Anuario da Facultade de Dereito da Universidade da Coruña

Vol. 26 (2022), pp. 64-88

ISSNe: 2530-6324 || ISSN: 1138-039X

DOI: https://doi.org/10.17979/afdudc.2022.26.0.9145

EL RECONOCIMIENTO FACIAL COMO INSTRUMENTO DE INVESTIGACIÓN Y PREVENCIÓN DEL DELITO

FACIAL RECOGNITION AS A CRIME INVESTIGATION AND PREVENTION TOOL

ANTÓN FRUCTUOSO FREIRE MONTERO
Fiscal - Fiscalía de Área de Ferrol
https://orcid.org/0000-0003-3056-1450

Recibido: 04/06/2022
Aceptado: 06/10/2022

Resumen: El reconocimiento facial es una moderna técnica de identificación biométrica susceptible de ser empleada en el ámbito de la investigación delictiva, así como en el campo de la seguridad. Tras la promulgación de la LO 7/2021, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, las autoridades españolas cuentan con un respaldo normativo para emplear dicha tecnología en este contexto; sin embargo, es preciso considerar su impacto en los derechos fundamentales de los ciudadanos, especialmente en el ámbito de la privacidad.

Palabras clave: Reconocimiento facial-Biometría-Inteligencia Artificial-Investigación y prevención de delitos-Privacidad.

Abstract: Facial recognition is a modern biometric identification technique that can be used in the field of criminal investigation, as well as in the field of security. After the enactment of Spanish Act on Data Protection in the Area of Police and Criminal Justice -Organic Law 7/2021-, Spanish authorities have regulatory support for using such technology in this context; however, its impact on the fundamental rights of citizens, especially in the area of privacy, must be considered.

Keywords: Facial recognition-Biometrics-Artificial Intelligence-Crime investigation and prevention-Privacy

Sumario: **I. INTRODUCCIÓN. BIOMETRÍA: CONCEPTO Y RÉGIMEN JURÍDICO. II. EL RECONOCIMIENTO FACIAL Y SU POSIBLE APLICACIÓN COMO INSTRUMENTO DE INVESTIGACIÓN DELICTIVA. III. EL RECONOCIMIENTO FACIAL AUTOMÁTICO Y SU POSIBLE USO COMO INSTRUMENTO DE PREVENCIÓN DEL DELITO. IV. CONCLUSIONES.**

* * *

I. INTRODUCCIÓN. BIOMETRÍA: CONCEPTO Y RÉGIMEN JURÍDICO

Un adecuado estudio del reconocimiento facial debe comenzar por señalar que se trata de una técnica enmarcada dentro de la biometría. La biometría es, según el diccionario de la RAE, el «estudio mensurativo o estadístico de los fenómenos o procesos biológicos». En opinión de Martín Brañas[1], es necesario que la biometría se sustente sobre la base de tres elementos: a) universalidad -todos los individuos somos portadores de determinadas características aptas para ser medidas y cuantificadas-, b) singularidad -esas características que todo sujeto posee son muchas veces dispares y sirven para resaltar la individualización de cada uno frente al resto-, y c) permanencia -pues se trata de elementos inalterables que perduran en el tiempo-. Además, este autor señala que, con independencia del factor biométrico del que se haga uso, el procedimiento de identificación siempre contará con cuatro fases: i) captura de datos, ii) procesado de esos datos, iii) extracción de peculiaridades y iv) comparación de los datos extraídos con los previamente almacenados.

Las técnicas de reconocimiento más conocidas son seguramente el análisis de las huellas dactilares o de los rasgos faciales de un individuo; no obstante, en realidad la biometría comprende técnicas muy variadas[2]. En este sentido, Rodríguez-Piñeiro Royo[3] distingue tres clases de datos biométricos: En primer lugar, pueden mencionarse los datos llamados «fisiológicos» (a), que se refieren a características físicas y fisiológicas de la persona; los datos fisiológicos más frecuentemente utilizados son la huella dactilar, el iris, la geometría de la mano, la retina, los vasos sanguíneos en determinadas partes del cuerpo, la voz, el sudor, las orejas y el ADN. En segundo lugar, nos encontramos con una categoría conformada por aquellos datos biométricos relacionados con el comportamiento de la persona: con sus actuaciones o con la forma en que realizan ciertas conductas (b); entre éstos destacan la escritura de un sujeto, su ritmo cardíaco, ritmo respiratorio, la firma, la manera en que utiliza un teclado, la forma de conducir, la forma de andar o de moverse, y

[1] MARTÍN BRAÑAS, Carlos, «Reconocimiento del delincuente: nuevas diligencias de identificación», *Boletín del Ministerio de Justicia*, *Año LXIX, Número 2182*, octubre de 2015, págs. 24 y 25.

[2] Sobre los múltiples sistemas de reconocimiento biométrico también puede consultarse a ESCAJEDO SAN EPIFANIO, Leire, *Tecnologías biométricas, identidad y Derechos fundamentales*, Editorial Aranzandi, Navarra, enero 2017, págs. 3 a 5.

[3] RODRÍGUEZ-PIÑEIRO ROYO, Miguel, «Las facultades de control de datos biométricos del trabajador», *Revista Temas Laborales*, número 150/2019, pág. 94.

la marcha. Finalmente, el autor explica que el Grupo de Trabajo del artículo 29[4] identifica un tercer tipo de controles biométricos (c), al que este organismo califica como «emergente», y que serían los de corte psicológico: la forma de reaccionar de la persona ante ciertas situaciones o pruebas, que pueden dar lugar a un perfil psicológico de ésta.

Por otra parte, la biometría también ha sido definida normativamente en el Reglamento 2016/679[5], disponiendo su artículo 4 que por «datos biométricos» han de entenderse 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»; por lo tanto, esta mención legal permite colegir que, sin lugar a duda, esta clase de datos entran en la categoría de los llamados «datos personales». No obstante, este tipo de información, además de constituir un «dato personal», es susceptible de ser incardinada en una categoría de datos merecedores de una «especial protección», señalando el artículo 9 del citado Reglamento que -salvo en las excepciones que figuran en el apartado 2- «queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física». Además, los datos biométricos se definen de forma idéntica en el artículo 3 apartado 13 de la Directiva 2016/680[6], previéndose igualmente unas reglas de tratamiento más estrictas en su artículo 10[7]. Tales normas de protección han sido objeto de trasposición en nuestro ordenamiento jurídico a través del artículo 9 de la LO 3/2018, de protección de datos de carácter personal y garantía de los derechos digitales[8], así como en el artículo 13 de la reciente LO 7/2021,

[4] Se trata de un órgano consultivo de la UE en materia de protección de datos y privacidad que opera de manera independiente. Recibe esta denominación debido a que fue creado por aplicación del artículo 29 de la Directiva 95/46/CE, y sus funciones se describen en el artículo 30 de esta Directiva, así como en el artículo 15 de la Directiva 2002/58/CE.

[5] Reglamento 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).

[6] Directiva 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.

[7] Artículo 10 del Reglamento 2016/680. Tratamiento de categorías especiales de datos personales.
El tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones 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 se permitirá cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado y únicamente cuando: a) lo autorice el Derecho de la Unión o del Estado miembro; b) sea necesario para proteger los intereses vitales del interesado o de otra persona física, o c) dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

[8] Artículo 9. Categorías especiales de datos.

de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales[9]. Finalmente, cabría hacer mención también al Convenio número 108 del Consejo de Europa, de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal; en relación con dicho texto, se aprobó en el año 2018 un Protocolo de modificación con el objeto de regular el tratamiento automatizado de datos personales, siendo ratificado por España el día 28/1/2021, y recogiéndose en su artículo 6.1 una expresa mención a los datos biométricos, nuevamente designados como una «categoría especial de datos»[10].

Este panorama legislativo conduce a la meridiana conclusión de que, en Europa en general y en España en particular, existe un nivel más elevado de protección en el tratamiento de los datos biométricos. Este superior estándar tuitivo responde al hecho de que su análisis o tratamiento implica una mayor afectación de los derechos fundamentales de la persona en cuestión; en opinión de Pérez de los Cobos Orihuel[11], el tratamiento de datos biométricos presenta un especial riesgo, por revelar información relativa a la salud y al parentesco, afectando al interesado y a terceros, o por permitir la identificación de una persona de forma única. En la misma dirección, la AEPD[12] ha advertido que la utilización de técnicas de análisis biométrico puede provocar la revelación no deseada de ciertos datos relativos al interesado y que poseen un marcado carácter íntimo, tales como su raza o género, su estado emocional, enfermedades, discapacidades y características genéticas, consumos de sustancias tóxicas… Así mismo, se ha escrito con acierto que el empleo de

---

1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.
Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda. (…)

[9] Artículo 13. Tratamiento de categorías especiales de datos personales.
1. El tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones 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, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física, sólo se permitirá cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado y cuando se cumplan alguna de las siguientes circunstancias:
a) Se encuentre previsto por una norma con rango de ley o por el Derecho de la Unión Europea.
b) Resulte necesario para proteger los intereses vitales, así como los derechos y libertades fundamentales del interesado o de otra persona física.
c) Dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos (…).

[10] El texto modificado del Convenio puede leerse igualmente en la página web del Consejo de Europa: https://www.coe.int/es/web/data-protection/convention108/modernised. Así mismo, puede consultarse el estado del proceso de ratificación por los diversos Estados parte en la página web del Consejo de Europa, en la dirección electrónica https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223.

[11] PÉREZ DE LOS COBOS ORIHUEL, Francisco de Asís, *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho Comparado*, Consejo de Europa, Estudio, 2018, pág. 15.

[12] Vid. la nota informativa «14 equívocos con relación a la identificación y la autenticación biométrica», AEPD, junio de 2020, punto 2. Disponible para consulta en la dirección electrónica https://www.aepd.es/sites/default/files/2020-06/nota-equivocos-biometria.pdf.

datos biométricos puede suponer una intensa injerencia en la privacidad del interesado y revelar una información muy sensible, no sólo porque se trata de datos personales, sino también porque son permanentes[13]. Esta circunstancia invasiva ha sido puesta de manifiesto recientemente en el ámbito laboral, al estudiar la utilización por parte del empleador de sistemas de control biométrico sobre los trabajadores, produciéndose en estos casos una supervisión del empresario con un carácter menos personal, pero no por ello menos invasivo[14]; igualmente, se han señalado los peligros inherentes al uso de esta clase de instrumentos de control laboral por parte de la Administración sobre los empleados públicos[15].

Parece evidente, por todo lo anteriormente referido, que en el tratamiento de datos biométricos queda nítidamente comprometido el derecho a la protección de datos de carácter personal (art. 18.4 CE), pudiendo verse concernido también el derecho a la intimidad de la persona en cuestión (art. 18.1 CE), en el caso de se extraiga de tales datos una información que pueda considerarse enmarcada en ese «ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario -según las pautas de nuestra cultura- para mantener una calidad mínima de la vida humana»[16]. Esta consideración obligará a valorar las circunstancias de cada caso en concreto, determinando en qué ocasiones los datos biométricos proporcionan una información relativa a esa parcela que el individuo puede querer mantener vedada al conocimiento de terceros. Así, el Tribunal Constitucional[17] no entendió que se afectase la intimidad personal -y en concreto, la

[13] GARTLAND, Claire, «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*, 5/7/2016. Puede consultarse en la dirección electrónica https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy.

[14] MERCADER UGUINA, Jesús R., «El futuro del trabajo y del empleo en la era de la digitalización y de la robótica», en la obra *Sociedad Digital y Derecho*, PIÑAR MAÑAS, José Luis; DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, Tomás, (Dir.), Imprenta Nacional del Boletín Oficial del Estado, Madrid, 2018, pág. 616.

[15] ARRÚE MENDIZÁBAL, Marta, «Los derechos a la intimidad, a la propia imagen y a la protección de datos de los empleados públicos vs el control por parte de la Administración», en *Revista General de Derecho del Trabajo y de la Seguridad Social, número 54, 2019*, punto 1.3. El artículo puede consultarse en la dirección electrónica http://laadministracionaldia.inap.es/noticia.asp?id=1510754. En particular, la autora advierte del peligro subyacente en el empleo de «aquellos datos biométricos que permiten obtener otra información personal que, no siendo necesaria para la identificación del trabajador, podría ser utilizada de forma discriminatoria. Así, por ejemplo, el iris puede desvelar el consumo de drogas, alcohol, o el padecimiento de algún tipo de enfermedad como la diabetes o la hipertensión, datos íntimos especialmente protegidos…».

[16] Vid. la sentencia del Tribunal Constitucional 231/1988, de 2 de diciembre, Fundamento Jurídico 2º.

[17] Véase el auto del TC 57/2007, de 26 de febrero, F. Jco. 4º: «De acuerdo con lo que acaba de exponerse carece de todo sustento constitucional afirmar que el derecho a la intimidad corporal se ve vulnerado por la utilización de la mano como instrumento identificativo. El ámbito de intimidad corporal constitucionalmente protegido protege "el sentimiento de pudor personal, en tanto responda a estimaciones y criterios arraigados en la cultura de la propia comunidad" (STC 218/2002, de 25 de noviembre, FJ 4). Es obvio que el derecho a la intimidad corporal no protege frente a una actuación como la presentación de la mano a una máquina o escáner, pues no puede decirse que entre en colisión con el criterio de recato arraigado socialmente acerca de la parte del cuerpo humano afectada, cuyo empleo a fines de identificación tiene, por lo demás, una ya larga tradición en nuestro país, en el que la impresión dactilar está incorporada al documento nacional de identidad desde hace tiempo…».

intimidad corporal- de un empleado público al que se le exigía aportar el perfil biométrico de su mano, con la finalidad de implantar un sistema de control de permanencia del personal, mediante el uso de un equipo digital en cuya base de datos se introduciría este perfil; en un contexto diverso, el Tribunal de Estrasburgo[18] consideró recientemente que la retención por el Estado británico de las huellas dactilares de un individuo, durante aproximadamente 7 años y sin contar con su consentimiento, sí supuso una injerencia en su vida privada, en el sentido convencional de la expresión -artículo 8 CEDH-.

En el ámbito de la investigación de delitos, la potencialidad lesiva que subyace en el empleo de esta categoría de datos se comprende mejor si se contempla desde la óptica de la denominada «teoría del mosaico de la privacidad». Esta tesis, con origen en la doctrina norteamericana, sostiene que las injerencias estatales en la privacidad de los ciudadanos pueden venir constituidas, bien por un acto individual del Estado (A), o bien por una secuencia de actos, cada uno de los cuales ostenta una inferior intensidad lesiva si son analizados por separado, pero que se enmarcan en una investigación más compleja y prolongada en el tiempo (B); en este último supuesto, cada uno de los actos individuales del Estado podrían definirse como simples teselas de un mosaico, debiendo valorarse la afectación de la privacidad del individuo observando el resultado conjunto de todos los actos o datos recabados, es decir, contemplando el mosaico en su integridad[19]. En los supuestos de investigaciones continuadas en el tiempo (B), debe considerarse además la posibilidad de que los órganos del Estado lleven a cabo procesos de almacenamiento y tratamiento automatizado de datos que permitan configurar un «perfil» o «fichero»[20] de la persona, lo cual puede constituir una injerencia en la privacidad, tal como ha sido advertido por la doctrina[21] y por la jurisprudencia del Tribunal Europeo de Derechos Humanos[22]; así mismo, ha de valorarse la capacidad de combinar la recogida de datos biométricos con otras modernas diligencias de investigación que permiten a las autoridades elaborar, en palabras

[18] Véase en esta línea la SETDH Gaughran vs United Kingdom, de 13 de junio de 2020, punto 63.

[19] Puede consultarse en esta línea la definición que de la referida teoría efectúan BELLOVIN, Steven M., HUTCHINS, Renée M., JEBARA, Tony & ZIMMECK, Sebastian, «When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning», en *New York University Journal of Law & Liberty [Vol. 8:555], 2014*, pág. 570.

[20] Debe mencionarse en esta línea la definición que de ambos conceptos es ofrecida por la anteriormente citada Directiva 2016/680, en cuyo artículo 3 punto 4) se describe la «elaboración de perfiles» como «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física»; por otra parte, en el punto 6) del mismo precepto se considera «fichero» a «todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o dispersado de forma funcional o geográfica».

[21] VELASCO NÚÑEZ, Eloy, «Tecnovigilancia, geolocalización y datos: aspectos procesales penales», artículo publicado en el *Diario La Ley*, *número 8338*, Sección Doctrina, 23/6/2014, pág. 3. En opinión del autor, estos perfiles que se crean sobre datos que aislados parecen inocuos, pero que convenientemente tratados vulneran nuestra privacidad, están obligando al Derecho a reinterpretar la necesidad de protegernos de ese plus de injerencia en la privacidad que aportan las máquinas.

[22] El Tribunal de Estrasburgo ha declarado que la recogida y almacenamiento por parte de agentes del Estado con carácter sistemático de datos de un individuo -v. gr., estudios, actividades políticas o antecedentes penales-, configurando un "fichero» relativo al sujeto, supone una injerencia en la privacidad de la persona (vid. STEDH Rotaru vs Rumanía, de 4 de mayo de 2000, puntos 43 y 44).

de la Sala Segunda del Tribunal Supremo, una «radiografía ideológica o religiosa»[23] del investigado. Sin duda, esta «radiografía», «fichero» o «perfil» tendría un carácter mucho más detallado e invasivo en el caso de que el Estado tuviese la capacidad de captar, manejar y almacenar datos biométricos de la persona en cuestión; adoptando la teoría anteriormente citada, podría decirse que estos datos conforman algunas de las teselas centrales, posiblemente las más relevantes o reveladoras, del mosaico de la privacidad de cada individuo.

II. EL RECONOCIMIENTO FACIAL Y SU POSIBLE APLICACIÓN COMO INSTRUMENTO DE INVESTIGACIÓN DELICTIVA

Una de las modernas posibilidades que se presentan al investigador penal, asociada a la técnica de captación de imágenes, es el uso de datos biométricos; en concreto, nos referiremos aquí al empleo de procedimientos de análisis de los rasgos faciales de un individuo: el reconocimiento facial, también llamado «reconocimiento biométrico de los rostros de las personas»[24]. Se trataría de extraer esta clase de datos de las imágenes del autor de un hecho delictivo que hayan sido captadas previamente en el ejercicio de la videovigilancia -preventiva o investigativa-, para posteriormente someter tales datos a determinados procesos de análisis que desemboquen en la determinación, con un elevado grado de certeza, de la identidad de esa persona. Es decir, nos hallaríamos ante la aplicación de las técnicas de análisis biométrico en relación con el material fotográfico y/o videográfico de la persona presuntamente responsable de un ilícito penal, bien hayan sido estas imágenes captadas por agentes de la policía judicial en ejercicio de funciones de investigación -art. 588 quinquies a) de la LECrim-, bien por los dispositivos de grabación

[23] STS 141/2020, de 13 de mayo, de la Sala Segunda, Fundamento de Derecho 2º. En este sentido, el TS se pronuncia sobre la afectación a la intimidad del investigado que puede generarse con el empleo de dispositivos de localización por GPS: «La intimidad como valor constitucional adquiere importantes matices axiológicos en función del alcance y la intensidad de la intromisión que cada uno de esos instrumentos tecnológicos permita. Sin embargo, tal forma de razonar no puede llevarnos a banalizar el acto de intromisión estatal que la utilización de un GPS representa en el círculo de derechos fundamentales de cualquier ciudadano. No faltarán los casos en que el conocimiento del lugar exacto en que se halla una persona se limite a otorgar una ventaja operativa a los investigadores. Pero son también imaginables espacios de ubicación que pierden su aparente neutralidad para precipitar una radiografía ideológica o religiosa del investigado. La asistencia a actos públicos de una determinada formación política, el seguimiento de actos de culto de una u otra confesión religiosa, la presencia en centros de ocio expresivos de la opción sexual del investigado o, en fin, la permanencia en un centro sanitario para cualquier intervención quirúrgica, son datos personales que pueden afectar al núcleo duro de la intimidad y quedar al descubierto si no se protege adecuadamente al ciudadano frente a la tentación de los poderes públicos de extremar injustificadamente los mecanismos de injerencia».

[24] SANCHÍS CRESPO, Carolina, «Principios rectores en la adopción de diligencias limitativas de los derechos reconocidos en el artículo 18 CE», artículo publicado en *Revista Boliviana de Derecho, número 31*, enero 2021, pág. 242. La autora menciona el reconocimiento biométrico de los rostros de los individuos como una de las mejoras fundamentales que puede proporcionar la tecnología en el marco de la investigación penal; no obstante, también advierte que estas mejoras, pudiendo ser tremendamente útiles en las pesquisas penales, «al mismo tiempo ponen en serio peligro, cuando no violentan directamente, los derechos fundamentales de las personas investigadas».

instalados con finalidad preventiva, ya sean estos de titularidad pública -artículos 22 de la LO 4/2015[25] y 1 de la LO 4/1997[26]-, o privada -artículo 42 de Ley 5/2014[27]-.

En la actualidad es relativamente habitual que las imágenes captadas en este contexto registren a individuos que se encuentran directa o indirectamente relacionados con la comisión de un delito, suponiendo entonces tales documentos gráficos una pieza clave para la investigación del hecho y la eventual destrucción de la presunción de inocencia del acusado[28]. Así mismo, es muy común que la persona encausada alegue no ser la que figura en las imágenes obrantes en la causa, manifestando a las autoridades que se trata de otro sujeto con una apariencia muy similar a la suya. En este contexto, el análisis de los rasgos faciales del individuo que aparece representado en las citadas imágenes y su cotejo con las imágenes del rostro del investigado puede constituir una herramienta de gran utilidad, determinando la coincidencia o no entre los datos analizados. En palabras de la Sala Segunda, «no es infrecuente que (…) los investigadores, que reconocieron al recurrente desde el primer momento por ser conocido para los mismos por detenciones anteriores, (…) procediesen a confirmar tal identificación a través del informe pericial comprensivo de un estudio fisionómico realizado a partir de las imágenes obtenidas de las cámaras de seguridad de la entidad bancaria -como dubitadas- y aquellas otras obtenidas de las reseñas fotográficas realizadas al tiempo de su detención -como indubitadas-»[29].

La Red de Laboratorios Forenses[30] de nuestro país define el estudio de identificación facial como un proceso tendente a comparar los rasgos faciales de dos individuos a partir de dos tipos de imágenes: (i) dubitadas e (ii) indubitadas. Las imágenes dubitadas (i) serían aquellas en las que se representan -con un nivel de nitidez suficiente- a uno o a varios individuos de identidad desconocida y que se hallan implicados en la perpetración del hecho delictivo -v.gr. las videograbaciones captadas por las cámaras de seguridad de un establecimiento comercial que ha sido objeto de un robo con fuerza-. Por otra parte, las imágenes indubitadas (ii) serían aquellas imágenes del investigado que las autoridades conservan en su poder, y que se sabe fehacientemente que corresponden a esta persona -normalmente, estas proceden de fuentes policiales, tales como las fotografías de una reseña policial o las correspondientes al documento de identidad-. Posteriormente, mediante la comparación de los rasgos existentes en las imágenes dubitadas e indubitadas

[25] LO 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana.
[26] 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.
[27]Ley 5/2014, de 4 de abril, de Seguridad Privada.
[28] Debe puntualizarse que el alcance incriminatorio de las imágenes será diferente en función de las circunstancias en las que sea captado el sujeto. Así, podrá constituir una prueba directa si en las imágenes se refleja con claridad a la persona cometiendo el hecho delictivo; por contra, será un mero indicio si, v.gr., muestra al individuo accediendo o abandonando el *locus criminis*, en los momentos anteriores o posteriores a la comisión del hecho, respectivamente.
[29] Véase en esta dirección el ATS 716/2020, de 15 de octubre, de la Sala Segunda, Fundamento de Derecho 1º.
[30] Vid. *Guía sobre estudios de identificación facial para jueces, fiscales e investigadores*, Red de Laboratorios Forenses Oficiales de España, Grupo de Trabajo en Identificación Facial, segunda revisión, marzo de 2021, punto 2.

se obtendrán analogías o discrepancias, que darán como resultado un determinado grado de similitud o de discrepancia entre los rostros estudiados.

Es conveniente resaltar que tal actividad no consiste en una mera observación o contemplación a simple vista de las imágenes captadas, sino que se procede a un análisis de los rasgos faciales, empleando para ello medios técnicos específicos que permitirán identificar de manera unívoca a una persona; esta circunstancia es muy significativa, pues como destaca el Reglamento 2016/679[31], esto determinará que no nos hallemos ante el simple tratamiento de datos personales, sino que se proceda al manejo de datos biométricos, merecedores por ende de una especial protección. Por otra parte, esta mecánica implica igualmente diferencias en un sentido procesal y probatorio, ya que el empleo de esta técnica no tendrá la consideración de prueba documental -como sí sucede con la reproducción de fotografías o vídeos de los hechos-, sino que deberá ser articulada como una prueba pericial; en consecuencia, habrán de ser citados a juicio los peritos fisionomistas autores del informe pertinente, a fin de que expliquen al Tribunal los procedimientos de análisis llevados a cabo para llegar a la conclusión de que la persona representada en las imágenes es -o no- el acusado.

En estos casos, la conjunción de ambos medios de prueba: (a) reproducción de las imágenes en las que se observa con claridad el rostro de un individuo relacionado directa o indirectamente con el hecho delictivo -prueba documental- y (b) resultado positivo de un análisis de identificación facial -prueba pericial-, implicará un soporte probatorio con un especial poder de convicción acerca de la participación del acusado en la comisión del hecho, debiendo respetarse siempre el principio de la apreciación de la prueba en conciencia por el Tribunal -artículo 741 LECrim-. Sobre el valor probatorio que esta diligencia puede alcanzar, la jurisprudencia[32] ha destacado la «precisión» que actualmente puede lograrse en la «comparación y medición entre dos rostros a partir de dos fotogramas». En un sentido contrario, el resultado negativo de un análisis de identificación facial será un elemento de signo favorable para el reo, bien constituyendo una circunstancia

[31] En esta línea, el considerando 51 del Reglamento dispone: El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física (…).

[32] Vid. STS 315/2016, de 14 de abril, Fundamento de Derecho 2º. La resolución es de interés para comprender los avances experimentados en relación con la efectividad de la técnica de reconocimiento facial; para ello la sentencia cita las consideraciones que sobre el valor de esta prueba se efectuaban por un pronunciamiento muy anterior (STS 61/2000, de 27 de enero de 2001): «Así como la identificación por las huellas dactilares (dactiloscopia) tiene un amplio consenso en el mundo científico de la criminalística, por la pluriformidad y variabilidad infinita de las crestas papilares, la pericia antropomórfica debe ser valorada con más cautela en cuanto utiliza rasgos o partes del rostro y del cuerpo de la persona para establecer la identidad. El universo de los signos distintivos que emplea esta última ciencia, nos sitúa ante un espectro de población muy amplio en el que pueden darse coincidencias o similitudes entre variados grupos de personas. Las partes del rostro de las personas, no son irrepetibles como sucede con las huellas dactilares, sino que pueden presentar características cercanas entre sí que, nos llevaría a la formación de un grupo de varias personas con rasgos similares a la que se trata de identificar. No hay obstáculo, paraque 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…».

determinante para conducir al dictado de una sentencia absolutoria, bien pudiendo conllevar con carácter previo el dictado de un auto sobreseimiento provisional de la causa respecto del investigado, ex artículos 2 y 641.2º de la LECrim.

La posibilidad de tratamiento de datos biométricos del investigado no goza, sin embargo, de un apoyo expreso en la LECrim. Naturalmente, el legislador primigenio no pudo ni tan siquiera haber imaginado tales posibilidades técnicas en el año 1882; sin embargo, existiendo ya un notable grado de conocimiento sobre el reconocimiento facial, no se aprovechó la reforma operada por la LO 13/2015[33] para incluir una referencia a esta diligencia. Sí se incluye una mención tangencial en el Anteproyecto de LECrim de 2020, al abordar, dentro de los «medios de investigación basados en datos protegidos», el «acceso y tratamiento a datos personales»; así, el artículo 516 de este texto introduce una diligencia de investigación consistente en el «cruce automatizado o inteligente de datos»[34]. En cualquier caso, hoy en día su utilización podría admitirse a través de una interpretación actualizada de las reglas de la norma procesal referentes a la «determinación del delincuente y sus circunstancias personales» - situadas en el Libro II, Título V, Capítulo III de la LECrim-. En particular, el artículo 373 de la LECrim señala que «Si se originase alguna duda sobre la identidad del procesado, se procurará acreditar ésta por cuantos medios fueren conducentes al objeto»; además, el artículo 374 del mismo texto legislativo ofrece otro soporte para la práctica de esta diligencia al establecer que: «El Juez hará constar, con la minuciosidad posible, las señas personales del procesado, a fin de que la diligencia pueda servir de prueba de su identidad».

La cuestión clave en este punto será determinar qué garantías se deberían de observar para poner en práctica esta medida, pues si bien la captación de imágenes en vías o lugares públicos es una diligencia de naturaleza meramente policial -art. 588 quinquies a) de la LECrim-, es razonable cuestionarse si el análisis de datos biométricos puede practicarse igualmente sin la intercesión judicial. Ante la inexistencia de una norma específica en ley procesal penal[35], actualmente será necesario consultar lo previsto en la LO

[33] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

[34] Artículo 516. Cruce automatizado o inteligente de datos.

1. A instancia del Ministerio Fiscal, el Juez de Garantías podrá autorizar la utilización de sistemas automatizados o inteligentes de tratamiento de datos para cruzar e interrelacionar la información disponible sobre la persona investigada con otros datos obrantes en otras bases de titularidad pública o privada, siempre que concurran los siguientes requisitos: a) que existan indicios basados en datos objetivos sobre la participación del investigado en los hechos objeto de investigación; b) que, en base a la naturaleza y características del hecho, resulte necesaria la práctica de la diligencia para esclarecer la responsabilidad del investigado en el mismo; y c) que el hecho investigado sea constitutivo de un delito castigado con una pena igual o superior a los tres años de prisión. 2. El acceso a las bases de datos con las que se realice el cruce o interrelación se regirá por lo dispuesto en el artículo anterior. 3. En todo caso, cuando la práctica de esta diligencia dé lugar al tratamiento de datos cuya cesión o uso esté sometido a autorización judicial, esta deberá recabarse con carácter previo a su realización.

[35] En el actual articulado de la LECrim, tan sólo hallamos normas que contendrían una habilitación genérica a los agentes de la autoridad para realizar esta diligencia; así, el artículo 282 en su párrafo primero dispone: «La Policía judicial tiene por objeto, y será obligación de todos los que la componen, averiguar los delitos públicos que se cometieren en su territorio o demarcación; practicar, según sus atribuciones, las diligencias

7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales[36]. La norma básica en este punto vendría establecida en el artículo 13.2 de esta Ley: «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». Esta disposición parece habilitar a la policía judicial a practicar de manera autónoma el análisis de reconocimiento facial, teniendo en cuenta lo que la LO 7/2021 considera «autoridades competentes»[37], «tratamiento»[38] y «datos biométricos»[39]. La misma conclusión parece desprenderse al examinar el Preámbulo de esta norma, en donde el legislador hace una mención de carácter expreso al tratamiento de imágenes faciales con la finalidad de investigación delictiva; así, en su punto IV establece que «…se exige que el tratamiento de categorías especiales de datos, como son los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical o los genéticos o biométricos, sólo pueda tener lugar cuando sea estrictamente necesario y se cumplan ciertas condiciones. Los datos biométricos (como las huellas dactilares o la imagen facial) sólo se consideran incluidos en esta categoría especial cuando su tratamiento está dirigido a identificar de manera unívoca a una persona física. Esta necesidad de identificación en las actuaciones amparadas legalmente se lleva a cabo, con frecuencia, por las distintas autoridades competentes. El propósito es singularizar los autores o partícipes de infracciones penales, así como poder reconocer si son las personas que se supone o se busca, y de esta forma, atribuir o exonerar, sin género de dudas, la participación en determinados hechos, gracias a posibles indicios o vestigios biométricos...». Además, tal

necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la Autoridad judicial».

[36] El artículo 1 de la LO 7/2021 dispone que el objeto de la norma será fijar «las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública».

[37] Artículo 4.1: Será autoridad competente, a los efectos de esta Ley Orgánica, toda autoridad pública que tenga competencias encomendadas legalmente para el tratamiento de datos personales con alguno de los fines previstos en el artículo 1.

En particular, tendrán esa consideración, en el ámbito de sus respectivas competencias, las siguientes autoridades:

a) Las Fuerzas y Cuerpos de Seguridad (…).

2. También tendrán consideración de autoridades competentes las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.

[38] Artículo 5.1: A los efectos de esta Ley Orgánica se entenderá por: b) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción

[39] Artículo 5.1 A los efectos de esta Ley Orgánica se entenderá por: l) «datos biométricos»: 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.

análisis podrá practicarse sin contar con el consentimiento del interesado, ex artículo 236 ter apartado 3 de la LOPJ[40] -en la redacción dada por la propia LO 7/2021-, lo cual supone una excepción a la «idea fundamental»[41] que subyace en el derecho fundamental a la protección de datos: que para la recogida, tratamiento y cesión de los datos de otra persona se debe disponer del consentimiento de esta.

En cualquier caso, la utilización de esta técnica habrá de realizarse siempre con observancia del principio de proporcionalidad, criterio que goza de un especial predicamento en el ámbito de la videovigilancia y la captación policial de imágenes[42]; en este sentido, debe considerarse que nos hallamos ante una diligencia susceptible de ser realizada sin la previa autorización del juez instructor, principal garante del respeto a los derechos fundamentales del investigado[43]. En nuestra opinión, será preciso (i) limitar el análisis de los rasgos faciales únicamente hasta el grado preciso para que los peritos puedan lograr la identificación -o no identificación- del acusado, vedando la posibilidad de extraer otra información del sujeto que ostente un carácter íntimo y sea innecesaria para los fines de la investigación – v. gr., consumo de drogas, su estado emocional, el padecimiento de alguna enfermedad o discapacidad, sus características genéticas…- Por otra parte, (ii) deberá procederse a la destrucción de los datos biométricos captados tan pronto como sea posible, evitando su almacenamiento y conservación en poder de las autoridades por más tiempo del imprescindible para la investigación del delito; esta destrucción, que impedirá la hipotética formación de «perfiles» o «archivos» con el significado que referíamos en el apartado anterior, es además una consecuencia de la supresión de datos de carácter personal, lo cual se configura como un derecho para el interesado y un deber para las autoridades -artículos 8.1 y 26 de la LO 7/2021, y artículo 236 quinquies de la LOPJ-.

---

[40] Artículo 236 ter.3 de la LOPJ: No será necesario el consentimiento del interesado para que se proceda al tratamiento de los datos personales en el ejercicio de la actividad jurisdiccional, ya sean éstos facilitados por las partes o recabados a solicitud de los órganos competentes, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba.

[41] ESPÍN LÓPEZ, Isidoro, «Los derechos fundamentales a la vida privada afectados por la investigación tecnológica y el fenómeno del entorno virtual», estudio doctrinal publicado en el *Boletín Oficial del Ministerio de Justicia, Año LXXV, Número 2.244*, octubre de 2021, Sección Doctrinal, pág. 51.

[42] Sobre la importancia del principio de proporcionalidad en el desarrollo de esta diligencia de investigación, puede leerse a GIMENO SENDRA, José Vicente, «La prueba preconstituida de la policía judicial», en *Revista catalana de seguretat pública*, *Número 22*, 2010, pág. 42; o NAVAJAS RAMOS, Luis, «La prueba videográfica en el proceso penal: su valor y límites para su obtención», en *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, *número 12*, 1998, pág. 159. En particular, alguna doctrina destaca que la proporcionalidad de la videovigilancia está directamente relacionada con el respeto al «núcleo duro» del derecho a la intimidad -verbi gratia, lo relativo a la vida sexual de un individuo-. Puede leerse en esta dirección a JUANATEY DORADO, Carmen y DOVAL PAIS, Antonio, «Límites de la protección penal de la intimidad frente a la grabación de conversaciones o imágenes», en *La protección de la intimidad*, BOIX REIG, Javier (Dir.) y JAREÑO LEAL, Ángeles (Coord.), Editorial Iustel, Madrid, 2010, pág. 157.

[43] LÓPEZ GUERRA, Luis, «El papel del juez en una sociedad democrática», en *Revista de estudios jurídicos*, *número 18*, año 2018, pág. 5. Para López Guerra, la función del juez en una sociedad democrática se ve así delimitada, formalmente, por la sujeción a la ley como expresión de la voluntad popular, y sustantivamente por el respeto a los derechos fundamentales establecidos tanto en el nivel nacional como en el internacional. Y esta doble delimitación supone una considerable complejidad, en la práctica, en el desarrollo de las funciones judiciales.

III. EL RECONOCIMIENTO FACIAL AUTOMÁTICO Y SU POSIBLE USO COMO INSTRUMENTO DE PREVENCIÓN DEL DELITO

Tras analizar el reconocimiento biométrico del rostro humano como una forma de investigación de los delitos, debe igualmente plantearse la posibilidad de que las autoridades utilicen esta técnica como una herramienta para prevenir su comisión, es decir, como un instrumento dirigido a garantizar la «seguridad ciudadana»[44]. En concreto, se trata de valorar la viabilidad jurídica del uso estatal de técnicas de reconocimiento facial que operan con carácter automático: sin la intervención inmediata de un ser humano. La utilización de esta clase de sistemas es una cuestión que suscita un notable interés en la actualidad, al estar incrementándose rápidamente su uso en el campo de la seguridad. De este modo, la organización INTERPOL cuenta con esta tecnología desde finales del año 2016, empleándola habitualmente para «lograr la identificación de terroristas, delincuentes, prófugos, personas de interés o desaparecidos»[45]. Al otro lado del Atlántico, se estimaba en 2016 que una cuarta parte de los cuerpos policiales de los Estados Unidos disponían de estos medios[46], mientras que las autoridades de ese país reconocieron que aproximadamente la mitad de las agencias federales de investigación contaban ya con tal tecnología en 2021[47]. Además, el reconocimiento facial automático se encuentra en una fase de constante perfeccionamiento a nivel técnico[48], gracias en buena medida al impulso

[44] Una definición auténtica de este bien jurídico puede verse en el Preámbulo de la LO 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, en su punto III, en el cual se describe la seguridad ciudadana como la «actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad de los ciudadanos, que engloba un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, orientadas a una misma finalidad tuitiva del bien jurídico así definido. Dentro de este conjunto de actuaciones se sitúan las específicas de las organizaciones instrumentales destinadas a este fin, en especial, las que corresponden a las Fuerzas y Cuerpos de Seguridad, a las que el artículo 104 de la Constitución encomienda proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana…».

[45] Así se explica en la página web de esta organización: https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Reconocimiento-facial.

[46] GARVIE, Clare, BEDOYA, Álvaro, y FRANKLE, Jonathan, «The Perpetual Line-Up: Unregulated Police Face Recognition in America», *Georgetown Law, Center on Privacy & Technology*, 18/10/2016, disponible en la dirección https://www.perpetuallineup.org/.

[47] Vid. el informe «Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees», *U.S. Government Accountability Office*, 13/7/2021. Puede consultarse este dato en la dirección web https://www.gao.gov/products/gao-21-105309.

[48] RAMOS RUBIO, Carlos, «Jornada sobre videovigilancia policial, experiencia acumulada y perspectivas de futuro», ponencia pronunciada en la Mesa redonda «Colaboración entre videovigilancia pública y privada», organizada por la *Comissió de Control dels Dispositius de Videovigilància de Catalunya* (CCDVC), Barcelona, 3/10/2014, punto II. La ponencia puede consultarse en la dirección electrónica http://interior.gencat.cat/web/.content/home/030_arees_dactuacio/seguretat/videovigilancia_policial/jornada_sobre_videovigilancia_policial/Videovigilancia_3-10-14_RAMOS.pdf. Señalaba el autor la existencia en este ámbito de programas con capacidad para identificar de forma simultánea múltiples caras en movimiento, de manera que «permite registrar sujetos de forma automática mediante captura de vídeo (*on-the-fly*), y funciona correctamente con ocultación parcial de la cara, uso de gafas, pañuelos o gorras, cambios en la expresión facial, condiciones difíciles de iluminación y rotaciones moderadas de la cara», pudiendo emplearse en «entornos de grandes multitudes en movimiento, tales como aeropuertos, estaciones de metro o tren, centros comerciales, estadios deportivos o núcleos urbanos».

que ejercen en este proceso las compañías tecnológicas que se dedican a la comercialización de esta clase de productos.

En la doctrina, Izquierdo Carrasco[49] define el reconocimiento facial automático como un procedimiento técnico de inteligencia artificial consistente en evaluar si dos imágenes faciales representan a una misma persona, basándose para tal fin en la comparación entre dos fuentes de información: de una parte, (a) una base de datos con los datos biométricos faciales -propiedades geométricas, tales como la distancia entre las pupilas, la posición de la nariz o la distancia entre la comisura de los labios- de una serie de personas identificadas -verbi gratia, las que provienen de las fotografías que se realizan a las personas detenidas en dependencias policiales-, y por otra, (b) las imágenes de personas no identificadas de las que un programa informático extrae tales datos biométricos faciales. Así, este procedimiento requiere instalar un elevado número de cámaras de videovigilancia para monitorizar determinadas zonas, v.gr. los recintos en los que se celebren eventos multitudinarios u otros puntos en los que, por diferentes motivos, las autoridades consideren que deben extremarse las medidas de seguridad; las cámaras captan los rasgos faciales de las personas que transitan por estos lugares y a continuación el programa informático procesa tales datos biométricos en tiempo real y los coteja con los obrantes en sus bases de datos, alertando de la presencia de individuos que se hallen incluidos en las listas de vigilancia de la policía. El reconocimiento facial automático se encuentra, por lo tanto, íntimamente vinculado con la videovigilancia, una técnica respecto de la que se ha defendido su notable utilidad en funciones de prevención del delito[50], llegando a ser calificada como «un instrumento privilegiado de control social» [51].

La cobertura normativa de este instrumento ha de buscarse nuevamente en la reciente la LO 7/2021, en cuyo artículo 13.2 se permite a las autoridades manejar datos biométricos no solamente con la finalidad de investigar hechos delictivos, sino también para prevenir su comisión y conjurar las posibles amenazas a la seguridad pública: «Las autoridades competentes, en el marco de sus respectivas funciones y competencias, podrán

[49] IZQUIERDO CARRASCO, Manuel, «La utilización policial de los sistemas de reconocimiento facial automático», artículo publicado en la *Revista Ius et Veritas, número 60*, mayo 2020, pág. 88.

[50] Puede consultarse a este respecto, ORTUÑO RODRÍGUEZ, Alicia Esther, «Doctrina constitucional en relación con el control mediante cámaras de videovigilancia», en *Cuadernos de Derecho Local, número 49*, febrero de 2019, Fundación Democracia y Gobierno Local, pág. 236. En esta línea, la autora refiere que «resulta constatable cómo en los últimos años han proliferado los sistemas de videovigilancia o equipos destinados a la supervisión de la conducta de las personas a través de cámaras, a los cuales pueden recurrir los sujetos públicos y privados para proteger a las personas y bienes en los ámbitos espaciales que les son propios, y que los poderes públicos utilizan a fin de preservar y garantizar la seguridad colectiva. Todos los responsables en la toma de decisión del empleo de cámaras de videovigilancia deben atender a los requisitos legalmente establecidos para su utilización y acerca del tratamiento de los datos personales que se obtienen mediante estos sistemas. (...) El ámbito de protección de la privacidad de las personas no está restringido a su vivienda o a lugares privados, sino que también debe ser protegido incluso en los espacios públicos y en la esfera de trabajo, pues la intimidad y la propia imagen son derechos fundamentales que le son inherentes y que se proyectan alrededor del individuo en cualquier momento y circunstancias, para asegurar una esfera de la personalidad libre de injerencias externas».

[51] Vid. GUERRIER, Claudine, *Security and Privacy in the Digital Era*, ISTE Ltd. And John Wiley & Sons Inc., 1ª Edición, 2016, pág. 202.

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». Un soporte legal mucho más genérico puede hallarse en los artículos 1.2, 3 y 16.1 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana[52].

En nuestra opinión, el empleo de esta técnica como un instrumento de control social ha de realizarse de forma muy cautelosa, siendo además conscientes de que existen instrumentos alternativos para promover esta misma finalidad[53]. Al situarnos fuera del ámbito de la investigación delictiva, la cuestión se traslada al campo de las medidas de carácter preventivo, situándonos en un terreno en el que, como señala Pérez-Cruz Martín[54]

[52] Artículo 1.2: Esta Ley tiene por objeto la regulación de un conjunto plural y diversificado de actuaciones de distinta naturaleza orientadas a la tutela de la seguridad ciudadana, mediante la protección de personas y bienes y el mantenimiento de la tranquilidad de los ciudadanos.
Artículo 3: Constituyen los fines de esta Ley y de la acción de los poderes públicos en su ámbito de aplicación:
a) La protección del libre ejercicio de los derechos fundamentales y las libertades públicas y los demás derechos reconocidos y amparados por el ordenamiento jurídico.
b) La garantía del normal funcionamiento de las instituciones.
c) La preservación de la seguridad y la convivencia ciudadanas.
d) El respeto a las Leyes, a la paz y a la seguridad ciudadana en el ejercicio de los derechos y libertades.
e) La protección de las personas y bienes, con especial atención a los menores y a las personas con discapacidad necesitadas de especial protección.
f) La pacífica utilización de vías y demás bienes demaniales y, en general, espacios destinados al uso y disfrute público.
g) La garantía de las condiciones de normalidad en la prestación de los servicios básicos para la comunidad.
h) La prevención de la comisión de delitos e infracciones administrativas directamente relacionadas con los fines indicados en los párrafos anteriores y la sanción de las de esta naturaleza tipificadas en esta Ley.
i) La transparencia en la actuación de los poderes públicos en materia de seguridad ciudadana.
Artículo 16. Identificación de personas.
1. En el cumplimiento de sus funciones de indagación y prevención delictiva, así como para la sanción de infracciones penales y administrativas, los agentes de las Fuerzas y Cuerpos de Seguridad podrán requerir la identificación de las personas en los siguientes supuestos:
a) Cuando existan indicios de que han podido participar en la comisión de una infracción.
b) Cuando, en atención a las circunstancias concurrentes, se considere razonablemente necesario que acrediten su identidad para prevenir la comisión de un delito.
En estos supuestos, los agentes podrán realizar las comprobaciones necesarias en la vía pública o en el lugar donde se hubiese hecho el requerimiento, incluida la identificación de las personas cuyo rostro no sea visible total o parcialmente por utilizar cualquier tipo de prenda u objeto que lo cubra, impidiendo o dificultando la identificación, cuando fuere preciso a los efectos indicados.
En la práctica de la identificación se respetarán estrictamente los principios de proporcionalidad, igualdad de trato y no discriminación por razón de nacimiento, nacionalidad, origen racial o étnico, sexo, religión o creencias, edad, discapacidad, orientación o identidad sexual, opinión o cualquier otra condición o circunstancia personal o social.

[53] Así, en el ámbito de la ciencia urbanística, algunos autores defienden la importancia de crear en las ciudades espacios que permitan desarrollar en sus habitantes un sentido de cohesión social comunitaria, lógicamente contrario a la comisión de hechos delictivos. Puede consultarse en esta línea a FLORIDA, Richard, *Las ciudades creativas*, Editorial Paidós, Barcelona, 2009, pág. 211.

[54] PÉREZ-CRUZ MARTÍN, Agustín Jesús, «Videovigilancia y derecho a la intimidad: ¿un nuevo ejemplo de conflicto entre el derecho a la seguridad pública y el derecho fundamental a la intimidad?», *Anuario da Facultade de Dereito da Universidade da Coruña, Número 1,* 1997, pág. 402. A su vez, el autor cita a Luchaire, quien expone que el delicado equilibrio entre seguridad y derechos fundamentales es una cuestión

se produce una colisión entre los derechos fundamentales y el derecho a la seguridad pública; como precisa este autor, no debe olvidarse que la seguridad pública es un bien jurídico que no tiene la naturaleza de derecho fundamental, sino que se configura como «una aspiración, un deseo social e individual, un resultado de la eficacia de la protección policial, en ningún caso un valor primero o superior». Existen, en esta línea, varios puntos dignos de consideración a la hora de valorar la utilización de técnicas de reconocimiento facial automático por los poderes públicos.

En primer lugar, es preciso señalar que el empleo de este instrumento se basa en el análisis de los rasgos faciales de los transeúntes y, por lo tanto, las autoridades estarán llevando a cabo un tratamiento de sus datos biométricos. Como ya se indicó anteriormente, debe considerarse en estos supuestos el elevado nivel de injerencia en la privacidad del sujeto identificado, pudiendo los datos biométricos ser fuente de una información muy sensible que, probablemente, muchas personas no deseen revelar. En este punto es necesario aclarar que el reconocimiento facial automático constituye una operación de «identificación biométrica» y no de «autenticación o verificación biométrica». La AEPD[55] ha advertido que se trata de dos conceptos diversos: la identificación biométrica (1) consiste en la identificación de un individuo por un sistema biométrico, siendo normalmente un proceso consistente en comparar sus datos biométricos -adquiridos en el momento de la identificación- con una serie de plantillas biométricas almacenadas en una base de datos, es decir, un proceso de búsqueda de correspondencias uno-a-varios. La verificación o autenticación biométrica (2), sin embargo, supone la comparación entre sus datos biométricos -adquiridos en el momento de la verificación- con una única plantilla biométrica almacenada en un dispositivo, es decir, se trata de un proceso de búsqueda de correspondencias uno-a-uno. Esta es una distinción de gran interés, pues en opinión de este organismo, con carácter general, los datos biométricos únicamente alcanzarán la consideración de «categoría especial de datos» -véase lo referido en el apartado 1 de este trabajo- en los supuestos en que se sometan a un tratamiento técnico dirigido a la identificación biométrica (uno-a-varios), pero no en el caso de verificación/autenticación biométrica (uno-a-uno). Esta consideración nos conduce, nuevamente, a sostener la necesaria observancia del principio de proporcionalidad en la aplicación del reconocimiento facial automático; entre otras cautelas, sería conveniente: i) limitar temporal, espacial y funcionalmente el empleo de esta técnica -es decir, habilitar su uso únicamente en determinados recintos o zonas geográficas, en momentos concretos, y sólo en los supuestos en los que sea preciso garantizar la seguridad a través de una exhaustiva identificación de los viandantes que no podría realizarse satisfactoriamente mediante las tradicionales actuaciones de identificación que son ejercidas de forma personal por parte de los funcionarios policiales-, ii) evitar la extracción de los rasgos faciales de cualquier información íntima y que no sea estrictamente necesaria para la identificación del

---

que, sintomáticamente, surge de forma cíclica en la doctrina, vid. LUCHAIRE, François, «La vidéosurveillance et la fouille des voitures devant le Conseil Constitutionnel», en *Revue de Droit Pénal, núm. 2, 1995*, págs. 575-577.

[55] Vid. Informe jurídico de la AEPD 36/2020, pág. 18. Puede consultarse en la dirección electrónica https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-informe-reconocimiento-facial-examenes.

individuo, y iii) cumplir con el deber legal[56] de supresión de los datos biométricos una vez completado el proceso de análisis y descartada la coincidencia con los datos registrados en las listas policiales.

Una segunda cuestión que merece ser advertida es que el empleo de esta técnica supone dar un paso más en la aplicación de las nuevas tecnologías en el ámbito de la prevención del delito; en este caso no se trata únicamente de manejar datos biométricos, sino que se introduce en este contexto otro componente novedoso: el funcionamiento de sistemas de inteligencia artificial. La inteligencia artificial se conceptúa doctrinalmente como la capacidad de una máquina para percibir y responder a su entorno de forma independiente, así como de realizar labores que normalmente requerirían de la inteligencia y de los procesos de toma de decisiones humanos, pero sin intervención directa de estos[57]. Como se ha advertido por algunos autores, el uso de la inteligencia artificial se está introduciendo rápidamente en múltiples ámbitos de la sociedad[58]. El artículo 14 de la citada LO 7/2021[59] parece dibujar un sistema en el que la «toma de decisiones basadas únicamente en un tratamiento automatizado» de datos personales se concibe con un carácter muy restrictivo cuando este proceso cause efectos jurídicos negativos en la persona interesada o pueda afectarle de una forma significativa. Lo cierto es que, contemplado desde una perspectiva jurídica, el uso de esta tecnología en el seno de procesos de toma de decisiones de relevancia legal plantea notables problemas de objetividad y opacidad, originando una profunda reflexión en la literatura jurídica, en la jurisprudencia e incluso en la legislación, especialmente en el ámbito europeo[60]. En esta dirección, se espera que

[56] El artículo 8.1 de la LO 7/2021 dispone en este sentido: El responsable del tratamiento determinará que la conservación de los datos personales tenga lugar sólo durante el tiempo necesario para cumplir con los fines previstos en el artículo 1.

[57] Esta definición puede leerse en la obra de RIGANO, Christopher, «Using Artificial Intelligence to address criminal justice needs», *National Institute of Justice, 208,* 2019, pág. 1.

[58] BULAMWINI, Joy & GEBRU, Timnit, «Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification», *Proceedings of Machine Learning Research, 81:1–15*, 2018, pág. 1. Artículo disponible para consulta en la dirección https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[59] Artículo 14. Mecanismo de decisión individual automatizado.

1. Están prohibidas las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente, salvo que se autorice expresamente por una norma con rango de ley o por el Derecho de la Unión Europea. La norma habilitante del tratamiento deberá establecer las medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluyendo el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada.

2. Las decisiones a las que se refiere el apartado anterior no se basarán en las categorías especiales de datos personales contempladas en el artículo 13, salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

3. Queda prohibida la elaboración de perfiles que dé lugar a una discriminación de las personas físicas sobre la base de categorías especiales de datos personales establecidas en el artículo 13.

[60] CIPPITANI, Roberto, MIRABILE, Antonella y ONOFRI, Martina, «"Objetividad científica" y sesgos en la toma de decisiones jurídicas: los casos de genética forense y de algoritmos», en *Revista Justicia y Derecho, Volumen 4, número 2*, año 2021, pág. 11. Se efectúa por los autores una exposición de los recientes pasos del legislador a nivel europeo en materia de inteligencia artificial: «La Unión Europea se ocupa en particular del tratamiento automatizado de datos en el artículo 22 del Reglamento (UE) n°2016/679 sobre la protección de datos personales. Además, se considera más ampliamente la cuestión de la utilización de algoritmos e

próximamente se emita un Reglamento europeo sobre inteligencia artificial, habiendo sido publicada ya su propuesta en abril de 2021[61]. Este texto se refiere específicamente al reconocimiento facial automático, al que define como un «sistema de identificación biométrica remota "en tiempo real" en espacios de acceso público»; además, la norma sitúa esta técnica en el ámbito de las prácticas de inteligencia artificial prohibidas, permitiendo su uso únicamente en supuestos muy limitados, con autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente, y exigiendo también a los Estados que establezcan normas internas detalladas para regular el uso de esta tecnología -vid. artículo 5 apartados 1 letra d), 2, 3 y 4 de la propuesta-.

Otra circunstancia relevante es la posibilidad de que se produzcan errores en esta clase de procesos de análisis; en esta línea, algún autor ha calificado los datos biométricos en general como «la peor forma de contraseña posible»[62]. En efecto, y a pesar de que en un principio pueda pensarse lo contrario, el reconocimiento facial automático no se trata de un instrumento infalible. En esta línea, la Red de Laboratorios Forenses de España[63], si bien reconoce grandes avances en el campo del reconocimiento facial automático, merced al progreso de los sistemas de Inteligencia Artificial y del *deep learning*, también pone de manifiesto importantes limitaciones en la práctica, por diversas causas: «A día de hoy ya ofrecen resultados muy interesantes a pesar de que existan ciertas limitaciones en la imagen como la resolución, pose, luminosidad, existencia de elementos de ocultación tales como gafas, diferencias temporales, etc.». En idéntica dirección, la AEDP[64] advierte notables

---

inteligencia artificial en la Resolución del Parlamento Europeo del 16 de febrero de 2017 con recomendaciones para la Comisión sobre "normas de Derecho civil sobre robótica"; en la Comunicación de la Comisión Europea del 25 de abril de 2018 sobre "Inteligencia Artificial para Europa" (COM(2018) 237 final); en la Comunicación de la Comisión Bruselas "Generar confianza en la inteligencia artificial centrada en el ser humano" del 8 de abril de 2019, COM(2019) 168 final) y, más recientemente, en el Libro Blanco sobre Inteligencia Artificial del 19 de febrero de 2020 (COM(2020) 65 final). En el marco del Consejo de Europa, el Comité de Expertos en Intermediarios de Internet publicó el estudio Algoritmos y Derechos Humanos en marzo de 2018 y poco después, el 3 de diciembre de 2018, la Comisión Europea para la Eficiencia de los Sistemas de Justicia (CEPEJ) aprobó la "Carta ética sobre la utilización de la inteligencia artificial en los sistemas de justicia y su entorno…».

[61] Vid. Propuesta de Reglamento del Parlamento europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial y se modifican determinados actos legislativos de la Unión, de 21/4/2021. El texto completo puede consultarse en la web https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206.

[62] KUGLER, Matthew B., «From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms» en *U.C. Irvine Law Review, Vol. [10:107]*, 2019, pág. 132. Artículo disponible para consulta en la dirección electrónica https://scholarship.law.uci.edu/ucilr/vol10/iss1/5. En concreto, razona el autor: *«Biometric information, whether a thumbprint, a voiceprint, or a record of facial geometry, can be seen as the worst form of password. It is both common to multiple vendors—you have only one thumb on each hand—and unchangeable. It is even, as discussed above, semipublic. This leads to the fear that a data breach or sale by one holder of a piece of a person's biometric information would compromise the security of all relationships that are verified by that same piece. And, once compromised, the very nature of biometrics would make it impossible to regain security; biometrics are hard to alter. This is why the immutability of biometrics and concerns about identity theft appear so often in discussions of biometrics…*».

[63] Vid. *Guía sobre estudios de identificación facial para jueces, fiscales e investigadores*, op. cit., punto 10.

[64] Así se destaca en la nota informativa *14 equívocos con relación a la identificación y la autenticación biométrica,* AEPD, junio de 2020, puntos 3, 5 y 6. Disponible para consulta en la dirección electrónica https://www.aepd.es/sites/default/files/2020-06/nota-equivocos-biometria.pdf.

deficiencias en el uso de tales instrumentos, tales como: i) falta de precisión en el resultado identificativo -con el riesgo de que se produzcan los llamados «falsos positivos» o «falsos negativos»-, ii) la imposibilidad de utilizar determinados tipos de biometría con algunas personas en casos de lesiones, accidentes o problemas de salud -hablándose entonces de una «incompatibilidad biométrica permanente», lo que podría suponer incluso una causa de exclusión social-, o iii) la capacidad técnica de burlar estos sistemas mediante el empleo de máscaras u otros elementos que disimulen los rasgos faciales del individuo.

Por último, y guardando relación con los dos puntos anteriores, diversa doctrina[65] ha planteado recientemente en este contexto el problema de los llamados «sesgos algorítmicos», pudiendo esto provocar resultados contrarios al principio de no discriminación -art. 14 CE-. Como explica Pérez Estrada[66] el problema de los sesgos algorítmicos en el uso del reconocimiento facial está íntimamente relacionado con los procesos de aprendizaje automático -lo que entendemos por «inteligencia artificial»- y con la opacidad en el desarrollo de tales operaciones. El origen de estas distorsiones se halla en el momento de configurar los sistemas de reconocimiento facial automático, pues es posible que para ello se manejen datos sesgados; en estos supuestos, los datos introducidos por las personas que diseñan los modelos de aprendizaje automáticos representan de un modo desequilibrado el género y la raza que en realidad componen la población sobre la que se va a aplicar la técnica. A esto debe añadirse la circunstancia de que el sistema detecta con una mayor eficacia los rasgos faciales más representados en la base de datos. En consecuencia, cuando existe una menor diversidad demográfica en el sistema, en comparación con la diversidad propia de la población de destino -en este supuesto, al utilizarse para identificar a personas que transitan por vías o espacios públicos, la sociedad en general-, se produce un mayor número de fallos en relación con los individuos pertenecientes a los grupos menos representados. En la práctica, los sesgos algorítmicos se traducen en una mayor tasa de error en función de la raza o del género[67] de las personas sobre las que se aplica el reconocimiento facial automático; en 2018, un estudio[68] de los resultados producidos en la aplicación de esta técnica por compañías privadas con fines comerciales reveló que la tasa de error en las identificaciones de mujeres de color era de un 34’7%, mientras que el error

[65] Puede consultarse en este sentido a DOMINGO JARAMILLO, Cristina, «Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana», en *El criminalista digital, 2ª época, número 9*, 2021, pág. 25. Disponible para consulta en la dirección http://revistaseug.ugr.es/index.php/cridi/article/view/20899.

[66] PÉREZ ESTRADA, Miren Josune, «La inteligencia artificial como prueba científica en el proceso penal español», artículo publicado en *Revista Brasileira de Direito Processual Penal, volumen 7, número 2*, Porto Alegre, maio-agosto de 2021, pág. 1400. En opinión de la autora, tales algoritmos están diseñados para tratar los datos como lo haría una persona y al combinarlos con la tecnología de reconocimiento facial se pueden obtener unos resultados más eficientes y complejos; sin embargo, el problema se halla en la evolución de estos algoritmos: no puede ser explicada de forma lógica, y por eso se provoca una opacidad en su proceso de uso.

[67] Sobre esta circunstancia discriminatoria, es de mucho interés el reciente informe de TURNER LEE, Nicol y CHIN, Caitlin, *Police surveillance and facial recognition: Why data privacy is imperative for communities of color*, publicado por The Brookings Institution, 12/4/2022. Puede consultarse en el enlace https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

[68] BULAMWINI, Joy, y GEBRU, Timnit, «Gender Shades…», cit., pág.1.

en los varones blancos apenas alcanzaba el 0'8%. Naturalmente, esta circunstancia discriminatoria debe ser objeto de subsanación por las autoridades antes de poner en práctica tal técnica de reconocimiento como un instrumento preventivo, pues no sólo es una situación contraria a nuestra Norma Fundamental -artículo 14 CE- y a los Tratados Internacionales que nos vinculan -artículo 2 de la Declaración Universal de Derechos Humanos y artículo 14 del Convenio Europeo de Derechos Humanos-, sino que se confronta igualmente con las disposiciones que regulan la actividad de seguridad ciudadana en general y las actuaciones de identificación de personas en particular -artículos 4.1 y 16.1.3º de la Ley Orgánica 4/2015-.

Para finalizar, es de interés observar cómo responde esta técnica después de someterse al tamiz jurisprudencial. Al tratarse de una tecnología muy novedosa, aún no pueden hallarse un gran número de pronunciamientos judiciales que analicen su significación jurídica y su impacto en los derechos fundamentales de los ciudadanos. No obstante, podemos mencionar dos resoluciones en este contexto.

En Derecho Comparado, encontramos la sentencia de 4/9/2019, del Alto Tribunal de Justicia de Inglaterra y Gales, Sala de lo Civil, Sección de apelación[69]. Siguiendo a Izquierdo Carrasco[70], en esta resolución se estudian las consecuencias a nivel jurídico que produjo la utilización desde mediados del año 2017 por parte de la policía de Gales del Sur de un sistema de reconocimiento facial automático, en tiempo real y con carácter masivo, denominado AFR (*Automated Facial Recognition*)[71]. La sentencia, utilizando la base dogmática sentada emanada de la STEDH S. and Marper vs UK (2008), aprecia en la aplicación de esta tecnología una afectación de la privacidad del artículo 8 CEDH, al producirse en ese proceso una obtención de información sobre un individuo que permite su identificación, así como un almacenamiento de tal información: los magistrados entienden que los datos biométricos son una clara fuente de información de carácter personal, y el hecho de que estos se obtengan de las características faciales de una persona -que libremente se muestran al caminar por vías o espacios públicos- no impide que se produzca tal afectación.

En España, la aplicación de sistemas de reconocimiento facial automático fue objeto de análisis en el Auto número 72/2021, de 15 de febrero, de la sección 9ª de la Audiencia Provincial de Barcelona. En esta ocasión, una conocida cadena de supermercados planteó al Tribunal la posibilidad de emplear esta tecnología mediante la colocación de dispositivos situados en la entrada a sus establecimientos, con el objeto de

[69] *High Court of Justice, Queen's Bench Division, Divisional court. Case* CO/4085/2018, asunto Bridges versus CCSWP (*Chief Constable of South Wales Police*) y SSHD (*Secretary of State for the Home Department*).

[70] Un minucioso comentario de esta sentencia puede hallarse en IZQUIERDO CARRASCO, Manuel, «La utilización…», cit., páginas 87 y siguientes.

[71] En síntesis, se trataba de un proyecto piloto consistente en la instalación de un elevado número de cámaras de videovigilancia en una de las principales calles de Cardiff, con el objeto de captar imágenes del público que asistía a grandes eventos (v.gr. conciertos o espectáculos deportivos), para a continuación proceder a procesarlas en tiempo real y compararlas con las imágenes de personas incluidas en las listas de vigilancia de la policía.

detectar el acceso de individuos que contaban con numerosos antecedentes por delitos de hurto cometidos en sus locales, y a los que se les había impuesto una prohibición judicial de entrada a alguno de sus locales. La citada resolución concluye la imposibilidad de utilizar estos sistemas de captación y análisis de datos biométricos por una entidad privada, habida cuenta de que se están tratando datos de merecedores de una «especial protección» en el sentido del artículo 9.1 del RGPD, y considerando igualmente que no se cumplían ninguna de las excepciones previstas en el apartado segundo del referido precepto; en particular, los magistrados inciden en el hecho de que el empleo de esta tecnología estaría dirigida en el caso que se analiza a la satisfacción de un interés privado y no público[72]. Es esta una feliz consideración que debería ser sostenida hoy en día[73] si se quiere garantizar el pleno respeto a nuestros derechos fundamentales; sin embargo, el elevado riesgo inherente a la utilización de esta tecnología por entidades privadas es una cuestión que, en cualquier caso, excede del marco del presente trabajo.

IV. CONCLUSIONES

El reconocimiento facial constituye una técnica de estudio de rasgos faciales que, en función de las circunstancias en que sean tomadas las imágenes dubitadas empleadas para el cotejo, permite lograr la identificación de un individuo con un razonable nivel de fiabilidad. Al basar su funcionamiento en el tratamiento de datos biométricos, se trata de una de las modernas tecnologías que están aflorando en la era digital, originando a nivel global lo que se ha designado de una forma elocuente como «cambios sísmicos»[74] en las tradicionales bases dogmáticas de la privacidad. En España, la reciente publicación la LO 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, permite que el Estado pueda plantearse la utilización del reconocimiento facial con fines de investigación o prevención del delito, al disponer de una norma que, siendo susceptible de ser mejorada, cumple razonablemente con los estándares de calidad de la ley[75] exigidos por el Tribunal de Estrasburgo.

---

[72] Así, se dispone en el Fundamento de Derecho Tercero: «...esta Sala no puede compartir que con la medida interesada se esté protegiendo el interés público, sino más bien, los intereses privados o particulares de la empresa en cuestión, pues como ya se ha explicitado en los párrafos anteriores, se estarían conculcando las garantías adecuadas en orden a la protección de los derechos y libertades de los interesados, no ya sólo de los que han sido penados y cuya prohibición de acceso les incumbe, sino del resto de personas que acceden al citado supermercado…».

[73] En este sentido, se ha conocido recientemente que el Estado británico ha multado a una compañía dedicada al desarrollo de técnicas de inteligencia artificial que había captado y almacenado más de 20 mil millones de imágenes faciales de ciudadanos; tales imágenes, habían sido obtenidas de plataformas como Facebook e Instagram, sin conocimiento de las redes sociales o permiso de los usuarios. Vid. MC CALLUM, Shiona, «Clearview AI fined in UK for illegally storing facial images», artículo publicado en el diario digital *BBC NEWS*, Sección Tecnología, el día 25/5/2022. La noticia puede consultarse en la web del citado diario https://www.bbc.com/news.

[74] Así se expresa el juez John Roberts al emitir la opinión del Tribunal Supremo de los Estados Unidos en el caso Carpenter v. United States, número 16-402, de 22/6/2018, punto III.

[75] Como destaca Lezertua Rodríguez, el TEDH no es exigente desde un punto de vista estrictamente formal pero sí que impone, en cambio, unas mayores exigencias en torno a la calidad de la norma destinada a poder

En el ámbito de la investigación delictiva, la utilización del reconocimiento facial como prueba pericial, en combinación con la prueba documental consistente en la reproducción de imágenes relativas al hecho delictivo -fotografías o vídeos-, puede suponer -según las circunstancias de cada caso- un instrumento de gran utilidad para esclarecer los hechos y lograr el conocimiento de la verdad material[76]. Esto debe considerarse no sólo desde una óptica acusatoria, pudiendo igualmente configurarse como un arma de estimable utilidad para el letrado defensor -así como para el juez instructor y el fiscal-, en orden a evitar el indeseable resultado de la condena de un inocente. Nuestra LECrim no contiene una previsión específica sobre esta diligencia; en este sentido, la elaboración de la pretendida nueva ley procesal penal podría ser una buena oportunidad para incorporar una mención a esta medida, si bien el Anteproyecto publicado en 2020 tampoco se pronuncia con carácter expreso en esta dirección.

Más allá de la investigación delictiva, actualmente es necesario plantearse también el empleo de esta técnica en el terreno de la seguridad, lugar en el que se está incrementando con un carácter vertiginoso el uso policial de sistemas de reconocimiento facial automático. La citada LO 7/2021 habilita igualmente a las autoridades para proceder al tratamiento de datos biométricos de los ciudadanos con fines de prevención, pero esta técnica suscita mayores dudas en un sentido jurídico, al introducir en su funcionamiento un componente de inteligencia artificial -esto es, permite la toma de decisiones de cierta relevancia legal sin la intervención directa de un ser humano-. Sobre esta cuestión será de gran interés conocer las disposiciones que contenga el Reglamento europeo sobre inteligencia artificial, norma cuya publicación se espera tenga lugar próximamente.

En ambos casos, bien se trate de investigar un delito o de prevenir su comisión, la aplicación por los poderes públicos de esta moderna técnica debería estar inspirada en todo momento por el principio de proporcionalidad, el cual, como indicaba Gentz[77] se erige como «el límite a los límites de los derechos fundamentales».

---

sustentar una injerencia estatal en un derecho convencional, vid. LEZERTUA RODRÍGUEZ, Manuel, «El derecho a la vida privada y familiar en la Jurisprudencia del TEDH», en *Perfiles del derecho constitucional a la vida privada y familiar*, LÓPEZ ORTEGA, Juan José (Dir.), CGPJ, 1996, pág. 88. En la misma línea, puede consultarse NARVÁEZ RODRÍGUEZ, Antonio, «Tutela de la privacidad e intercepción pública de las comunicaciones», en la obra *Delito e informática: algunos aspectos. Cuadernos penales José María Lidón*, ECHANO BASALDUA, Juan Ignacio, Universidad de Deusto, Bilbao, 2007, pág. 319.

[76] Este ha de ser el principio central y fundamental de cualquier procedimiento penal europeo según SCHÜNEMANN, Bernd, «Cuestiones básicas de la estructura y reforma del procedimiento penal bajo una perspectiva global», en *Derecho Penal y Criminología*, Volumen 25, Número 76, 2004, pág. 184. Traducción de SACHER, Mariana, BACIGALUPO, Silvina y BAZA, Lourdes.

[77] GENTZ, Manfred, «Zur Verhältnismäßkeit von Grundrechtseingriffen», en *Neue Juristische Wochenschrift (NJW)*, *35*, 1968, págs. 1600-1601.

BIBLIOGRAFÍA

ARRÚE MENDIZÁBAL, Marta, «Los derechos a la intimidad, a la propia imagen y a la protección de datos de los empleados públicos vs el control por parte de la Administración», en *Revista General de Derecho del Trabajo y de la Seguridad Social, número 54, 2019*. El artículo puede consultarse en la dirección electrónica http://laadministracionaldia.inap.es/noticia.asp?id=1510754.

BELLOVIN, Steven M., HUTCHINS, Renée M., JEBARA, Tony & ZIMMECK, Sebastian, «When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning», en *New York University Journal of Law & Liberty [Vol. 8:555], 2014*.

BULAMWINI, Joy & GEBRU, Timnit, «Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification», *Proceedings of Machine Learning Research, 81:1–15*, 2018. Artículo disponible para consulta en la dirección https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

CIPPITANI, Roberto, MIRABILE, Antonella y ONOFRI, Martina, «"Objetividad científica" y sesgos en la toma de decisiones jurídicas: los casos de genética forense y de algoritmos», en *Revista Justicia y Derecho, Volumen 4, número 2*, año 2021.

DOMINGO JARAMILLO, Cristina, «Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana», en *El criminalista digital, 2ª época, número 9*, 2021. Disponible para consulta en la dirección http://revistaseug.ugr.es/index.php/cridi/article/view/ 20899.

ESCAJEDO SAN EPIFANIO, Leire, *Tecnologías biométricas, identidad y Derechos fundamentales*, Editorial Aranzandi, Navarra, enero 2017.

ESPÍN LÓPEZ, Isidoro, «Los derechos fundamentales a la vida privada afectados por la investigación tecnológica y el fenómeno del entorno virtual», estudio doctrinal publicado en el *Boletín Oficial del Ministerio de Justicia, Año LXXV, Número 2.244*, octubre de 2021, Sección Doctrinal.

FLORIDA, Richard, *Las ciudades creativas*, Editorial Paidós, Barcelona, 2009.

GARTLAND, Claire, «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*, 5/7/2016. Puede consultarse en la dirección electrónica https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy.

GARVIE, Clare, BEDOYA, Álvaro, y FRANKLE, Jonathan, «The Perpetual Line-Up: Unregulated Police Face Recognition in America», *Georgetown Law, Center on Privacy & Technology*, 18/10/2016, disponible en la dirección https://www.perpetuallineup.org/.

GENTZ, Manfred, «Zur Verhältnismäßkeit von Grundrechtseingriffen», en *Neue Juristische Wochenschrift (NJW*), *35*, 1968.

GIMENO SENDRA, José Vicente, «La prueba preconstituida de la policía judicial», en *Revista catalana de seguretat pública*, *Número 22,* 2010.

GUERRIER, Claudine, *Security and Privacy in the Digital Era*, ISTE Ltd. And John Wiley & Sons Inc., 1ª Edición, 2016.

IZQUIERDO CARRASCO, Manuel, «La utilización policial de los sistemas de reconocimiento facial automático», artículo publicado en la *Revista Ius et Veritas, número 60*, mayo 2020.

JUANATEY DORADO, Carmen. y DOVAL PAIS, Antonio, «Límites de la protección penal de la intimidad frente a la grabación de conversaciones o imágenes», en *La*

protección de la intimidad, BOIX REIG, Javier (Dir.) y JAREÑO LEAL, Ángeles (Coord.), Editorial Iustel, Madrid, 2010.

KUGLER, Matthew B., «From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms» en *U.C. Irvine Law Review, Vol. [10:107]*, 2019. Artículo disponible para consulta en la dirección electrónica https://scholarship.law.uci.edu/ucilr/vol10/iss1/5.

LEZERTUA RODRÍGUEZ, Manuel, «El derecho a la vida privada y familiar en la Jurisprudencia del TEDH», en *Perfiles del derecho constitucional a la vida privada y familiar*, LÓPEZ ORTEGA, Juan José (Dir.), CGPJ, 1996.

LÓPEZ GUERRA, Luis, «El papel del juez en una sociedad democrática», en *Revista de estudios jurídicos, número 18,* año 2018.

MARTÍN BRAÑAS, Carlos, «Reconocimiento del delincuente: nuevas diligencias de identificación», *Boletín del Ministerio de Justicia*, *Año LXIX, Número 2182*, octubre de 2015.

MERCADER UGUINA, Jesús R., «El futuro del trabajo y del empleo en la era de la digitalización y de la robótica», en la obra *Sociedad Digital y Derecho*, PIÑAR MAÑAS, José Luis; DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, Tomás, (Dir.), Imprenta Nacional del Boletín Oficial del Estado, Madrid, 2018.

NARVÁEZ RODRÍGUEZ, Antonio, «Tutela de la privacidad e intercepción pública de las comunicaciones», en la obra *Delito e informática: algunos aspectos. Cuadernos penales José María Lidón*, ECHANO BASALDUA, Juan Ignacio, Universidad de Deusto, Bilbao, 2007.

NAVAJAS RAMOS, Luis, «La prueba videográfica en el proceso penal: su valor y límites para su obtención», en *Eguzkilore: Cuaderno del Instituto Vasco de Criminología, número 12*, 1998.

ORTUÑO RODRÍGUEZ, Alicia Esther, «Doctrina constitucional en relación con el control mediante cámaras de videovigilancia», en *Cuadernos de Derecho Local, número 49*, febrero de 2019, Fundación Democracia y Gobierno Local.

PÉREZ-CRUZ MARTÍN, Agustín Jesús, «Videovigilancia y derecho a la intimidad: ¿un nuevo ejemplo de conflicto entre el derecho a la seguridad pública y el derecho fundamental a la intimidad?», *Anuario da Facultade de Dereito da Universidade da Coruña, Número 1,* 1997.

PÉREZ DE LOS COBOS ORIHUEL, Francisco de Asís, *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho Comparado*, Consejo de Europa, Estudio, 2018.

PÉREZ ESTRADA, Miren Josune, «La inteligencia artificial como prueba científica en el proceso penal español», artículo publicado en *Revista Brasileira de Direito Processual Penal, volumen 7, número 2*, Porto Alegre, maio-agosto de 2021.

RODRÍGUEZ-PIÑEIRO ROYO, Miguel, «Las facultades de control de datos biométricos del trabajador», *Revista Temas Laborales*, número 150/2019.

RAMOS RUBIO, Carlos, «Jornada sobre videovigilancia policial, experiencia acumulada y perspectivas de futuro», ponencia pronunciada en la Mesa redonda «Colaboración entre videovigilancia pública y privada», organizada por la *Comissió de Control dels Dispositius de Videovigilància de Catalunya* (CCDVC), Barcelona, 3/10/2014. La ponencia puede consultarse en la dirección electrónica http://interior.gencat.cat/web/.content/home/030_arees_dactuacio/seguretat/videovigilancia_policial/jornada_sobre_videovigilancia_policial/Videovigilancia_3-10-14_RAMOS.pdf.

RIGANO, Christopher, «Using Artificial Intelligence to address criminal justice needs», *National Institute of Justice, 208,* 2019.

SANCHÍS CRESPO, Carolina, «Principios rectores en la adopción de diligencias limitativas de los derechos reconocidos en el artículo 18 CE», artículo publicado en *Revista Boliviana de Derecho, número 31*, enero 2021.

SCHÜNEMANN, Bernd, «Cuestiones básicas de la estructura y reforma del procedimiento penal bajo una perspectiva global», en *Derecho Penal y Criminología*, Volumen 25, Número 76, 2004. Traducción de SACHER, Mariana, BACIGALUPO, Silvina y BAZA, Lourdes.

TURNER LEE, Nicol y CHIN, Caitlin, *Police surveillance and facial recognition: Why data privacy is imperative for communities of color*, publicado por The Brookings Institution, 12/4/2022. Puede consultarse en el enlace https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

VELASCO NÚÑEZ, Eloy, «Tecnovigilancia, geolocalización y datos: aspectos procesales penales», artículo publicado en el *Diario La Ley*, *número 8338*, Sección Doctrina, 23/6/2014.