacto de los derechos fundamentales y el registro en la base de datos: aspectos críticos en caso de urgencia

La utilización excepcional de los sistemas de identificación biométrica requiere, como no podía ser de otra forma, de una autorización previa que se encuentra supeditada a la concurrencia simultánea de dos acciones cuyo ejercicio recaerá sobre la autoridad garante del cumplimiento del Derecho, entendiendo por ésta, aquella autoridad pública competente para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de las mismas[27], es decir, aquella autoridad competente en la represión e investigación de los delitos.

El primero de los requisitos, consiste en llevar a cabo una evaluación sobre el impacto que puede ocasionar la identificación biométrica en los derechos fundamentales, tal y como se contempla en el artículo 27 del RIA. Al respecto, esta evaluación se conceptúa como una obligación ceñida al supuesto concreto cuando sea la primera vez que se utiliza el sistema de alto riesgo, ya que en situaciones posteriores que tengan cierta similitud, no será necesario llevar a cabo evaluaciones originales para cado caso concreto, pero sí, mantener las anteriores actualizadas.

La evaluación de impacto consistirá en completar un formulario, a través de un sistema automatizado, en el que se deberán hacer constar una serie de aspectos que se pueden agrupar, en nuestra opinión, en tres grandes bloques:

---

[26] Al respecto DE HOYOS SANCHO, Montserrat, "El Proyecto de Reglamento de la Unión Europea sobre inteligencia artificial, los sistemas de alto riesgo y la creación de un ecosistema de confianza", BARONA VILAR, Silvia (coord.) *Justicia Poliédrica en periodo de mudanza,* Tirant lo Blanch, Valencia, 2022, pp. 414 y ss.

[27] Esta definición viene recogida en el artículo 3.45 del Reglamento de Inteligencia Artificial.

1) Descripción del sistema de Alto Riesgo**:** En la evaluación deberá llevarse a cabo una descripción de aquellos elementos que conformarán la puesta en marcha de la medida, así como el periodo de tiempo y la frecuencia de su utilización y el despliegue de la misma en relación con el objetivo que debe cumplir.
2) Identificación de los riesgos y de los afectados: Una vez se ha llevado a cabo la descripción del sistema de alto riesgo, procede, a continuación, identificar a las personas o colectivos que pueden verse afectados por la medida, así como, los riesgos específicos que se pueden derivar de su utilización para los mismos.
3) Medidas de supervisión y actuación frente a riesgos: Finalmente, se deberá prever qué medidas de supervisión humana se realizarán durante el empleo del sistema de alto riesgo, así como enumerar aquellas acciones que deben adoptarse en caso de que dichos riesgos se materialicen, incluidos los acuerdos de gobernanza interna y los mecanismos de reclamación.

El segundo de los requisitos se basa en el registro, previo a su utilización, del sistema de inteligencia artificial en la base de datos de la Unión Europea. Para ello, será necesario, siguiendo lo indicado en el anexo VIII del RIA, aportar una serie de datos que podemos condensar en los siguientes aspectos:

1) Identificación del proveedor y datos de contacto: Será necesario proporcionar el nombre, dirección y datos de contacto del proveedor del sistema de IA, así como de cualquier persona que actúe en su nombre y, si corresponde, del representante autorizado. También se deben incluir detalles que permitan la identificación y trazabilidad del sistema de IA, como su nombre comercial y cualquier referencia adicional específica.
2) Descripción del sistema de IA: Posteriormente, se deberá describir la finalidad prevista del sistema de IA y las funciones que desempeña, así como una explicación concisa de la lógica de funcionamiento y los datos que utiliza. Además, debe especificarse la situación actual del sistema, indicando si está comercializado, en servicio, retirado, o ha dejado de comercializarse. Por último, se deberá aportar la información sobre el tipo, número y caducidad de los certificados de conformidad, además de una copia del certificado y la declaración UE de conformidad, cuando sea aplicable.
3) Detalles adicionales y requisitos específicos: El anexo del Reglamento requiere la inclusión de una lista de los Estados miembros donde el sistema se ha comercializado en la Unión Europea, debiendo proporcionar una serie de instrucciones de uso en formato electrónico, a menos que se trate de sistemas en áreas sensibles como el cumplimiento de la ley, migración, asilo y control fronterizo, por lo que, este último requisito no sería de aplicación en el ámbito de los sistemas de identificación biométrica.

Así, tanto la evaluación de impacto relativa a los Derechos Fundamentales como el registro previo en la base de datos de la Unión Europea serán los dos requisitos *sine qua non* para la obtención de la autorización.

No obstante, en casos de urgencia el RIA permite la utilización de los sistemas de identificación biométrica sin el oportuno registro en la base de datos, siempre y cuando el registro se complete con posterioridad sin demora indebida.

En torno a esta cuestión debemos realizar una somera crítica a esta previsión pues resulta un tanto ambigua y, aporta, en nuestra opinión, una incerteza jurídica impropia tanto del espíritu del reglamento como del objeto de estudio en cuestión. Al respecto, esta previsión deja abierta la posibilidad a la utilización de sistemas de identificación sin que estos se encuentren registrados y, en consecuencia, se sometan previamente a un escrutinio pertinente y útil a nivel europeo. Resulta evidente, que esta circunstancia únicamente se permitiría en situaciones de urgencia debidamente justificadas, sin embargo, no se establece en ningún momento qué puede entenderse por tal o cuándo se podría producir dicha urgencia, desde un punto de vista práctico u operativo, lo que consideramos absolutamente necesario con el objetivo de evitar un posible abuso de las situaciones de urgencia que conviertan la excepción en la regla general.

A ello debe añadirse, también, la ausencia de concreción respecto del tiempo que debe transcurrir desde que comienza su uso hasta que se procede a su registro pues, únicamente se alude a que debe realizarse sin demora lo que invita a realizar una interpretación subjetiva del concepto que, en función de las circunstancias, puede abarcar un periodo de tiempo lo suficientemente amplio en el que incluso se haya dado por finalizada la utilización de la identificación, más aún, si nos encontramos ante casos de urgencia. Por ello, consideramos conveniente una actualización de este aspecto en el que se concrete el periodo de tiempo máximo que debe transcurrir entre la utilización y el registro con el propósito de aportar un plus de garantismo respecto a esta cuestión.

Una posible solución, cuya práctica podría resolver el óbice no resuelto en el reglamento, sería que la autorización indicara la necesidad de completar el registro en un tiempo concreto y determinado, supeditando el mismo a la validez de la autorización, de forma que, si en el plazo indicado por la autoridad judicial no se ha procedido al registro del sistema, la autorización decayera en base al incumplimiento formal de la condición.

Esta propuesta, quizás pueda resultar ciertamente controvertida en relación con el devenir de la información y los resultados obtenidos, los cuales, deberían ser suprimidos y desechados automáticamente al igual que sucedería en el caso de que la medida se practique, en casos de urgencia, sin la debida autorización judicial, si en el plazo máximo de 24 horas desde el comienzo de la utilización no se lleva a cabo la oportuna solicitud.

Por otra parte, no hay ninguna previsión, para los casos de urgencia, respecto de la evaluación de impacto de los Derechos Fundamentales, por lo que debemos con-

siderar que este requisito debe cumplirse en todo caso permaneciendo inalterable su obligatoriedad también en aquellos supuestos de cierta premura.

4.2. Principios necesarios para la adopción de la medida

Junto a la concurrencia de los aspectos examinados, la autoridad judicial competente debe tener en cuenta una serie de principios de obligada observancia cuya ponderación será necesaria para poder adoptar la medida. Estos principios son: el principio de idoneidad, de especialidad, de excepcionalidad, de necesidad y de proporcionalidad.

4.2.1. Principio de idoneidad

A tenor de lo dispuesto en el artículo 588 bis a) de la Ley de Enjuiciamiento Criminal, en adelante LECrim, este principio permitirá definir el ámbito objetivo, subjetivo y la duración de la medida en virtud de su utilidad. Desde la perspectiva europea, lo cierto es que el reglamento únicamente alude a los principios de proporcionalidad y necesidad como aquellos que deben ser valorados para la adopción de la medida. No obstante, los diferentes escenarios que permiten determinar la idoneidad de la misma son aludidos reiteradamente, de forma separada, sin agruparlos en los principios que deben ser tenidos en cuenta para tal fin.

Por esta razón, consideramos conveniente adoptar una sistemática más coherente, dando paso al principio de idoneidad en relación con la identificación biométrica como medida de investigación para los fines previstos en el ámbito de un proceso penal.

Así, será conveniente delimitar ese ámbito objetivo respecto de la finalidad que persigue la investigación y su conveniente correlación con los resultados que la medida puede aportar para los fines previstos durante la práctica de la identificación en un lugar concreto y determinado. Desde un punto de vista subjetivo la idoneidad podrá exigir la identificación de los sujetos afectados por la misma, estableciendo un grupo concreto de afectados para evitar que la medida pueda afectar indiscriminadamente a una colectividad no determinada. En último lugar, la idoneidad permitirá valorar la adecuación temporal de la medida limitándola en un espacio temporal adecuado a la investigación penal que evite, así, un uso excesivo y dilatado en el tiempo.

4.2.2. Principio de especialidad

El artículo 588 bis a) de la LECrim exige, en virtud del principio de especialidad, que una medida esté relacionada con la investigación de un delito concreto y, en consecuencia, no podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva. Este precepto, se encuentra relacionado con la previsión del reglamento, contenida en el artículo 5.3, que alude a la existencia de pruebas objetivas o de indicios claros de los que se deduzca que la medida es conveniente para lograr el resultado concreto de la investi-

gación en base a la especialidad de la misma. Aunque en nuestra LECrim se relaciona la especialidad con el delito concreto, desde la perspectiva europea la tendencia se invierte moderadamente tomando como referencia los objetivos de la investigación en vez de los delitos que, aunque enunciados genéricamente, se puede observar como la consecución de los objetivos es el criterio preferente a tenor de lo dispuesto en el RIA.

4.2.3. Principio de excepcionalidad y necesidad

Ambos principios se recogen de forma conjunta en nuestra LECrim, poniendo de manifiesto el legislador la íntima conexión que existe entre ambos. La aplicación de estos principios indica que la identificación biométrica en espacios de acceso público solo podrá acordarse cuando no existan otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.

Como ya se ha puesto de relevancia previamente, la afectación de esta medida a los derechos fundamentales de las partes objeto de investigación, así como también, de terceros afectados de forma indirecta, implica, necesariamente, que el recurso a la identificación biométrica se repute excepcional, no solo atendiendo a los objetivos de la investigación sino, también, a la práctica común en aquellos supuestos. Es decir, el hecho de encontrarnos ante uno de los supuestos permitidos de forma excepcional en el RIA no habilita, de forma automática, al empleo de la identificación biométrica en espacios de acceso público. Su posibilidad, comporta que deban de observarse todos los principios que estamos desarrollando bajo una perspectiva prudente, cautelosa y sumamente garantista[28]. Ello implica, que su utilización sea percibida por las autoridades públicas como el último recurso en defecto de medidas anteriores que no han podido satisfacer los objetivos de la investigación y, por lo tanto, la medida se conciba como necesaria para el esclarecimiento de determinados hechos.

4.2.4. Principio de proporcionalidad

La adopción de una medida de investigación en el seno de un proceso penal puede, en ocasiones, resultar conflictiva por la afectación que la misma puede tener sobre los derechos de los ciudadanos. Por ello, el principio de proporcionalidad se erige como límite a cualquier injerencia estatal sobre los derechos fundamentales cuando se produce una desproporción entre el fin perseguido y los medios empleados[29].

---

[28] Algunas garantías adicionales a las expuestas son tratadas por ETXEBERRIA GURIDI, José Francisco, "Sistemas biométricos (el reconocimiento facial en particular) y sus aplicaciones", CALAZA LÓPEZ, Sonia y LLORENTE SÁNCHEZ-ARJONA, Mercedes (dir.), *Inteligencia Artificial legal y administración de justicia,* Aranzadi, Cizur Menor, 2022, pp. 171 y ss.

[29] SAN MIGUEL CASO, Cristina, "Medidas de investigación limitativas de derechos fundamentales", SÁNCHEZ GÓMEZ, Raúl y MONTORO SÁNCHEZ, Juan Alejandro (coord.), *Manual de Derecho Procesal Penal para guardias civiles,* Dykinson, Madrid, 2021, p. 132.

En palabras de GONZÁLEZ-CUELLAR deberá valorarse "si el sacrificio de los intereses individuales que comporta la injerencia guarda una relación razonable o proporcionada con la importancia del interés público que se trata de salvaguardar"[30].

Concretamente, en relación con el objeto de estudio de este trabajo, la proporcionalidad respecto a la identificación biométrica pivotará sobre tres aspectos esenciales como son los límites geográficos, temporales y personales. Al respecto, consideramos que estos tres elementos serán decisivos para valorar, tras el oportuno análisis relativo a la excepcionalidad y la necesidad, la proporcionalidad en sentido estricto pues, si tan solo uno de esos límites resulta desproporcionado en aras al interés público y a los objetivos de la investigación, la autorización decaerá en base al incumplimiento de este principio.

En definitiva, el principio de proporcionalidad actúa como contrapeso para evitar un uso desmedido y ciertamente invasivo respecto de los derechos fundamentales del conjunto de la ciudadanía pues, no debemos olvidar que la identificación biométrica en espacios de acceso público practicada de forma remota afectará tanto al sujeto principal sobre el que recaerá la investigación, como a aquellas personas que transiten por el ámbito geográfico determinado y previsto para la adopción de la medida. Por lo tanto, el análisis de proporcionalidad debe realizarse desde una perspectiva amplia que sopese no solo los derechos que pueden verse comprometidos en el ámbito de la investigación, sino también, extramuros de la misma desde una perspectiva colectiva.

El conjunto de principios y requisitos que deben observarse como garantías previas para la puesta en marcha de la medida, se extiende, también, una vez que la misma ha finalizado pues el diseño del control que se ejerce en relación con la identificación biométrica abarca tanto la fase inicial de su autorización como las notificaciones que deben realizarse una vez la identificación se lleva a cabo.

Así, el RIA contempla la obligación de notificación de todo uso que se realice respecto de un sistema de identificación biométrica a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos, ya que sobre ambas recaerá, posteriormente, el deber de presentar a la Comisión informes anuales sobre la utilización de estos sistemas en el territorio nacional al objeto de realizar, desde el ámbito europeo, un control de su utilización y publicar los resultados y observaciones pertinentes de todos los estados miembros.

5. CONCLUSIÓN

Una vez analizados, de manera por minorizada, alguno de los aspectos más importantes que la nueva regulación europea concede a los sistemas de identificación biométrica en espacios de acceso público, le corresponde al legislador nacional adoptar las directrices oportunas en torno a la materia. Para la consecución de este

[30] GONZÁLEZ-CUÉLLAR SERRANO, Nicolás, "El principio de proporcionalidad en el derecho procesal español", *Cuadernos de Derecho Público,* núm. 5, 1998, p. 208.

fin, se debe partir de dos ideas básicas; la normativa de máximos adoptada a nivel europeo y el espíritu garantista del reglamento. Al respecto, las pautas contenidas en el RIA permitirán a los estados miembros desarrollar leyes más restrictivas sobre el uso de sistemas de identificación biométrica, pero, en ningún caso, las previsiones nacionales podrán albergar mayores supuestos de aplicación o límites y principios con un carácter menos taxativo.

Por esta razón, la posibilidad de delimitar el uso de las técnicas biométricas puede ser una oportunidad para continuar la senda marcada por la Unión Europea, aportando un plus de garantismo que colme ciertas deficiencias puestas de manifiesto en el trabajo. De esta forma, consideramos prioritario huir de términos ciertamente ambiguos e indeterminados y delimitar de forma clara y concisa los lapsos temporales que aún, están por definir. Además, será necesario por parte del legislador llevar a cabo una atribución de funciones entre los distintos organismos y autoridades nacionales que, con carácter generalista y procedimental han sido creados por el reglamento europeo.

En suma, podemos concluir que la regulación analizada ha colmado las expectativas de todos los estados miembros, lograda a través de un largo camino de debate, consenso y diálogo entre los distintos países y organismos. Sin duda alguna, la protección de los derechos fundamentales de los ciudadanos debe ser una prioridad aun cuando éstos deban sufrir ciertas restricciones en aras a garantizar intereses jurídicos relevantes para la sociedad en su conjunto. Solo a través de una regulación garantista, eficaz y proteccionista seremos capaces de conjugar todos los intereses en juego y permitir la utilización de sistemas de identificación biométrica para fines previamente determinados.

6. BIBLIOGRAFÍA

AYLLÓN GARCÍA, Jesús Daniel, "La inteligencia artificial como medio de difusión y control de las fake news", VILLEGAS DELGADO, César y MARTÍN RÍOS, Pilar (coord.), *El derecho en la encrucijada tecnológica: Estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial,* Tirant lo Blanch, Valencia, 2022, pp. 217-239.

AYLLÓN GARCÍA, Jesús Daniel, "La inteligencia artificial como un medio para administrar justicia", BUENO DE MATA, Federico y GONZÁLEZ PULIDO, Irene (dir.), *Fodertics 8: estudios sobre tecnologías disruptivas y justicia*, Comares, Madrid, 2020, pp. 3-14.

BARONA VILAR, Silvia, "Tecnología biométrica y datos biométricos. Bondades y peligros. No todo vale", *Actualidad Jurídica Iberoamericana,* núm. 21, 2024, pp. 298-331.

BARONA VILAR, Silvia, *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice,* Tirant lo Blanch, Valencia, 2021.

BARRIO ANDRÉS, Moisés, "Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia Artificial" en BARRIO ANDRÉS, Moisés (dir.) *El Reglamento Europeo de Inteligencia Artificial,* Tirant lo Blanch, Valencia, 2024, pp. 21-47.

BORGES BLÁZQUEZ, Raquel, *Inteligencia artificial y proceso penal,* Aranzadi, Navarra, 2021.

COTINO HUESO, Lorenzo, "Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos", BALAGUER CALLEJÓN, Francisco y COTINO HUESO, Lorenzo (coord.) *Derecho público de la inteligencia artificial*, Fundación Manuel Giménez Abad, Zaragoza, 2023, pp. 347-402.

DE HOYOS SANCHO, Montserrat, "El Proyecto de Reglamento de la Unión Europea sobre inteligencia artificial, los sistemas de alto riesgo y la creación de un ecosistema de confianza", BARONA VILAR, Silvia (coord.) *Justicia Poliédrica en periodo de mudanza,* Tirant lo Blanch, Valencia, 2022, pp. 403-421.

ETXEBERRIA GURIDI, José Francisco, "El uso de sistemas de inteligencia artificial (IA) de identificación biométrica remota en espacios públicos en la ley europea de IA", *Actualidad Jurídica Iberoamericana,* núm. 21, 2024, pp. 528-565.

ETXEBERRIA GURIDI, José Francisco, "Sistemas biométricos (el reconocimiento facial en particular) y sus aplicaciones", CALAZA LÓPEZ, Sonia y LLORENTE SÁNCHEZ-ARJONA, Mercedes (dir.), *Inteligencia Artificial legal y administración de justicia,* Aranzadi, Cizur Menor, 2022, pp. 151-180.

FREIRE MONTERO, Antón Fructuoso, "El reconocimiento facial como instrumento de investigación y prevención del delito", *Anuario da Facultade de Dereito da Universidade da Coruña*, Vol. 26, 2022, pp. 64-88.

GÓMEZ COLOMER, Juan Luis, "Los actos de investigación garantizados basados en las nuevas tecnologías", GÓMEZ COLOMER, Juan Luis, y BARONA VILAR, Silvia (coord.), *Proceso Penal. Derecho Procesal III,* 4ª edición, Tirant lo Blanch, Valencia, 2024.

GÓMEZ COLOMER, Juan Luis "Derechos fundamentales, proceso e inteligencia artificial: una reflexión", CALAZA LÓPEZ, Sonia y LLORENTE SÁNCHEZ-ARJONA, Mercedes (dir.), *Inteligencia Artificial legal y administración de justicia,* Aranzadi, Cizur Menor, 2022, pp. 257-287.

GONZÁLEZ-CUÉLLAR SERRANO, Nicolás, "El principio de proporcionalidad en el derecho procesal español", *Cuadernos de Derecho Público,* núm. 5, 1998, pp. 191-218.

IGLESIAS CANLE, Inés Celia, "Reconocimiento facial y proceso penal", CASTILLEJO MANZANARES, Raquel y NOYA FERREIRO, Lourdes (coord.) *Inteligencia artificial y proceso penal: un reto para la justicia,* Aranzadi, Cizur Menor, 2023, pp.179-211.

RAMÓN FERNÁNDEZ, Francisca, "La aplicación de la inteligencia artificial y su desarrollo en el ámbito de la videovigilancia y los drones", RAMÓN FERNÁNDEZ, Francisca (coord.), *Ciencia de datos y perspectiva de la inteligencia artificial,* Tirant lo Blanch, Valencia, 2024, pp. 211-270.

RIDAURA MARTÍNEZ, María Josefa, "El reconocimiento facial como herramienta para garantizar la seguridad: de la incertidumbre ¿a un escenario de certeza?",

CAAMAÑO, Francisco y JOVE VILLARES, Daniel (dir.), *Tecnologías abusivas y derecho,* Tirant lo Blanch, Valencia, 2024, pp. 139-185.

RODRÍGUEZ DEL BLANCO, Alfredo, "Detectando los riesgos de la inteligencia artificial en la instrucción penal", *Revista General de Derecho Procesal,* núm. 64, 2024, pp. 1-66.

SAN MIGUEL CASO, Cristina, "Inteligencia artificial y algoritmos: La controvertida evolución de la tutela judicial efectiva en el proceso penal", *Estudios Penales y Criminológicos,* núm. extra-44, 2023, pp. 1-23.

SAN MIGUEL CASO, Cristina, "La aplicación de la Inteligencia Artificial en el proceso: ¿un nuevo reto para las garantías procesales?", *Revista Ius et Scientia: Revista electrónica de Derecho y Ciencia,* vol. 7, núm. 1, 2021, pp. 286-303.

SAN MIGUEL CASO, Cristina, "Medidas de investigación limitativas de derechos fundamentales", SÁNCHEZ GÓMEZ, Raúl y MONTORO SÁNCHEZ, Juan Alejandro (coord.), *Manual de Derecho Procesal Penal para guardias civiles,* Dykinson, Madrid, 2021, pp.130-139.

SÁNCHEZ MARTÍNEZ, María Olga, "El impacto de la sociedad digital en los derechos humanos", SOLAR CAYÓN, José Ignacio y SÁNCHEZ MARTÍNEZ, María Olga. (coord.), *El impacto de la inteligencia artificial en la teoría y práctica jurídica,* La Ley, Madrid, 2022, pp. 115-143.

TOMÁS MALLÉN, Beatriz, "Las sinergias entre el Reglamento General de Protección de Datos de la Unión Europea y el Convenio 108+ del Consejo de Europa", GARCÍA MAHAMUT, Rosario y TOMÁS MALLÉN, Beatriz (Eds.), *El Reglamento General del Protección de Datos. Un enfoque nacional y comparado,* Tirant lo Blanch, Valencia, 2019, pp. 57-89.

Dykinson, S.L.

Universidad de Alcalá

ISSN: 1888-3214