EL USO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL (IA) DE IDENTIFICACIÓN BIOMÉTRICA REMOTA EN ESPACIOS PÚBLICOS EN LA LEY EUROPEA DE IA*

THE USE OF ARTIFICIAL INTELLIGENCE (AI) SYSTEMS FOR REMOTE BIOMETRIC IDENTIFICATION IN PUBLICLY ACCESSIBLE SPACES IN THE EUROPEAN AI LAW

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 528-565

* Este trabajo ha sido redactado en el marco del Proyecto de investigación "Claves para una justicia digital y algorítmica con perspectiva de género" (expediente: PID2021-123170OB-I00) financiado por MCIN/AEI/10.13039/501100011033.

José Francisco
ETXEBERRIA
GURIDI

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: El uso de la biometría para el esclarecimiento y persecución de hechos criminales y, sobre todo, de su autor tiene un largo recorrido histórico. La aplicación de sistemas de inteligencia artificial con tales fines de identificación biométrica multiplica exponencialmente su eficacia. Pero, a su vez, se incrementa la afectación en los derechos de los ciudadanos. El texto de la Ley Europea de Inteligencia Artificial aborda esta delicada cuestión no sin dejar de suscitar una viva polémica.

PALABRAS CLAVE: Artificial Intelligence; remote biometric identification; personal data; private life.

ABSTRACT: *The use of biometrics to clarify and prosecute criminal acts and, above all, their perpetrator has a long. The application of artificial intelligence systems for such biometric identification purposes multiplies their effectiveness exponentially. But, at the same time, the impact on citizens' rights increases. The text of the European Artificial Intelligence Act addresses this delicate issue, but without failing to spark lively controversy.*

KEY WORDS: *Inteligencia Artificial; identificación biométrica remota; datos personales; vida privada.*

I. INTRODUCCIÓN.

La biometría en cuanto estudio de los fenómenos o procesos biológicos, ha estado muy presente a lo largo de la evolución del Derecho. Usualmente del Derecho Penal o Procesal Penal, pero no de forma exclusiva. Dejando ahora al margen los extremos de las teorías de LOMBROSSO, las aportaciones extraordinarias de la criminalística tienen con frecuencia como fundamento precisamente el análisis de vestigios de carácter biológico como es el caso de las pruebas de ADN o de las huellas dactilares, entre otros[1]. No hay que perder de vista que una de las funciones del proceso penal consiste justamente en acreditar la autoría de los hechos criminales, esto es, determinar el elemento subjetivo del objeto que se va a juzgar en dicho proceso.

Los rasgos físicos, fisiológicos o de naturaleza similar que resultan adecuados al efecto de identificar a personas concretas pueden ser tratados con sistemas de Inteligencia Artificial (IA) potenciando exponencialmente su eficacia individualizadora, mediante el tratamiento algorítmico de los datos de carácter biométrico[2]. De este modo, estos sistemas se tornan en eficaces instrumentos que admiten múltiples aplicaciones. Sobre este punto, ya hace más de una década el Grupo de Trabajo del Art. 29 de la Directiva 95/46/CE, de 24 de octubre de 1995, sobre tratamiento de datos personales y a la libre circulación de estos

1 Vid. sobre algunos antecedentes al respecto Richard González, M.: "Los sistemas biométricos de reconocimiento facial en la Unión Europea en el marco del desarrollo de la Inteligencia Artificial", *Justicia*, 2023, núm. 1, pp. 158-160.

2 El desarrollo de la tecnología permitiría que la obtención, registro y cotejo de datos biométricos se produzca con una rapidez y eficacia no vista hasta ahora. Vid. Richard González, M.: "Los sistemas", cit., p. 153; Cotino Hueso, L.: "Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos", en AA.VV.: *Derecho Público de la Inteligencia Artificial*, (coord. por F. Balaguer Callejón y L. Cotino Hueso), Fundación Manuel Giménez Abad, Madrid, 2023, pp. 354 y ss.

• José Francisco Etxeberria Guridi
Catedrático de Derecho Procesal. Universidad del País Vasco/Euskal Herriko Unibertsitatea. Correo electrónico: patxi.etxeberria@ehu.eus

datos[3], distinguía su uso como: a) Medio de autenticación/verificación biométrica ("one-to-one comparison"). En este supuesto se comparan dos plantillas biométricas pertenecientes supuestamente a la misma persona para determinar si, efectivamente, la persona que aparece en ambas es la misma. Este proceso de búsqueda de correspondencias "uno-a-uno" admite varias modalidades. Por ejemplo, lo usual resulta que una de las plantillas biométricas se halle previamente almacenada y en el momento en que interese se obtenga la segunda plantilla. Pero no siempre resulta necesario el almacenamiento de dicha plantilla en un fichero[4]; b) Medio de identificación biométrica ("one-to-many comparison"). En estos supuestos, la plantilla biométrica que se obtiene se compara con otras plantillas biométricas almacenadas en uno o en varios ficheros o bases de datos, esto es, se trataría de un proceso de búsqueda de correspondencias "uno-a-varios". En esta modalidad de identificación se pueden distinguir aquellos supuestos en los que la comparación se realiza frente a un fichero o base de datos en el que conste que figura la plantilla biométrica de la persona a identificar ("closed-set identification"), de aquéllos en los que la búsqueda de correspondencia se realiza sin tener constancia de dicha circunstancia ("open-set identification"); y c) Medio de categorización/segregación biométrica ("matching general characteristics"). En esta modalidad el sistema biométrico actúa como un proceso que permite extraer características de un individuo con el objeto de determinar su pertenencia a un grupo con características predefinidas a fin de adoptar una medida específica. En este caso, lo importante no es identificar o verificar a un individuo, sino asignarle automáticamente una categoría determinada (la pertenencia a un grupo étnico, la edad, el sexo, etc.).

Siendo numerosos los ámbitos en los que resultan susceptibles de aplicación los sistemas IA indicados, también son amplios los espectros de derechos e intereses de los ciudadanos que pueden resultan afectados de la aplicación de tales sistemas. El tratamiento de datos de carácter personal ya implica, de por sí, una incidencia en el derecho a la vida privada de los sujetos afectados en esta nueva dimensión de la privacidad que comienza a adquirir sustantividad propia como derecho fundamental autónomo en la década de los ochenta del siglo pasado y que tiene reflejo en esa precisa época en el art. 18.4 CE. Pero, además, los datos personales que sirven de fundamento a estas técnicas de identificación

3 Vid. "Documento de trabajo sobre biometría" del GT29; Dictamen 3/2012 GT29 sobre la evolución de las tecnologías biométricas (WP193).

4 La FRA (European Union Agency for Fundamental Rights) se refiere, por ejemplo, a la posibilidad de que las características biométricas se incorporen a un documento de identidad o a un pasaporte, de modo que en los controles fronterizos se escanee la imagen que aparece en el documento y se compare mediante tecnologías de reconocimiento facial con la imagen que se obtiene en momento real en el punto de control, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, p. 7. Utilizado en los servicios móviles y en línea (reconocimiento facial, de voz, de huella dactilar) puede funcionar conforme a esta modalidad "en lugar de un nombre de usuario y contraseña" para acceder a un servicio o a un dispositivo en línea o móvil (Dictamen 2/2012, de 22 de marzo, sobre reconocimiento facial en los servicios en línea y móviles, p. 3).

poseen unas particularidades especiales que los hacen merecedores de una especial protección: se trata de los datos biométricos. Según el 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 (RGPD en adelante) y la Directiva (UE) 2016/680, de 27 de abril de 2016, también sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales pero para fines de prevención y represión penal, estos datos biométricos pertenecen a la "categoría especial de datos" (arts. 9 y 10 respectivamente) y por este motivo están sujetos a restricciones en su tratamiento y a garantías adicionales en los supuestos excepcionales en que sea posible[5].

Por otro lado, el empleo de esos datos biométricos con fines de identificación que es objeto de este estudio es el que se materializa en espacios públicos ("one-to-many comparison"). Ello implica la afectación a un número cuantioso de ciudadanos cuyos datos biométricos serán objeto de tratamiento. Esta implementación debe ajustarse, por consiguiente, de una manera rigurosa al principio de proporcionalidad de la medida, para evitar en lo posible situaciones abusivas. Pero la incidencia en los derechos de los ciudadanos va más allá de un tratamiento masivo de unos datos por muy especiales que sean. El empleo de esos sistemas implica sujetar a vigilancia y control determinados espacios públicos, en los que, siquiera de forma más atenuada, también se desarrollan aspectos de la vida privada de los ciudadanos. Y en los que también se desarrollan, por constituir el lugar idóneo para ello, otras expresiones de la libertad del individuo como el derecho de reunión o el de manifestación. La vigilancia de tales espacios utilizando sistemas que permiten identificar a quienes participan en esas demostraciones puede producir un efecto disuasorio innegable en la libertad de los ciudadanos.

No se agotan en los mencionados los riesgos que implica el uso de sistemas IA de reconocimiento biométrico. Estos sistemas se basan usualmente, pero no exclusivamente, en el tratamiento de imágenes faciales (reconocimiento facial) que ya han sido objeto de aplicación práctica en no pocos lugares. La experiencia ha demostrado que los índices de error, en forma de falso positivo o de falso negativo, no son desdeñables, ni mucho menos. El uso de algoritmos sesgados es la causa esencial de tales deficiencias. Lo preocupante son las graves consecuencias asociadas a tales errores y que se han traducido en ciertas ocasiones en privaciones de libertad de las personas erróneamente identificadas.

Todo lo anterior explica que, el que nos ocupa, sea un tema vinculado a la polémica, pero no artificiosa, sino fruto de una preocupación real por la incidencia que en los derechos de los ciudadanos tiene el uso de tales sistemas. Polémica

5 Cano Ruiz, I.: "Artículo 9. Categorías especiales de datos", en AA.VV.: *Protección de Datos: Comentarios a la Ley Orgánica de Protección de Datos y Garantías Digitales (en relación con el RGPD)* (dir. por M. Arenas Ramiro y A. Ortega Giménez), Sepín, Madrid, 2019, p. 82.

que se ha evidenciado, de otra parte, durante la tramitación de la trascendental Ley Europea de IA. La posición de las instituciones europeas implicadas en el procedimiento legislativo ha sido encontrada. Sobre este punto en especial. La Propuesta inicial de la Comisión (Propuesta de Reglamento IA) de 2021, de la que hace un seguimiento sin separarse en lo esencial el Consejo, ha sido enmendada de forma radical por el Parlamento Europeo, que ha llegado a proponer una prohibición casi absoluta de los sistemas IA que nos van a ocupar. Aunque no hayan sido atendidas en el texto definitivo consensuado, ha de reconocerse que venían precedidas de serias objeciones planteadas al respecto por las máximas autoridades institucionales sobre protección de datos de la propia UE[6].

Este trabajo se centrará en el análisis de este trascendental texto europeo, limitando el mismo desde una óptica procesal al empleo de los sistemas IA de identificación biométrica con fines de lo que, en el texto, se denomina aplicación de la ley ("law enforcement"), esto es, lo relacionado con la prevención y la represión penal.

II. PREVIA ACLARACIÓN CONCEPTUAL.

Según lo adelantado, el uso de los sistemas IA que nos ocupan ha generado un encendido debate con posiciones encontradas incluso en el seno de las propias instituciones europeas. Se trata, pues, de una cuestión compleja que afecta, como se ha dicho, a un amplio abanico de derechos y libertades, y de un numeroso grupo de personas. La primera cuestión a tratar ha de ser, por consiguiente, la de aclarar qué ha de entenderse por sistemas IA de identificación biométrica remota en tiempo real y en espacios públicos, con los fines de prevención y represión penal.

Esta necesidad de definir de la manera más precisa posible el significado de esta modalidad de sistema IA se hace más evidente, si cabe, en el caso de una disposición normativa llamada a ser aplicada y a ser vinculante en un espacio como el europeo en el que conviven ordenamientos jurídicos diversos y con particularidades propias significativas. Es el ámbito de la justicia penal el último reducto que los Estados miembros suelen querer preservar en el ejercicio de su soberanía y es el más refractario a las ideas de cooperación y armonización, de ahí las diferencias institucionales y normativas. Afortunadamente, este instrumento normativo que nos ocupa contiene, como nos tiene acostumbrados el legislador europeo en normas trascendentales, un capítulo relativo a las definiciones de los

6 Aunque no se ha publicado aún oficialmente el texto definitivo de la Ley de IA, se hizo público que el pasado 8 de diciembre de 2023 se alcanzó un acuerdo entre las tres instituciones implicadas (trílogos) que fue aprobado por el Parlamento Europeo el 13 marzo de 2024 en primera lectura [P9_TA(2024)0138] y al que nos referiremos, con las debidas precauciones, como "texto definitivo".

conceptos fundamentales objeto de regulación. Otra afortunada costumbre con la que nos regala con frecuencia el legislador europeo, sobre todo en casos como el presente, en el que se aborda una materia novedosa y con gran repercusión económica, comercial y jurídica, es la de acompañar el texto de la norma de una amplia exposición de considerandos explicativos, no sólo de las razones que la impulsan, sino también aclaratorios del significado de las disposiciones que se contienen. En ocasiones, como esta que nos ocupa, de una extensión considerablemente amplia, pero las más de las veces, también en ésta, justificada.

1. La identificación biométrica.

El texto inicial de Propuesta remitido por la Comisión (21.04.2021) comienza el abordaje de la materia con alusiones y definiciones de lo que ha de entenderse por "sistemas IA de identificación biométrica", pero prescinde del significado de identificación biométrica en sí mismo. Este silencio resulta llamativo en la medida en que ya resultaba usual y admitida la clasificación de las aplicaciones de la biometría con fines de: autenticación o verificación biométrica, por un lado; identificación biométrica, por otro lado; y categorización biométrica, por último. Esta omisión ha sido colmada en posteriores versiones del texto.

Tampoco contiene una referencia expresa a la "identificación biométrica" el texto del Consejo (Orientación general de 06.12.2022), pero sí aclara que quedan excluidos de la definición los "sistemas de verificación o autenticación cuyo único propósito es confirmar que una determinada persona física es la persona que afirma ser y los sistemas que se utilizan para confirmar la identidad de una persona física con el único fin de tener acceso a un servicio, un dispositivo o un local" [considerando (8)].

Sin embargo, el texto enmendado que presenta el Parlamento Europeo (de 14.06.2023 y que utiliza la denominación de Ley de IA) contiene muy relevantes aportaciones en el tema que nos ocupa y una de ellas es la expresa contraposición entre identificación, verificación y categorización biométricas. Además, el texto enmendado del Parlamento, no sólo define lo que ha de entenderse por identificación biométrica, sino que también amplía el elenco de rasgos humanos que constituyen los datos biométricos sobre los que se fundamenta la identificación. Esto es relevante, pues parece ser que tales aportaciones han sido atendidas en el texto definitivo de la Ley IA.

Conforme al texto del Parlamento, ha de entenderse por identificación biométrica "el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual y psicológico para determinar la identidad de una persona comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos (identificación `uno respecto a

varios´)" [nuevo art. 3.33 ter)]. Esta propuesta del Parlamento ha sido asumida en el texto definitivo. También la definición expresa de "verificación biométrica" en contraposición a la identificación, que con anterioridad a las enmiendas no se recogía en el texto. Ahora sí.

Resulta de esencial relevancia esta precisión conceptual. Los sistemas de identificación biométrica remota representan la especie de la categoría de identificación biométrica, pero esta última es una categoría más amplia, pues la identificación biométrica a distancia solo resulta posible en determinados supuestos o expresiones de la identificación biométrica, pero no en todo caso.

En la definición del Parlamento, incorporada al texto definitivo, sobresale no sólo el hecho mismo de definir el concepto, sino los términos en los que lo hace. De la anterior definición resulta que la identificación biométrica tiene lugar comparando los datos biométricos de la persona cuya identidad se quiere determinar, con los datos biométricos de personas que se encuentran almacenados en bases de datos. El concepto o definición de "dato biométrico" resulta esencial a tales efectos, pues constituye la esencia de esos sistemas. Y aquí la sorpresa.

Según la definición de identificación biométrica arriba recogida, los rasgos o características biométricas humanas que se utilizan con tal finalidad identificativa son las de "tipo físico, fisiológico, conductual y psicológico". La referencia a las características psicológicas de la persona con fines identificativos es nueva. No estaba recogida en el texto originario de la Comisión. Pero lo que resulta más relevante, no se corresponde exactamente con la definición de datos biométricos".

Sin perjuicio de que ahondemos más adelante en el concepto de dato biométrico sobre el que descansa la identificación biométrica, resulta oportuna una parada en los siempre ilustrativos considerandos que, también en este caso, muestran ejemplos o supuestos de lo que de forma más genérica se indica en la definición. El texto enmendado del Parlamento Europeo añadió un nuevo considerando (7 bis) -enmienda núm. 22- en el que tras la definición del concepto "identificación biométrica" en los términos indicados arriba, menciona ejemplos de los rasgos humanos susceptibles de tratamiento automatizado, así, la cara, el movimiento ocular, las expresiones faciales, la forma del cuerpo, la voz, el habla, el modo de andar, la postura, la frecuencia cardíaca, la presión arterial, el olor, las pulsaciones de tecla, las reacciones psicológicas (ira, angustia, dolor, etc.)".

Llama la atención, como se ha indicado, la referencia a las reacciones psicológicas (ira, angustia, dolor, etc.) en el listado de rasgos o características humanas susceptibles de tratamiento automatizado. No tanto por constituir algo novedoso, sino, más bien, por contraposición al texto inicial de Propuesta de la Comisión que no hacía referencia a ello. Novedoso no lo es tanto, pues ya el

Dictamen 3/2012, de 27 de abril de 2012, del Grupo de Trabajo del Artículo 29 hacía alusión a las mismas. Este último Dictamen mencionaba entre las técnicas biométricas las relativas al patrón de venas, a las impresiones dactilares o a la firma biométrica, además de las expresamente citadas en el considerando (7 bis) del texto del Parlamento. Pero también contenía menciones a los aspectos psicológicos. Así, distinguía entre las técnicas biométricas dos categorías principales, las basadas en aspectos físicos y fisiológicos, por un lado, y las basadas en aspectos comportamentales o conductuales, por otro lado. Pero, a su vez, no olvidaba hacer referencia al, en ese momento, "reciente ámbito de las técnicas basadas en elementos psicológicos, que incluyen la medición de la respuesta a situaciones concretas o pruebas específicas que se ajusten a un perfil psicológico"[7].

La mención de las reacciones psicológicas entre la relación de características humanas susceptibles de tratamiento con fines de identificación biométrica que incorporan las enmiendas del Parlamento Europeo han pasado al texto definitivo de la Ley IA. Al menos en la definición del concepto de identificación biométrica del art. 3.35. Sin embargo, existe una cierta disfunción con lo previsto en el nuevo considerando (15), pues en el mismo sí se hace mención a los rasgos físicos, fisiológicos y conductuales, con mención expresa de los mismos ejemplos que los citados en el texto del Parlamento Europeo, pero no así a las características psicológicas. Parece que se trata de un mero olvido, al hacer mención de las características psicológicas en el articulado del texto definitorio de la identificación biométrica, pero no en los considerandos.

No podemos dejar pasar la oportunidad al menos de aludir a dos cuestiones estrechamente vinculadas a la identificación biométrica. Por un lado, la formulación por parte del Parlamento Europeo en su texto enmendado de un nuevo concepto próximo pero diferenciado del de datos biométricos, se trata de los denominados "datos de base biométrica", esto es, "los datos obtenidos a partir de un tratamiento técnico específico relativos a las señales físicas, fisiológicas o conductuales de una persona física" [33 bis)]. Los elementos en común son incuestionables, sobre todo la base biométrica de ambos conceptos. Sin embargo, falta en estos últimos la referencia a la aptitud identificadora unívoca de las personas propia de los datos biométricos en sentido estricto. Nos referiremos más adelante al respecto, sólo dejar señalado que este nuevo concepto no ha sido asumido en el texto definitivo.

7 Dicho Dictamen 3/2012 contiene otras referencias al respecto, así, la posibilidad de que de las características de la cara (reconocimiento facial) se pueda determinar, no solo la identidad, sino también "las características fisiológicas y psicológicas" de la persona; o la incorporación de una nueva categoría de datos biométricos -de segunda generación- en los que lo determinante no es tanto la identidad, sino otras circunstancias igualmente útiles: "Los avances en tecnologías y redes informáticas están propiciando asimismo la subida de lo que se considera la segunda generación de datos biométricos basada en la utilización de los rasgos de comportamiento y psicológicos solos o combinados con otros sistemas clásicos que conforman sistemas multimodales". Dictamen 3/2012, pp. 4, 17 y 23.

La otra cuestión vinculada al tema que nos ocupa es la relativa a los sistemas de reconocimiento de emociones. La deducción de emociones tiene lugar, también en este caso, a partir de los datos biométricos. Además, de lo que se entienda por reconocimiento de emociones dependerá la existencia de más elementos en común con la identificación biométrica, y consiguientes dificultades de deslinde. Si nos ajustamos a la definición inicial contenida en el texto de la Comisión, y que coincide con la finalmente asumida en el texto definitivo, se entiende por sistema de reconocimiento de emociones "un sistema de IA destinado a detectar o deducir las emociones o las intenciones de personas físicas a partir de sus datos biométricos" [arts. 3.34) y 3.39) respectivamente].

Entre ambas versiones se han sucedido, no obstante, otros textos con definiciones que presentan ciertas diferencias. Así, la Orientación general del Consejo de la UE añadía a la finalidad de detección o deducción de emociones o de intenciones de personas físicas, la de los "estados mentales" de las mismas [también art. 3.34)]. Más amplia aún es la definición recogida en el texto del Parlamento Europeo, que a la inferencia de emociones e intenciones, añade la de los pensamientos y estados de ánimo. Estas incorporaciones aproximan más los sistemas de reconocimiento de emociones a los rasgos psicológicos dirigidos a la identificación biométrica.

Como se ha dicho, el texto definitivo de la Ley IA vuelve a la versión más restrictiva correspondiente al texto inicial de la Comisión, eliminando las referencias a los estados mentales o de ánimo y a los pensamientos. En todo caso, cuando se dispone a enumerar ejemplos, lo hace en un sentido amplio similar al del texto del Parlamento, y así podemos comprobarlo en su considerando (18) al afirmar que el reconocimiento de emociones "se refiere a emociones o intenciones como la felicidad, la tristeza, la indignación, la sorpresa, el disgusto, el entusiasmo, la vergüenza, la satisfacción y la diversión. No incluye estados físicos, como el dolor o el cansancio".

2. El concepto de dato biométrico.

El concepto de dato biométrico resulta esencial y fundamento de la identificación biométrica. Como recoge el texto definitivo de la Ley IA en su considerando (14) los datos biométricos permiten una pluralidad de aplicaciones al hacer posible la autenticación, la identificación y la categorización de las personas físicas y, a su vez, el reconocimiento de sus emociones. Creemos nosotros que también los polígrafos o instrumentos similares a los que igualmente se refiere la Ley de IA, podrían incluirse en esa categoría, pues tienen un indudable fundamento biométrico.

Conviene aclarar su significado, pues, al menos aparentemente, existen disfuncionalidades en los textos analizados en torno al concepto señalado. El texto originario de la Comisión definía los datos biométricos como "los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" [art. 3.33)]. Esto es, de manera absolutamente idéntica a la definición contenida en el RGPD y en la Directiva (UE) 2016/680. Esta coincidencia nada tiene de extraño, más bien lo contrario, como además lo recuerda el considerando (7) del texto original con una llamada a la definición contenida en ambos textos normativos sobre protección de datos personales y a la necesidad de que se "interprete en consonancia con ella".

De la definición destacamos, por un lado, que los datos obtenidos mediante el tratamiento técnico correspondiente tienen una nítida aptitud para la identificación unívoca de las personas, y pone como ejemplos de ello la imagen facial y los datos dactiloscópicos; por otro lado, que el tratamiento recae sobre rasgos o características físicas, fisiológicas o conductuales. Curiosamente, la referencia a la capacidad identificadora única característica de los datos biométricos desaparece en la definición que de este concepto se recoge en el art. 3.33) del texto del Consejo de la UE (Orientación general de 06.12.2022). El resto de la definición no varía. Esta falta de sintonía podría salvarse con lo contenido en el considerando (7) antes mencionado, que es muy similar al del texto original de la Comisión, pero tampoco absolutamente idéntico. Ya no dice, evidentemente, que la noción de dato biométrico "coincide" con el concepto del RGPD y la Directiva (UE) 2016/680, pero sí que la misma "debe interpretarse" en consonancia con el recogido en estos textos. Algo similar ocurre con el texto definitivo de la Ley IA, pues al definir el dato biométrico alude al tratamiento automatizado de características físicas, fisiológicas y conductuales de una persona física, pero sin mencionar tampoco aquí la eficacia identificadora única del dato personal resultante. En cualquier caso, la definición de dato biométrico en el texto definitivo de la Ley de IA sí se refiere a los ejemplos paradigmáticos de datos de tal naturaleza presentes en todas las definiciones normativas de los mismos, a saber, a las imágenes faciales y a los datos dactiloscópicos. La ausencia de referencia al potencial identificativo de los datos biométricos también puede salvarse con lo dispuesto en el considerando (14). En el mismo, se afirma que la noción de dato biométrico de la Ley de IA se ha de "interpretar" en consonancia con lo dispuesto al respecto en los textos esenciales sobre protección de datos [RGPD, Directiva (UE) 2016/680 y Reglamento (UE) 2018/1725]. Pero no se llega a sostener, a diferencia por ejemplo de la inicial Propuesta de la Comisión, que la noción de dato biométrico "coincida" con la recogida en las normas de referencia sobre protección de datos.

Creemos que la posición del Parlamento Europeo cuando aborda la cuestión de la identificación biométrica es la más coherente desde un plano sistemático con el contexto conceptual de lo que ha de entenderse por datos biométricos en el espacio de la UE. Por comenzar, en el texto de enmiendas del Parlamento se opta por no definir el concepto de dato biométrico y por hacer una remisión al concepto de los datos biométricos "tal como se definen en el artículo 4, punto 14, del Reglamento (UE) 2016/679". Resulta llamativo que solamente se haga alusión al concepto de dato biométrico contenido en el RGPD y no en otros textos de la UE igualmente relevantes en materia de protección de datos. Por ejemplo, en la Directiva (UE) 2016/680 o el Reglamento (UE) 2018/1725. Llama igualmente la atención que el considerando (7) no corrija la omisión de esos textos normativos, máxime cuando eran ya mencionados en la Propuesta inicial de la Comisión y lo son en el texto definitivo de la Ley de IA. En todo caso, ignorando esas circunstancias, la definición de dato biométrico recogido en el RGPD coincide plenamente con la contenida en los instrumentos normativos omitidos.

Ahora bien, en nuestra opinión, la principal aportación del texto del Parlamento es la incorporación de un concepto nuevo, próximo al de dato biométrico, pero no coincidente totalmente con él. Además, este nuevo concepto adquiere pleno sentido en un contexto en el que datos relativos a la biometría pueden ser valiosos para múltiples finalidades, sin necesidad de reunir las condiciones de los datos biométricos en sentido estricto, y que pueden implicar igualmente serias amenazas para los derechos y libertades de las personas. Sobre todo, cuando esos datos "relativos" a la biometría pueden ser objeto de tratamiento mediante sistemas de IA.

Cabía solucionar este entuerto mediante dos alternativas posibles, factibles al menos: modificar el concepto de dato biométrico, dotándolo de un contenido más extenso, por un lado, o introducir un nuevo concepto diferente al de dato biométrico en sentido estricto, pero con fundamento igualmente en rasgos biométricos y con múltiples virtualidades cuando son objeto de tratamiento automatizado. El Parlamento Europeo se decantó por esta segunda opción con un nuevo concepto que denomina "datos de base biométrica".

3. Los datos de base biométrica.

El nuevo concepto de "datos de base biométrica" se define en el texto enmendado del Parlamento Europeo como "los datos obtenidos a partir de un tratamiento técnico específico relativos a señales físicas, fisiológicas o conductuales de una persona física" [art. 3.33 bis)]. Conforme a esta definición, los datos de base biométrica presentan un incuestionable sustrato común compartido con los datos biométricos en sentido estricto, pues en ambos casos son datos resultantes de un tratamiento técnico de señales físicas, fisiológicas o conductuales de una persona

física. El principal elemento diferenciador es que desaparece de la definición la idoneidad para identificar de forma única a las personas físicas, característica de los datos biométricos en sentido estricto. Sin perjuicio de otras diferencias menos relevantes[8]. Aunque, como se ha comprobado, también desaparece esta particularidad identificativa unívoca de la definición de dato biométrico en el texto definitivo de la Ley IA[9].

Parece evidente que el legislador europeo (en este caso el Parlamento con sus enmiendas) ha pretendido con este novedoso concepto que no quedaran fuera del ámbito regulatorio posibles aplicaciones de sistemas de IA que tuvieran por objeto datos que, sin pertenecer a la categoría de biométricos en sentido estricto, poseen un innegable fundamento biométrico. No es de extrañar si reparamos un poco en los supuestos en los que en la Ley de IA los sistemas de IA se utilizan para el tratamiento de los mencionados "datos de base biométrica".

En efecto, según el texto propuesto por el Parlamento Europeo, los datos basados en la biometría pueden conducir a la identificación de una persona física, pero no necesariamente. De este modo, añade en el considerando (7) -enmienda núm. 21- tras la referencia a lo que ha de entenderse por datos biométricos en sentido estricto, que "los datos basados en técnicas biométricas son nuevos datos resultantes de un procesamiento técnico específico relativo a señales físicas, fisiológicas o conductuales de una persona física, como las expresiones faciales, los movimientos, la frecuencia cardíaca, la voz, las pulsaciones de tecla o el modo de andar, que pueden, en algunos casos, permitir identificar o confirmar la identificación unívoca de una persona física". La alusión a que sólo en "algunos casos" este tipo de datos puede conducir a la identificación unívoca de una persona adquiere pleno sentido si nos atenemos a algunos de los ejemplos citados -expresiones faciales, movimientos, frecuencia cardíaca- que difícilmente pueden considerarse dotados de tal aptitud.

8 El texto del Parlamento Europeo, por ejemplo, ha optado por referirse a las "señales" ("signals") físicas, fisiológicas y conductuales de las personas, en lugar de a las "características" ("features") de idéntica clase que sigue utilizando con motivo de la identificación biométrica o, por remisión, de los datos biométricos. Seguramente tiene que ver con la capacidad individualizadora o identificativa de las "características", mayor que la de las "señales". Otro elemento diferenciador lo hallamos en que omite al referirse a estos datos de base biométrica hacerlo como "datos personales", pero no nos cabe duda de que sí nos hallamos ante datos de esa naturaleza considerando la amplitud con la que se definen los datos personales en los textos normativos al respecto, pues se refieren no sólo a la información relativa a una persona física identificada, sino también "identificable", entendiendo por esto último "toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona [art. 4.1) RGPD y art. 3.1) Directiva (UE) 2016/680]. Vid. sobre la definición de persona identificable los comentarios de Romeo Casabona, C.M.: "Datos personales (comentario al artículo 4.1 RGPD)", en AA.VV.: *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (dir. por A. Troncoso Reigada), Tomo I, Thomson-Aranzadi, Cizur Menor, 2021, pp. 585-589.

9 Aunque con remisión en su considerando (14) al RGPD, al Reglamento (UE) 2018/1725 y a la Directiva (UE) 2016/680 en cuanto a la necesidad de interpretar dicho concepto conforme a estos textos normativos.

Dos son los ámbitos en los que el texto del Parlamento Europeo emplea este nuevo concepto de "datos de base biométrica". Por un lado, en relación con la denominada "categorización biométrica" y, por otro, en relación con los "sistemas de reconocimiento de emociones". En el primer caso, la "asignación de personas físicas a categorías concretas, o inferencia de sus características y atributos" puede realizarse "en función de sus datos biométricos y sus datos de base biométrica, o que puedan inferirse a partir de dichos datos" [art. 3.35)]. En el segundo caso, se define al sistema de reconocimiento de emociones como aquél destinado a detectar o deducir las emociones, los pensamientos, los estados de ánimo o las intenciones de individuos o grupos a partir de sus datos biométricos y sus "datos de base biométrica" [art. 3.34)].

Estos datos de base biométrica, aparentemente inocuos por carecer por sí mismos de esa capacidad de individualizar de forma unívoca a las personas, pueden adquirir, en cambio, una nueva y más amplia dimensión cuando son tratados mediante IA, pues a partir de ellos pueden inferirse rasgos o características afectantes a la vida privada o tener contenido sensible. Particularmente llamativa es la circunstancia de que el texto del Parlamento Europeo es partidario de una amplia prohibición de los sistemas de reconocimiento de emociones -con fines de persecución penal o gestión de fronteras, en lugares de trabajo y centros educativos- [art. 5.1.d quinquies)][10] y de una prohibición casi absoluta de los sistemas de categorización biométrica -salvo cuando se destinen a fines terapéuticos basados en el consentimiento informado de la persona expuesta- [art. 5.1.b bis)][11]. Y al margen de estos supuestos prohibidos, los sistemas de IA que utilicen datos biométricos "o basados en la biometría" para extraer conclusiones sobre las características personales de las personas físicas "deben clasificarse de alto riesgo" [considerando (33 bis) y Anexo III.1.a bis)].

Con todo, pese a la relevancia que implica en nuestra opinión este nuevo concepto de datos de base biométrica, lo cierto es que el texto del Parlamento Europeo no es siempre claro al referirse a los rasgos o características que pueden servir de fundamento a tales datos frente a los datos biométricos en sentido

10 Los argumentos empleados por el Parlamento Europeo para fundamentar la amplia prohibición de los sistemas de IA de reconocimiento de emociones descansan en la escasa fiabilidad científica de los mismos y el consiguiente riesgo de abusos que puede derivarse. Así, afirma en sus considerandos que "las emociones o sus formas de expresión y su percepción varían de forma considerable entre culturas y situaciones, e incluso en una misma persona. Algunas de las deficiencias principales de estas tecnologías son la fiabilidad limitada (las categorías de emociones no se expresan de forma coherente a través de un conjunto común de movimientos físicos o psicológicos ni se asocian de forma inequívoca a estos), la falta de especificidad (las expresiones físicas o psicológicas no se corresponden totalmente con las categorías de emociones) y la limitada posibilidad de generalizar (los efectos del contexto y la cultura no se tienen debidamente en cuenta)" [considerando (26 quater)].

11 Las razones por las que conforme al texto del Parlamento habían de prohibirse los sistemas de IA que clasifican a las personas físicas asignándolas a categorías específicas, en función de ciertas características sensibles o protegidas, ya sean conocidas o inferidas, radica en su carácter "especialmente intrusivos" y en que "vulneran la dignidad humana y presentan un gran riesgo de discriminación" contraria al art. 21 de la Carta de Derechos Fundamentales de la UE (CDFUE), y al art. 9 del RGPD [considerando (16 bis)].

estricto. En este sentido, el considerando (7) del texto enmendado menciona refiriéndose a los datos de base biométrica a "señales" físicas, fisiológicas y conductuales tales como las expresiones faciales, los movimientos, la frecuencia cardíaca, la voz, las pulsaciones de tecla o el modo de andar. Pero, a su vez, el considerando (7 bis) relativo a la "identificación biométrica" basada en la comparación de datos biométricos en sentido estricto, vuelve a repetir algunos de los "rasgos" humanos citados en el considerando precedente como susceptibles de tratamiento automatizado -en concreto el movimiento ocular, las expresiones faciales, la voz, el modo de andar, la frecuencia cardíaca-.

Resulta evidente que muchos de estos rasgos o características no son por sí solos suficientes para determinar la identificación indubitada de una persona física. Este argumento resulta válido para las características humanas de tipo psicológico -auténtica novedad incorporada en el concepto de identificación biométrica, basada, insistimos, en la comparación de datos biométricos en sentido estricto- pues escasa o nula virtualidad han de tener por sí solas a efectos de establecer la identidad de una persona las reacciones psicológicas (ira, angustia, dolor, etc.) que se mencionan como ejemplo en el considerando (7 bis).

Se ha de concluir, pues, que junto a los rasgos de la persona que permiten identificarla de forma indubitada -patrón de venas, iris, retina, huella dactiloscópica, imagen facial, ADN, etc.- existen otras características, como las mencionadas más arriba y que incluirían los relativos a los datos de base biométrica, que carecen por sí mismas de tal eficacia, pero que pueden contribuir a ello. Ya se anticipó en tal sentido el Grupo del Art. 29 en su Dictamen 3/2012, sobre evolución de las tecnologías biométricas, con referencia a las nuevas tendencias sobre biometría mencionando la utilización de las denominadas "tecnologías biométricas ligeras" ("soft biometrics") que se caracterizan, precisamente, por "el uso de rasgos muy comunes no aptos para distinguir claramente o identificar a un individuo, pero que permiten mejorar los resultados de otros sistemas de identificación".

No puede negarse que los rasgos más comunes mencionados, si bien pueden resultar útiles, no son por lo general atribuibles a una sola persona. Esta deficiencia es la que puede resultar de la opción por una concepción excesivamente amplia de dato biométrico. En tal sentido, el Dictamen 4/2007 del Grupo de Trabajo del Art. 29 (WP 136), sobre el concepto de datos personales, de 20 de junio de 2007, definía los datos biométricos como propiedades biológicas, características fisiológicas, pero también "rasgos de la personalidad o tics", exigiendo a todos ellos que fueran al mismo tiempo "atribuibles a una sola persona y mensurables"[12].

12 Esta definición se reproduce en el apartado de las definiciones del Dictamen 3/2012 (WP193) en el que se añade que "los datos biométricos cambian irrevocablemente la relación entre el cuerpo y la identidad, ya que hacen que las características del cuerpo humano sean legibles mediante máquinas y estén sujetas a un uso posterior".

Como puede fácilmente entenderse, las dificultades de atribución a una sola persona de los rasgos indicados no siempre son idénticas, siendo mayores en el caso de los de personalidad o tics.

Esto último ha de vincularse con la posibilidad de combinar diversas tecnologías biométricas que hagan más eficaz el objetivo de identificación unívoca, en su caso. Esto es, se trataría de los denominados sistemas multimodales o biometría muldimodal que es definida por el Dictamen 3/2012 reiterado como la "combinación de diversas tecnologías biométricas con el fin de aumentar la exactitud o rendimiento del sistema (también se denomina biometría a varios niveles)". Este Dictamen añade que estos sistemas pueden funcionar de distintas maneras, bien recogiendo datos biométricos diferentes con distintos sensores, bien realizando múltiples lecturas del mismo elemento biométrico o bien utilizando algoritmos múltiples para la extracción de características de la misma muestra biométrica.

4. Sistema de identificación biométrica "remota".

Como se ha dicho anteriormente, la identificación biométrica consiste en comparar los datos biométricos obtenidos de una persona física con los conservados previamente en bases de datos o ficheros con la finalidad de identificar a aquélla (a diferencia de la verificación). La obtención de los rasgos o características de la persona física tiene lugar, en el caso que nos ocupa, de forma "remota". ¿Qué significa esto último? La definición que al respecto recoge el texto definitivo de la Ley IA nos procura no pocas pistas. Así, se define el sistema de identificación biométrica remota como "un sistema de IA destinado a identificar a personas físicas generalmente a distancia, sin su participación activa, comparando sus datos biométricos con los que figuran en un repositorio de datos de referencia" [art. 3.41)]. Dos elementos de esa definición pueden servir para entender el calificativo: por un lado, que la identificación se produce "generalmente a distancia"; y, por otro lado, que la misma tiene lugar "sin su participación activa". Esta definición coincide plenamente con la recogida en la Orientación general del Consejo de la UE. No así con las definiciones que contienen el texto original de la Comisión y el del Parlamento Europeo. En estos últimos, no se hace expresamente referencia a que no sea precisa la participación activa de la persona afectada y se da por hecho que la identificación será siempre a distancia. En ambos, a diferencia del texto definitivo que guarda silencio al respecto, se añade que el usuario o implementador del sistema desconoce de antemano si la persona en cuestión se encontrará en las bases de datos de referencia y podrá, por lo tanto, ser identificada.

El carácter remoto del uso de estos sistemas de identificación biométrica limita en extremo los datos biométricos susceptibles de ser capturados para su comparación con los existentes en las bases de datos de referencia. Queremos

decir que la captura de datos biométricos para su posterior comparación con otros almacenados requiere, en la mayoría de los supuestos, el conocimiento y la colaboración de la persona afectada. Por ejemplo, las huellas dactilares, muestras de ADN, el iris o la retina. Resulta complicado imaginar de qué modo se pueden obtener a distancia los datos biométricos procedentes de esas "fuentes de datos biométricos". Esto nos induce a pensar que la identificación biométrica "remota" se reducirá en la mayoría de los casos al tratamiento de la imagen facial mediante las tecnologías de reconocimiento facial, considerando la facilidad en la captura de dichas imágenes[13], dejando ahora al margen los sistemas de categorización biométrica que constituyen, igualmente, un ámbito propicio para el tratamiento de datos biométricos a distancia o remotamente.

Esta misma idea puede inferirse de la referencia al posible uso simultáneo de los sistemas de identificación biométrica que hace el texto definitivo de la Ley IA en su considerando (17). En este último se afirma que los sistemas de identificación biométrica remota se usan para detectar "simultáneamente" varias personas con fines de identificación sin necesidad de la colaboración activa de las mismas. Por ahora se nos ocurre, casi exclusivamente, la tecnología de reconocimiento facial remota o a distancia.

5. Sistema de identificación biométrica remota "en tiempo real".

El sistema de identificación biométrica ante el que se plantean serias prevenciones es, no sólo el que tiene lugar a distancia, sino también de manera inmediata. Tiene que ver con el hecho de que, siendo el resultado de la comparación positivo, se adoptarán decisiones con seria repercusión en la esfera del individuo y de sus derechos (proceder, por ejemplo, a la inmediata detención del identificado sin opción de una supervisión humana con el intervalo de tiempo suficiente). Con esta finalidad de una mejor protección del individuo se ha pretendido incluir una definición del término "en tiempo real" que no se limite exclusivamente al instantáneo momento. En tal sentido, se define la expresión que encabeza este apartado como "un sistema de identificación biométrica remota en el que la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa. Este término engloba no solo la identificación instantánea, sino también demoras mínimas limitadas, a fin de evitar su elusión"

13 En efecto, al tratar la Agencia de los Derechos Fundamentales de la Unión Europea (FRA) de las ventajas atribuibles al reconocimiento facial como sistema de identificación, afirma que la imagen facial es más o menos única, no puede ser alterada, no puede ser ocultada con facilidad y, a diferencia de otros datos biométricos como la huella dactilar o el ADN, es fácil de obtener, de manera que resulta de ordinario imposible que una persona pueda evitar que su imagen facial sea obtenida y monitorizada en un espacio público, FRA, *Facial recognition,* cit., p. 5.

[art. 3.42)]. Dicho en otras palabras, los sistemas en tiempo real implican el uso de material "en directo" o "casi en directo" [considerando (17)][14].

Siendo clara la intencionalidad del legislador europeo, la manera en la que se ha expresado su idea en el texto ha variado en las diferentes versiones del mismo. Curiosamente, la versión definitiva es calcada a la del texto originario de la Comisión. La Orientación general del Consejo (06.12.2022) optó, sin embargo, por referirse a la recogida de los datos biométricos, la comparación y la identificación que tiene lugar "instantáneamente o casi instantáneamente". El texto del Parlamento Europeo prefirió, sin embargo, referirse a la ausencia de demora significativa en términos de instantaneidad o de demora limitada, suprimiendo la alusión al carácter mínimo de la demora cuando no sea instantánea. En conclusión, lo relevante es evitar toda posibilidad de eludir la aplicación de las normas contempladas en la Ley de IA en relación con el uso "en tiempo real" de los sistemas de identificación biométrica remota –prohibiéndolo o condicionando dicho uso a una serie de restricciones- generando fraudulentamente demoras mínimas.

Las prevenciones vinculadas al uso de sistemas de IA de identificación biométrica remota no serían aplicables, por consiguiente, cuando las actuaciones de obtención, comparación e identificación no tienen lugar "en tiempo real". Esto es, el uso de tales sistemas sería considerado como de alto riesgo, como muchos otros, y sujeto a una serie de condiciones, pero no recaería sobre ellos la prohibición de partida y la admisibilidad excepcional, en su caso, aplicables a los sistemas de identificación en tiempo real. A esta modalidad de sistema de identificación biométrica que no tiene lugar en tiempo real la Ley de IA las denomina "en diferido", aunque la definición de la misma se formula por simple exclusión, esto es, todo sistema de identificación biométrica remota "que no sea un sistema de identificación biométrica remota `en tiempo real´" [art. 3.43)]. En los sistemas de identificación biométrica "en diferido" los datos biométricos se han recabado previamente, a partir de imágenes o grabaciones que pueden proceder de diversas fuentes, y que han sido generadas con anterioridad a la aplicación del sistema. Es la comparación de esos datos biométricos con los que se disponen en

14 De hecho, una de las objeciones que al uso de los sistemas de IA de identificación biométrica que nos ocupan plantea el importante Dictamen 5/2021, de 18 de junio de 2021, sobre la inicial Propuesta de Reglamento de IA, aprobado conjuntamente por el Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección (SEPD), máximas autoridades en protección de datos en la UE, consiste precisamente en que no está claro qué deberá entenderse por "demora significativa". Pero no sólo eso, sino que, además, resta importancia a la dicotomía entre tiempo real o no, pues la intrusión del tratamiento no depende de que la identificación se produzca de un modo u otro; y por ello mismo se critica que se considere como un factor atenuante el hecho de que la identificación biométrica pueda tener lugar con "demora significativa". Se objeta al respecto en dicho Dictamen, que un sistema de identificación masiva es capaz de identificar a miles de personas en solo unas horas o la probabilidad de que la identificación biométrica a distancia en el contexto de una protesta política tenga un efecto disuasorio significativo en el ejercicio de los derechos y libertades fundamentales, como la libertad de reunión y asociación y, más en general, en los principios fundacionales de la democracia [apartado (31)].

bases de datos de referencia y, en su caso, la identificación la que tiene lugar con una demora significativa.

En estos supuestos, los riesgos antes mencionados –inmediatez en las consecuencias, escasas oportunidades para realizar comprobaciones o correcciones adicionales- no tendrían idéntica envergadura. En todo caso, tampoco pueden ignorarse los riesgos inherentes a los sistemas de IA destinados a la identificación a la identificación biométrica remota de las personas físicas, con independencia de si su uso es en tiempo real o en diferido. Ambas modalidades adolecen de imprecisiones técnicas que pueden dar lugar a resultados sesgados y tener consecuencias discriminatorias. Siendo esto especialmente importante en lo que respecta a la edad, la etnia, la raza, el sexo o la discapacidad. No es baladí, como tendremos ocasión analizar, que el texto del Parlamento Europeo propusiera extender la prohibición del uso de los sistemas de IA de identificación biométrica remota "en tiempo real" también al empleo "diferido" de los mismos. Aunque en este segundo supuesto la prohibición podría exceptuarse mediante la concurrencia de rigurosos presupuestos.

6. Sistema de identificación biométrica remota en tiempo real en "espacio de acceso público".

Las cautelas que contempla la Ley de IA sobre el uso de los sistemas de IA de identificación biométrica remota y en tiempo real se justifican igualmente por el lugar físico o espacio en el que tiene lugar aquella identificación biométrica. El texto se refiere a la identificación biométrica de personas físicas en espacios de acceso público. Dos cuestiones han de ser destacadas al respecto. Por un lado, que el uso de dispositivos tecnológicos que posibilitan la identificación biométrica de personas físicas en los indicados espacios incrementa exponencialmente la posibilidad de afección de una infinidad de sujetos. Es decir, de una manera indiscriminada en el sentido literal del término. Esto es, sin discernir ni diferenciar a las personas físicas concretas susceptibles de identificación biométrica en función de su condición de sospechosas de infracciones ya cometidas, de peligrosas en relación a futuras infracciones, de víctimas desaparecidas, etc. Cualquier persona física que transite por el espacio sometido a observación puede ser objeto de los sistemas de IA de identificación biométrica. Por otro lado, así como los espacios más vinculados a la privacidad –vivienda o espacios cerrados- han merecido la protección incuestionable por parte del Derecho, no ha ocurrido lo mismo en relación a la posible afectación de los derechos de los ciudadanos cuando la "vida privada" se desarrolla en espacios públicos. Al menos ha acontecido así hasta fechas recientes.

Sobre este punto, la intencionalidad de la Ley de IA en la protección de los derechos de los sujetos afectados es evidente. Para ello utiliza una concepción

amplia del significado de espacio de acceso público. Préstese atención a que dicha amplitud definitoria no debe ser interpretada como una posibilidad igualmente extensa de injerencia en los derechos de los ciudadanos. Al contrario, siendo el punto de partida, como veremos, el de la prohibición de los sistemas de IA de identificación biométrica remota cuanto más amplio sea el espacio objeto de prohibición mejor tutelados resultarán los derechos de las personas afectadas por tales sistemas.

Como decíamos, el texto de la Ley de IA opta por un concepto amplio de espacio de acceso público, priorizando la condición pública del acceso sobre la condición pública de la titularidad de dicho espacio. Así, define la noción de "espacio de acceso público" 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" [art. 3.44)].

Esto ya supone una diferencia notable con lo establecido en otras disposiciones normativas cuya aplicación pueda solaparse por coincidir en mayor o menor grado en el ámbito de aplicación. Así, la LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, se refiere en cuanto a su objeto a la grabación de imágenes y sonidos "en lugares públicos, abiertos o cerrados" (art. 1.1). De igual modo, la LO 7/2021, de 26 de mayo, por la que se transpone la Directiva (UE) 2016/680, regula la instalación de sistemas de videocámaras fijas en "las vías o lugares públicos" (art. 16.1). Conforme a la primera norma citada la cuestión no podría ser resuelta de forma distinta, considerando la finalidad preventiva de la misma y que las Fuerzas Policiales sólo pueden actuar en espacios públicos. La LO 7/2021, por su parte, tiene un ámbito de aplicación mucho más amplio, pues comprende la protección de datos personales obtenidos, no sólo para la prevención, sino también para la persecución y enjuiciamiento de infracciones penales. Aunque el precepto concreto referido sí tenga connotaciones de claro contenido preventivo.

Como se ha dicho, la Ley de IA utiliza un concepto amplio de lugar de acceso público. Dicha definición nos da ya unas claves concretas para su delimitación. Al tratarse de un lugar "físico" quedan excluidos los espacios en línea[15]. Por otro lado, resulta indiferente, por ejemplo, que se trate de propiedad privada o pública. Otro elemento delimitador importante es el del carácter indeterminado del número de personas físicas con acceso. De modo que no puede considerarse de acceso

15 Considerando (19). Sobre esta segunda dimensión pueden consultarse, entre otros, el Dictamen 02/2012, de 22 de marzo de 2012, sobre reconocimiento facial en los servicios en línea y móviles del GT29 (WP 192). No es del mismo parecer el recogido en el Dictamen conjunto 5/2021 del CEPD y del SEPD, al afirmar que, por razones de coherencia, los sistemas de IA para la identificación remota a gran escala en espacios en línea deberán prohibirse en virtud del art. 5 de la Propuesta [apartado (32)].

público el espacio al que únicamente pueden acceder determinadas personas físicas definidas. Los siempre ilustrativos considerandos ponen como ejemplos de lugar excluido del acceso público los locales de 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 pertinentes [considerando (19)].

El lugar físico no pierde su condición de espacio de acceso público por la circunstancia de que tenga una capacidad limitada o restringida. Tampoco, y esto es más relevante a los efectos de su delimitación, si dicho acceso está sujeto al cumplimiento de determinadas condiciones que pueden satisfacer un número indeterminado de personas, por ejemplo, según el considerando (19), adquiriendo una entrada o título de transporte, registrándose previamente o teniendo una determinada edad. También es importante destacar que resulta indiferente a los efectos de atribuir el carácter de accesibilidad pública al lugar, la naturaleza de la actividad que se desarrolle en el mismo, siempre que se cumplan los anteriores requisitos. En todo caso, la suma de los anteriores condicionantes en la delimitación del espacio de acceso público no termina de despejar todas las interrogantes concebibles, de ahí que el considerando correspondiente, el (19), concluya afirmando que "no obstante, se debe determinar caso por caso si un espacio es de acceso público o no teniendo en cuenta las particularidades de la situación concreta".

7. Sistema de identificación biométrica remota en tiempo real en espacio de acceso público "con fines de aplicación de la ley".

Las prevenciones a que venimos refiriéndonos en relación al uso de sistemas de IA de identificación biométrica se centran en dicho uso con fines de aplicación de la ley. Dicho ámbito es de por sí apto para generar situaciones de riesgo que pueden pugnar con los derechos fundamentales de los ciudadanos. Muy explícitamente, podemos encontrar en el texto de la Ley de IA aserciones en las que se constata que, atendiendo a su función y responsabilidad, las actuaciones de las autoridades encargadas de la aplicación de la ley que implican determinados usos de sistemas de IA "se caracterizan por un importante desequilibrio de poder y pueden dar lugar a la vigilancia, la detención o la privación de libertad de una persona física, así como a otros efectos negativos sobre los derechos fundamentales que garantiza la Carta" [considerando (59)]. Por consiguiente, se trata de un ámbito en el que serán considerados como de alto riesgo múltiples sistemas de IA diseñados para usarse con los mencionados fines.

Ahora bien, esto nos conduce a tener que precisar qué ha de entenderse por fines de aplicación de la ley. Aquí claramente se ha optado en la versión española de la expresión por una traducción literal de la expresión inglesa "law enforcement" que por sí misma, esta última, tiene una incuestionable connotación

de que la ley que se aplica es la penal. No así en la traducción literal española. Hubiera sido preferible una expresión análoga en la traducción a las de otras versiones en las que se enfatiza el elemento de la "criminalidad" (así, "à des fines répressives" francesa o "zu Strafverfolgungszwecken" alemana). Para entender, pues, el verdadero significado de la expresión que nos ocupa hemos de acudir nuevamente al apartado de las definiciones conforme a las cuales, se entiende por tales "las actividades realizadas por las autoridades encargadas de la aplicación de la ley, o en su nombre, para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública" [art. 3.46)].

Nos hallamos nuevamente ante una definición muy amplia de la expresión "fines de aplicación de la ley". La misma contempla actuaciones de prevención de infracciones penales, así como de represión de las ya cometidas. Amplitud que se acrecienta con la referencia a las amenazas para la seguridad pública. En todo caso, esta extensión del término es coincidente con el objeto a que se refieren, tanto la Directiva (UE) 2016/680, como la LO 7/2021 por la que se transpone.

III. PUNTO DE PARTIDA: PROHIBICIÓN DE LOS SISTEMAS DE IDENTIFICACIÓN BIOMÉTRICA REMOTA EN ESPACIOS DE ACCESO PÚBLICO CON FINES DE APLICACIÓN DE LA LEY.

La Ley de IA opta por un enfoque normativo basado en los riesgos. Conforme al mismo, se diferencian, por un lado, prácticas prohibidas de IA, por otro lado, sistemas de IA de alto riesgo, sujetos a obligaciones y requisitos específicos, y, por último, sistemas de IA sujetos a normas armonizadas de transparencia (art. 1). Pues bien, el régimen jurídico de los sistemas de identificación biométrica que nos ocupan es bastante particular. En principio se integran en el Título II correspondiente a las prácticas de IA prohibidas [art. 5.1.h)]. Pero no se trata de una prohibición absoluta, pues acto seguido, el mismo precepto admite su uso condicionado a la observación de unos estrictos requisitos orientados a que el mismo resulte excepcional y proporcionado y rodeado de ciertas garantías. En estos casos excepcionales los sistemas de IA de identificación biométrica remota pasarían a formar parte de los sistemas IA de alto riesgo contemplados en el Anexo III por remisión del art. 6. 2).

Las razones por las que el texto de la Ley de IA adopta como punto de partida la prohibición de los sistemas de IA de identificación biométrica remota que nos ocupan –prohibición no absoluta, como veremos- están recogidas en el propio texto. Ya se ha indicado que, sin necesidad de descender todavía al concreto caso que nos ocupa, con carácter general las actuaciones de las autoridades encargadas

de la aplicación de la ley que implican determinados usos de sistemas de IA "se caracterizan por un importante desequilibrio de poder y pueden dar lugar a la vigilancia, la detención o la privación de libertad de una persona física, así como a otros efectos negativos sobre los derechos fundamentales que garantiza la Carta" [considerando (59)]. Conforme a dicho considerando, estos riesgos pueden derivarse de diversos factores vinculados a la precisión, fiabilidad y transparencia del sistema de IA. Así, pueden ser consecuencia de la cuestionable calidad de los datos utilizados en el entrenamiento, del no cumplimiento de los requisitos oportunos en términos de precisión o solidez, o del indebido diseño y prueba previos a su introducción en el mercado o puesta en servicio. Además, añade este mismo considerando, "podría impedir el ejercicio de importantes derechos procesales fundamentales, como el derecho a la tutela judicial efectiva y a un juez imparcial, así como los derechos de la defensa y la presunción de inocencia, sobre todo cuando dichos sistemas de IA no sean lo suficientemente transparentes y explicables ni estén bien documentados".

Siendo los anteriores los riesgos genéricos derivados del uso de sistemas de IA en el ámbito de la persecución penal, los concretos que se derivan para la identificación biométrica y que motivarían una inicial prohibición también son reconocidos de forma expresa por el texto de la Ley de IA. Así, se afirma que el uso de tales sistemas de IA invade especialmente los derechos y las libertades de las personas afectadas, en la medida en que "puede afectar a la vida privada de una gran parte de la población, provocar la sensación de estar bajo una vigilancia constante y disuadir indirectamente a los ciudadanos de ejercer su libertad de reunión y otros derechos fundamentales" [considerando (32)][16]. Se vuelve a insistir, además, en que las imprecisiones técnicas de los sistemas de inteligencia artificial destinados a la identificación biométrica remota de personas físicas "pueden dar lugar a resultados sesgados y entrañar efectos discriminatorios", siendo esto particularmente relevante cuando se trata de edad, etnia, raza, sexo o discapacidad[17]. Y a ello hay que añadir, como se ha dicho, que el riesgo para

16 La LO 4/1997 ya contemplaba en relación a la videovigilancia en espacios públicos, su incidencia en derechos como el de reunión. También sobre los efectos disuasorios de la videovigilancia en otros derechos como la libertad ideológica, el derecho de reunión y de manifestación y la libertad sindical y el derecho de huelga, vid. Arzoz Santisteban, X: "Videovigilancia y derechos fundamentales", en AA.VV.: *Videovigilancia: Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de datos personales* (dir. por J.F. Etxeberria Guridi), Tirant lo Blanch, Valencia, 2011, pp. 177-179.

17 Son numerosos los estudios sobre la existencia de sesgos y su repercusión en la elaboración de algoritmos, en concreto la presencia de diferenciales demográficos ("demographic differentials") en los algoritmos de reconocimiento facial. Vid. Buolamwini, J. y Gebru, T.: "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classication", *Proceedings of Machine Learning Research*, 2018, núm. 81, pp. 1-15; Grother, P.; Ngan, M. y Hanaoka, K.: *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*, U.S. Department of Commerce, 2019, [https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf]. Con carácter más general vid. Martínez Martínez, R.: "Inteligencia artificial desde el diseño", *Revista catalana de dret públic*, 2019, núm. 58, p. 73; Fernández Hernández, C.: "La nueva estrategia europea sobre el dato y la inteligencia artificial. Foto fija de un diseño en evolución", *Derecho Digital e Innovación*, 2020, núm. 5, p. 2; Guzmán Fluja, V.: "Sobre la aplicación de la inteligencia artificial a la solución de conflictos", en AA.VV.: *Justicia civil y penal en la era global* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2017, p. 70.

los derechos y las libertades de las personas afectadas se incrementa cuando los sistemas operan "en tiempo real", debido a la inmediatez de las consecuencias y las escasas oportunidades para realizar comprobaciones o correcciones adicionales [considerandos (32) y (54)].

A los anteriores argumentos que justificarían la prohibición del uso de estos sistemas de IA de identificación biométrica en espacios públicos, añade el texto de enmiendas del Parlamento Europeo que los mismos pueden otorgar a las partes que los implementan "una posición de poder incontrolable" [considerando (8)]. No es ésta, sin embargo, la principal contribución del Parlamento Europeo, sino su propuesta de prohibición absoluta de tales sistemas de IA, sin excepción. El único supuesto que resultaría admisible en opinión de Parlamento, pero también condicionado, sería el relativo a los sistemas de IA de identificación biométrica remota en espacios de acceso público, pero no "en tiempo real", sino "en diferido".

Las enmiendas del Parlamento Europeo en el sentido prohibitivo mencionado, traen causa de antecedentes previos como la Resolución del Parlamento Europeo, de 6 de octubre de 2021[18], que a su vez arranca de un previo Informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior de dicho Parlamento, de 13 de julio de 2021[19]. En su Resolución, el Parlamento insta en su apartado (26), la "prohibición permanente" del uso de "análisis automatizados o el reconocimiento en espacios accesibles al público de otras características humanas, como los andares, las huellas dactilares, el ADN, la voz y otras señales biométricas y de comportamiento". No resulta fácil identificar el verdadero alcance de la "prohibición permanente" instada, pues en otros apartados, y referido al empleo de sistemas de reconocimiento facial para la identificación biométrica con fines coercitivos prefiere hacer referencia a una "moratoria" al despliegue de tales sistemas, más que a una prohibición, hasta que se den al menos determinados requisitos y condiciones.

Igualmente crítico, y partidario de la prohibición de los sistemas de IA de identificación biométrica remota que analizamos, es el Dictamen conjunto 5/2021 del CEPD y del SEPD, relativo a la Propuesta de Reglamento inicial de la Comisión. En el mismo se subraya que la identificación biométrica remota de las personas en espacios de acceso público supone un riesgo elevado de intrusión en la vida privada, por lo que se reclama la necesidad de un enfoque más estricto. Se pone el acento en la cuestionable necesidad y proporcionalidad de la aplicación de tales sistemas de IA. Así, el uso de sistemas de IA podría plantear graves problemas de proporcionalidad, ya que podría implicar el tratamiento de datos de un número

18 Sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales [P9_TA(2021)0405].

19 A9-0232/2021.

indiscriminado y desproporcionado de personas para la identificación de solo unas pocas [apartado (30)]. Por todas estas razones, el CEPD y el SEPD piden una "prohibición general" del uso de la IA para el reconocimiento automatizado de rasgos humanos en espacios de acceso público, como los rostros, pero también la marcha, las huellas dactilares, el ADN, la voz, las pulsaciones de teclas y otras señales biométricas o conductuales, "en cualquier contexto" [apartado (32)][20].

IV. EXCEPCIONES A LA PROHIBICIÓN DE LOS SISTEMAS DE IDENTIFICACIÓN BIOMÉTRICA REMOTA EN ESPACIOS DE ACCESO PÚBLICO CON FINES DE APLICACIÓN DE LA LEY.

Se ha reiterado a lo largo de este trabajo que los numerosos y trascendentes riesgos para los derechos fundamentales que se encuentran vinculados al uso de los sistemas de IA de identificación biométrica a los que nos referimos, han derivado en la opción de su prohibición por parte del legislador europeo. Sin embargo, también se ha insistido, esta prohibición no es absoluta, sino que bajo determinadas condiciones su uso resulta admisible. En efecto, comienza el art. 5 del Título II de la Ley de IA (titulado este último como "prácticas de IA prohibidas") disponiendo de forma categórica que "estarán prohibidas" una serie de prácticas de IA, procediendo a continuación a enumerar las mismas hasta alcanzar en la letra h) de dicho precepto la referencia, como práctica prohibida, al "uso de sistemas de identificación biométrica remota `en tiempo real´ en espacios de acceso público por las autoridades encargadas de la aplicación de la ley, o en su caso en su nombre". Pero una vez enumerado el supuesto de uso proscrito, continúa acto seguido el enunciado normativo con la expresión "salvo y en la medida en que (…)". Esto es, la prohibición no es terminante, sino que admite excepciones, que es lo que veremos.

1. Objetivos legítimos.

Para que el empleo de sistemas de identificación biométrica remota a que nos referimos, en principio prohibidos, resulte justificado es preciso que el mismo esté dirigido a la consecución de unos fines expresamente determinados en dicha letra h). La concurrencia de tales objetivos no es por sí sola suficiente para justificar el empleo de los mencionados sistemas de identificación biométrica al exigir el precepto que concurra una "estricta necesidad" de unos (medios) respecto de los

20 Como ya se ha recogido "supra", el CEPD y el SEPD consideran que no existen razones para excluir de la prohibición la identificación biométrica remota masiva que tiene lugar en línea, o la identificación biométrica remota producida con "demoras significativas"; pero, además, incluye en esa propuesta de "prohibición general" la de la identificación biométrica remota con fines distintos a los de persecución penal al afirmar que el carácter intrusivo del tratamiento no depende necesariamente de su finalidad, pues "el uso de este sistema para otros fines, como la seguridad privada, representa las mismas amenazas para los derechos fundamentales al respeto de la vida privada y familiar y a la protección de los datos personales".

otros (fines). Esto último ya nos remite al carácter extraordinario de tal posibilidad de empleo[21].

El primero de los objetivos contemplados como justificativos sería el de la "búsqueda selectiva de víctimas específicas de secuestro, trata de seres humanos y explotación sexual de seres humanos y la búsqueda de personas desaparecidas" [h).i)]. Se aprecia en el enunciado de dicho supuesto la aspiración por concretar al máximo el marco y límites que hacen posible su admisibilidad, cumpliendo con las exigencias derivadas de que el tratamiento de los datos personales lo sean para fines determinados, explícitos y legítimos[22]. La búsqueda no sólo ha de ser "selectiva" -en contraposición a indiscriminada-, sino también de víctimas "específicas", esto es, ya determinadas. Otro tanto ha de decirse de la concreción expresa de los delitos por los que pasan a ser víctimas (secuestro, etc.) conforme al enunciado del precepto. No se trata de la búsqueda de víctimas de cualquier delito. Las infracciones mencionadas tienen en común que la víctima tiene restringida e impedida su libertad ambulatoria. La diferencia es notable con la versión inicial de la Propuesta de Reglamento de la Comisión y con la versión (Orientación general) del Consejo de la UE que se referían, sin más, a "un delito", sin dar mayor relevancia a la modalidad del mismo.

Junto a las víctimas, este concreto supuesto se refiere al empleo de sistemas de identificación biométrica en la búsqueda de personas desaparecidas. En este caso se amplía el ámbito subjetivo contemplado en el texto original de la Comisión que se refería exclusivamente a los menores desaparecidos. Se ha de entender, a los efectos de evitar la incidencia indiscriminada, que se trata también de una búsqueda selectiva de personas concretas.

El segundo de los objetivos que la Ley de IA estima admisibles en el empleo de sistemas de identificación biométrica, es el de 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 [h).ii)]. Claramente se perfilan de nuevo en este segundo supuesto los límites que marcan la excepcionalidad del mismo, por un lado, en relación a la naturaleza de la amenaza -específica, importante, inminente, real, actual o previsible, por lo tanto, de cierta entidad y gravedad, y con proximidad temporal, lo que reduce razonablemente la duración cronológica en el uso de los sistemas de identificación

21 El art 52.1 de la CDFUE condiciona cualquier limitación en el ejercicio de los derechos en ella reconocidos a que la misma sea, entre otros requisitos, respetuosa con el principio de proporcionalidad y, por lo tanto, "necesaria" para alcanzar objetivos de interés general reconocidos por la UE. Es constante la doctrina del TJUE cuando afirma que tales limitaciones exceden de lo "estrictamente necesario" cuando el objetivo de interés general "puede alcanzarse razonablemente de manera tan eficaz por otros medios menos atentatorios respecto de los derechos fundamentales de los interesados" (vid., entre otras, la STJUE, de 30 de enero de 2024, en el asunto C-118/22).

22 Arts. 5.1.b) RGPD y 4.1.b) Directiva (UE) 2016/680 (principios relativos al tratamiento).

biométrica-, por otro lado, en la relevancia de los bienes jurídicos a proteger que pueden verse afectados.

El tercer y último objetivo que podría justificar excepcionalmente el uso de los sistemas de identificación biométrica que nos ocupan consistiría en la localización o identificación de una persona sospechosa de haber cometido un delito a efectos de una investigación, enjuiciamiento o ejecución de sanciones penales por alguno de los delitos mencionados en el nuevo Anexo II que sea punible en el Estado miembro de que se trate con una pena o medida de seguridad privativa de libertad cuya duración máxima sea al menos de cuatro años [h).iii)][23]. Esta tercera salvedad refleja igualmente las consecuencias del proceso negociador entre las tres instituciones europeas competentes.

La versión inicial de la Comisión y el texto del Consejo (Orientación general) contemplaban esta salvedad a la prohibición de los sistemas analizados de forma tan amplia que difícilmente resultaba conciliable con la excepcionalidad ("estrictamente necesario") y el carácter restringido de los supuestos de admisión. Esto es, su proporcionalidad era cuestionable. Además, como se ha dicho, el Parlamento Europeo era partidario de una prohibición absoluta de estos sistemas de identificación biométrica, salvo que se tratara de una identificación en diferido y, también en estos casos, con relevantes limitaciones. Finalmente se ha optado por una solución intermedia, aunque más próxima a la de los postulados del texto en su versión original.

La Propuesta original de la Comisión permitía excepcionar la prohibición con la finalidad de detectar, localizar o identificar a sospechosos de haber cometido cualquiera de los delitos comprendidos en el art. 2.2 de la Decisión Marco 2002/584/JAI, de 13 de junio de 2002, relativa a la orden europea de detención y entrega. Esto es, los que se han venido a denominar "eurodelitos" en la medida en que se han reproducido por remisión en numerosos instrumentos normativos europeos relativos a la cooperación judicial penal y al reconocimiento mutuo de resoluciones judiciales. La amplitud de la excepción era aún mayor en el texto del Consejo, pues a los anteriores añadía cualquier "otro delito" para el que la normativa del Estado miembro de que se trate imponga una pena o medida de seguridad privativa de libertad cuya duración máxima sea de al menos 5 años.

23 Los delitos que comprende el Anexo II son los siguientes: terrorismo; tráfico de seres humanos; explotación sexual de niños y pornografía infantil; tráfico ilícito de estupefacientes y sustancias psicotrópicas; tráfico ilícito de armas, municiones y explosivos; asesinato, lesiones corporales graves; comercio ilícito de órganos y tejidos humanos; tráfico ilícito de materiales nucleares o radiactivos; secuestro, retención ilegal y toma de rehenes; crímenes dentro de la jurisdicción de la Corte Penal Internacional; apoderamiento ilícito de aeronaves/buques; violación; delitos ambientales; robo organizado o a mano armada; sabotaje; participación en una organización criminal involucrada en uno o más delitos enumerados anteriormente.

Estas excepciones a la prohibición de los sistemas de identificación biométrica como punto de partida son de tal amplitud que existía un riesgo evidente de que lo excepcional fuera precisamente la prohibición. El texto definitivo reduce, por un lado, el listado de infracciones inicial de forma considerable (justamente a la mitad). Quedan al margen muchos de los delitos contemplados en la Decisión Marco 2002/584/JAI que tienen en común su carácter patrimonial o económico (fraudes, estafas, falsificaciones, etc.), manteniéndose en esencia los delitos más relacionados con bienes jurídicos como la vida, la libertad, la integridad, la libertad e indemnidad sexuales, etc. Por otro lado, se ha aumentado el umbral punitivo justificativo de los tres a los 4 años de duración. En todo caso, el listado resulta todavía excesivamente amplio en nuestra opinión considerando el elevado número de personas que pueden verse afectadas por la vigilancia e identificación biométrica de forma indiscriminada y puede derivar en desproporcionalidad.

En su descargo hay que matizar que se trata de un objetivo o finalidad justificativa, pero no por sí mismo legítimo, pues han de darse otras muchas condiciones y requisitos al objeto de asegurar la proporcionalidad de la medida.

2. Principio de proporcionalidad.

El alcance de los objetivos legítimos indicados a través de los sistemas de identificación biométrica ha de sujetarse a determinados presupuestos en aras de garantizar su proporcionalidad tal como exige el art. 52.1 CDFUE[24]. Concretados los primeros, el texto de la Ley de IA fija, a su vez, una serie de criterios orientados sin duda a que sirvan a la ponderación de la proporcionalidad de dicho uso en el caso concreto. Así, el apartado 2 del art. 5 dispone que los sistemas de identificación biométrica que nos ocupan, prohibidos en principio, "sólo podrán desplegarse" conforme a los legítimos objetivos analizados y para confirmar la identidad de la persona que constituya el objetivo específico teniendo en cuenta, para ello, una serie de aspectos.

Por un lado, la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema. Por otro lado, las consecuencias que la utilización del sistema tendría para los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias. Nos

24 Dice así el precepto: "Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás".

encontramos ante criterios de ponderación que resultan habituales en el juicio sobre la proporcionalidad de la medida[25].

El art. 5.2 hace igualmente referencia expresa a la proporcionalidad en las condiciones de uso de los sistemas de identificación biométrica remota y de forma también expresa se citan en el mismo con gran acierto las limitaciones temporales, geográficas y personales[26]. En efecto, resulta obvio que si han de ponderarse las consecuencias que para los derechos y libertades de los ciudadanos se han de derivar de los sistemas de identificación biométrica (gravedad, probabilidad y magnitud) la fijación de límites temporales a su uso resulta determinante, pues mayor será la incidencia cuanto más se extienda cronológicamente la aplicación de aquéllos (mayor será el número de personas que transiten en dicho espacio de acceso público). Igualmente trascendental resulta la necesidad de establecer limitaciones al espacio de acceso público afectado (geográficas). Ello obliga a no utilizar de forma indiscriminada desde una visión espacial los sistemas de identificación biométrica, sino limitar su uso a los espacios en los que indiciariamente pudieran hallarse las víctimas o personas desaparecidas o donde pudieran localizarse también indiciariamente las personas sospechosas de haber cometido los delitos arriba relacionados o los espacios correspondientes a las infraestructuras críticas concretas afectadas. Las limitaciones que proceden desde el ámbito subjetivo también resultan significativas. Si la víctima, persona desaparecida o presunto autor del delito cuya identidad biométrica se pretenda establecer presentan determinadas características o rasgos específicos, el sistema de IA se debería limitar a centrarse en aquellas personas físicas que presentan tales rasgos descartando las restantes respecto de las cuales no se procederá a la obtención de la plantilla biométrica correspondiente, ni a la comparación con los datos biométricos almacenados previamente.

Al hilo de lo anterior, resulta igualmente esencial a efectos de ponderar la proporcionalidad de la medida, la expresa obligación que condiciona la autorización del uso de los sistemas de identificación biométrica remota a que las autoridades competentes para la represión penal realicen con carácter previo a su aplicación una evaluación de impacto relativa a los derechos fundamentales (art. 5.2.III). El art. 27 de la Ley de IA ya contempla con carácter general la obligación que corresponde al implementador de sistemas de IA de alto riesgo de llevar a cabo una evaluación de impacto relativa a la protección de datos impuesta por el art. 35 del RGPD y el art.

25 Estos criterios ya existen en nuestro ordenamiento procesal penal bajo la denominación de los principios de excepcionalidad y necesidad y con análogo significado (art. 588 bis.a.5 LECrim).

26 Iglesias Canle, I.C.: "Registros biométricos y su aplicación al proceso penal en España e Italia", en AA.VV.: *Inteligencia Artificial legal y Administración de Justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Aranzadi, Cizur Menor, 2022, p. 348.

27 de la Directiva (UE) 2016/680[27]. Ahora, se incorpora en el texto definitivo una nueva obligación de evaluar en el uso de sistemas de identificación biométrica el impacto, no sólo respecto de la protección de datos, sino que de forma conjunta a esta, respecto de los "derechos fundamentales", contemplada en el art. 27 de la Ley de IA. Esta evaluación de impacto ha de realizarse con anterioridad a la implementación del sistema. También se ha de proceder por parte de las autoridades competentes en la persecución penal al registro del sistema en la base de datos de la UE para sistemas de alto riesgo contemplados en el Anexo III (art. 49 Ley de IA). El art. 5.2.III contempla como única salvedad que en casos de urgencia debidamente justificados, podrá comenzarse a usar el sistema, sin perjuicio de que se proceda al registro posteriormente sin demora indebida.

3. Autorización judicial o de una autoridad administrativa independiente.

Junto a los requisitos hasta ahora señalados, añade el art. 5.3 como justificativo del mismo, que cualquier uso concreto de un sistema de identificación biométrica remota "en tiempo real" en un espacio de acceso público con fines represivos "estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente del Estado miembro donde vaya a utilizarse dicho sistema". Aunque el texto constitucional español no imponga expresamente la reserva jurisdiccional para este tipo de actuaciones, no cabe duda de que se ha pretendido con la exigencia de dicha autorización judicial establecer un marco de garantías suficiente ante la entidad de las injerencias en un amplio grupo de afectados. Las dudas surgen a la hora de concretar qué órgano jurisdiccional concreto será el competente para autorizar, en su caso, el empleo de los sistemas de identificación biométrica que nos ocupan.

En efecto, algunas de las finalidades que legitiman el uso de tales sistemas tienen indudablemente una clara naturaleza procesal penal. Así la búsqueda selectiva de víctimas de los delitos graves citados más arriba o la localización e identificación de personas sospechosas de haber cometido los delitos que figuran en el Anexo II de la Ley de IA. Siendo esto así, la autorización podría corresponder al órgano jurisdiccional del orden penal que resulte competente, es decir, usualmente el Juez de Instrucción o el Juez Central de Instrucción pues algunos de los delitos del Anexo II se encuadrarían en el listado de los del art. 65 LOPJ competencia de la Audiencia Nacional. Sin embargo, otras finalidades legitimadoras se corresponden con una naturaleza preventiva de carácter administrativo, así la búsqueda de

27 Para ello se utilizará, dice el mencionado precepto, la información facilitada conforme al art. 13 de la Ley de IA, también relativo a los sistemas de IA de alto riesgo (transparencia y comunicación de información a los implementadores). Vid. con carácter general sobre la evaluación de impacto Miralles López, R.: "La evaluación de impacto relativa a la protección de datos (comentario al artículo 35 RGPD)", en AA.VV.: *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, (dir. por A. Troncoso Reigada), Tomo I, Civitas, Cizur Menor, 2021, pp. 2137-2162.

personas desaparecidas no relacionadas con un hecho delictivo o la prevención de amenazas de terrorismo u otras graves cuando sean específicas, importantes e inminentes. Ya se ha visto que los fines de aplicación de la ley ("law enforcement"), tal como vienen definidos en la Ley de IA, comprenden un amplio abanico de actividades que van desde la prevención del delito hasta su enjuiciamiento y ejecución, pero incluye también la protección y prevención frente a amenazas para la seguridad pública [art. 3 (46)]. De naturaleza administrativa algunas, por lo tanto, y procesal penal otras. Igual amplitud encontramos en la definición de autoridades encargadas de la aplicación de la ley, que ostentan una u otra naturaleza dependiendo de las funciones que tengan atribuidas.

En el caso de que una autoridad jurisdiccional debiera de autorizar el empleo de sistemas de identificación biométrica remota que se vincula con fines preventivos, podría corresponder dicha competencia a los Juzgados de lo Contencioso-administrativo, que ya cuentan en la actualidad con facultad para autorizar la entrada en domicilios u otros edificios cuyo acceso requiera el consentimiento de su titular para la ejecución forzosa de actos de la Administración (art. 91.2 LOPJ).

La alternativa a la autorización judicial podría ser, según el texto de la Ley de IA, la autorización previa de una "autoridad administrativa independiente" del Estado miembros donde vaya a utilizarse el sistema en cuestión. Aunque pareciera un contrasentido calificar como independiente a una autoridad administrativa, lo cierto es que no constituye para nada una realidad absolutamente extraña. En materia de protección de datos, sin ir más lejos, se exige que en cada Estado miembro de la UE exista una autoridad de control independiente, que no deja de tener naturaleza administrativa. La LO 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, dispone sobre este punto que "la Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal" (art. 44.1)[28]. No con ello queremos sugerir que estas autoridades de control independiente sean las más adecuadas para autorizar el uso de sistemas de identificación biométrica remota en casos puntuales. Ya tienen reconocidas otras facultades importantes en la materia que nos ocupa.

En el ordenamiento jurídico español bien podrían satisfacer esa condición de autoridad administrativa independiente las Comisiones de Videovigilancia contempladas en la LO 4/1997, de videovigilancia en espacios públicos por las FF. y CC. de Seguridad. Se trata esta Comisión de un órgano colegiado presidido por un Magistrado (art. 3.1) que ha de ser el Presidente del Tribunal Superior de

28 Las autoridades administrativas independientes de ámbito estatal están mencionadas en la Ley 40/2015, de Régimen Jurídico del Sector Público y son definidas como "entidades de derecho público que, vinculadas a la Administración General del Estado y con personalidad jurídica propia, tienen atribuidas funciones de regulación o supervisión de carácter externo sobre sectores económicos o actividades determinadas, por requerir su desempeño de independencia funcional o una especial autonomía respecto de la Administración General del Estado, lo que deberá determinarse en una norma con rango de Ley" (art. 109).

Justicia de la Comunidad Autónoma respectiva (art. 3.2) y en "cuya composición no serán mayoría los miembros dependientes de la Administración autorizante" (art. 3.1). La composición y funcionamiento de la Comisión, así como la participación de los municipios en ella, se determinan reglamentariamente, y en la medida en que determinadas Comunidades Autónomas tienen competencias en materia de seguridad pública, dicha composición es diversa en cada caso, pero respetando en la misma el requisito de no resultar mayoría la administración autorizante. Estas Comisiones no autorizan el uso de sistemas de videovigilancia, sino que informan al respecto de modo preceptivo y vinculante (art. 3.3). Aunque estas Comisiones de Videovigilancia pudieran satisfacer la demanda de ser autoridad independiente[29], no por ello desaparecerían todos los inconvenientes que se plantean si trasladamos este escenario al contexto de la identificación biométrica remota sin las oportunas reformas legales. Ya hemos visto, por ejemplo, que la Ley de IA contempla una definición muy amplia de los espacios de acceso público que incluyen incluso los de naturaleza privada o los que sirven para fines muy diversos (ocio, mercantiles, etc.). La LO 4/1997 contempla una definición mucho más restrictiva de tales espacios, de los que se excluyen, entre otros muchos, los privados.

La autorización arriba indicada irá precedida de una solicitud de la autoridad competente para la aplicación de la ley ("law enforcement") conforme a las normas detalladas del derecho nacional interno a las que haremos referencia después. Sin embargo, cuando en casos de urgencia no sea posible obtener dicha autorización[30], podrá comenzar a hacerse uso de los sistemas de identificación biométrica remota sin la misma, siempre y cuando sea solicitada aquélla a la mayor brevedad y en todo caso antes de las 24 horas. Si fuera denegada la autorización, se procederá inmediatamente a interrumpir el uso de los sistemas de identificación biométrica y a desechar suprimir todos los datos y resultados de salida que se hayan obtenido (art. 5.3.I)[31]. La solicitud de las autoridades competentes en la aplicación de la ley

29 Ver acerca de las Comisiones de Videovigilancia: De la Iglesia Chamarro, A.: "Las Comisiones de Garantías de la Videovigilancia", *Revista de Derecho Político*, 2007, núm. 68, pp. 217; Etxeberria Guridi, J.F.: "La Comisión de Videovigilancia y Libertades del País Vasco: funciones y experiencias", en AA.VV.: *Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de los datos personales*, (dir. por J.F. Etxeberria Guridi), Tirant lo Blanch, Valencia, 2011, pp. 107-142.

30 Se refieren los considerandos como tales a las situaciones en las que "la necesidad de utilizar los sistemas en cuestión sea tan imperiosa que imposibilite, de manera efectiva y objetiva, obtener una autorización antes de iniciar el uso". Aunque no lo diga expresamente la Ley de IA en su articulado, sí se especifica en los considerandos, cerrando al máximo los resquicios a una actuación inadecuada, que en la solicitud de autorización ex post habrán de indicar los motivos por los que no se ha realizado la solicitud con anterioridad. Además, para estas situaciones de urgencia, el uso de tales sistemas de IA debería limitarse "al mínimo imprescindible" y cumplir las salvaguardias y las condiciones oportunas, conforme a lo estipulado en el Derecho interno y según corresponda en cada caso concreto de uso urgente por parte de las autoridades encargadas de la aplicación de la ley [considerando (35)].

31 La expresión "todos los datos", viene a significar todos los vinculados con el uso del sistema concreto cuya autorización ha sido denegada, así los datos de entrada directamente obtenidos mediante el uso del sistema de IA en cuestión y los resultados y datos de salida directamente vinculados con la autorización denegada. Quedarían excluidos de esta drástica solución los datos de entrada que hubieran sido legalmente adquiridos conforme a otra norma nacional o de la UE [considerando (35)]

ha de ser motivada, pues se habrá de justificar la concurrencia de los requisitos por los que un uso prohibido en principio resulta admisible. Por las mismas razones habrá de ser motivada la autorización judicial o de la administración independiente, aunque no se diga nada al respecto[32]. Lo que sí queda claro de forma reiterada en la versión definitiva del texto es el carácter vinculante de la decisión que adopte la autoridad judicial o la administrativa independiente.

Aunque no resulte precisa ninguna otra autorización, sí se requiere a efectos de transparencia (gobernanza) la intervención de otras autoridades. En concreto, dispone el art. 5.4 que cada uso que de sistemas de identificación biométrica remota se haga se deberá notificar a las respectivas, autoridad nacional de protección de datos, por un lado, y autoridad nacional de vigilancia del mercado, por otro. Estas autoridades habrán, a su vez, de remitir anualmente un informe a la Comisión respecto de los usos de sistemas de identificación biométrica remota en espacios públicos que les hayan sido notificados. A su vez, la Comisión publicará informes anuales al respecto (art. 5.6).

4. La previsión legislativa en el Derecho interno.

La primera de las garantías que contempla el art. 52.1 CDFUE a los efectos de que resulte admisible cualquier limitación en el ejercicio de los derechos y libertades reconocidos por dicha Carta, es que la misma esté establecida por la ley. El texto de la Ley de IA parte, como se ha dicho, de la prohibición del uso de los sistemas de identificación biométrica remota a que nos referimos, pero fija a continuación una serie de requisitos y condiciones que pueden excepcionar dicha prohibición. El art. 5 que hemos ido analizando hasta ahora constituye el marco regulatorio en el que tienen cabida las salvedades a la prohibición general. Constituiría un marco de máximos, que en principio no podría ser rebasado por el ordenamiento concreto de cada Estado miembro, pero que deja a éstos un margen de actuación soberano dentro de aquellos límites. De ahí que la Ley de IA apremie a los Estados miembros a que aborden la regulación de la materia ajustando cada uno la misma a sus particularidades normativas e institucionales. El apremio es, por otra parte, específico. No se trata de regular la materia, sino de que se dote en cada caso de las "reglas detalladas necesarias" (art. 5.5).

32 El deber de motivación se deriva de los requisitos que condicionan la concesión de la autorización según el texto de la Ley, esto es, que con fundamento en las pruebas objetivas o los indicios claros expuestos ante la autoridad judicial o administrativa, se acredita que el uso del sistema de identificación biométrica remota en cuestión resulta necesario y proporcionado para alcanzar algunos de los objetivos legítimos especificados en el apartado 1 y determinados en la solicitud, y en particular que queda limitada a lo que resulte estrictamente necesario en relación al alcance temporal, geográfico y personal. La ley impone igualmente que la autoridad competente para la autorización considere en su decisión las circunstancias y criterios mencionados en el apartado 2 -gravedad, probabilidad y alcance de los perjuicios de no emplear el sistema de IA en cuestión; gravedad, probabilidad y alcance de los perjuicios en los derechos y libertades de las personas afectadas, etc.- (art. 5.3.II).

La primera expresión del margen de actuación autónoma de los Estados miembros reside en la opción de incorporar o no el posible uso de los sistemas de identificación biométrica remota en el ordenamiento interno. Comienza el precepto mencionado indicando que los Estados miembros "podrán decidir contemplar la posibilidad de autorizar" el uso de sistemas de identificación biométrica remota. Más contundente, afirma el considerando (37) que aquéllos "siguen siendo libres de no ofrecer esa posibilidad en absoluto". Si los Estados miembros optan en su ordenamiento por incorporar la posibilidad excepcional contemplada en la Ley de IA, mantienen igualmente el margen de actuación para decidir si lo hacen en toda su extensión o "parcialmente", como también contempla el texto de la Ley. En cualquier caso, esa libertad de opción no puede exceder, como se ha dicho, del marco permisivo de la Ley de IA, esto es, "dentro de los límites y en las condiciones que se indican en los apartados 1.h), 2 y 3". Las "reglas detalladas" del derecho interno habrán de especificar respecto de cuales objetivos legítimos a perseguir del apartado h) -búsqueda selectiva de víctima, de persona desaparecida, etc.- podrán las autoridades competentes autorizar el uso de sistemas de identificación biométrica remota, y respecto de cuales delitos mencionados en el subapartado iii). Esas mismas "reglas detalladas" habrán de especificar, igualmente, los pormenores del procedimiento de solicitud, concesión y ejercicio de las autorizaciones concedidas, así como lo relativo a la supervisión y notificación relacionadas con aquéllas.

Hacemos hincapié, con el entrecomillado, en la exigencia de una regulación pormenorizada en el derecho nacional de los Estados miembros. Esta es una cuestión que se le resiste con frecuencia al legislador español[33], que usualmente regula lo relativo a la necesaria previsión legal de actuaciones restrictivas de derechos y libertades con retraso y al albur de previa jurisprudencia de los tribunales[34]. E insistimos en ello, precisamente, porque no podemos sustraernos al deber de denunciar que el único precepto que actualmente podría resultar aplicable en este sentido en cumplimiento de la exigencia de previsión legal habilitante, no puede estimarse que cumple con tales exigencias de precisión y suficiencia, ni para el caso concreto que analizamos ahora -identificación biométrica remota-, ni para ningún otro.

Nos referimos a la lamentable disposición que sobre el uso de datos biométricos se contempla en la LO 7/2021, de protección de datos personales tratados para fines de prevención y represión penal. El art. 13 de dicha LO, relativo al tratamiento

33 Se trata ésta de una exigencia particularmente destacada en la materia que nos ocupa. Vid. Cotino Hueso, L.: "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial. Los altos estándares que exigen el Tribunal Constitucional alemán y otros tribunales, que no se cumplen ni de lejos en España", *Revista General de Derecho Administrativo,* 2023, núm. 63, pp. 1-22.

34 Ejemplo ilustrativo, la LO 13/2015, de 5 de octubre, que modifica la LECrim para regular medidas de investigación tecnológicas.

de categorías especiales de datos personales -entre los que se incluyen los datos biométricos dirigidos a identificar de manera unívoca a una persona física-, dispone que dicho tratamiento "sólo se permitirá" cuando resulte estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado y cuando se cumplan alguna de las circunstancias que se mencionan, entre las que se incluye que se "encuentre previsto por una norma con rango de ley o por el Derecho de la Unión Europea". Esta es una reproducción literal de la exigencia de previsión legal contemplada en el art. 10 de la Directiva (UE) 2016/680. Por ese mismo motivo estimamos que resulta absolutamente insuficiente, y una parodia a la exigencia de regulación detallada, la previsión contemplada en el apartado 2 del precepto indicado cuando dispone que "las autoridades competentes, en el marco de sus respectivas funciones y competencias, podrán tratar datos biométricos dirigidos a identificar de manera unívoca a una persona física con los fines de prevención, investigación, detección de infracciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública"[35].

Queda pendiente, por lo tanto, de perfilar cuál es la opción del legislador español en cuanto al uso de los sistemas de identificación biométrica remota, una vez denunciada la insuficiente previsión del art. 13.2 LO 7/2021 contemplada desde las exigencias reclamadas por el art. 5.5 de la Ley de IA. Con qué extensión pretende que resulten admisibles los sistemas de identificación biométrica en el marco, siempre, de lo previsto en la Ley de IA. En todo caso, procede ahora ya señalar que la libertad limitada reconocida a los Estados miembros a la hora de regular la materia puede derivar en una regulación jurídica dispar en los distintos Estados miembros y resultar un inconveniente desde el punto de vista de la cooperación judicial en materia penal y del reconocimiento mutuo de resoluciones judiciales -sería el caso de la orden europea de investigación, que podría experimentar asimetrías desde el punto de vista de los derechos fundamentales afectados y de la posibilidad o no de restricciones en los mismos-.

V. BREVES CONCLUSIONES.

Los sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley (penal) repercuten sobremanera en un amplio abanico de derechos fundamentales y conllevan aparejados elevados riesgos de actuación sesgada y discriminatoria. Ante esta tesitura, la recientemente aprobada Ley de IA está llamada a desempeñar un papel esencial. Reflejo de la situación descrita, ha quedado patente la distinta sensibilidad para con los derechos de los ciudadanos afectados entre las distintas instituciones europeas llamadas a

35 Vid. igualmente al respecto las críticas de Suárez Xavier, P.R.: *Informe sobre aspectos bioéticos, legales y procesales del derecho a la intimidad y el uso de procedimientos de reconocimiento facial por las fuerzas y cuerpos de seguridad*, Colex, Madrid, pp. 68 y ss.

participar en el procedimiento legislativo. La posición del Parlamento Europeo ha resultado esencial, poniendo freno a las iniciales propuestas de la Comisión y del Consejo al respecto.

Como resultado de los riesgos expresados, la Ley de IA europea adopta como punto de partida la prohibición del uso de los sistemas de identificación biométrica señalados. Sin embargo, esta prohibición no es absoluta y en el marco de determinados presupuestos y conforme a los principios de estricta necesidad y proporcionalidad puede resultar admisible. Ha de entenderse que los límites fijados en la Ley de IA para que el uso de tales sistemas resulte admisible han de considerarse de máximos y que corresponde a los Estados miembros concretar en cada ordenamiento y mediante "reglas detalladas" los criterios y parámetros mencionados. Esta cuestión resulta esencial, bajo el riesgo de que la regla general de la prohibición se pervierta y se convierta en excepción.

BIBLIOGRAFIA

Arzoz Santisteban, X: "Videovigilancia y derechos fundamentales", en AA.VV.: *Videovigilancia: Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de datos personales* (dir. por J.F. Etxeberria Guridi), Tirant lo Blanch, Valencia, 2011.

Buolamwini, J. y Gebru, T.: "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classication", *Proceedings of Machine Learning Research*, 2018, núm. 81.

Cano Ruiz, I.: "Artículo 9. Categorías especiales de datos", en AA.VV.: *Protección de Datos: Comentarios a la Ley Orgánica de Protección de Datos y Garantías Digitales (en relación con el RGPD)* (dir. por M. Arenas Ramiro y A. Ortega Giménez), Sepín, Madrid, 2019.

Cotino Hueso, L.: "Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos", en AA.VV.: *Derecho Público de la Inteligencia Artificial* (coord. por F. Balaguer Callejón y L. Cotino Hueso), Fundación Manuel Giménez Abad, Madrid, 2023.

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

De la Iglesia Chamarro, A.: "Las Comisiones de Garantías de la Videovigilancia", *Revista de Derecho Político,* 2007, núm. 68.

Escajedo San-Epifanio, L.: *Tecnologías biométricas, identidad y derechos fundamentales,* Aranzadi, Cizur Menor, 2017.

Etxeberria Guridi, J.F.: "La Comisión de Videovigilancia y Libertades del País Vasco: funciones y experiencias", en AA.VV.: *Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de los datos personales* (dir. por J.F. Etxeberria Guridi), Tirant lo Blanch, Valencia, 2011.

European Union Agency for Fundamental Rights (FRA): *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020.

Fernández Hernández, C.: "La nueva estrategia europea sobre el dato y la inteligencia artificial. Foto fija de un diseño en evolución", *Derecho Digital e Innovación*, 2020, núm. 5.

Grother, P.; Ngan, M. y Hanaoka, K.: *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*, U.S. Department of Commerce, 2019, [https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf].

Guzmán Fluja, V.: "Sobre la aplicación de la inteligencia artificial a la solución de conflictos", en AA.VV.: *Justicia civil y penal en la era global* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2017.

Iglesias Canle, I.C.: "Registros biométricos y su aplicación al proceso penal en España e Italia", en AA.VV.: *Inteligencia Artificial legal y Administración de Justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Aranzadi, Cizur Menor, 2022.

Martínez Martínez, R.: "Inteligencia artificial desde el diseño", *Revista catalana de dret públic*, 2019, núm. 58.

Miralles López, R.: "La evaluación de impacto relativa a la protección de datos (comentario al artículo 35 RGPD)", en AA.VV.: *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (dir. por A. Troncoso Reigada), Tomo I, Civitas, Cizur Menor, 2021.

Richard González, M.: "Los sistemas biométricos de reconocimiento facial en la Unión Europea en el marco del desarrollo de la Inteligencia Artificial", *Justicia*, 2023, núm. 1.

Romeo Casabona, C.M.: "Datos personales (comentario al artículo 4.1 RGPD)", en AA.VV.: *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (dir. por A. Troncoso Reigada), Tomo I, Thomson-Aranzadi, Cizur Menor, 2021.

Suárez Xavier, P.R.: *Informe sobre aspectos bioéticos, legales y procesales del derecho a la intimidad y el uso de procedimientos de reconocimiento facial por las fuerzas y cuerpos de seguridad*, Colex, Madrid.