UNIVERSIDAD DE MURCIA

http://revistas.um.es/analesderecho

ANALES de DERECHO

ANÁLISIS JURÍDICO DEL USO DE LA INTELIGENCIA ARTIFICIAL EN EL RECONOCIMIENTO DE PATRONES BIOMÉTRICOS

Aplicaciones en la lucha contra la criminalidad y sus límites

SUSANA JIMÉNEZ LÓPEZ

Investigadora predoctoral, Universidad de Lleida

ANDREA PLANCHADELL GARGALLO

Catedrática de Derecho Procesal, Universidad Jaume I

CAROLINA VILLACAMPA ESTIARTE

Catedrática de Derecho Penal, Universidad de Lleida

SERVICIO DE PUBLICACIONES

UMU

Análisis jurídico del uso de la inteligencia artificial en el reconocimiento de patrones biométricos: aplicaciones en la lucha contra la criminalidad y sus límites

Resumen

El objetivo principal de este trabajo es analizar el uso de la inteligencia artificial en el reconocimiento de patrones biométricos como herramienta para prevenir, detectar y combatir la criminalidad. El estudio presenta la necesidad de promulgar una regulación que garantice la optimización de la tarea policial mediante el uso de estos sistemas, sin menoscabar los derechos fundamentales y preservando el derecho al habeas data. Asimismo, se expone la conveniencia de depositar la responsabilidad del tratamiento de los datos biométricos utilizados en este ámbito en las autoridades policiales y judiciales, como garantes de la seguridad pública.

Palabras clave: *Inteligencia Artificial, reconocimiento de patrones biométricos, habeas data, raspado de imágenes.*

"Legal analysis of the use of artificial intelligence in biometric pattern recognition: applications in the fight against crime and their limits"

Abstract

The major aim of this research is analysing the use of artificial intelligence in biometric pattern recognition as a tool to forestall, detect and fight against crime. The study highlights the need of enacting a regulation that ensures the optimisation of the police task by using the aforementioned systems. Crucially, such regulation must guarantee the protection of fundamental rights, as well as the right to habeas data. In this line, the convenience of allocating the liability of biometric data treatment used in this field in the law enforcement and judicial authorities, as guarantors of public security, is presented.

Keywords*: Artificial Intelligence, biometric pattern recognition, habeas data, image scraping.*

I. INTRODUCCIÓN.

La irrupción de la inteligencia artificial (en adelante IA) en nuestro día a día es una realidad a la que, poco a poco, nos vamos habituando, con mayor o menor entusiasmo[1]. A diario nos llegan noticias sensacionalistas sobre la aplicación de herramientas de IA en diferentes aspectos de nuestra cotidianeidad, presentándola como una tecnología incomprensible e impredecible, de manera que se genera oposición y recelo a su uso. Paralelamente, las grandes corporaciones se están aprovechando de la dependencia tecnológica de la sociedad actual para capturar y tratar nuestros datos con el objetivo de provocar sutiles modificaciones en nuestra manera de pensar o actuar, sin que ni tan siquiera seamos conscientes de ello, constituyendo una injerencia inaceptable en nuestras vidas[2].

[1] BARONA VILAR, S., "Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia", *Revista Jurídica Digital UANDES, volumen 3, núm. 1*, 2019, pp. 1-17.

[2] El Tribunal de Justicia de la Unión Europea (en adelante TJUE) en su sentencia, C-446/21, de 4 de octubre de 2024, resolvió la cuestión prejudicial planteada por el Tribunal Supremo de lo Civil y Penal de Austria sobre la interpretación de los artículos 5, 6 y 9 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, en adelante RGPD), en relación con el supuesto tratamiento ilícito por parte de Facebook Ireland Ltd. (actualmente Meta Platforms Ireland Ltd.) de los

La ausencia de transparencia, información y un marco regulatorio sólido en la implementación de la IA provoca desconfianza social y en ocasiones rechazo.

Sin embargo, se trata de una herramienta con un enorme potencial que puede aportar numerosos beneficios, entre otros, en el ámbito del sistema de justicia penal[3], tal y como en su momento lo hicieron otros avances científico-tecnológicos, como el análisis de huellas dactilares o el estudio del ADN que han sido, en ocasiones, determinantes para esclarecer crímenes o identificar a víctimas, incluso años después de que los casos hubieran sido archivados por no disponer de indicios para seguir la línea de investigación acertada[4]. En esta línea, el desarrollo de sistemas de reconocimiento de patrones biométricos mediante tecnología de IA puede contribuir tanto a resolver investigaciones, identificando a los sospechosos de la comisión de hechos delictivos ya cometidos, como a la prevención y disuasión de futuras conductas criminales[5].

Por este motivo, en este trabajo se aborda el uso de la IA en el reconocimiento de patrones biométricos para combatir la criminalidad, estudiando e intentando alumbrar dónde deberían establecerse los límites para poder aprovechar las ventajas que aportan estas técnicas, sin que supongan un ataque a los derechos fundamentales.

Para ello se procede, inicialmente, al estudio de la catalogación de los datos biométricos como datos personales de categoría especial. A continuación, se examina la regulación

datos personales de un usuario, el cual, después de revelar públicamente su orientación sexual en una mesa redonda, comenzó a recibir publicidad basada en esta información a través de Facebook. Esta sentencia se encuentra disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62021CJ0446.

El TJUE declaró que el artículo 5.1.c) del RGPD debe interpretarse en el sentido de que el principio de "minimización de datos" no autoriza a un responsable del tratamiento de datos, como lo es una operadora de una red social en línea, a agregar, analizar y tratar datos obtenidos del interesado de la misma plataforma, o fuera de ella, para proponer publicidad específica, sin limitación temporal y sin distinción respecto a la naturaleza de esos datos.

Asimismo, el TJUE resolvió que el artículo 9.2.e) del RGPD "debe interpretarse en el sentido de que el hecho de que una persona se haya manifestado sobre su orientación sexual en una mesa redonda abierta al público no autoriza al operador de una plataforma de red social en línea a tratar otros datos relativos a la orientación sexual de esa persona obtenidos, en su caso, fuera de dicha plataforma a partir de aplicaciones y de sitios de Internet de terceros asociados, con el fin de agregar y de analizar tales datos para proponerle publicidad personalizada".

[3] MIRÓ LLINARES, F., "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología, núm. 20*, 2018, pp. 87-130.

[4] DÍAZ RODRÍGUEZ, V., "Sistemas biométricos en materia criminal: un estudio comparado", *Revista IUS, volumen 7, núm. 31*, 2013, pp. 28-47.

[5] JAIN, A. K. y ROSS, A., "Cerrando la brecha: de la biometría a la ciencia forense", *Philosophical Transactions of the Royal Society B: Biological Sciences, volumen 370, núm. 1674*, 2015, ID: 20140254.

actualmente existente a nivel europeo sobre el tratamiento de datos biométricos mediante aplicaciones de IA, haciendo especial referencia al recién aprobado Reglamento de Inteligencia Artificial[6] (en adelante AIA, por *Artificial Intelligence Act*) y ahondando en el uso automatizado de patrones biométricos. Seguidamente, se analiza la transposición de la normativa europea al régimen jurídico español y, partiendo de sus deficiencias, se presenta la conveniencia de promulgar una normativa estatal con rango de Ley Orgánica para regular el uso de patrones biométricos orientada a combatir la criminalidad, apuntando las líneas que esta ley debería abordar para ofrecer seguridad jurídica a las fuerzas del orden en el uso de esta tecnología, al tiempo que se garanticen los derechos fundamentales. Finalmente, se analizan los sistemas de reconocimiento facial mediante herramientas de raspado de imágenes en la red, por ser un ejemplo especialmente controvertido.

II. CONCEPTO DE DATOS BIOMÉTRICOS Y SU CATALOGACIÓN COMO DATOS PERSONALES DE CATEGORÍA ESPECIAL.

El Parlamento Europeo y el Consejo de la Unión Europea han definido[7] los datos biométricos como "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

De este modo, para discernir si estamos ante un dato biométrico se deberán tener en cuenta tres factores: la naturaleza de los datos (características físicas, fisiológicas o de conducta), la forma de obtención (a partir de un tratamiento técnico específico) y la finalidad (la identificación única de una persona)[8].

Dicho esto, cuando hablamos de datos biométricos, en todo caso, nos estamos refiriendo a datos catalogados como personales, que el Parlamento Europeo y el Consejo han

[6] Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

[7] Artículo 4.14 del RGPD.

[8] SANTISTEBAN GALARZA, M., "Reconocimiento facial y protección de datos: una respuesta provisional a un problema pendiente", *Revista de Derecho de la UNED, núm. 28*, 2021, pp. 499-526.

definido —artículo 3.1 de la Directiva (UE) 2016/680 y artículo 4.1 del RGPD— como "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos 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". En este contexto, hay que tener en cuenta que el tratamiento de datos biométricos no solo puede suponer una importante intromisión en la privacidad de las personas por la naturaleza de los datos[9], sino también porque éstos son permanentes[10].

De acuerdo con la definición de datos biométricos y conforme a lo señalado en el "Libro Blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza"[11] de la Comisión Europea, estos datos pueden emplearse con dos finalidades distintas[12]. En primer lugar, para la identificación, es decir, mediante un tratamiento técnico se crea una plantilla de los datos biométricos de la persona a identificar y esta se compara con otras plantillas almacenadas en una base de datos ("uno-a-varios"), con el objetivo de determinar su identidad entre varias posibles. Y, en segundo lugar, para la

[9] Según la "teoría del mosaico de la privacidad" múltiples injerencias menores en la privacidad de los individuos cuando se relacionan entre sí (como sucede con el tratamiento de datos en la era de la tecnología) y se perlongan en el tiempo deben valorarse en su conjunto, como un mosaico, ya que de esta manera pueden suponer una intensa afectación a la privacidad. Véase: BELLOVIN, S. M., HUTCHINS, R. M., JEBARA, T. y ZIMMECK, S., "When enough is enough: Location tracking, mosaic theory, and machine learning", *New York University Journal of Law & Liberty*, *volumen 8, núm. 51*, 2013, pp. 556-628.

[10] GARTLAND, C., "Biometrics Are a Grave Threat to Privacy", artículo publicado en la versión digital del diario *The New York Times*, en la sección *The Opinion Pages*, 5 de julio de 2026, disponible en: https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy.

[11] Libro Blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza de la Comisión Europea, Bruselas, 19.2.2020, COM(2020) 65 final, p. 26:

"En lo que se refiere al reconocimiento facial, por «identificación» se entiende que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella. La «autenticación» (o «verificación»), por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; así, las dos plantillas se comparan para determinar si la persona de las dos imágenes es la misma. Este procedimiento se emplea, por ejemplo, en las puertas de control automatizado de fronteras empleadas en los controles fronterizos de los aeropuertos."

[12] LYNCH, N., "Facial Recognition Technology in Policing and Security—Case Studies in Regulation", *Laws, volumen 13, núm. 3*, 2024, 35.

verificación o autenticación, que consiste en cotejar la plantilla biométrica del individuo con una única referencia previamente registrada ("uno-a-uno"), a fin de corroborar su identidad[13].

Pues bien, establecida esta diferenciación en el uso de los datos biométricos, cabe señalar que hasta mayo de 2022 se venía entendiendo que únicamente se consideraban datos biométricos de categoría especial aquellos que estaban dirigidos a la identificación[14].

De esta manera se realizaba una interpretación restrictiva tanto del artículo 9 del RGPD, como del artículo 10 de la Directiva (UE) 2016/680, en virtud de la cual solo se clasifican de categoría especial para su tratamiento a aquellos datos biométricos "dirigidos a identificar de manera unívoca a una persona".

No obstante, diversos autores[15] han cuestionado la solidez de esta distinción. Si analizamos el funcionamiento de un sistema de reconocimiento facial diseñado para verificar la identidad de un individuo —como el acceso a instalaciones o aplicaciones— vemos que en todo caso se está produciendo un tratamiento técnico de datos biométricos para crear una plantilla y compararla. Por lo tanto, en la creación de la plantilla se produce un nuevo tratamiento de datos biométricos, momento que puede derivar en una pérdida de control de la finalidad para la que fueron recopilados y, consecuentemente, se está produciendo una operación sobre categorías especiales de datos personales en los términos del artículo 9.2 del RGPD.

En línea con esta perspectiva, el Comité Europeo de Protección de Datos (en adelante CEPD[16]) en sus Directrices 05/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito policial[17], mantiene la distinción funcional entre verificación e identificación

[13] Así se define en el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del Grupo de Trabajo creado en virtud del artículo 29 de la Directiva 95/46/CE.

[14] La Agencia Española de Protección de Datos en su "Informe de Gabinete Jurídico N/REF: 0036/2020", pág. 17-21, establecía que "con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autentificación biométrica (uno-a-uno)".

[15] SANTISTEBAN GALARZA, M., "Reconocimiento… cit", pp. 499-526; COTINO HUESO, L., "Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal", *El cronista del Estado Social y Democrático de Derecho, núm. 100*, 2022, pp. 68-79.

[16] CEPD o *European Data Protection Board (EDPB)*.

[17] Versión 2.0, adoptada el 26 de abril de 2023, después de someterla a consulta pública.

biométrica. Sin embargo, introduce como novedad relevante que ambas modalidades constituyen un tratamiento de datos personales y, en particular, un tratamiento de categorías especiales de datos personales[18]. Por tanto, su utilización queda en principio prohibida por el artículo 9.1 del RGPD, salvo que concurra alguna de las excepciones dispuestas en el artículo 9.2 que legitime dicho tratamiento.

III. MARCO LEGAL DEL TRATAMIENTO DE LOS DATOS BIOMÉTRICOS EN EL ENTORNO POLICIAL EN LA UNIÓN EUROPEA.

Consciente de la importancia de garantizar la protección del tratamiento de datos personales como un derecho fundamental y teniendo en cuenta los nuevos retos provocados por el desarrollo tecnológico en este ámbito, la Unión Europea consideró necesario establecer una normativa específica que complementara al RGPD en el ámbito penal. Por ello, el 27 de abril de 2016, adoptó paralelamente al mencionado reglamento la Directiva (UE) 2016/680[19], con el fin de regular el tratamiento de datos por parte de las autoridades competentes en la prevención, investigación, detección y enjuiciamiento de infracciones penales.

Posteriormente, ante la expansión de las tecnologías de IA en múltiples entornos, el Parlamento Europeo adoptó en marzo de 2024 el AIA, aprobado por el Consejo en mayo del mismo año. Este reglamento constituye la primera normativa global sobre IA, y específicamente, la primera que regula el uso automatizado de datos biométricos en el ámbito de la prevención e investigación del delito.

A continuación, y partiendo de dicha normativa, se analizará el tratamiento de datos biométricos en el entorno policial europeo. En primer lugar, se abordará la regulación contenida en la Directiva (UE) 2016/680 y las observaciones del CEPD en sus Directrices 05/2022. En segundo lugar, se examinará el AIA como *lex specialis*, en particular respecto al uso de sistemas de IA para la identificación biométrica en tiempo real en

[18] Artículo 12 de las Directrices 05/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito policial: "*While both functions – authentication and identification – are distinct, they both relate to the processing of biometric data related to an identified or identifiable natural person and therefore constitute a processing of personal data, and more specifically a processing of special categories of personal data*".

[19] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

espacios públicos con fines policiales y su aplicación a técnicas de categorización y reconocimiento de emociones.

1. Análisis de la Directiva (UE) 2016/680 respecto al tratamiento de datos biométricos y de las Directrices 5/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley.

Conforme a los considerandos 19 del RGPD y 10 a 12 de la Directiva (UE) 2016/680, el tratamiento de datos biométricos realizado por las autoridades competentes[20] con fines penales[21] —ya sea para la identificación, autentificación o verificación— se rige por el artículo 10 de la Directiva (UE) 2016/680. En los demás casos, resulta de aplicación el RGPD. De este modo, la normativa a aplicar dependerá de la finalidad perseguida (prevención, investigación y enjuiciamiento criminal) y no de la cualidad de los afectados (investigados o terceras personas que puedan ser captadas por estos sistemas)[22].

Asimismo, cabe señalar que el uso de esta tecnología por parte de las empresas de seguridad privada, con carácter general, quedaría fuera de la aplicación de la Directiva (UE) 2016/680, al no ser consideradas como "autoridades competentes" y, atendiendo a la intrusión que puede acarrear para los derechos fundamentales[23], deberían ceñirse a lo dispuesto en el RGPD.

Así pues, el uso de datos biométricos en el entorno policial, con las finalidades mencionadas, estará sujeto a lo establecido en el artículo 10 de la Directiva (UE) 2016/680. Por consiguiente, el tratamiento de categorías especiales de datos personales —como los que revelan "el origen étnico o racial, las opiniones políticas, las convicciones

[20] Entendiendo como tales, según el considerando 11 de la Directiva (UE) 2016/680 "no solo se deben incluir las autoridades públicas tales como las autoridades judiciales, la policía u otras fuerzas y cuerpos de seguridad, sino también cualquier otro organismo o entidad en que el Derecho del Estado miembro haya confiado el ejercicio de la autoridad y las competencias públicas a los efectos de la presente Directiva".

[21] Fuera de estas finalidades y aunque el tratamiento de los datos biométricos sea realizado por las autoridades mencionadas en el anterior epígrafe, y siempre que dicho tratamiento esté comprendido en el ámbito del Derecho de la Unión, será de aplicación lo dispuesto en el RGPD, teniendo en cuenta lo establecido en el considerando 12 de la Directiva (UE) 2016/680.

[22] SANTISTEBAN GALARZA, M., "Reconocimiento…cit", pp. 499-526.

[23] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEDP), "La AEPD analiza en un informe el uso de sistemas de reconocimiento facial por parte de las empresas de seguridad privada", 2020, disponible en: https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/AEPD-informe-sistemas-reconocimiento-facial-empresas-seguridad-privada.

religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física"— solo será admisible cuando resulte estrictamente necesario, cuente con las garantías adecuadas para los derechos y libertades del titular de los datos y únicamente cuando: disponga de autorización expresa del Derecho de la Unión o del Estado Miembro, sea necesario para proteger intereses vitales del interesado o de otra persona física, o cuando los datos hayan sido divulgados manifiestamente por el propio interesado.

En relación con dicho artículo, el CEPD, a través de las Directrices 05/22, formula una serie de observaciones relevantes sobre el uso de tecnologías de reconocimiento facial en el entorno policial, las cuales se sintetizan a continuación.

El tratamiento solo se permitirá cuando concurra el criterio indispensable de la "estricta necesidad"[24], en el sentido de la reiterada jurisprudencia del Tribunal de Justicia de la Unión Europea[25]; es decir en condiciones más restrictivas que las de mera necesidad. De este modo, se requerirá la existencia de "criterios objetivos para definir las circunstancias y condiciones bajo las cuales el procesamiento puede realizarse, excluyendo así cualquier tratamiento de carácter general o sistemático"[26].

El punto 44 de las Directrices 05/22 subraya que el uso de reconocimiento facial en el ámbito policial debe estar regulado por una ley específica que delimite con claridad los tipos delictivos y la gravedad de éstos que pueden justificarlo, excluyendo expresamente

[24] SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (SEPD) o *EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)*, "Manual para la evaluación de la necesidad de las medidas que limiten el derecho fundamental a la protección de datos de carácter personal", 2017, pp. 7-8, disponible en: https://www.edps.europa.eu/system/files/2021-12/17-06-01_necessity_toolkit_es.pdf.

[25] En la sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 30 de enero de 2024, asunto C-118/22, NG contra Direktor na Glavna direktsia Natsionalna politsia pri Ministerstvo na vatreshnite raboti -- Sofia, el TJUE se pronuncia a propósito del procedimiento prejudicial planteado en relación con la protección de las personas físicas en lo que respecta al tratamiento de datos personales para fines de lucha contra las infracciones penales de la Directiva (UE) 2016/680, entre otros, respecto al artículo 10 (tratamiento de los datos biométricos y genéticos y la estricta necesidad). El TJUE declara que la conservación general e indiferenciada de los datos biométricos y genéticos hasta el fallecimiento de las personas condenadas penalmente por un delito doloso para permitir verificar su eventual implicación en otras infracciones penales (sin tomar en consideración ni la naturaleza ni la gravedad del delito que dio lugar a la condena penal firme u otras circunstancias particulares que lo justifiquen) es contraria al Derecho de la Unión, ya que no cumple con el principio de la estricta necesidad. Esta resolución se encuentra disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62022CJ0118.

[26] Punto 73 de las Directrices 05/2022 del CEPD, sobre el uso de la tecnología de reconocimiento facial en el ámbito policial.

los delitos menores. Además, exige[27] que la normativa nacional que transponga el artículo 10 de la Directiva (UE) 2016/680 detalle de forma precisa las condiciones en las que las autoridades pueden tratar los datos biométricos y otras categorías especiales, previa consulta con la autoridad nacional de protección de datos. Esta regulación debe evitar formulaciones genéricas (no admitiendo una "redacción igualmente general y abstracta" que la utilizada por la Directiva), para dar seguridad jurídica a las autoridades competentes a la hora de invocar una base jurídica sólida en la que sustentar el tratamiento de este tipo de datos. Más adelante analizaremos la transposición que ha hecho el legislador español de esta normativa.

En esta misma línea interpretativa, el CEPD también aclara[28] que la mera detección de rostros mediante cámaras inteligentes, con la finalidad de detectar comportamientos anómalos o violentos, emociones o siluetas, no constituye necesariamente un sistema de reconocimiento facial, siempre que estas técnicas no comporten la identificación unívoca de una persona y, por tanto, no están sujetas a las limitaciones del procesamiento de datos personales de categoría especial.

No obstante, el CEPD advierte que el reconocimiento facial sí implica el tratamiento masivo de datos sensibles, lo que puede afectar no solo a la privacidad, sino también a derechos fundamentales como la dignidad, la libertad de movimiento y de reunión, entre otros. Por ello, considera que su uso debe limitarse estrictamente a contextos de necesidad y proporcionalidad, como la identificación de autores de delitos graves o actos terroristas y no emplearse como una "solución milagrosa"[29].

Además, sostiene que el reconocimiento biométrico remoto en espacios públicos constituye en numerosas ocasiones un riesgo inaceptable en una sociedad democrática, por lo que debe partirse de una regulación que prohíba de manera general su uso[30]. Igualmente, califica de "indeseables" las aplicaciones biométricas destinadas a inferir

[27] Punto 72 de las Directrices 05/2022 del CEPD, sobre el uso de la tecnología de reconocimiento facial en el ámbito policial.

[28] Punto 14 de las Directrices 05/2022 del CEPD, sobre el uso de la tecnología de reconocimiento facial en el ámbito policial.

[29] Punto 105 de las Directrices 05/2022 del CEPD, sobre el uso de la tecnología de reconocimiento facial en el ámbito policial.

[30] Punto 106 de las Directrices 05/2022 del CEPD, sobre el uso de la tecnología de reconocimiento facial en el ámbito policial.

emociones, proponiendo su prohibición salvo en casos excepcionalmente justificados. Finalmente, advierte que el uso policial de bases de datos construidas a partir de imágenes faciales obtenidas masivamente en la red[31], para ser cotejadas con la imagen de una persona buscada, no satisface el principio de estricta necesidad exigido por el Derecho de la Unión[32].

En resumen, el CEPD establece las líneas rojas a los legisladores, tanto de los Estados Miembros, como de la Unión Europea, así como a las Fuerzas y Cuerpos de Seguridad (en adelante FCS), que no deben traspasar en el uso del reconocimiento facial. El CEPD apela a que su utilización se produzca en situaciones de estricta necesidad (entre las cuales excluye las técnicas de *image scraping*), que se determine su tratamiento únicamente para delitos de singular gravedad, que el legislador nacional realice una transposición concreta de la normativa y, finalmente, que se parta de la prohibición, salvo en determinadas excepciones, de la vigilancia masiva y del reconocimiento de emociones.

2. Análisis del Reglamento de Inteligencia Artificial respecto al uso automatizado de IA para la identificación biométrica en tiempo real en espacios públicos con fines policiales, la categorización y el reconocimiento de emociones.

A continuación, se examina la regulación prevista en el AIA, como ley específica, respecto al uso automatizado de patrones biométricos para la identificación, categorización y reconocimiento de las emociones de las personas físicas, atendiendo a su clasificación según los niveles de riesgo que comporta y las restricciones impuestas. Asimismo, se exponen algunas deficiencias en la protección de los derechos fundamentales y se analiza alguna jurisprudencia relevante en esta materia.

2.1. Uso automatizado de datos biométricos mediante sistemas de IA para la identificación.

El AIA excluye de su ámbito las aplicaciones de verificación y autentificación biométrica, por considerarlas de menor riesgo en términos de afectación a los derechos fundamentales. En contraste, cataloga los sistemas de identificación biométrica como de

[31] Mediante un software se extraen de manera automática datos de la red, tales como imágenes faciales (*image scraping*) accesibles en línea.

[32] Punto 107 de las Directrices 05/2022 del CEPD, sobre el uso de la tecnología de reconocimiento facial en el ámbito policial.

alto riesgo, con la finalidad de garantizar que su tratamiento se produzca con un nivel elevado de protección para estos derechos y debido a que imprecisiones técnicas pueden comportar efectos discriminatorios relevantes.

Conviene mencionar, que el AIA se configura como *lex specialis* respecto al artículo 10 de la Directiva (UE) 2016/680, en lo relativo al uso de sistemas de IA para la identificación biométrica a distancia en tiempo real en espacios de acceso público con fines policiales[33]. En consecuencia, impide que las autoridades policiales puedan invocar la Directiva para justificar el tratamiento de estos sistemas fuera de los límites estrictamente previstos en el AIA.

El artículo 5 del AIA prohibe el uso de la identificación biométrica a distancia[34] en tiempo real[35] en lugares accesibles al público[36] con fines policiales, salvo en supuestos excepcionales. Estas excepciones incluyen la búsqueda selectiva de víctimas de delitos como el secuestro, la trata de seres humanos o la explotación sexual, así como la localización de personas desaparecidas. También se permite su uso para prevenir amenazas específicas y sustanciales contra la vida o la integridad física de las personas, incluidas amenazas reales o previsibles de ataques terroristas. Por último, se contempla su utilización para localizar o identificar a sospechosos de determinados delitos que conlleven una pena privativa de libertad superior a cuatro años, según la legislación del Estado Miembro correspondiente[37].

Además, prevé como requisito para llevar a cabo esta práctica que será necesaria autorización judicial o administrativa previa, salvo en situaciones debidamente justificadas de urgencia, en las que podrá iniciarse el uso del sistema, siempre que sin

[33] AIA, considerando 23.

[34] Según apunta el AIA, la identificación "a distancia" debe entenderse como aquélla que se lleva a cabo sin la participación activa del afectado.

[35] Tal y como dispone el AIA, "en tiempo real" debe interpretarse como contraposición a realizar la identificación "a posteriori", con imágenes almacenadas previamente y que solo después se produce la identificación. No se puede escapar de la regulación por el hecho de realizar la identificación con un retraso menor.

[36] El AIA considera "lugares accesibles al público" aquellos lugares físicos accesibles a un número indeterminado de personas, ya sean de titularidad pública o privada, y excluye específicamente los espacios en línea.

[37] AIA, Título II "Prácticas de IA prohibidas", artículo 5.1.d).

demora y en el plazo máximo de 24 horas se solicite la debida autorización a la autoridad competente[38].

El AIA dispone que el uso de las aplicaciones de identificación biométrica deberá realizarse de manera proporcionada, legítima y cuando sea estrictamente necesario, señalando que nunca deberán ser utilizados para la identificación indiscriminada, sino de manera selectiva, tanto respecto a los individuos a identificar, como a la ubicación, así como al ámbito temporal. Además se deberá realizar a partir de imágenes legalmente obtenidas y respetando los límites temporales de su almacenamiento.

Una vez expuesta brevemente la regulación del AIA, conviene reflexionar sobre los sistemas excluidos de la prohibición[39] del artículo 5, como aquellos que no operan en tiempo real, que se implementan fuera de espacios públicos (por ejemplo, en entornos laborales educativos, virtuales o penitenciarios), o se utilizan con fines distintos a los policiales (como la seguridad privada, la defensa o la inteligencia). Estos supuestos, al quedar al margen de las exigencias de autorización judicial o administrativa, pueden entrañar mayores riesgos para los derechos fundamentales y evidencian la necesidad de una regulación específica que los aborde adecuadamente.

En todo caso, las exclusiones de las regulaciones normativas por motivos de seguridad nacional, y tal y como se recoge en la sentencial del Tribunal Constitucional alemán de 19 de mayo de 2020 (1 BvR 2835/17)[40], no deben entenderse como una excepción de la aplicabilidad de la Constitución y del respeto a los derechos fundamentales.

Llegados a este punto, cabe preguntarse si la novedosa aprobación del AIA y demás normativa garantiza de manera suficiente la grave injerencia que puede suponer para los derechos fundamentales de los ciudadanos el uso de la IA en el reconocimiento facial automatizado.

Sin duda, la nueva regulación es un primer paso adelante en la preservación de las intromisiones en la vida privada y en la intimidad de las personas que libremente

[38] AIA, Título II "Prácticas de IA prohibidas", artículo 5.3.

[39] COTINO HUESO, L., "Sistemas… cit", pp. 68-79.

[40] Tribunal Constitucional Federal de Alemania, sentencia de la Sala Primera, sobre el asunto BvR 2835/17, de 19 de mayo de 2020, paras. 1-332. Disponible en: https://www.bverfg.de/e/rs20200519_1bvr283517en.html.

deambulan por los espacios públicos. En este sentido, cabe señalar que bajo el paraguas de protección que ofrece actualmente el AIA a los veintisiete Estados Miembros de la Unión Europea, no se podrían amparar usos preventivos de sistemas de reconocimiento facial automático en lugares públicos como el que fue avalado por el Alto Tribunal de Justicia de Inglaterra y Gales, en su sentencia de 4 de septiembre de 2019[41].

En esta sentencia, la autoridad judicial se pronunciaba respecto al proyecto piloto "*AFR*[42] *Locate*" puesto en marcha por la policía de Gales del Sur. Este proyecto consistía en la utilización policial en eventos, concretos y singulares, de cámaras de videovigilancia que grababan a los asistentes, utilizaban herramientas de reconocimiento facial para procesar sus datos biométricos y los comparaban en tiempo real con los de un listado de personas buscadas. En el caso de no darse coincidencia, los datos eran borrados inmediatamente. Por el contrario, cuando el sistema daba un resultado con una puntuación que alumbraba una alta posibilidad de coincidencia, alertaba a los agentes de policía para que realizaran las comprobaciones oportunas y decidieran cómo proceder. De esta manera, el sistema no provocaba una respuesta automatizada sobre el sospechoso.

El Alto Tribunal analizaba la injerencia que efectivamente reconocía en la vida privada de los reconocidos por el sistema[43], de acuerdo con lo previsto en el artículo 8 del Convenio Europeo de Derechos Humanos. Ahora bien, concluía que esta injerencia no suponía una vulneración per se del derecho fundamental a la vida privada y que el uso que realizó la policía de Gales del Sur estaba amparado en el derecho consuetudinario para prevenir y detectar delitos de manera "ampliamente suficientes"[44].

Asimismo, el mencionado órgano judicial disponía en su sentencia que el tratamiento de los datos biométricos en el caso analizado, que permitía obtener información singular de una persona e identificarla de manera unívoca, estaba sujeto a las disposiciones sobre

[41] Alto Tribunal de Justicia de Inglaterra y Gales, caso CO/4085/2018, asunto La Reina (a solicitud de Edward Bridges) contra el Jefe de Policía de Gales del Sur. Disponible en vLex: https://vlex.co.uk/vid/the-queen-on-application-818735609.

[42] *Automated Facial Recognition.*

[43] IZQUIERDO CARRASCO, M., "La utilización policial de los sistemas de reconocimiento facial automático", *IUS ET VERITAS, núm. 60*, 2020, pp. 86-103.

[44] JACK, G., "UK High Court upholds police use of automated facial recognition technology to identify suspects", publicado en la revista digital *Human Rights Law Centre*, 30 de septiembre de 2019, disponible en: https://www.hrlc.org.au/human-rights-case-summaries/2019/10/30/uk-high-court-upholds-police-use-of-automated-facial-recognition-technology-to-identify-suspects.

datos de carácter personal de la Unión Europea y, en particular, a la mencionada Directiva (UE) 2016/680.

Finalmente, la sentencia se pronunciaba respecto a la posible afectación al principio de no discriminación del algoritmo utilizado, por los posibles sesgos discriminatorios que se alegaban respecto a las diferencias de las tasas de acierto en la identificación según el color de la piel y el género. Con relación a esto, la autoridad judicial consideraba por un lado que no había quedado probada la existencia de una discriminación algorítmica y, por otro lado, que el sistema no incidía de manera automática en la toma de decisiones sobre el individuo señalado como sospechoso, sino que la decisión de la actuación a llevar a cabo era siempre del policía que realizaba las comprobaciones correspondientes.

Por tanto, el Alto Tribunal de Justicia de Inglaterra y Gales avalaba el uso que la policía de Gales del Sur había hecho en 2017 de "*AFR Locate*" en su sentencia de 2019, decisión que actualmente no sería ajustada a las garantías establecidas en el AIA para el uso de estos sistemas automáticos de reconocimiento facial por parte de los Estados Miembros de la UE, entre los cuales no figura el Reino Unido.

Retomando la cuestión que se planteba anteriormente respecto a si la actual regulación es capaz de garantizar de manera suficiente las instrusiones a los derechos fundamentales que puede comportar el uso del reconocimiento facial automatizado, como se ha mencionado, es un primer paso, pero no es suficiente. Hoy en día nos encontramos ante diferentes situaciones cotidianas que quedan fuera de esta regulación, en las que como ciudadanos nos vemos abocados a padecer el uso y tratamiento de nuestros datos biométricos, sin que exista un consentimiento totalmente libre, ni suficientemente informado. En algunos entornos no existe un sistema alternativo para obtener la misma funcionalidad (accesos a gimnasios, fichaje horario en las empresas, apertura de puertas en el entorno laboral), por lo que no podemos hablar de un consentimiento plenamente libre. Además, tampoco podemos decir que estemos suficientemente informados sobre en qué va a consistir el tratamiento de nuestros datos, con qué finalidad, quién va a tener acceso a ellos, cuánto tiempo van a ser almacenados, con qué medidas de protección se van a guardar y si ante vulnerabilidades de seguridad vamos a ser debidamente alertados.

En este sentido se pronunció la sección 9ª de la Audiencia Provincial de Barcelona en su auto 72/2021 de 15 de febrero de 2021[45], en el cual analizaba el uso de medios automatizados de captación de datos biométricos por parte de la distribuidora Mercadona en la entrada de sus establecimientos, para detectar si dos personas, que habían sido condenadas por delito de robo y que tenían una prohibición de entrada en una de sus tiendas, incumplían dicha proscripción. El auto denegaba el uso de estos sistemas aludiendo a que la medida no resultaba proporcionada, ni idónea, dado que no se estaba protegiendo un interés público, sino privado. Y todo ello, a costa de conculcar la protección de unos datos, los biométricos, que merecen una especial protección en el sentido del artículo 9.1 del RGPD, sin que se dieran ninguna de las excepciones previstas en su párrafo segundo y, en concreto, la obligatoriedad que el usuario dé su consentimiento para procesar sus datos. Cosa que claramente no sucedía, ni con los dos individuos condenados, ni con el resto de clientes que accedían a los establecimientos.

El tribunal apuntaba que no se podía tener en cuenta el argumento esgrimido por Mercadona, respecto a que no existía tratamiento de datos debido a la rapidez con la que el sistema actuaba (0.3 segundos) y que una vez no encontrada coincidencia, el sistema borraba inmediatemente los datos. El auto señalaba que "por muy rápido que sea, existe una violación de la privacidad".

Cabe mencionar que, en su auto, la Audiencia Provincial de Barcelona ya destacaba la ausencia de un marco normativo suficiente dedicado a regular este tipo de tratamientos para la correcta definición de la licitud de este tipo de tratamientos, y que con la reciente aprobación del AIA esta deficiencia no ha quedado debidamente resuelta.

2.2. Uso de datos biométricos mediante sistemas de IA para la categorización y el reconocimiento de emociones.

Según el AIA, la categorización biométrica consiste en "la asignación de personas físicas a categorías específicas sobre la base de sus datos biométricos"[46]. Entre ellos, el sexo, el género, la orientación sexual, el origen étnico, los tatuajes, el color de pelo y ojos, los

[45] Audiencia Provincial de Barcelona, sentencia 72/2021, de 15 de febrero. Disponible en vLex: https://vlex.es/vid/870895897.

[46] AIA, considerando 7 ter.

rasgos de comportamiento, la personalidad, la orientación política, las creencias religiosas o la salud.

El AIA prohibe las prácticas de IA de categorización biométrica[47], pero levanta esta interdicción cuando la finalidad sea la detección, prevención o investigación de delitos, siempre que los datos se hayan adquirido de conformidad al Derecho de la Unión, en cuyo caso el sistema de IA será considerado de alto riesgo[48].

Por su parte, el AIA define las aplicaciones de reconocimiento de emociones o intenciones mediante sistemas biométricos de IA como aquellas destinadas a inferir la "felicidad, tristeza, ira, sorpresa, asco, vergüenza, excitación, desprecio, satisfacción y diversión"[49]. Para llegar a los resultados, se analizan expresiones faciales, corporales (el movimiento de las manos o la cabeza), así como el tono de la voz. El mismo AIA alerta de la escasa base científica en la que sustentar la validez y robustez de los resultados arrojados por estas herramientas, dado que la diversidad cultural, generacional, situacional e individual, dificulta su parametrización, lo cual puede abocar a la obtención de resultados discriminatorios[50], aparte de ser aplicaciones sumamente instrusivas para los derechos de las personas.

El AIA prohibe[51] el uso de sistemas biométricos para el reconocimiento de emociones en los entornos laborales y educativos, y exceptua su prohibición para fines médicos y de seguridad. En tales circunstancias, como ocurre en el caso de las herramientas de categorización biométrica, los clasifica como de alto riesgo[52].

Tanto en el caso de la categorización, como en el caso del reconocimiento de emociones, el AIA obliga a los responsables de estos procediminetos a informar a las personas expuestas a estas aplicaciones de tal circunstancia. Ahora bien, excluye de esta

[47] AIA, Título II "Prácticas de IA prohibidas", artículo 5.1.b.bis.

[48] AIA, AIA, anexo III, apartado 1.aa.

[49] AIA, considerando 8 bis.

[50] BARONA VILAR, S., "Inteligencia artificial o la algoritmización de la vida y de la justicia: ¿solución o problema?", *Revista boliviana de Derecho, núm. 28,* 2019, pp. 18-49.

[51] AIA, Título II "Prácticas de IA prohibidas", artículo 5.1.dc.

[52] AIA, anexo III, apartado 1.ab.

imposición cuando de conformidad con el Derecho de la Unión la finalidad sea la detección, prevención o investigación de delitos.

Por lo tanto, el uso de estas técnicas en el entorno policial no está prohibida por el AIA, pero sí supeditada a los requisitos, antes mencionados, que se establecen para los sistemas catalogados de alto riesgo. Por lo que el uso de aplicaciones como IBorderCtlR[53] no quedaría, de por sí, al margen de la ley. Ahora bien, cabe preguntarse si el hecho de que el Estado evalúe qué pensamos, cómo nos sentimos o nuestro estado anímico, no supone un ataque intolerable a la libertad cognitiva[54]. Y todo ello sin menospreciar, que como ya apunta el AIA, los resultados que ofrece esta tecnología no gozan de un aval científico debido a que resulta complicado que se pueda realizar una objetiva parametrización de los comportamientos de las personas para inferir sus emociones, teniendo en cuenta no solo la diversidad cultural, sino también la individual. Y, por tanto, este tipo de algoritmos no suponen solamente una intensa injerencia en la esfera más personal de los individuos evaluados, sino que además pueden perpetuar los sesgos discriminatorios[55]. Asimismo, cabe añadir que, en numerosas ocasiones, como sucede en el caso de IBorderCtlR, o en otros sistemas de "detección de mentiras" utilizados en el entorno policial[56], la persona

[53] *Intelligent Portable Border Control System.* Proyecto desarrollado con la financiación de la Unión Europea para el control fronterizo, mediante tecnología biométrica verifica la identidad y detecta las emociones de los viajeros con la funcionalidad, entre otras, de actuar como un detector de mentiras.

[54] Actualmente, existe un debate científico entorno a la necesidad de calificar la libertad cognitiva como un derecho fundamental, para poder dotarla de la debida protección (neuroderechos), tanto en el sentido del autodominio cerebral, como en el de la privacidad mental. Véase BORBÓN, D. y MUÑOZ, J. M., "El neuroderecho a la libertad cognitiva: fundamentos y alcance de un derecho emergente", *IUS ET SCIENTIA, volumen 10, núm. 1,* 2024, pp. 103-131; ALBARRACÍN TORRES, M. A., "El derecho a la libertad cognitiva como una propuesta de abordaje a los riesgos de la creciente aplicación de las neurotecnologías en el cerebro humano", *UNIVERSITAS, Revista de Filosofía, Derecho y Política, núm. 45*, 2024, pp. 112-122.

[55] Diversos estudios han demostrado la presencia de sesgos discriminatorios en los modelos algorítmicos de las herramientas de IA aplicadas en el entorno policial en general, así como en los sistemas de reconocimiento de patrones biométricos en particular. Estos sesgos pueden manifestarse en función del origen étnico, el color de piel, la edad, el género u otros factores personales. Véase SANABRIA MOYANO, J. E., ROA AVELLA, M. D. P, y LEE PÉREZ, O. I., "Tecnología de reconocimiento facial y sus riesgos en los derechos humanos", *Revista Criminalidad, volumen 64, núm. 3*, 2022, pp. 61-78; BUOLAMWINI, J., y GEBRU, T., "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", en *Conference on Fairness, Accountability, and Transparency, Proceedings of Machine Learning Research*, Nueva York (Estados Unidos), 23 y 24 de febrero de 2018, pp. 77-91; TACCA, M. A. T., "El uso de sistemas biométricos con Inteligencia Artificial: ¿una vulneración a los derechos humanos?", *YachaQ: Revista de Derecho, núm.18*, 2025, pp. 27-40.

[56] Como VeriPol, utilizado por el Cuerpo Nacional de Policía en España para estimar las probabilidades que una denuncia sea falsa. Véase LA MONCLOA, "La Policía Nacional pone en funcionamiento la

sometida a dicho escrutinio se encuentra en una posición de desigualdad[57], bajo presión y en circunstancias coercitivas que pueden provocar en sí mismas, estados de nerviosismo en el individuo que alteren los propios resultados.

IV. MARCO LEGAL DEL TRATAMIENTO DE LOS DATOS BIOMÉTRICOS EN EL ENTORNO POLICIAL EN ESPAÑA.

Una vez expuesta la normativa a nivel de la Unión Europea sobre el tratamiento de datos biométricos, y en especial sobre el reconocimiento facial como uno de sus usos más destacados, pasamos a analizar el marco legal español en este ámbito. Para ello, en primer lugar, presentaremos la transposición hecha por el legislador español de la normativa europea, apuntando sus carencias. A continuación, examinaremos el encaje normativo del reconocimiento facial como diligencia de investigación por parte de las FCS, por ser un ejemplo de tratamiento de datos biométricos que puede contribuir a mejorar la eficiencia de las investigaciones. Y, finalmente, vistos los déficits normativos, formularemos una propuesta de los aspectos que debería abordar una futura Ley Orgánica que regule el uso del reconocimiento de patrones biométricos para combatir la criminalidad a nivel estatal.

1. Transposición de la normativa de la Unión Europea al ordenamiento jurídico español.

Como se ha mencionado anteriormente, el CEPD requiere que el legislador nacional transponga el artículo 10 de la Directiva (UE) 2016/680 precisando y definiendo las circunstancias del tratamiento de datos biométricos en el entorno policial, destacando que no debe admitirse una "redacción igualmente general y abstracta"[58] que la expuesta en la Directiva.

Seguidamente, analizamos brevemente cómo el legislador español ha transpuesto —mediante el artículo 13 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento

aplicación informática VeriPol para detectar denuncias falsas", 2018, disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2018/271018veripol.aspx.

[57] El resultado obtenido de un sistema que evalúe la idoneidad de un individuo sometido, por ejemplo, a un sistema de control transfronterizo, para transitar o entrar en un país, puede condicionar de manera significativa su futuro inmediato, sin en muchas ocasiones capacidad de rebatir la decisión de forma inminente, dadas las circunstancias de desigualdad en las que se produce.

[58] Punto 72 de las Directrices 05/2022 del CEPD, sobre el uso de la tecnología de reconocimiento facial en el ámbito policial.

de infracciones penales y de ejecución de sanciones penales— el artículo 10 de la Directiva (UE) 2016/680 a nuestro ordenamiento jurídico.

Como señala Cotino, el artículo 13 apenas aporta valor añadido[59], ya que el legislador español se ha limitado a reproducir el contenido del artículo 10 Directiva 2016/680. Aunque incorpora dos apartados adicionales —uno que justifica el tratamiento de datos biométricos por las autoridades competentes para fines de seguridad pública y otro que establece garantías reforzadas para menores y personas con la capacidad modificada judicialmente—, el precepto carece de la especificidad y concreción que exige el CEPD.

De lo expuesto, se puede afirmar que la transposición del artículo 10 de la Directiva (UE) 2016/680 por parte del legislador español no cumple con los requisitos apuntados por el CEPD en las Directrices 05/22 cuando señalaba la necesidad de que los legisladores nacionales huyeran de la redacción genérica y abstracta de la Directiva, con el objetivo de garantizar una base jurídica sólida para el tratamiento de este tipo de datos en el ámbito policial. Por lo tanto, estamos ante una regulación estatal insuficiente para amparar el tratamiento de datos biométricos de manera específica en este ámbito. Esta insuficiencia debería ser subsanada por el legislador español para evitar haber de justificar el uso de los datos biométricos en el entorno policial de manera genérica de acuerdo con lo establecido en la Directiva (UE) 2016/680.

2. Un ejemplo de tratamiento de datos biométricos: el reconocimiento facial como diligencia de investigación policial y su encaje en el ordenamiento jurídico español.

En la práctica policial es habitual contar con imágenes de la comisión de un hecho delictivo donde aparezca un autor, de manera más o menos reconocible, al que se haya de identificar. Cuando este reconocimiento se realiza mediante un tratamiento técnico específico de las características físicas del individuo a identificar (imágenes dubitadas) para ser comparadas con las de otros de los cuáles se conoce su identidad (imágenes indubitadas), nos encontramos en el entorno del tratamiento de datos biométricos. El uso de sistemas de IA de reconocimiento facial constituye un ejemplo de tratamiento de datos biométricos que se está extendiendo por parte de las FCS en su cometido de combatir la

[59] COTINO HUESO, L., "Sistemas… cit", pp. 68-79.

criminalidad, ya que su uso puede contribuir a agilizar la identificación de sospechosos, testigos y/o víctimas de hechos delictivos.

Por ello, a continuación se analiza la validez de esta técnica para determinar la identidad de un individuo y su encaje en el procedimiento penal español.

La Ley de Enjuiciamiento Criminal española no prevé de manera expresa el tratamiento de datos biométricos. No obstante, su utilización con la finalidad de identificar al sospechoso podría admitirse al amparo del artículo 373[60]. Además, teniendo en cuenta lo dispuesto en el artículo 13.2[61] de la Ley Orgánica 7/2021, esta actuación podría llevarse a cabo por la policía, como autoridad competente, sin previa autorización judicial[62].

Respecto a la validez de las herramientas informáticas para la comparación y medición de los rasgos faciales, no existe una regulación expresa, por ello debe acudirse a lo establecido por la jurisprudencia. Al respecto se pronunció el Tribunal Supremo en la STS 315/2016, de 14 de abril[63]. En ella se valora la evolución de las técnicas de tratamiento de reconocimiento facial desde su sentencia de STS 61/2000, de 27 de enero de 2001, en la cual realizaba una comparativa entre la robustez de las técnicas de identificación dactiloscópicas con "un amplio consenso en el mundo científico" y la "cautela" con la que se debían valorar los resultados de los tratamientos de identificación antropomórfica. En este sentido, establece que "No hay obstáculo, para que esta técnica se pueda utilizar como elemento valioso de investigación que permita hacer una aproximación hacia la persona sospechosa, pero es difícil atribuirle, en todos los casos, el valor de prueba plena e indiscutible".

Este es otro de los aspectos que debería haberse abordado en la transposición de la Directiva (UE) 2016/680 al ordenamiento jurídico estatal, para establecer las garantías de

[60] Artículo 373 de la Ley de Enjuiciamiento Criminal: "Si se originase alguna duda sobre la identidad del procesado, se procurará acreditar ésta por cuantos medios fueren conducentes al objeto".

[61] Artículo 13.2 de la Ley Orgánica 7/2021: "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".

[62] FREIRE MONTERO, A. F., "El reconocimiento facial como instrumento de investigación y prevención del delito", *Anuario da Facultade de Dereito da Universidade da Coruña, núm. 26*, 2022, pp. 64-88.

[63] Tribunal Supremo, sentencia 315/2016, de 14 de abril. Disponible en vLex: https://vlex.es/vid/637465525.

fiabilidad y robustez necesarias a las técnicas de tratamientos de identificación antropomórfica en el entorno policial, así como para dotar a las FCS de una base jurídica sólida en la que poder apoyar sus diligencias de investigación.

Por lo tanto, en la actualidad, el uso de sistemas de IA de reconocimiento facial[64] como diligencia de investigación policial tendría la consideración de prueba pericial, de manera que los peritos que hayan elaborado los informes fisonómicos o de cotejo del rostro deberán ser citados en el juicio oral para conformar la libre valoración de la prueba por parte del tribunal juzgador[65].

3. Propuesta de Ley Orgánica para proteger el derecho al *habeas data* en el uso del reconocimiento de patrones biométricos para combatir la criminalidad.

Tal y como ha quedado evidenciado a lo largo de este estudio, carecemos de un adecuado marco normativo estatal que permita aprovechar las ventajas que aportan las aplicaciones de reconocimiento de patrones biométricos para combatir la criminalidad, ofreciendo seguridad jurídica a las diligencias de investigación realizadas mediante estas técnicas por las FCS y, a la vez, salvaguardar los derechos fundamentales, en especial el derecho al *habeas data*.

Por ello, se propone la promulgación de una nueva normativa a nivel estatal, con rango de Ley Orgánica[66], para regular el uso del reconocimiento de patrones biométricos mediante IA por parte de las FCS tanto en la prevención, como en la detección e investigación del delito. El uso de esta tecnología no debe considerarse, per se, como un ataque a los derechos fundamentales, dado que, si estos sistemas son utilizados con los límites y garantías oportunos, pueden contribuir a garantizar un nivel más alto de

[64] En el tiempo transcurrido entre la mencionada sentencia STS 315/2016 y la actualidad, las técnicas de reconocimiento facial, todavía, no gozan de un aval científico equiparable al que sí tienen los resultados de otras pruebas científicas que se utilizan en el procedimiento penal, tales como los análisis de ADN o de las huellas dactilares. Véase: DE MIGUEL BERIAIN, I. y PÉREZ ESTRADA, M. J., "La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados", *Revista De Derecho De La UNED, núm. 25*, 2019, pp. 531-561; PÉREZ ESTRADA, M. J., "La inteligencia artificial como prueba científica en el proceso penal español", *Revista Brasileira de Direito Processual Penal, volumen 7, núm. 2*, 2021, pp. 1385-1385.

[65] GÓMEZ COLOMER, J. L., "La prueba científica, motor de cambios esenciales en el proceso penal moderno", *Revista Brasileira de Direito Processual Penal, volumen 7, núm. 2*, 2021, pp. 1385-1410.

[66] Por afectar al desarrollo de los derechos fundamentales y las libertades públicas, en concreto a lo establecido en el artículo 18.4 de la Constitución Española "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

seguridad y, por tanto, dotar de un entorno más propicio a la ciudadanía para que pueda disfrutar con mayor seguridad del libre ejercicio de sus derechos y libertades.

Después de un debate profundo con los diferentes actores del sistema de justicia penal, el legislador debería pronunciarse respecto al uso de patrones biométricos mediante IA, entre otros, en los aspectos que a continuación se apuntan.

En primer lugar, se deberían regular las bases de datos policiales que contienen información biométrica (cuya identificación es indubitada) con la que se pueden cotejar los datos biométricos dubitados de las personas a identificar. También debería ser objeto de ordenación establecer en qué situaciones la policía puede, sin autorización judicial o administrativa, utilizar estas aplicaciones en sus labores de prevención, detección e investigación delincuencial para identificar a víctimas, testigos o investigados. Hay que tener en cuenta que la utilización del reconocimiento facial en diferentes diligencias, como la de vigilancia y seguimiento por parte de la policía, puede contribuir a reducir los errores de los investigadores a la hora de seguir al objetivo correcto, así como a minimizar las atribuciones de hechos delictivos a personas identificadas equivocadamente.

Estas bases de datos, como es exigible en un Estado de Derecho, deben tener plena cobertura legal y convendría que fueran creadas, gestionadas y tratadas, dentro del marco normativo vigente por las fuerzas policiales, como organismos públicos encargados de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana.

Asimismo, es necesario establecer estándares adecuados, basados en estudios científicos rigurosos, que permitan evaluar que los resultados ofrecidos por estos procedimientos cumplan con la calidad, trazabilidad, fiabilidad, robustez, explicabilidad y transparencia[67] necesarias para garantizar su aceptación como prueba en el juicio oral. Esto permitirá respetar el derecho a la contradicción, sin que ello implique que el órgano juzgador o las partes del procedimiento tengan que ser expertos en el detalle de la programación de los algoritmos (como no lo son en otras técnicas, como la del análisis del ADN o de las huellas dactilares, ampliamente aceptadas por la jurisprudencia).

[67] Se debe huir de los algoritmos de caja negra de los cuáles se desconoce el proceso de toma de decisiones que lleva a obtener los resultados.

En segundo lugar, resultaría oportuno que el legislador disponga en qué circunstancias concretas las FCS puedan utilizar sistemas automáticos de reconocimiento facial en tiempo real, respetando el marco legal general establecido en el artículo 5 del AIA. Se deberían fijar de manera clara y concreta los límites al uso de estas herramientas para garantizar el respeto a los derechos fundamentales. Ahora bien, también es responsabilidad del legislador establecer cuándo sí pueden ser usados y en qué circunstancias, ya que se debe dotar a la policía de la seguridad jurídica para poder utilizar esta tecnología en diferentes contextos, donde puede ser tremendamente útil para detectar a individuos que pueden suponer una amenaza grave a la seguridad de las personas.

Por este motivo, sería provechoso que el legislador se pronunciase respecto a si el uso de la identificación mediante patrones biométricos en tiempo real para la prevención puede ser usada en diferentes entornos sensibles, como los son las infraestructuras críticas (aeropuertos, centrales nucleares,…), grandes eventos (conciertos, concentraciones deportivas[68],…) u otros. De igual manera, también se deberían definir las circunstancias en las que se admite el uso de estas técnicas para detectar a los sospechosos de haber realizado un cierto tipo de crímenes, estableciendo un catálogo de delitos, las circunstancias de su utilización, el órgano que, en su caso, debe autorizarlas, así como el intervalo temporal.

Por tanto, resulta deseable que se establezcan los límites del uso de esta tecnología como diligencia de investigación en la Ley de Enjuiciamiento Criminal, de igual manera que se regulan otras medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución Española. Como se ha mencionado anteriormente, el tratamiento de los datos biométricos mediante sistemas de IA incide en la limitación del

[68] Según se expuso en el *XXI International Congress of the International Association of Penal Law, Artificial Intelligence and Criminal Law*, celebrado en París del 25 al 28 de junio de 2024, Francia no dispone de una regulación normativa para que la FCS puedan utilizar sistemas de IA de reconocimiento facial. Ahora bien, ante la celebración de los Juegos Olímpicos de París 2024, de manera excepcional y experimental, se promulgó una autorización *ad hoc* para permitir el uso por parte de las fuerzas del orden del reconocimiento automático en tiempo real en espacios públicos con la instalación de 4.000 cámaras. El sistema comparaba los patrones biométricos de los transeúntes con los de una base de datos previamente configurada. La medida se justificó en base a que el balance entre riesgos y beneficios se consideró proporcional y que cumplía con el requisito de estricta necesidad. Para ello, según los ponentes, se valoraron cinco elementos: la utilidad al apoyo al trabajo de las FCS, los riesgos que comportaba (señalando que el sistema no podía ser utilizado para una finalidad diferente, como lo es la delincuencia ordinaria menor), la ley (apuntando que para asegurar la libertad pública se justificaba el uso de esta tecnología), el beneficio obtenido para la paz pública y la fiabilidad de los resultados. Señalar que este software fue desarrollado en una colaboración público-privada.

uso de la informática para garantizar el honor y la intimidad personal regulado en el artículo 18.4 de la mencionada Carta Magna.

En tercer lugar, sería conveniente definir los supuestos excepcionales en los que serán admitidas las comparativas con las bases de datos biométricos obtenidos mediante técnicas de raspado de imágenes en la red. Sería positivo que los cuerpos de seguridad pudieran disponer, dentro de la legalidad, de las herramientas tecnológicas del siglo XXI para combatir situaciones de agresiones relevantes para la seguridad pública, respectando los derechos fundamentales de la ciudadanía a la que sirven.

En cuarto lugar, el legislador debería asumir la responsabilidad de delimitar el uso de las aplicaciones de categorización y reconocimiento de emociones, para que estos sistemas, por un lado, no provoquen un aumento de las discriminaciones y desigualdades sociales, y, por otro lado, no afecten a la libertad de pensamiento y a la libertad cognitiva. En este sentido, es responsabilidad de los Estados salvaguardar el autodominio cerebral y la privacidad mental en esta era tecnológica. Si queremos tener una sociedad rica, libre, diversa y con capacidad de evolucionar, debemos no solo respetar el pensamiento del otro expresado de manera libre, sino también evitar cualquier injerencia cognitiva en la libertad de pensamiento.

Finalmente, convendría regular qué consecuencias debe comportar la negativa de las grandes corporaciones tecnológicas con relación a su deber de colaboración con las FCS, así como con los organismos judiciales, respecto a las peticiones de informaciones relativas a la identificación de sus usuarios o a su actividad. Es evidente, que la Unión Europea ha quedado rezagada en la carrera desenfrenada encabezada por Estados Unidos y China en el desarrollo de IA, lo que provoca que la mayoría de la tecnología de IA utilizada en Europa provengan de fuera de la Unión. Esto puede comportar una ineficacia real de la legislación tanto de la Unión Europea[69], como de sus Estados Miembros. Por ello, sería conveniente que el legislador estableciera los mecanismos legales adecuados para garantizar que las herramientas de IA que operan o afectan a sus ciudadanos cumplen con los estándares legales establecidos a nivel nacional.

[69] RICHARD GONZÁLEZ, M., "Los sistemas biométricos de reconocimiento facial en la Unión Europea en el marco del desarrollo de la Inteligencia Artificial", *Justicia, núm. 1*, 2023, pp. 147-281.

V. CLEARVIEW AI: UN SISTEMA DE RECONOCIMIENTO FACIAL BASADO EN EL RASPADO DE IMÁGENES EN LA RED.

A continuación, se analizarán específicamente los sistemas de reconocimiento facial basados en IA que emplean técnicas de raspado de imágenes en la red, dado que constituyen un ejemplo particularmente controvertido por la significativa intromisión que representan en la privacidad de millones de usuarios. Estos sistemas, actualmente utilizados por diversas empresas privadas, plantean importantes desafíos éticos y legales. Asimismo, se examinará su grado de fiabilidad, atendiendo a la consistencia de los resultados que esta tecnología ofrece en la práctica.

Las técnicas de *image scraping* consisten en la utilización de *software* para extraer automáticamente imágenes de la web[70]. Un ejemplo de esta técnica es el sistema de reconocimiento facial desarrollado por la empresa Clearview AI, con sede en Estados Unidos. Este software, creado en 2017 bajo el pretexto de ser útil a la policía para la identificación de sospechosos, ha recopilado más de 40.000 millones[71] de imágenes obtenidas de páginas web y de publicaciones en perfiles de redes sociales (Facebook, YouTube, Twitter, Instagram y otras) para crear una base de datos que autodenominan "policial".

Clearview AI ofrece sus servicios a los organismos encargados de la seguridad pública (previo pago) para cotejar las imágenes de los individuos a identificar (sospechosos que han podido ser captados por vídeos o fotografías cometiendo un crimen) con los millones de imágenes que han recopilado en su base de datos. De esta manera, Clearview AI continúa alimentando su base de datos con las imágenes de las personas a identificar que la propia policía introduce en el sistema para buscar su coincidencia.

Según una investigación realizada por *The New York Times*[72], todo este proceso se está llevando a cabo sin que la aplicación haya sido probada, ni evaluada su precisión, por un

[70] ILHAM, A.A. y NURTANIO, I., "Optimización de búsqueda de imágenes con web scraping, procesamiento de texto y algoritmos de similitud de coseno", publicado en la *Conferencia Internacional IEEE de 2020 sobre Comunicaciones, Redes y Satélites (Comnetsat)*, Batam (Indonesia), 17 y 18 de diciembre de 2020, pp. 346-350.

[71] Dato extraído de la web de la propia empresa (https://www.clearview.ai/).

[72] HILL, K., "The Secretive Company That Might End Privacy as We Know It", artículo publicado en la versión digital del diario *The New York Times*, 18 de enero de 2020, disponible en: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

organismo independiente; careciendo del consentimiento informado de los afectados de que sus imágenes van a ser recolectadas y tratadas con esta finalidad y sí, supuestamente, violando los términos de servicio de los sitios web (como de Facebook). Y, lo que es más preocupante, sin disponer de garantías que avalen que los resultados que se ponen a disposición de la policía no han sido manipulados.

No obstante las controversias que suscita, numerosos cuerpos policiales se han visto seducidos porque consideran que esta herramienta es "eficaz" a la hora de establecer rápidas coincidencias entre las imágenes de los sospechosos a identificar y las imágenes almacenadas en la base de datos de la empresa proveedora del servicio. Además, destacan que no es necesario que la calidad de las imágenes a identificar sea extremadamente alta y que incluso permite coincidencias en imágenes en las que el rostro aparece parcialmente cubierto por gorras, gafas u otros elementos. El hecho de que unas imágenes en las que aparece el autor de un hecho delictivo, del que se desconoce su identidad, sean introducidas en el sistema y que éste, en pocos instantes, sea capaz de procesarlas, compararlas con más de 40.000 millones de fotografías y dar como resultado las imágenes coincidentes y los enlaces a los sitios web de dónde provienen, resulta ser una herramienta atractiva para los investigadores policiales para identificar a los sospechosos, incluso en ausencia de una marco normativo claro que regule sus condiciones de uso y sin que pueda acreditarse la validez de sus resultados.

Clearview AI empezó a ser usado por diferentes policías estatales de Estados Unidos[73] y su uso se extendió rápidamente a Europa. Ahora bien, diferentes países de la Unión Europea (tales como Italia, Francia y Grecia) han sancionado el uso de este sistema por las fuerzas del orden por incumplir los principios fundamentales del RGPD[74]. También el *Information Commissioner Office* de Reino Unido sancionó[75] a Clearview AI por la

[73] La policía estatal de Indiana fue la primera en utilizar esta tecnología para identificar con éxito al autor de una agresión que había quedado registrada en vídeo por un testigo.

[74] CONSEJO EUROPEO DE PROTECCIÓN DE DATOS, "*Facial recognition: Italian SA fines Clearview AI EUR 20 million*", 2022, disponible en: https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en.

[75] Clearview IA ganó el recurso de apelación a esta sanción, ya que el tribunal consideró (sin entrar a valorar si constituía o no infracción al RGPD) que el asunto quedaba fuera de los límites jurisdiccionales del RGPD, al tratarse de una empresa extranjera. Véase: GREENE, T., "Empresa estadounidense de vigilancia y reconocimiento facial Clearview AI gana recurso contra el RGPD en tribunal británico", artículo publicado en la versión digital de *Cointelegraph*, 19 de octubre de 2023, disponible en:

violación del Reglamento General de Protección de Datos de Reino Unido, por el tratamiento, la recopilación y la conservación indefinida de datos de sus ciudadanos.

Tras un período inicial de baja visibilidad, Clearview AI adoptó una estrategia proactiva en respuesta al descrédito reputacional sufrido a raíz de los resultados de la investigación de *The New York Times* y de las sanciones impuestas por algunas autoridades europeas. Su CEO, Hoan Ton-That, optó por reposicionar públicamente la empresa, destacando en su web[76] su estrecha colaboración gratuita con el gobierno de Ucrania a propósito de la invasión rusa. En su estrategia comunicativa actual, Clearview AI enfatiza el uso de su tecnología de reconocimiento facial para identificar a combatientes, espías y fallecidos de ambos bandos[77], así como para la localización de menores ucranianos trasladados ilegalmente a territorio ruso y la reunificación familiar de las personas desplazadas[78]. Asimismo, publicitan su contribución al refuerzo de la seguridad en puntos de control fronterizo.

Señalar, que esta colaboración "gratuita"[79] con el gobierno de Ucrania ha permitido que el número de fotografías de la base de datos de Clearview AI se viera incrementada en un 400% desde el inicio de la guerra[80].

El AIA ha catalogado como práctica de IA prohibida[81] estos procedimientos de raspado no selectivo de imágenes faciales de Internet, así como de grabaciones de CCTV[82]. Ahora bien, debido a las especiales circunstancias provocadas por el ataque ruso que está viviendo Ucrania desde febrero de 2022, pocos se han atrevido a poner el foco en si el

https://es.cointelegraph.com/news/us-surveillance-facial-recognition-firm-clearview-ai-wins-gdpr-appeal-uk-court.

[76] https://www.clearview.ai/.

[77] El gobierno de Ucrania pretende así contrarrestar la propaganda institucional rusa que niega el gran número de víctimas, también en el bando ruso, que se están produciendo por la invasión rusa.

[78] BERGENGRUENK V., "Ukraine's 'Secret Weapon' Against Russia Is a Controversial U.S. Tech Company", artículo publicado en la versión digital *Time*, 14 de noviembre de 2023, disponible en: https://time.com/6334176/ukraine-clearview-ai-russia.

[79] "Si no estás pagando por el producto, entonces tú eres el producto". Véase documental "The Social Dilemma" (información disponible en: https://thesocialdilemma.com/).

[80] Según manifestó el CEO de Clearview AI a Time.

[81] AIA, Título II "Prácticas de IA prohibidas", artículo 5.1.d ter.

[82] *Closed Circuit Television.*

uso de estas técnicas supone una intromisión inaceptable para la privacidad de las personas o sobre el grado de robustez y validez de sus resultados.

No obstante, cabe preguntarse qué pasará cuando la guerra acabe, y si las instituciones ucranianas estarán dispuestas a renunciar al uso de esta tecnología con el control social que conlleva, bajo la excusa de estar sometidos a la posibilidad de una nueva amenaza. Asimismo, hay que tener en consideración que las imágenes que forman parte de la base de datos de Clearview AI, lo son de todos. Es decir, de personas de todo el mundo que ni están siendo víctimas directas del asedio, ni victimarios, por lo que la laxitud en las garantías de los derechos fundamentales de las personas afectadas no se circunscribe a los sometidos directamente al conflicto, sino que nos afecta a todos. Además, hay que señalar que no parece que Clearview AI esté por la labor de restringir la comercialización de sus servicios a situaciones extraordinarias, o a eliminar de sus bases de datos los datos obtenidos bajo condiciones de excepcionalidad, como lo es una guerra.

Con todo, la existencia de empresas privadas como Clearview AI, u otras similares, que puedan estar haciendo un tratamiento fraudulento del raspado de imágenes en Internet, no debe comportar la automática y generalizada prohibición de estos sistemas. No debe perderse de vista que este tipo de tecnología puede ayudar de manera inminente y efectiva a las fuerzas del orden a identificar a víctimas, sospechosos o testigos de hechos delictivos graves y sensibles, así como a evitar actos terroristas. Pero para poder hacer un uso transparente, objetivo, no discriminatorio y ajustado a derecho, la responsabilidad del sistema debe recaer en los estados como garantes de la seguridad pública. Las Administraciones Públicas no deben delegar en empresas privadas ni la garantía en la consistencia de los resultados[83], ni la gestión de datos tan especialmente sensibles como lo son los biométricos[84].

[83] Las empresas privadas persiguen generar ganancias, ya sea de manera directa o indirecta. Pretender que ofrezcan datos de manera objetiva, a pesar de que puedan ir en contra de sus legítimos intereses empresariales y/o personales, no debe ser lo esperado por parte de los organismos encargados de hacer cumplir la ley. Por ejemplo, ¿es previsible que consten los datos biométricos en la base de datos de Clearview AI del hijo de su CEO para que éstos puedan ser cotejados con los de un sospechoso de terrorismo?, ¿Clearview AI alumbrará una coincidencia de identificación de datos biométricos a las fuerzas del orden para resolver un crimen que pueda hacer bajar sus acciones o su valor empresarial? Las respuestas probablemente serán negativas.

[84] El tratamiento y análisis de los datos personales en general y los datos biométricos en particular, son unos valiosos activos no solo en el ámbito empresarial, sino también en el social, político, académico, etcétera. Por ello, ha surgido un nuevo concepto para su protección, el denominado derecho al *habeas data*, para

VI. CONCLUSIONES.

Del análisis jurídico realizado sobre el uso de la IA en el reconocimiento de patrones biométricos para la prevención, detección e investigación del delito se evidencia que la Unión Europea ha tomado conciencia de la necesidad de regular su utilización, a fin de salvaguardar derechos fundamentales tan esenciales como la intimidad, la privacidad y la no discriminación. Por ello, ha promulgado el primer marco normativo de IA a nivel global, lo que constituye un hito inicial relevante en la regulación del uso de esta tecnología, entre otros, en el ámbito policial.

Ahora bien, es imprescindible que los Estados Miembros desarrollen los instrumentos normativos, institucionales y técnicos para garantizar un uso eficaz de estos procedimientos para combatir la criminalidad, asegurando al mismo tiempo el respeto pleno a los valores fundamentales de la Unión.

Para una implementación eficaz del AIA, será fundamental que su transposición legislativa en cada Estado Miembro sea específica, coherente y de alta calidad. Asimismo, las Administraciones Públicas deben asumir plenamente su responsabilidad en la garantía de la seguridad pública, sin delegar en actores privados —que persiguen sus legítimos objetivos de negocio— el control sobre la calidad, objetividad y fiabilidad de los sistemas de IA de reconocimiento biométrico, ni la gestión de sus bases de datos. La recuperación de la soberanía digital exige inversión pública en investigación, formación e innovación, así como impulsar un trabajo transversal colaborativo entre expertos en informática, derecho y filosofía para desarrollar tecnologías de identificación facial confiables, éticas y transparentes.

Asimismo, los resultados deben ser avalados por estudios científicos rigurosos, para que gocen en el proceso penal de la fiabilidad que actualmente tienen otros sistemas, como los de identificación dactiloscópica, y que puedan ser sometidos al principio de contradicción por las partes del proceso.

dotar a los titulares de los datos de las garantías adecuadas de información, acceso, rectificación y cancelación, con el objetivo de garantizar derechos fundamentales como la intimidad o la información. Véase: BUITRAGO BOTERO, D. M. "El valor de los datos personales en Colombia", *Revista CES Derecho, volumen 7, núm. 1*, Medellín (Colombia), 2016, pp. 1-2.

En relación con la oportunidad e idoneidad del recurso a estos sistemas de IA, el estudio ha evidenciado la profunda injerencia que puede derivarse de la identificación automática de las personas en espacios públicos, así como de la utilización de técnicas de raspado de imágenes masivo en la red. No obstante, también ha puesto de manifiesto que el reconocimiento facial puede constituir una herramienta valiosa en contextos específicos para combatir la criminalidad. Por ello, se concluye que no se debe utilizar el reconocimiento de patrones biométricos mediante IA como remedio prodigioso en aras de garantizar una seguridad pública absoluta —lo que, ni siquiera así, sería factible—, pero tampoco se debe renunciar a él, siempre que su uso esté fundamentado en los principios de necesidad y proporcionalidad consagrados en materia de derechos fundamentales. Esto exige una evaluación rigurosa del contexto, de los fines perseguidos, de los riesgos involucrados y de la idoneidad de esta tecnología frente a otras alternativas menos intrusivas.

Por este motivo, consideramos ineludible que el legislador español desarrolle una normativa con rango de Ley Orgánica que preserve el *habeas data* y que ofrezca seguridad jurídica a las FCS para hacer más efectiva y eficiente su labor.

En definitiva, sostenemos que las situaciones de excepcionalidad invocadas en nombre de la seguridad nacional no deben comportar una laxitud en la preservación de los derechos fundamentales. La construcción de una sociedad verdaderamente comprometida con los derechos humanos esenciales exige la consolidación de un marco normativo robusto y transparente, fruto de un debate social informado y maduro que delimite con claridad las reglas aplicables en escenarios de crisis o amenaza significativa.

VII. BIBLIOGRAFÍA

ALBARRACÍN TORRES, M. A., "El derecho a la libertad cognitiva como una propuesta de abordaje a los riesgos de la creciente aplicación de las neurotecnologías en el cerebro humano", *UNIVERSITAS, Revista de Filosofía, Derecho y Política, núm. 45*, 2024, pp. 112-122.

BARONA VILAR, S., "Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia", *Revista Jurídica Digital UANDES, volumen 3, núm. 1*, 2019, pp. 1-17.

BARONA VILAR, S., "Inteligencia artificial o la algoritmización de la vida y de la justicia: ¿solución o problema?", *Revista boliviana de Derecho, núm. 28*, 2019, pp. 18-49.

BELLOVIN, S. M., HUTCHINS, R. M., JEBARA, T. y ZIMMECK, S., "When enough is enough: Location tracking, mosaic theory, and machine learning", *New York University Journal of Law & Liberty, volumen 8, núm. 51*, 2013, pp. 556-628.

BORBÓN, D. y MUÑOZ, J. M., "El neuroderecho a la libertad cognitiva: fundamentos y alcance de un derecho emergente", *IUS ET SCIENTIA, volumen 10, núm. 1*, 2024, pp. 103-131.

BUITRAGO BOTERO, D. M. "El valor de los datos personales en Colombia", *Revista CES Derecho*, volumen 7, núm. 1, Medellín (Colombia), 2016, pp. 1-2.

BUOLAMWINI, J., y GEBRU, T., "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", en *Conference on Fairness, Accountability, and Transparency, Proceedings of Machine Learning Research*, Nueva York (Estados Unidos), 23 y 24 de febrero de 2018, pp. 77-91.

COTINO HUESO, L., "Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal", *El cronista del Estado Social y Democrático de Derecho, núm. 100*, 2022, pp. 68-79.

DE MIGUEL BERIAIN, I. y PÉREZ ESTRADA, M. J., "La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados", *Revista De Derecho De La UNED, núm. 25*, 2019, pp. 531-561.

DÍAZ RODRÍGUEZ, V., "Sistemas biométricos en materia criminal: un estudio comparado", *Revista IUS, volumen 7, núm. 31*, 2013, pp. 28-47.

GÓMEZ COLOMER, J. L., "La prueba científica, motor de cambios esenciales en el proceso penal moderno", *Revista Brasileira de Direito Processual Penal, volumen 7, núm. 2*, Porto Alegre (Brasil), 2021, pp. 1385-1410.

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

ILHAM, A.A. y NURTANIO, I., "Optimización de búsqueda de imágenes con web scraping, procesamiento de texto y algoritmos de similitud de coseno", publicado en la *Conferencia Internacional IEEE de 2020 sobre Comunicaciones, Redes y Satélites (Comnetsat)*, Batam (Indonesia), 17 y 18 de diciembre de 2020, pp. 346-350.

IZQUIERDO CARRASCO, M., "La utilización policial de los sistemas de reconocimiento facial automático", *IUS ET VERITAS, núm. 60*, 2020, pp. 86-103.

JAIN, A. K. y ROSS, A., "Cerrando la brecha: de la biometría a la ciencia forense", *Philosophical Transactions of the Royal Society B: Biological Sciences, volumen 370, núm. 1674*, 2015, ID: 20140254.

LYNCH, N., "Facial Recognition Technology in Policing and Security—Case Studies in Regulation", *Laws, volumen 13, núm. 3*, 2024, 35.

MIRÓ LLINARES, F., "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología, núm. 20*, 2018, pp. 87-130.

PÉREZ ESTRADA, M. J., "La inteligencia artificial como prueba científica en el proceso penal español", *Revista Brasileira de Direito Processual Penal, volumen 7, núm. 2*, 2021, pp. 1385-1385.

RICHARD GONZÁLEZ, M., "Los sistemas biométricos de reconocimiento facial en la Unión Europea en el marco del desarrollo de la Inteligencia Artificial", *Justicia, núm. 1*, 2023, pp. 147-281.

SANABRIA MOYANO, J. E., ROA AVELLA, M. D. P, y LEE PÉREZ, O. I., "Tecnología de reconocimiento facial y sus riesgos en los derechos humanos", *Revista Criminalidad, volumen 64, núm. 3*, 2022, pp. 61-78.

SANTISTEBAN GALARZA, M., "Reconocimiento facial y protección de datos: una respuesta provisional a un problema pendiente", *Revista de Derecho de la UNED, núm. 28*, 2021, pp. 499-526.

TACCA, M. A. T., "El uso de sistemas biométricos con Inteligencia Artificial: ¿una vulneración a los derechos humanos?", *YachaQ: Revista de Derecho, núm.18*, 2025, pp. 27-40.

VIII. WEBGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEDP), "La AEPD analiza en un informe el uso de sistemas de reconocimiento facial por parte de las empresas de seguridad privada", 2020, disponible en: https://www.aepd.es/prensa y-

comunicacion/notas-de-prensa/AEPD-informe-sistemas-reconocimiento-facial-empresas-seguridad-privada.

BERGENGRUENK V., "Ukraine's 'Secret Weapon' Against Russia Is a Controversial U.S. Tech Company", artículo publicado en la versión digital *Time*, 14 de noviembre de 2023, disponible en: https://time.com/6334176/ukraine-clearview-ai-russia.

GARTLAND, C., "Biometrics Are a Grave Threat to Privacy", artículo publicado en la versión digital del diario *The New York Times*, en la sección The Opinion Pages, 5 de julio de 2026, disponible en: https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy.

GREENE, T., "Empresa estadounidense de vigilancia y reconocimiento facial Clearview AI gana recurso contra el RGPD en tribunal británico", artículo publicado en la versión digital de *Cointelegraph*, 19 de octubre de 2023, disponible en: https://es.cointelegraph.com/news/us-surveillance-facial-recognition-firm-clearview-ai-wins-gdpr-appeal-uk-court.

HILL, K., "The Secretive Company That Might End Privacy as We Know It", artículo publicado en la versión digital del diario *The New York Times*, 18 de enero de 2020, disponible en: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

JACK, G., "UK High Court upholds police use of automated facial recognition technology to identify suspects", publicado en la revista digital *Human Rights Law Centre*, 30 de septiembre de 2019, disponible en: https://www.hrlc.org.au/case-summaries/2019-10-30-uk-high-court-upholds-police-use-of-automated-facial-recognition-technology-to-identify-suspects/.

LA MONCLOA, "La Policía Nacional pone en funcionamiento la aplicación informática VeriPol para detectar denuncias falsas", 2018, disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2018/271018veripol.aspx.

IX. JURISPRUDENCIA CITADA

Alto Tribunal de Justicia de Inglaterra y Gales, caso CO/4085/2018, asunto La Reina (a solicitud de Edward Bridges) contra el Jefe de Policía de Gales del Sur. Disponible en vLex: https://vlex.co.uk/vid/the-queen-on-application-818735609.

Audiencia Provincial de Barcelona, sentencia 72/2021, de 15 de febrero. Disponible en vLex: https://vlex.es/vid/870895897.

Tribunal Constitucional Federal de Alemania, sentencia de la Sala Primera, sobre el asunto BvR 2835/17, de 19 de mayo de 2020, paras. 1-332. Disponible en: https://www.bverfg.de/e/rs20200519_1bvr283517en.html.

Tribunal de Justicia de la Unión Europea (Gran Sala), 62022CJ0118, de 30 de enero de 2024 sobre el asunto C-118/22, NG contra Direktor na Glavna direktsia Natsionalna politsia pri Ministerstvo na vatreshnite raboti – Sofia. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62022CJ0118.

Tribunal de Justicia de la Unión Europea (Sala Cuarta), 62021CJ0446, de 4 de octubre de 2024, sobre el asunto C-446/21, Maximilian Schrems contra Meta Platforms Ireland Ltd, anteriormente Facebook Ireland Ltd. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62021CJ0446.

Tribunal Supremo, sentencia 315/2016, de 14 de abril. Disponible en vLex: https://vlex.es/vid/637465525.