https://doi.org/10.18800/iusetveritas.202001.004

La utilización policial de los sistemas de reconocimiento facial automático(*)(**)

Comentario a la sentencia del Alto Tribunal de Justicia de Inglaterra y Gales de 4 de septiembre de 2019

Police use of automatic facial recognition systems: Commentary on the judgment of the High Court of Justice of England and Wales of September 4th, 2019

Manuel Izquierdo Carrasco(***)
Universidad de Córdoba (Córdoba, España)

Resumen: Este trabajo analiza una reciente sentencia del Alto Tribunal de Justicia de Inglaterra y Gales, donde se enjuicia la utilización por parte de una fuerza de policía de un sistema de Reconocimiento Facial Automático (AFR) en ciertos eventos públicos. En particular, la sentencia examina si la utilización de esta técnica es contraria al artículo 8 del Convenio Europeo de Derechos Humanos (derecho al respeto a la vida privada y familiar); conculca la legislación de protección de datos de carácter personal; o tiene un sesgo discriminatorio contrario al principio de igualdad. Con respecto a lo primero, se concluye que el reconocimiento facial automático supone una injerencia en la vida privada, aunque para fundamentar esta posición ofrecemos una argumentación jurídica distinta a la de la sentencia. Seguidamente, se estudia el fundamento legal de dicha injerencia y su proporcionalidad. Con respecto a lo segundo, se reconoce que la utilización del AFR conlleva un tratamiento de datos de carácter personal especialmente sensibles, pero que dicho tratamiento cumple la normativa aplicable. Finalmente, se expone la inexistencia de datos sólidos que apoyen que AFR origina unas consecuencias discriminatorias para las mujeres y las minorías raciales. Todo este análisis se completa con referencias a la legislación peruana del objeto de estudio.

Palabras clave: Reconocimiento Facial Automático - Inteligencia Artificial - Alto Tribunal de Justicia de Inglaterra y Gales - Policía - Derecho a la vida privada - Convenio Europeo de Derechos Humanos - Protección de Datos de Carácter Personal - Seguridad - Discriminación

Abstract: This paper analyses a recent judgment from the High Court of Justice regarding the use of automated facial recognition (AFR) at public events by police forces. In particular, the judgment focuses on the questions whether the use of such technique might be contrary to article 8 of the European Convention on Human Rights (right to respect for private and family life), whether this instrument is compatible with the legislation on personal data protection and whether it has a bias towards certain groups of people that might be in conflict with the equality principle. Concerning the first issue, the author reaches the conclusion that the automated facial recognition

(*) Nota del Editor: este artículo fue recibido el 27 de abril de 2020 y su publicación fue aprobada el 18 de mayo de 2020.
(**) Proyecto de investigación PGC-2018-093760-B-100 (Mº Ciencia, Innovación y Universidades, Fondos FEDER). Grupo de Investigación de la Junta de Andalucía SEJ-196.
(***) Abogado por la Universidad de Córdoba y Doctor en Derecho por la misma casa de estudios. Catedrático de Derecho Administrativo en la Universidad de Córdoba. Contacto: manuel.izquierdo@uco.es

represents an interference with the claimant´s rights under the ECHR, analyzing its necessity and proportionality. Regarding the second question, the paper states that the AFR uses personal data that are particularly sensitive; nevertheless, its use seems to be in accordance with the law. Finally, the judgment concludes that the existence of an ethnic or gender bias in the use of the AFR cannot be asserted. The Peruvian legislation on these issues is highly considered through the whole study.

Keywords: Automated Facial Recognition - Artificial intelligence - High Court of Justice of England and Wales - Police - Right to respect for private life - European Convention on Human Rights - Personal Data Protection - Security - Discrimination

1. Introducción

Con fecha 4 de septiembre de 2019, el Alto Tribunal de Justicia de Inglaterra y Gales, Sala de lo Civil, Sección de apelación(1), ha dictado una relevante sentencia (en ella se afirma que podría ser la primera vez en el mundo en la que un tribunal se enfrenta a esta cuestión) donde se analizan diversas cuestiones jurídicas vinculadas con la utilización por parte de las fuerzas policiales de sistemas de reconocimiento facial automático en tiempo real de carácter masivo (AFR, *Automated Facial Recognition*)(2). El demandante fue Edward Bridges, un activista por las libertades civiles que vive en Cardiff. El demandado, el Jefe de la Policía de Gales del Sur (*South Wales Police*, en adelante SWP). Desde mediados de 2017, con la financiación del Departamento del Interior del gobierno del Reino Unido, este cuerpo policial había llevado a cabo un proyecto piloto, conocido como "*AFR Locate*", consistente en el despliegue en una serie de concretos eventos (la final de la Champions League, partidos internacionales de rugby, conciertos, un día de Navidad en una concurrida calle comercial de Cardiff, etc.) de cámaras de vigilancia para capturar imágenes digitales del público asistente, que en tiempo real se procesaban y comparaban con imágenes digitales de personas en listas de vigilancia compiladas por SWP(3). El demandante asistió a dos de esos eventos y, aunque no había prueba de ello, la parte demandada aceptó como hipótesis, para que el tribunal pudiera pronunciarse sobre el fondo, que la imagen de su cara fue captada por alguna de las cámaras de vigilancia empleadas en el proyecto. En cualquier caso, el Sr. Bridges no estaba en ninguna de las listas de vigilancia empleadas por SWP.

Lo que la sentencia enjuicia es si este tipo de actuación policial se adecúa a la legalidad. En particular, lo que el demandante alega y la sentencia analiza es que esta utilización de sistemas de reconocimiento facial automático es contraria al artículo. 8 del Convenio Europeo de Derechos Humanos (derecho al respeto a la vida privada y familiar); conculca la legislación de protección de datos de carácter personal; y vulnera el deber de igualdad al que están sometidas las autoridades públicas en el ejercicio de sus funciones (o dicho de otro modo, supone

(1) 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).

(2) Debe tenerse en cuenta que esta técnica del reconocimiento facial automático en tiempo real también está disponible para la Policía Nacional del Perú. A este respecto, puede consultarse la Resolución Vice Ministerial 029-2014-IN/VGI, de 14 de abril de 2014, que aprueba la estandarización de la "Solución informática para el incremento de la capacidad del sistema biométrico dactilar-AFIS PNP y la incorporación de la funcionalidad de reconocimiento facial en el proceso de identificación biométrica de la PNP", en el punto 11 de las especificaciones técnicas requeridas establece que el sistema deberá incluir "las aplicaciones necesarias para la captura de rostros en formato vídeo (…) con las condiciones técnicas necesarias para la aplicación de las herramientas de reconocimiento facial" y en el punto 13 que "la funcionalidad de identificación biométrica fácil debe permitir la consulta de la información de reconocimiento facial e información demográfica (…) por ejemplo de imágenes captadas por las cámaras de vigilancia administradas por la Central de Emergencias 105 y la flota de Patrulleros Inteligentes").
Según un informe del grupo de investigación *Carnegie Endowment for International Peace* son alrededor de 75 los países que están utilizando activamente herramientas de Inteligencia Artificial como el reconocimiento facial para la vigilancia (https://carnegieendowment.org/files/AI_Global_Surveillance_Index1.pdf). A nivel global, el informe sostiene que son las empresas chinas lideradas por Huawei y Hikvision las que están suministrando gran parte de la tecnología de vigilancia de Inteligencia Artificial a países de todo el mundo. También menciona a NEC de Japón, además de IBM, Palantir y Cisco de EE.UU.

(3) Generalmente, en cada evento, se elaboraron tres listas de vigilancia: una lista de vigilancia "roja", integrada por personas sospechosas de haber cometido un delito grave o que habían sido arrestadas en el mismo evento en el año anterior; una lista de vigilancia "ámbar", compuesta por personas buscadas con orden de arresto; y una lista de vigilancia "púrpura", con personas sospechosas de haber cometido un delito en el área de SWP. En conexión con esta delimitación objetiva de estas distintas listas, los protocolos de SWP también vinculan a las mismas una serie de actuaciones por parte de los agentes policiales -aunque estos tienen margen de valoración- (roja, respuesta inmediata; ámbar, arresto; verde, identificación con finalidad de inteligencia o investigación policial). Las listas de vigilancia utilizadas por SWP en los mencionados eventos han comprendido entre 400 y 800 personas en cada ocasión.

una actuación discriminatoria). En los siguientes epígrafes, analizaremos cada una de esas cuestiones, pero antes -al igual que hace la sentencia- describamos a grandes rasgos la tecnología de reconocimiento facial automático y su implementación en *AFR Locate*.

2. Aproximación técnica al reconocimiento facial automático

El reconocimiento facial automático es un procedimiento técnico de inteligencia artificial consistente en evaluar si dos imágenes faciales representan a la misma persona. El sistema se basa en la comparación entre dos fuentes de información:

- 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 imágenes faciales de personas identificadas -por ej., las que provienen de las fotografías que se realizan a las personas detenidas en dependencias policiales[4]. Según el contexto y la finalidad con la que se use el sistema de reconocimiento facial automático, esta base de datos puede estar integrada por todas las imágenes que posea el cuerpo policial, cuando el sistema se utiliza en procesos rutinarios de investigación; o por imágenes de un número limitado de personas seleccionadas, con las que se constituye una lista de observación o vigilancia, cuando el sistema se utiliza para eventos concretos en tiempo real[5].
- Imágenes de personas no identificadas, de las que un programa informático extrae los datos biométricos faciales. Las fuentes de estas imágenes pueden ser varias: por un lado, aquellas que se pueden obtener, por ej., de grabaciones realizadas por las Fuerzas y Cuerpos de seguridad o por sistemas de vigilancia privados y que con posterioridad son tratadas en dependencias policiales con este fin; y por otro, aquellas que se obtienen y son tratadas en tiempo real mediante un circuito cerrado de televisión (CCTV) en un determinado evento en el que se esté aplicando el sistema de reconocimiento facial automático.

La sentencia comentada sólo se ocupa de aquellos supuestos en los que existe una lista de observación concreta y las imágenes se obtienen y tratan en tiempo real en un determinado evento (esto es lo que el mencionado proyecto piloto policial denominó "*AFR Locate*").

Una vez que se tienen las dos fuentes de información que se quieren cotejar, el sistema realiza una comparación a través del correspondiente programa informático[6] que otorga una puntuación a la similitud entre dos caras, de tal manera que a partir de una determinada puntuación (valor umbral) cuyo nivel se puede configurar, el sistema informa de una posible coincidencia. Ante ese resultado de existencia de una posible coincidencia, el protocolo de actuación de SWP prevé que el agente policial que esté gestionando el sistema debe valorar si esa coincidencia es correcta o no y, si la considera viable, ha de informar a los agentes desplegados en el operativo policial para que intervengan. Estos agentes desplegados harán ellos mismos su propia evaluación de la situación y tomarán la medida adecuada a ello. Por tanto, en ningún momento el

(4) Aunque no procede que nos detengamos ahora en esta cuestión, en España, de conformidad con el vigente marco normativo fundamentalmente, la legislación de protección de datos de carácter personal-, las fotografías empleadas para la expedición del Documento Nacional de Identidad no podrían ser objeto de una utilización sistemática, completa y rutinaria con esta finalidad por parte de las Fuerzas y Cuerpos de Seguridad.
En el Perú, la mencionada Resolución Vice-Ministerial 029-2014-IN/VGI, de 14 de abril de 2014, que aprueba la estandarización de la "Solución informática para el incremento de la capacidad del sistema biométrico dactilar-AFIS PNP y la incorporación de la funcionalidad de reconocimiento facial en el proceso de identificación biométrica de la PNP", en el punto 20 del Anexo, dispone que el sistema deberá disponer de una "Interfaz con el Sistema de Reconocimiento Facial de RENIEC. Se precisa que la implementación de esta interfaz sólo será exigible, siempre que el Ministerio del Interior suscriba los acuerdos o convenios interinstitucionales con la RENIEC que la hagan viable (…) Esta interfaz tiene como objetivo realizar la búsqueda en automático contra la base de datos de RENIEC, después de obtener negativo en la base de datos de identificación biométrica de la DIREJCRI-PNP". Debe tenerse en cuenta que el Registro Nacional de Identificación y Estado Civil (RENIEC) es el organismo autónomo encargado de la identificación de los peruanos y que tiene entre sus funciones el otorgamiento del documento nacional de identidad, gestionando la base de datos de identificación biométrica vinculada a dicho otorgamiento. Desconocemos si dicha interfaz se ha implementado efectivamente y el uso que, en su caso, se haga de la misma.

(5) La sentencia cita que la capacidad máxima para una lista de observación del sistema empleado en concretos eventos, vinculada con la capacidad de procesamiento informático en tiempo real, es de 2.000 imágenes. El sistema es capaz de escanear 50 caras por segundo, aunque eso no significa necesariamente 50 personas diferentes. Por ejemplo, se calcula que en un partido de rugby se pudieron procesar 21.500 caras.

(6) SWP utilizó un software de reconocimiento facial desarrollado y patentado por NEC llamado "NeoFace Watch".

sistema genera por sí mismo una actuación administrativa automatizada(7), sino que ofrece una información que debe ser valorada y evaluada conforme a las circunstancias por los agentes policiales. Sin duda alguna, esta forma de proceder supone una importante salvaguarda que es destacada por la sentencia.

Si no se producen coincidencias, como ocurre en la abrumadora mayoría de los casos, el sistema no retiene la imagen facial de las personas ni su plantilla biométrica, que son eliminadas de manera automática e inmediata, sin que ni el agente policial que está gestionando el sistema ni ningún otro puedan acceder a esos datos(8). No obstante, la grabación realizada por el circuito cerrado de televisión se conserva durante 31 días conforme a la normativa aplicable(9). Los datos asociados con una coincidencia se retienen dentro del sistema de reconocimiento facial automático durante 24 horas. La plantilla biométrica, aunque haya coincidencia, se elimina inmediatamente; y la lista de observación -con sus imágenes y plantillas biométricas- también se elimina en el plazo de 24 horas tras el operativo.

3. El reconocimiento facial automático y el artículo 8 del Convenio Europeo de Derechos Humanos

Como se ha dicho, el primer fundamento del recurso judicial era la conculcación del art. 8 del Convenio Europeo de Derechos Humanos(10). Este precepto establece lo siguiente:

> "1. Toda persona tiene derecho al respeto de su vida privada y familiar (…)
>
> 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

(7) Una muestra de algo próximo a una decisión administrativa automatizada, se puede observar en la colocación de puertas que funcionan sobre la base del reconocimiento facial automático para el control de la entrada en territorio nacional, desde un vuelo internacional, en los aeropuertos. En algunos aeropuertos españoles, lo que antes eran numerosos puestos de control policial personal han sido sustituidos por unos torniquetes automáticos en los que el viajero debe colocar su pasaporte, para, entre otras cosas, extraer los datos biométricos incluidos en el mismo, y permitir que una cámara le haga una fotografía con la que se efectúa el correspondiente reconocimiento facial automático. En caso de resultar positivo, la puerta se abre, esto es, se ha superado el control de entrada, aunque es cierto que, tras los torniquetes, algunos agentes del Cuerpo Nacional de Policía supervisan el funcionamiento del sistema y atienden aquellos supuestos en los que el sistema remite a ellos. Este control automático es más fiable y eficiente que el tradicional control visual por parte de los agentes. Además, puesto que la fotografía se efectúa en un ambiente controlado, su fiabilidad y precisión es mucho mayor que cuando esa captura de imágenes faciales tiene lugar en condiciones variables (de ángulo, de luz, posición, movimiento, entre otros), lo que ocurre en los supuestos enjuiciados en la sentencia que nos ocupa.
Desde el día 28 de agosto de 2006, todos los pasaportes que se expiden por los equipos radicados dentro del territorio nacional español corresponden al denominado pasaporte electrónico, que incorpora un chip embebido en su portada posterior que contiene el dato biométrico relativo a la imagen facial del titular del documento, además de los datos personales que se contienen en las líneas OCR de lectura mecánica. Desde el 28 de junio de 2009 se incorporan, además, las impresiones dactilares de los dedos índices de ambas manos o los que, en su defecto, correspondan.

(8) Para ofrecer una idea del alcance de este procesamiento de imágenes, téngase en cuenta que en las más de 50 ocasiones que se utilizó el sistema en el mencionado proyecto piloto entre los años 2017 y 2018, se escanearon alrededor de 500.000 caras -lo que no significa necesariamente 500.000 personas diferentes, dado que el sistema capta y procesa la cara de una misma persona en distintos momentos-.

(9) En el caso del Perú, esta materia está regulada por el Decreto Legislativo 1218, de 23 de septiembre de 2015, que aprueba el Decreto Legislativo que regula el uso de las cámaras de videovigilancia, y la Ley 30120 – Ley de apoyo a la seguridad ciudadana con cámaras de videovigilancia públicas y privadas. Además, existen otras leyes sectoriales que establecen el uso de cámaras de videovigilancia en rubros específicos. Vid. también el Decreto Supremo 007-2020-IN, que aprueba el Reglamento del Decreto Legislativo 1218, Decreto Legislativo que regula el uso de las cámaras de videovigilancia y de la Ley 30120, Ley de Apoyo a la Seguridad Ciudadana con Cámaras de Videovigilancia Públicas y Privadas, y dicta otras disposiciones. El artículo 17.2 de este Reglamento establece que las imágenes, vídeos o audios grabados se deben almacenar por un plazo mínimo de 45 días calendario, salvo disposición distinta en normas sectoriales.

(10) En el caso del Perú, en el plano internacional, vid. el artículo 11 de la Convención Americana Sobre Derechos Humanos (Pacto de San José, 1969) que proclama que "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia […]". En el plano interno, el artículo 2, numeral 6, de la Constitución política del Perú reconoce el derecho que toda persona tiene "A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".

Para resolver esta alegación, de manera congruente con el contenido del precepto trascrito, el Tribunal analiza de manera sucesiva las siguientes tres cuestiones:

- Si el AFR supone una injerencia del derecho al respeto a la vida privada (ap. 1)
- En caso de que suponga esa injerencia, si está prevista por ley (ap. 2)
- En caso de que suponga esa injerencia, si respeta el principio de proporcionalidad (ap. 3)

3.1. El reconocimiento facial automático y el derecho al respeto a la vida privada. Una exposición crítica de la fundamentación del Alto Tribunal

3.1.1. La argumentación de la sentencia comentada

Con respecto al Derecho al respeto a la vida privada, la doctrina ha destacado que "probablemente nos encontramos ante el derecho más imprecisamente recogido en el texto del Convenio, lo que ha llevado a que su alcance haya quedado extremadamente expuesto a una interpretación judicial muy basada en el caso concreto" (Pérez De Los Cobos, 2018, p. 6). Según la jurisprudencia del Tribunal Europeo de Derechos Humanos, que reitera la sentencia comentada, la "vida privada" es un concepto amplio que no es susceptible de una definición exhaustiva, pero que, en cualquier caso, no se puede restringir a los ámbitos más propios de la esfera íntima de la persona, tales como su domicilio u otras dependencias privadas, dejando fuera otros aspectos de su identidad, desarrollo personal y relaciones sociales. Pero la sentencia comentada también insiste en que se trata de un derecho que no está exento de límites y a este respecto reitera tres elementos que deben tenerse en cuenta:

- Que la supuesta amenaza o asalto a la vida privada del individuo alcance un cierto nivel de gravedad, esto es, sea de cierta entidad (*a certain level of seriousness*).
- Que, atendiendo a las circunstancias, el sujeto afectado pueda alegar una expectativa razonable de privacidad (*reasonable expectation of privacy*).
- El alcance de las justificaciones que se enumeran en el artículo 8.2 CEDH.

En lo que nos ocupa, interesan particularmente los dos primeros (pues el tercero entra en juego en otro momento del proceso lógico de análisis y sobre él volveremos más adelante), que serán los que sigamos para sistematizar los distintos argumentos desarrollados por la sentencia, aunque formalmente el Alto Tribunal de Justicia no sigue este esquema-.

a) La expectativa razonable de privacidad. A juicio del Cuerpo policial, la utilización de *AFR Locate* no supone una injerencia en el derecho a la vida privada por cuanto una persona no podría tener una expectativa razonable de privacidad al caminar en un lugar público y, por tanto, podría esperar que su imagen pudiera ser grabada. Por el contrario, la sentencia parte de que el hecho de que el reconocimiento facial automático tome como fuente imágenes captadas en un lugar público no es motivo suficiente para excluir una injerencia en el derecho a la vida privada, pues considera -en la misma línea que el TEDH- que aunque esa expectativa es importante no es un factor concluyente. A este respecto, recuerda la STEDH, *asunto P.G. y J.H. v. United Kingdom* (recurso 44787/98), de 25 de septiembre de 2001:

> "A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain"(11) [el resaltado es nuestro] (ap. 57).

Esto es, no se excluye esa injerencia a la vida privada cuando se trate de grabaciones sistemáticas o permanentes del espacio público.

b) El umbral mínimo de gravedad de la injerencia. Análisis crítico de la argumentación ofrecida. Para el Cuerpo policial, la utilización de *AFR Locate*, al tratarse de un procedimiento casi instantáneo en el que no se archivan los datos, no alcanza el umbral mínimo de gravedad.

La sentencia admite que en supuestos anteriores la jurisprudencia inglesa ha rechazado que el simple acto de tomar fotografías pueda ser considerado una

(11) "Una persona que camina por la calle será, inevitablemente, visible por cualquier otra persona que también esté presente. El monitoreo (vigilancia) por medios tecnológicos del mismo escenario público (por ejemplo, un vigilante de seguridad a través de un circuito cerrado de televisión) tiene una naturaleza similar. Sin embargo, puede plantearse la existencia de una afectación a la vida privada, cuando exista una grabación sistemática o permanente de dicho escenario o ámbito público" (traducción propia).

injerencia a los efectos del artículo 8 CEDH si no va acompañado de ciertas "circunstancias agravantes". Igualmente, añade que un cacheo ordinario superficial de las personas o la apertura de bolsos y similares a los que los pasajeros se someten de manera rutinaria en los aeropuertos es algo casi familiar y esperado, por lo que no tendría sentido apreciar ahí una violación *prima facie* del artículo 8 y pedir al Estado que justificara esas medidas con referencia al artículo 8.2 CEDH. En nuestra opinión, en este punto la sentencia mezcla o confunde dos planos: uno, el conceptual de si esa actuación administrativa supone una injerencia en la vida privada, y otro, el del pragmatismo judicial.

No obstante, el Alto Tribunal considera que el uso de AFR va mucho más allá de la simple toma de una fotografía y, a partir de ahí, se centra en el hecho de que el sistema recopila y almacena (aunque por un brevísimo espacio de tiempo) datos biométricos de carácter personal y abunda en cómo el TEDH ha enfatizado la importancia de la protección de datos personales como parte de la protección de los derechos del art. 8 CEDH. Particular interés tiene la STEDH, asunto *S. and Marper v. United Kingdom* (recursos 30562/04 y 30566/04), de 4 de diciembre de 2008, que presenta una gran proximidad con el caso ahora enjuiciado, pues se cuestionaba la retención policial de datos biométricos en forma de registros de huellas dactilares y muestras de ADN. Esta sentencia sostiene lo siguiente:

> "El mero hecho de almacenar datos relativos a la vida privada de una persona constituye una injerencia en el sentido del artículo 8 (Sentencia Leander contra Suecia [TEDH 1987, 4] de 26 marzo 1987, ap. 48, serie A núm. 116). Poco importa que la información almacenada se utilice o no posteriormente (Sentencia Amann contra Suiza [TEDH 2000, 87] [GS], núm. 27798/1995, ap. 69, TEDH 2000-II). Sin embargo, para determinar si la información de carácter personal conservada por las autoridades hace que entre en juego uno de los citados aspectos de la vida privada, el Tribunal tendrá debidamente en cuenta el contexto particular en el que ha sido recogida y conservada la información, el carácter de los datos consignados, la manera en la que son utilizados y tratados y los resultados que pueden extraerse de ellos (ver, *mutatis mutandis*, Friedl [TEDH 1995, 4] , previamente citada, opinión de la Comisión, aps. 49-51, y Peck contra el Reino Unido [JUR 2003, 50030], anteriormente citada, ap. 59)". (ap. 67).

Y ante la alegación de que las huellas dactilares no serían inteligibles para una persona no experta y en ausencia de otras huellas con las que compararlas, la mencionada sentencia del TEDH añade que "ello no modifica el hecho de que las huellas dactilares contengan información única de la persona afectada y permitan una identificación precisa en muchas circunstancias. Las huellas dactilares son, por lo tanto, susceptibles de atentar contra la vida privada y su conservación sin el consentimiento de la persona afectada no se puede considerar una medida neutra o insignificante" (ap. 84)[12].

Por tanto, la sentencia del Alto Tribunal de Justicia de Inglaterra y Gales concluye que estos mismos razonamientos son trasladables a la tecnología AFR, pues la misma supone la extracción de información e identificadores únicos sobre un individuo que permite su identificación con precisión en una amplia gama de circunstancias. Esos datos biométricos, solos o junto con otros metadatos registrados, son una clara fuente de información personal y el hecho de que ello derive de las características faciales de una persona que se manifiestan en público no resta valor a esa conclusión. Pero llegados a este punto, la sentencia efectúa las siguientes afirmaciones que no compartimos plenamente:

> "The fact that, save where a match is detected, facial biometric information is retained for only a very short period, does not affect the analysis. The application of Article 8 is not dependent on the long-term retention of biometric data. It is sufficient if biometric data is captured, stored and processed, even momentarily. The mere storing of biometric data is enough to trigger Article 8 and the subsequent use (or discarding) of the stored information has no bearing (see S v. United Kingdom at [67], above). Accordingly, the fact that the process involves the near instantaneous processing and discarding of a person's biometric data where there is no match with anyone on the watchlist (and such data is never seen by or available to a human agent) does not matter"[13] (ap. 59).

Finalmente, debe mencionarse que la sentencia también concluye, aunque ello no era objeto del debate, que esa injerencia en el derecho a la vida privada no sólo se producía

(12) También el Tribunal de Justicia de la Unión Europea ha considerado que la toma y conservación de huellas dactilares "constituyen una vulneración -entiéndase con mayor propiedad "injerencia"- de los derechos de respeto de la vida privada" (ap. 30) (STJUE, de 17 de octubre de 2013, as. C-291/12, Michael Schwarz y Stadt Bochum, ECLI:EU:C 2013, 670).

(13) "El hecho de que (…) la información biométrica facial sea retenida por un período muy breve de tiempo no afecta al análisis (…) El mero almacenamiento de datos biométricos es suficiente para activar el artículo 8 y el uso posterior (o descarte) de la información almacenada no es relevante. En consecuencia, el hecho de que el proceso implica el procesamiento casi instantáneo y el descarte de una persona cuyos datos biométricos no presenten coincidencia con nadie de la lista (de tal manera que los datos nunca son vistos ni están disponibles para un agente humano) no importa" (traducción propia).

sobre aquellas personas que eran grabadas y de las que se extraían sus datos biométricos, sino también sobre aquellas personas que están en la lista de observación, aunque esa información se haya extraído de una base de datos policial.

3.1.2. Crítica a la argumentación expuesta y propuesta de una alternativa

Es cierto que el TEDH afirma que el mero hecho de almacenar datos relativos a la vida privada de una persona constituye una injerencia en el sentido del artículo 8, pero inmediatamente añade, como hemos transcrito, que para resolver si esa injerencia afecta al derecho a la vida privada "el Tribunal tendrá debidamente en cuenta el contexto particular en el que ha sido recogida y conservada la información, el carácter de los datos consignados, la manera en la que son utilizados y tratados y los resultados que pueden extraerse de ellos". Esto es, a nuestro juicio, el Alto Tribunal no aplica correctamente la jurisprudencia del TEDH cuando afirma que "el uso posterior de la información almacenada no tiene importancia" y hace que casi todo pivote en la existencia de un almacenamiento. La mencionada STEDH, asunto *S. and Marper v. United Kingdom*, que el Alto Tribunal utiliza como fundamento, incluye la manera en que son utilizados y tratados los datos como uno de los criterios, junto a otros, que se deben tener en cuenta para dilucidar si esa injerencia -el almacenamiento- afecta o no a alguno de los aspectos incluidos en el derecho a la vida privada. Igualmente, la STEDH, asunto *Perry v. United Kingdom*, razona lo siguiente:

> "Bien que les voix des suspects dans l'affaire P.G. et J.H. eussent été enregistrées sur un support permanent pendant qu'ils étaient interrogés par des agents de police dans une salle ouverte d'un commissariat, cet enregistrement effectué à des fins d'analyse ultérieure a été considéré comme un traitement de données à caractère personnel portant atteinte au droit des intéressés au respect de leur vie privée (voir l'arrêt P .G. et J.H. précité, §§ 59-60). Pareils enregistrements réalisés au moyen de dispositifs de surveillance peuvent également tomber sous le coup de l'article 8 § 1 de la Convention lorsque leur divulgation, par ses modalités ou son ampleur, excède ce à quoi les intéressés peuvent raisonnablement s'attendre. Dans l'arrêt Peck c. Royaume-Uni (no 44647/98, arrêt du 28 janvier 2003, CEDH 2003 - ...), la communication aux média pour diffusion du film de la tentative de suicide du requérant enregistrée par des caméras de télévision en circuit fermé avait été considérée comme une ingérence grave dans sa vie privée, alors même qu'il se trouvait dans un lieu public au moment des faits"(14) (ap. 38).

Obsérvese nuevamente cómo la afectación al derecho a la vida privada en los dispositivos de videovigilancia que graban no se hace depender expresamente del hecho de que graben (almacenen) sino de la modalidad y amplitud de su divulgación. Igual ocurre en la mencionada STEDH, asunto *P.G. y J.H. v. United Kingdom* (recurso 44787/98), de 25 de septiembre de 2001, que razona lo siguiente: "Cuando se tomaron fotografías de un reclamante en una manifestación pública en un lugar público y conservadas por la policía en un expediente, la Comisión no encontró ninguna interferencia en la vida privada, dando peso al hecho de que la fotografía fue tomada y conservada como registro de la manifestación y no se había tomado ninguna medida para identificar a las personas fotografiadas en esa ocasión mediante el tratamiento de datos". (ap. 58). Esto es, se habían almacenado datos relativos a la vida privada de una persona (fotografías), pero no se aprecia interferencia en la vida privada.

Además, recuérdese que en la citada STEDH asunto *S. and Marper v. United Kingdom*, el Tribunal afirmaba que un monitoreo por personal de seguridad privada a través de un circuito cerrado de televisión tenía una naturaleza similar a las personas que estando en la calle ven a otras personas que están paseando, esto es, no suponía una injerencia en el derecho a la protección de la vida privada. Y debe tenerse en cuenta que ese monitoreo a través de un circuito cerrado de televisión puede conllevar también un almacenamiento instantáneo (no permanente) y procesamiento de las imágenes capturadas (por ejemplo, para la aplicación de un software que mejore la calidad de la imagen).

(14) "Aunque las voces de los sospechosos en el asunto P.G. y J.H. habían sido grabadas en un soporte permanente mientras eran interrogados por agentes de policía en una sala abierta de una comisaría, esta grabación, efectuada con la finalidad de un análisis posterior, fue considerada como un tratamiento de datos de carácter personal que infringía el derecho de los interesados a respetar su vida privada (véase P.G. y J.H. supra, párr. 59-60). Grabaciones similares realizadas utilizando dispositivos de vigilancia también pueden estar comprendidas en el ámbito del artículo 8.1 del Convenio cuando su divulgación, en atención al modo o amplitud con la que se efectúa, exceda de lo que los interesados puedan razonablemente esperar. En la sentencia Peck c. Reino Unido (núm. 44647/98, sentencia de 28 de enero de 2003, CEDH 2003), la transmisión a los medios de comunicación para su difusión del vídeo del intento de suicidio del reclamante grabado por unas cámaras de circuito cerrado de televisión (colocadas por la Administración local) fue considerada una grave injerencia en su vida privada, a pesar de que estaba en un lugar público en el momento de los sucesos" [traducción propia]. Las cámaras fueron colocadas por la Administración local y la difusión a los medios de comunicación se hizo con la finalidad de poner en valor la utilidad de su colocación.

En definitiva, aunque es cierto que el Tribunal Europeo de Derechos Humanos ha efectuado afirmaciones que vinculan el mero almacenamiento o grabación de datos personales con la afección al derecho a la vida privada, entendemos que las mismas deben analizarse en su contexto(15), y que no pueden obviarse otros elementos que en esas mismas sentencias se recogen a la hora de efectuar ese enjuiciamiento, en particular, los siguientes: las circunstancias en las que ha sido recogida y conservada la información; el carácter de los datos consignados; la manera en la que son utilizados y tratados; y los resultados que pueden extraerse de ellos.

Con esos presupuestos, conviene insistir en dos aspectos:

- Las plantillas biométricas de las imágenes faciales captadas, haya o no coincidencia, no se retienen y son eliminadas de manera inmediata y automática, sin que ni el agente policial que gestiona el sistema ni ningún otro pueda acceder a ellas. Las imágenes faciales captadas también se eliminan automática e inmediatamente si no hay coincidencia y si hay coincidencia, se da a entender que se conserva durante 24 horas junto con otros metadatos. La grabación realizada por el circuito cerrado de televisión se conserva durante 31 días(16). En definitiva, los datos biométricos son sólo objeto del almacenamiento transitorio indispensable, que se cuenta en segundos, para su tratamiento inmediato (recuérdese que el sistema es capaz de escanear 50 imágenes faciales por segundo). Otros datos personales, imágenes faciales y grabación de vídeo, sí son objeto de un almacenamiento temporal.
- En todos los supuestos enjuiciados por las sentencias citadas del TEDH el almacenamiento de esos datos era permanente(17).

Por tanto, es necesario buscar otros fundamentos más sólidos para la defensa de esta injerencia en la vida privada que la mera existencia de un almacenamiento de los datos durante los segundos necesarios para permitir el procesamiento de las imágenes. A esa conclusión llevan no sólo los argumentos que hemos expuesto, sino también el testeo de la postura mantenida por el Alto Tribunal ante otro supuesto de utilización del reconocimiento facial automático por parte de la policía. Nos referimos al supuesto arriba mencionado de utilización de esta técnica en los aeropuertos en el control de entrada en territorio nacional (nota a pie 8). La traslación de esa postura debería llevar a mantener que ello también supone una injerencia en el derecho a la vida privada, por cuanto la técnica es similar y también se produce ese almacenamiento transitorio necesario para el procesamiento de la imagen.

No obstante, a nuestro juicio, es insostenible mantener que hay aquí una injerencia en la vida privada. Todo viajero que utiliza un aeropuerto en un vuelo internacional sabe sin ningún género de duda que va a ser sometido a un control policial de identidad. No hay en ello injerencia alguna en la vida privada y, a nuestro juicio, resulta irrelevante que eso lo haga un agente policial mirando la cara y el pasaporte o lo haga un sistema automático de reconocimiento facial. En definitiva,

(15) Con respecto al artículo 8 del Convenio Europeo de Derechos Humanos, debemos confesar que "a menudo es muy complejo y no resulta prudente extraer conclusiones generales a partir de la lectura de los pronunciamientos del TEDH, pues las circunstancias particulares del caso concreto suelen adquirir tal relevancia en la doctrina formulada, que no es posible hacer una lectura de la misma desligada de tales circunstancias" (Pérez de los Cobos, 2018, p. 6). Además, en algunos pronunciamientos, tampoco es fácil discernir hasta qué punto se está discutiendo si hay injerencia o no en el derecho a la vida privada, o si la misma es lícita y justificada.

(16) No obstante, a los efectos de una construcción teórica de carácter general sobre el reconocimiento facial automático, se debería prescindir de este dato pues no es algo consustancial a dicho procedimiento.

(17) En la STEDH, asunto Leander contra Suecia (rec. 9248/1981), de 26 marzo de 1987, se trataba de un registro secreto de carácter policial donde se incorporaba información relevante para la seguridad nacional relativa a personas individualizadas y que se utilizaba, entre otras cosas, para evaluar la aptitud de candidatos para puestos de trabajo importantes desde el punto de vista de la seguridad. En el caso enjuiciado, se trataba precisamente de una persona a la que se le había rechazado un puesto de trabajo por este motivo y, por tanto, con datos que no podía refutar.
En la STEDH, asunto Amann contra Suiza (rec. 27798/1995), de 16 de febrero de 2000, se trataba de un fichero para la seguridad del Estado. A comienzos de los años ochenta, el solicitante, hombre de negocios, importó a Suiza aparatos depilatorios, de los que hizo publicidad en varias revistas. El 12 de octubre de 1981, una mujer le telefoneó desde la embajada, entonces soviética, de Berna para pedir un aparato depilatorio. Esta llamada telefónica fue interceptada por el ministerio público de la Confederación, el cual pidió al servicio de información de la policía del cantón de Zurich que investigara al solicitante. Se redactó una ficha personal que es la que se conserva en el mencionado fichero.
Finalmente, en la STEDH, asunto S. y Marper contra Reino Unido (rec. 30562/2004 y 30566/2004), de 4 de diciembre de 2008, se trataba de la conservación en ficheros policiales de huellas dactilares y muestras y perfiles de ADN de dos personas detenidas por distintos motivos, pero que nunca fueron condenadas.

en este supuesto de testeo, el criterio de la expectativa razonable de privacidad tiene un peso muy alto, que, en cualquier caso, prueba que el mero hecho de la existencia de ese almacenamiento transitorio para el tratamiento no es tan determinante como de la sentencia comentada se deduce.

Recuérdese que el SWP defendía que este reconocimiento facial automático no suponía injerencia en la vida privada por cuanto se trataba de un procedimiento instantáneo en el que no se archivaban los datos (como se ha dicho, dejemos de lado, por no ser relevante a los efectos teóricos que nos ocupa, el hecho de que la grabación de vídeo sí se archivaba). A este respecto, en ausencia de ese archivo, podría pensarse que es difícil imaginar que esos datos puedan llegar a conocimientos de terceros(18) o ser utilizados con otra finalidad distinta. El propio TEDH ha considerado que la simple vigilancia de los comportamientos y gestos del individuo en un lugar público a través de un sistema de videovigilancia que no almacena esos datos visuales no constituye una injerencia en su vida privada (vid., por ej., Herbecq y la asociación "Ligue des Droits de l'homme" v. Belgique, requêtes 32200/96 et 32201/96, Decisión de la Comisión de 14 de enero de 1998). No obstante, a nuestro juicio, hay tres elementos esenciales, que conectan con los criterios del TEDH antes enumerados, que hacen que esa doctrina no deba ser trasladable a este supuesto:

- El primero, vinculado con la mencionada expectativa razonable de privacidad o, para utilizar unos términos utilizados en esos criterios, con el contexto en el que la información es recogida. Una persona debe razonablemente prever que su comportamiento en ciertos tipos de espectáculos públicos o actividades similares va a ser objeto de vigilancia policial, que se realizará bien mediante la presencia directa de agentes o bien mediante un sistema de videovigilancia sin grabación. Además, hay una conexión directa y casi unívoca entre la técnica utilizada y su finalidad. El objeto es vigilar los comportamientos humanos en un determinado lugar y para ello se utiliza una técnica que muestra imágenes de ese comportamiento. No hay más. Por el contrario, cuando se añade el reconocimiento facial automático, se produce un notable salto cualitativo. No es razonablemente previsible que una persona considere que su asistencia a un partido de fútbol va a ser utilizada por la policía con la finalidad de verificar si sobre ella recae, por ejemplo, una orden de búsqueda y captura.
- El segundo, el carácter de los datos que se obtienen. En la videovigilancia policial sin grabación, los datos personales que se obtienen son los mismos que se obtendrían con la presencia de agentes de policía en el sitio. No obstante, en este supuesto, no es así. Los datos biométricos que se consiguen sería imposible que un agente policial los adquiriera con su mera presencia. A lo sumo, el agente podría llevar unas fotografías de sospechosos e intentar buscar esas caras entre el público asistente. Nada parecido a la obtención de unos datos biométricos.
- El tercero, el uso de esos datos y el resultado. En la videovigilancia sin grabación si el sistema capta un comportamiento constitutivo de, por ej., un delito, el sujeto podrá ser detenido por ese motivo. Por el contrario, en el sistema de reconocimiento facial automático (en particular, en las condiciones expuestas), lo que ofrece es una valoración de la posible coincidencia facial, que podrá originar que el sujeto sea llevado a dependencias policiales para verificar efectivamente su identidad (por ej., mediante las huellas dactilares) y puede que esa verificación sea positiva o no. En definitiva, el uso de los datos puede originar unos perjuicios en los ciudadanos que la simple videovigilancia sin grabación no genera. Bien es cierto que se afirma que la decisión última de actuación le corresponde al agente policial, sobre la base de su apreciación, pero tampoco se puede negar que la valoración ofrecida por el sistema de reconocimiento facial automático tendrá un notable peso en esa apreciación.

Todos estos elementos nos llevan a concluir que efectivamente hay en este supuesto una injerencia en el derecho a la vida privada, pero no tanto por ese almacenamiento instantáneo, sino por estos otros elementos que acabamos de exponer y que conectan directamente con los criterios arriba mencionados a los que se refiere el Tribunal Europeo de Derechos Humanos: el contexto en el que la información es recogida,

(18) De la descripción que se ofrece en la sentencia se desprende que el procesamiento de las imágenes faciales se realiza *in situ*. Otro tipo de riesgos para la seguridad y el respeto de la vida privada se generaría si dicha información se trasladara por internet para un tratamiento centralizado en alguna dependencia pública, pues ello haría posible que tal información, por ejemplo, fuera interceptada por un pirata informático o grabada para ser utilizada con otros fines.

el carácter de los datos consignados, la manera en la que son utilizados y tratados y los resultados que pueden extraerse de ellos.

3.2. La base legal suficiente de la injerencia en el derecho al respeto a la vida privada

El hecho de que la utilización del reconocimiento facial automático en el contexto que es analizado por la sentencia suponga una injerencia en el derecho al respeto a la vida privada no supone *per se* una vulneración de este derecho, sino, más bien, la constatación de un hecho. Para dilucidar si concurre esa vulneración, una vez apreciada la injerencia, debe acudirse a los otros dos elementos que recoge el artículo. 8 CEDH y que ya mencionamos. El primero de ellos es que dicha injerencia "esté prevista por la ley" (artículo. 8.2 en su versión en español) (*in accordance with the law*, artículo. 8.2 en su versión en inglés). Con respecto a esta exigencia, dos son los aspectos que analiza la sentencia que, en buena medida -aunque con singularidades en el planteamiento-, conecta con la construcción habitual en la doctrina administrativista de la vertiente positiva y negativa del sometimiento de la Administración al principio de legalidad:

- Si es necesaria una habilitación legal específica para poder utilizar esta tecnología (a)
- Si ese marco normativo es suficiente (b)

a) Con respecto a la primero, el demandante considera que debe haber una normativa específica que habilite a las fuerzas policiales para el uso del reconocimiento facial automático en este contexto. No obstante, el planteamiento del Alto Tribunal es distinto. Este parte de que los agentes de policías son sujetos del *common law* que tienen el deber, reconocido por el derecho consuetudinario, de mantener el orden público y de prevenir y detectar delitos (*crime*). Y este deber conlleva el poder, también de derecho consuetudinario, de tomar las medidas que tengan como finalidad prevenir y detectar esas infracciones penales. No hay una definición exhaustiva de esas potestades, pero la jurisprudencia admite que son todas aquellas necesarias para esos fines (Rice v Connolly, 1966, 2 QB 414 a 419B-C). Pero inmediatamente esa jurisprudencia matiza que estos poderes de derecho consuetudinario no autorizan métodos intrusivos (*intrusive methods*) para obtener información, como la entrada a una propiedad privada (R (Catt) v Association of Chief Police Officers, 2015, AC 1065). Esos métodos intrusivos conectan con la intrusión física o interferencia con los derechos de la persona sobre su vivienda o sobre su integridad corporal. El empleo de esos métodos intrusivos sí exige la promulgación de poderes legales específicos. A este respecto, la sentencia trae a colación que el acto de tomar huellas dactilares requiere generalmente la colaboración o el uso de la fuerza sobre el individuo, por lo que se está ante un método intrusivo que requirió la aprobación de poderes legales específicos. Por tanto, lo que el Alto Tribunal analiza es si la utilización de AFR supone un método intrusivo en los términos expuestos y concluye que no, dado que no es necesaria ninguna entrada física, contacto o fuerza para obtener dichos datos. A la misma conclusión llega con respecto a la compilación de las listas de observación. En definitiva, los poderes de *common law* de la policía son "ampliamente suficientes" para el uso de *AFR Locate*, sin que se necesiten nuevos poderes específicos sobre ello.

   El planteamiento expuesto es propio del Derecho anglosajón y plantearía mayores dificultades en el Derecho Administrativo peruano o en el derecho español, donde el juego del principio del sometimiento de la Administración a la Ley es distinto.

b) Con respecto a lo segundo, la exigencia de conformidad con la ley (*in accordance with the law* standard) requiere que el marco normativo aplicable, que la sentencia advierte que no debe ser necesariamente específico, sino que puede derivar de las regulaciones existentes en el contexto del derecho consuetudinario, sea suficiente. Para ello, las exigencias fundamentales que debe cumplir son las siguientes:

   - Accesibilidad. Esto es, ese marco normativo debe ser público y comprensible.
   - Brindar una protección adecuada frente a la arbitrariedad o la actuación inadecuada. A este respecto, debe tenerse en cuenta que la sentencia advierte que en los términos en los que se enjuicia la utilización de *AFR Locate* no se está ante un supuesto de vigilancia encubierta que conllevaría el sometimiento a la Regulation of Investigatory Powers Act 2000 ("RIPA") y, siguiendo la doctrina del TEDH, a unas exigencias mayores vinculadas con la necesidad de una autorización judicial o de una autoridad administrativa independiente.
   - Previsibilidad, aunque ello no supone que deban estar codificadas las respuestas a cada posible problema.

Tras un análisis de toda la normativa general aplicable (la legislación sobre protección de datos de carácter personal, los códigos de buenas prácticas aprobados con base en esa legislación y las propias directrices locales de la Policía, procedimientos operativos, informes de implementación y política de SWP en procesamientos sensibles), la sentencia concluye que existe un marco legal claro, suficiente, accesible y previsible que delimita si se puede hacer uso del reconocimiento facial automático, cuándo se puede hacer uso del mismo y cómo. Llama la atención la amplitud de la naturaleza de los documentos públicos que la sentencia tiene en cuenta a estos efectos, pues, por ej., buena parte de los contenidos relativos al cómo se debe utilizar se encuentran en las mencionadas Directrices propias del Cuerpo policial. En cualquier caso, la sentencia deja abierta la puerta a que este marco normativo deba ser objeto de una revisión en el futuro para reevaluar su suficiencia.

3.3. Que constituya una medida que, en una sociedad democrática, sea necesaria. El principio de proporcionalidad

Para justificar una injerencia en el derecho al respeto de la vida privada, el Alto Tribunal reitera que deben cumplirse con las cuatro exigencias recogidas en la sentencia Bank Mellat v. Tesoro de Su Majestad (2) [2014] AC 700, de 19 de junio de 2013:

- Que la finalidad perseguida por la medida sea lo suficientemente importante para justificar la limitación de un derecho fundamental.
- Que la medida esté racionalmente conectada con la finalidad
- Que no haya otra medida menos intrusiva que pudiera haberse utilizado sin comprometer de manera inaceptable la finalidad perseguida
- Que, teniendo en cuenta todo lo anterior y la gravedad de las consecuencias, se haya alcanzado un equilibrio justo entre los derechos del individuo y los intereses de la comunidad.

Esto es, a grandes rasgos, lo que en la doctrina española se conoce como las tres reglas del principio de proporcionalidad: el juicio de idoneidad, el juicio de necesidad y el juicio de proporcionalidad en sentido estricto (Rebollo Puig, 2019, p. 23).

Para el Alto Tribunal, los problemas se centran en la tercera y cuarta exigencia, esto es, si no hay otras medidas menos restrictivas para alcanzar los mismos objetivos (el juicio de necesidad) y si se ha alcanzado ese equilibrio justo (el juicio de proporcionalidad en sentido estricto). Aunque la argumentación no individualiza el análisis de ambos criterios y todo aparece mezclado, la conclusión es contundente: la utilización del AFR en el caso concreto objeto de enjuiciamiento no es desproporcionada. En cuanto a la necesidad, podrían traerse a colación los siguientes dos argumentos de la sentencia:

- Se trata de identificar a concretos individuos sobre los que hay buenas razones para considerar que podían estar en la zona afectada por el dispositivo de AFR y sobre los que había un interés policial justificado. A este respecto, fuera del objeto de la demanda, la sentencia advierte que la inclusión de cualquier persona en la lista de observación y el consiguiente procesamiento de sus datos personales sin una justificación suficiente probablemente supondría una injerencia ilegal sobre el derecho al respeto de la vida privada.
- En la mayoría de los eventos, al menos una persona de la lista de observación ha sido identificada, lo que a menudo ha originado la detención de personas buscadas que, de no ser así, no habrían sido identificadas. La videovigilancia por circuitos cerrados de televisión no permite la consecución de este objetivo. Durante el proyecto piloto, la tecnología *AFR Locate* ha permitido el arresto de 37 individuos que no se hubieran podido localizar por los métodos tradicionales.

En cuanto a la proporcionalidad en sentido estricto, la sentencia parte de que la injerencia en el derecho al respeto a la vida privada del demandante fue muy reducida, prácticamente se limitó a un instantáneo procesamiento algorítmico y eliminación de sus datos biométricos y ningún agente de policía se dirigió o habló con él. En el otro lado de la balanza coloca los siguientes datos: en algunos de los eventos donde se utilizó la tecnología se habían producido alteraciones del orden público en anteriores ocasiones; el sistema se usó en un espacio abierto, de manera transparente y por tiempo limitado; el propósito era específico y limitado a tratar de identificar concretos sujetos; y nadie fue arrestado injustamente.

Finalmente, la sentencia insiste en que este análisis de proporcionalidad se hace con base en las circunstancias concurrentes en el caso concreto, advirtiendo que cada supuesto habrá de ser analizado de manera individual, aunque concluye que el sistema no presenta un problema claro o sistémico de déficit de proporcionalidad de tal manera que se pudiera decir que el uso futuro de esta tecnología sería inevitablemente desproporcionado.

4. El reconocimiento facial automático y la protección de datos de carácter personal

4.1. Los datos biométricos son datos personales y la exigencia de licitud en el tratamiento

En primer lugar, debe advertirse que aunque los despliegues de *AFR Locate* recurridos tuvieron lugar antes de la aprobación en el Reino Unido de la Ley de Protección de Datos de 2018, ambas partes solicitan y el Tribunal acepta pronunciarse como si esa Ley hubiera estado vigente, forma de proceder completamente ajena al Derecho español. En buena medida, esa Ley perseguía la incorporación a la legislación del Reino Unido de la siguiente normativa de la Unión Europea: el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante RGPD); y la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. Por este motivo, con la finalidad de dotar a estos comentarios de un alcance más general, siempre que sea posible, conectaremos las argumentaciones del Alto Tribunal no con esa Ley, que es lo que en la sentencia se hace, sino directamente con la normativa de la Unión Europea.

SWP acepta que el uso de *AFR Locate* implica el tratamiento de datos personales de las personas que se incluyen en la lista de observación, pero rechaza que eso mismo ocurra con respecto a las imágenes que son capturadas y procesadas por el equipo, por cuanto SWP ni puede ni intenta identificar a ninguna de esas personas, salvo aquellas que están en la lista de observación.

El artículo 4 RGPD define los datos personales, en lo que nos interesa, como "toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante (…) o uno o varios elementos propios de la identidad física (…) de dicha persona"[19]. A este respecto, el Alto Tribunal recuerda que la STJUE, de 11 de diciembre de 2014, *František Ryneš y Úřad pro ochranu osobních údajů*, as. C-212/13, ECLI:EU:C:2014:2428, afirmó de manera rotunda que "la imagen de una persona grabada por una cámara constituye un dato personal (…), en la medida en que permite identificar a la persona afectada" (ap. 22). En esa misma línea, la sentencia comentada considera que, por su naturaleza, los datos biométricos faciales son información sobre una persona física, singulares de esa persona y distintos de todos los de las demás. Esos datos biométricos faciales se utilizan para distinguir a esa persona de cualquier otra persona para que pueda llevarse a cabo el proceso de análisis de correspondencia. En definitiva, los datos biométricos faciales claramente comprenden datos personales porque, *per se*, permiten la identificación inmediata de una persona. En la actualidad, el mencionado artículo 4 RGPD define expresamente los datos biométricos como "*datos personales* obtenidos a partir de un tratamiento 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" [la cursiva es nuestra][20].

La consecuencia que deriva de esta indiscutible calificación de los datos como personales es que el cuerpo policial (SWP) debe tratarlos con sometimiento a los principios de protección de datos recogidos en la legislación y, en particular, pues así lo plantea el recurrente, a la exigencia de licitud[21].

(19) En los mismos términos, la definición contenida en el artículo 3 de la Directiva 2016/680. En el Perú, el artículo 2 de la Ley 29733, Ley de protección de datos personales, define "datos personales" como "Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados" y "datos sensibles", entre otros, como los "datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular […]".

(20) En términos prácticamente idénticos, el artículo 3.13 de la Directiva 2016/680.

(21) El artículo 4 Directiva 2016/680 enumera los principios a los que queda sometido el tratamiento de datos personales en este ámbito: licitud y lealtad; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; seguridad, integridad y confidencialidad; y responsabilidad proactiva. Debe tenerse en cuenta que estos principios no coinciden plenamente con los recogidos en el artículo 5 RGPD.

Sobre la licitud, el artículo 6 RGPD establece que el tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones[22]:

> "a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
>
> b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
>
> c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
>
> d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
>
> e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
>
> f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
>
> Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones".

El Alto Tribunal considera que la utilización de *AFR Locate* por un cuerpo policial encaja en la letra f) (tratamiento necesario para la satisfacción de intereses legítimos perseguidos por el responsable, siempre que sobre dichos intereses no prevalezcan derechos y libertades fundamentales). Debe advertirse que eso es así conforme a la legislación del Reino Unido, pero que el precepto reproducido del RGPD precisamente excluye este supuesto en el tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones. En cualquier caso, el Alto Tribunal añade que tampoco descarta que el caso se pueda encuadrar en los supuestos recogidos en las letras c) (cumplimiento de una obligación legal) y e) (ejercicio de poderes públicos), que encajarían más adecuadamente con lo previsto en el artículo 8 de la Directiva 2016/680 sobre la licitud del tratamiento.

4.2. *AFR Locate* y la Directiva (UE) 2016/680

Seguidamente, el Alto Tribunal analiza si el tratamiento de datos personales realizado por *AFR Locate* cumple con ciertas previsiones contenidas en la Ley de Protección de Datos (DPA, 2018) aplicables 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[23]. En ese ámbito, la legislación del Reino Unido sigue la mencionada Directiva (UE) 2016/680, cuyo artículo 10 establece que el tratamiento de datos biométricos dirigidos a identificar de manera unívoca a 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.

Con respecto a esta normativa específica, son varias las cuestiones a las que la sentencia se enfrenta: si el régimen específico de la Directiva 2016/680 -en puridad, de su normativa de transposición al Reino Unido- es aplicable a *AFR Locate* (2.1); si *AFR Locate* cumple con los tres requisitos de la Sección 35 (5) DPA 2018 (sobre la base del artículo 10

(22) Reproducimos el artículo 6 RGPD puesto que en términos generales es lo que recoge la normativa que analiza la sentencia. No obstante, el artículo 8 de la Directiva 2016/680, dado su ámbito de aplicación más acotado, restringe estos supuestos que fundamentan la licitud del tratamiento a "que sea necesario para la ejecución de una tarea realizada por una autoridad competente, para los fines establecidos en el artículo 1, apartado 1, y esté basado en el Derecho de la Unión o del Estado miembro". Recuérdese que esos fines son la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

(23) Como se ha dicho en la nota anterior, el RGPD excluye de su ámbito de aplicación esta categoría de tratamiento de datos personales. Para ello debe acudirse a la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Esta Directiva, todavía no transpuesta al ordenamiento español, pues debía haberse hecho antes de mayo de 2018, está destinada a los ámbitos policiales y de la Justicia. Pretende asegurar que los datos de las víctimas, testigos y sospechosos de la comisión de delitos se encuentren debidamente protegidos en el ámbito de una investigación criminal o de aplicación de la ley. A la vez, se pretende que esta armonización normativa facilite la cooperación transfronteriza de la policía y los fiscales para combatir más eficazmente el crimen y el terrorismo en la Unión Europea.

Directiva 2016/680) (2.2); y si se ha realizado la correspondiente evaluación de impacto relativa a la protección de datos (2.3).

4.2.1. Sobre la aplicación del régimen específico de la Directiva 2016/680 a *AFR Locate*

SWP admite que el régimen específico que supone la Directiva 2016/680 (en puridad, la normativa de transposición al Derecho del Reino Unido) es aplicable al tratamiento de los datos biométricos de las personas que están en la lista de observación, pero no a los datos biométricos de las personas cuyas caras son capturadas por las cámaras del circuito cerrado de televisión que utiliza *AFR Locate*.

Por este motivo, lo primero que analiza la sentencia es si *AFR Locate* implica el tratamiento de datos biométricos con el propósito de "identificar de manera unívoca a una persona física", que es de lo que habla el mencionado artículo 10. Para interpretar esta expresión acude al Informe Explicativo del Protocolo de 2018 por el que se modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automático de datos personales. En el punto 18 de ese informe se explica que "identificable" no se refiere solo a la identidad civil o legal del individuo como tal, "sino también a lo que puede individualizar o diferenciar a una persona de otros (y, por ende, permitir tratar de manera diferente). Esta *individualización* se puede realizar, por ejemplo, refiriéndose a la persona específicamente o a un equipo o conjunto de equipos (computadora, teléfono celular, cámara fotográfica, equipos de videojuegos, etc.) mediante un número de identificación, seudónimo, datos biométricos o genéticos, datos de ubicación, dirección IP u otro elemento identificador.

El uso de seudónimos o de un identificador digital/identidad digital no lleva al anonimato de los datos, dado que el titular en todo caso puede ser identificable o individualizado. Por lo tanto, los datos seudónimos deberán considerarse datos personales y se encuentran dentro del alcance de las disposiciones del Convenio". Con este presupuesto, el punto 58 añade que: "El tratamiento de datos biométricos, es decir, datos que resultan de un tratamiento de datos específico técnico relacionado con las características físicas, biológicas o fisiológicas de un individuo que permiten una identificación o autenticación exclusiva del individuo, también se considera sensible cuando es utilizado justamente para identificar exclusivamente al titular de datos". Y finalmente, el punto 59 aclara lo relativo al tratamiento de imágenes:

> "El contexto del tratamiento de imágenes es importante para determinar la naturaleza sensible de los datos. Por lo general, el tratamiento de imágenes no involucrará el tratamiento de datos sensibles, ya que las imágenes solo se encontrarán dentro de la definición de datos biométricos cuando sean tratadas a través de un medio técnico específico que permita la identificación o autenticación exclusiva del individuo. Además, cuando el tratamiento de imágenes se planeare para revelar información racial, étnica o de salud (ver el punto siguiente), dicho tratamiento será considerado tratamiento de datos sensibles. Por el contrario, por lo general, las imágenes tratadas mediante un sistema de videovigilancia por meras razones de seguridad en un área de compras no será considerado tratamiento de datos sensibles".

Evidentemente, con estos presupuestos, la sentencia concluye que también el tratamiento de imágenes que realiza *AFR Locate* de las personas cuyas caras son capturadas constituye un tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona física (los datos biométricos de los miembros del público son procesados para que cada individuo también sea identificado de manera única y así poder efectuar la comparación con la lista de observación) y, por consiguiente, queda sometido a las exigencias del mencionado artículo 10 Directiva 2016/680.

4.2.2. Si AFR Locate cumple con los requisitos de la Sección 35 (5) DPA 2018 (sobre la base del artículo 10 Directiva 2016/680)

Los tres requisitos que se incluye en la Sección 35 (5) y que van algo más allá de lo previsto en el artículo 10 de la Directiva 2016/680 son los siguientes:

- Que el procesamiento sea estrictamente necesario para la aplicación de la ley.
- Que el procesamiento sea necesario bien para el ejercicio de una función atribuida a una persona por *enactment or rule of law*, bien por razones de un relevante interés público.
- Que el responsable del tratamiento disponga de un documento apropiado en el que se establezcan, entre otros contenidos, los procedimientos para asegurar el cumplimiento de los principios de protección de datos y las políticas de conservación y borrado de los datos personales procesados.

Con respecto al primer requisito, que conecta con el principio de proporcionalidad, la sentencia se remite a lo que expusimos más arriba con respecto a la reclamación en virtud del artículo 8 CEDH. En definitiva, la existencia de justificaciones precisas y particularmente sólidas que fundamenten

este procesamiento de datos especialmente sensibles, que la sentencia aprecia que concurren.

A propósito del segundo requisito, también remitiéndose a argumentos anteriores, la sentencia identifica que el *rule of law* relevante es el ya mencionado deber del derecho consuetudinario de prevenir y detectar delitos.

Finalmente, sobre el tercer requisito, la sentencia identifica que existe un documento titulado "*Policy on Sensitive Processing for Law Enforcement Purposes under Part 3 Data Protection Act 2018. South Wales Police (SWP) Automated Facial Recognition (AFR). Processing biometric data to uniquely identify a person*", de noviembre de 2018. La sentencia advierte que este documento es excesivamente genérico y que, en algunos aspectos, se limita a reproducir lo que establece la ley sin concreción alguna. Sin embargo, el Alto Tribunal de Justicia, tras efectuar estas observaciones, renuncia expresamente a resolver si el documento cumple con los mencionados requisitos de contenido, remitiendo este análisis al *Information Commissioner* (autoridad independiente del Reino Unido creada para proteger los derechos de información).

4.2.3. Si se ha realizado la correspondiente evaluación de impacto relativa a la protección de datos

El artículo 27 de la Directiva 2016/680 dispone lo siguiente:

> "1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, suponga un alto riesgo para los derechos y libertades de las personas físicas, los Estados miembros dispondrán que el responsable del tratamiento lleve a cabo, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales.
>
> 2. La evaluación mencionada en el apartado 1 incluirá, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos riesgos, y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar la conformidad con la presente Directiva, teniendo en cuenta los derechos e intereses legítimos de los interesados y las demás personas afectadas".

En esta línea se pronuncia también la sección 64 de la DPA 2018. SWP preparó una evaluación de impacto con respecto al uso de equipos AFR, pero el recurrente sostiene que la misma es defectuosa por cuanto en esa evaluación se parte de que el uso de *AFR Locate* no supone el tratamiento sensible de datos personales de los miembros del público (recuérdese que este punto de partida ha sido rechazado por la sentencia comentada).

Ante esta cuestión, lo primero de lo que se ocupa la sentencia es de cuál debe ser el alcance de su control sobre el cumplimiento del deber por parte de la autoridad competente de una evaluación de impacto. A este respecto, la sentencia considera que la noción de evaluación obliga a realizar un juicio razonable basado en una investigación y consideración razonables. Por tanto, cuando el responsable del tratamiento ha llevado una evaluación concienzuda, aunque quizás no correcta, añadimos nosotros, el Tribunal no puede ir más allá. El Tribunal podrá considerar que se ha incumplido dicha obligación cuando es visible que el responsable ha abordado su evaluación sobre una base que es demostrablemente falsa o de una manera que es claramente deficiente. A este respecto, la sentencia (párr. 146) trae a colación su propia jurisprudencia sobre la evaluación del deber de igualdad del sector público, en su juicio R (Unison) v Lord Chancellor [2016] ICR 1, Underhill LJ hizo esta observación, que considera plenamente aplicable:

> "[…] to the extent that views are expressed on matters requiring assessment or evaluation the court should go no further in its review than to identify whether the essential questions have been conscientiously considered and that any conclusions reached are not irrational. Inessential errors or misjudgements cannot constitute evidence of the breach of the duty"[24] (párr. 106).

Con este enfoque, la sentencia concluye que la evaluación de impacto preparada por SWP cumple con las exigencias normativas, por cuanto explica claramente el tratamiento de datos propuesto, trata específicamente la posibilidad de violación de los derechos del artículo 8 CEDH (aunque SWP no apreciaba dicha vulneración) y prevé salvaguardas para el tratamiento de los datos personales de los miembros del público (aunque SWP consideraba que no había ahí tratamiento especialmente sensible).

(24) "[...] en la medida en que se expresen opiniones sobre asuntos que requieran evaluación (*assessment or evaluation*), el tribunal no debe avanzar más en su revisión que identificar si las preguntas esenciales han sido tenidas en cuenta concienzudamente y que cualquier conclusión alcanzada no sea irracional. Los errores no esenciales o los juicios erróneos no pueden constituir evidencia del incumplimiento del deber" [traducción propia].

5. El reconocimiento facial automático y la prohibición de la discriminación en las actuaciones de la administración pública

Según el artículo 149 (1) de la Ley de Igualdad de 2010, las autoridades públicas, en el ejercicio de sus funciones, deben tener en cuenta, entre otras cuestiones, la necesidad de eliminar la discriminación, el acoso, la victimización y cualquier otra conducta prohibida por esta Ley de Igualdad y de fomentar las buenas relaciones entre personas que comparten una característica protegida relevante y personas que no. A este respecto, el recurrente considera que *AFR Locate* vulnera estas exigencias por cuanto ese sistema puede producir resultados indirectos discriminatorios por razón de sexo/raza, porque produce una tasa más alta de coincidencias falsas positivas para rostros femeninos y/o para grupos étnicos negros y minoritarios(25).

La sentencia considera que la reclamación tiene un aire de irrealidad (*air of unreality*) por cuanto ni cuando comenzó la prueba de *AFR Locate* ni con posterioridad hay evidencia firme de que el software produzca resultados que sugieran discriminación indirecta. Es cierto que alguno de los expertos que comparecieron en el juicio declararon que estos sesgos son una característica común de los sistemas AFR y que ello depende del conjunto de datos utilizado por la empresa desarrolladora del software para "entrenar" el sistema(26), pero también reconocieron que no podían confirmarlo en el caso concreto. Además, el SWP aportó datos estadísticos de la utilización del sistema en la que no se evidenciaba ese sesgo discriminatorio por razón de género. Finalmente, la sentencia insiste en que el sistema no genera una actuación administrativa automática, sino que es un funcionario policial el que revisa la potencial coincidencia que ofrece el sistema y actúa en consecuencia. Por todo ello, rechaza esta reclamación.

6. Conclusiones

El análisis de la sentencia del Alto Tribunal de Justicia de Inglaterra y Gales que hemos realizado a lo largo de este trabajo nos permite extraer las siguientes conclusiones:

Primera. La utilización policial de un sistema de Reconocimiento Facial Automático

(25) Con carácter general, sobre los sesgos discriminatorios en el uso de la inteligencia artificial, tiene particular interés en el ámbito que nos ocupa el conocido Caso *Loomis*. En el año 2013, Eric Loomis fue detenido por agentes de policía del Estado de Wisconsin (Estados Unidos) cuando conducía un vehículo implicado en un tiroteo. Se le acusó de huir de la policía y utilizar un vehículo sin la autorización de su propietario. El señor Loomis se declaró culpable de ambos delitos con la esperanza de que ello fuera tenido en cuenta para no ingresar en prisión. El fiscal aportó un informe elaborado por el programa informático Compas, desarrollado por la empresa privada Northpointe Inc, según el cual el Sr. Loomis tenía un riesgo elevado de reincidencia y de cometer actos violentos. Con esta base, el juez impuso al Sr. Loomis una pena de 6 años de prisión. Dicha sentencia fue recurrida con el argumento de que se había vulnerado el derecho del Sr. Loomis a un proceso con todas las garantías porque no podía discutir los métodos utilizados por el programa informático Compas dado que el algoritmo era secreto. No obstante, el Tribunal Supremo del Estado de Wisconsin rechazó esta supuesta vulneración del derecho de los acusados al debido proceso por cuanto el programa informático se limitaba a integrar los criterios habituales que utilizan los jueces para valorar la peligrosidad criminal futura de un sujeto (antecedentes penales, comportamiento frente a los agentes policiales, […]) y los jueces mantenían su capacidad para entender su posible mal funcionamiento [Sentencia 13 de julio de 2016: State v. Loomis, 881, N.W.2d 749, 7532 (Wis, 2016). Sobre esta cuestión, vid. Romeo Casabona (2018, *in totum*).
A este respecto, la Comisión Europea para la Eficiencia de la Justicia (CEPEJ), dentro del Consejo de Europa, ha aprobado la Carta Ética Europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno (31 sesión plenaria, 3-4 diciembre 2018).

(26) A pesar de la posición del Alto Tribunal de Justicia -congruente con las pruebas aportadas en el proceso-, es cierto que esos sesgos discriminatorios de los sistemas de reconocimiento facial automático han sido puestos de manifiesto en otras instancias públicas. En esta línea, un memorándum del Comité de Supervisión y Reforma (*Committee on Oversight and Reform*) del Congreso de los Estados Unidos, de 20 de mayo de 2019, bajo el título "Tecnología de Reconocimiento Facial (parte 1): su impacto en nuestros derechos civiles y libertades", afirma lo siguiente: "On March 22, 2017, the Committee held a hearing to review federal law enforcement's uses and policies on facial recognition technology. The Committee found that 18 states have memoranda of understanding with the FBI to share their databases and that, as a result, more than half of American adults are part of facial recognition databases. *It also found that facial recognition technology misidentifies women and minorities and a much higher rate than white males, increasing the risk of racial and gender bias*". (la cursiva es nuestra) ("El 22 de marzo de 2017, el Comité celebró una audiencia para revisar los usos y políticas de las fuerzas del orden federales sobre la tecnología del reconocimiento facial. El Comité encontró que 18 Estados tienen memorandos de entendimiento con el FBI para compartir sus bases de datos y que, como resultado, más de la mitad de los adultos estadounidenses están incluidos en bases de datos de reconocimiento facial. *También encontró que la tecnología de reconocimiento facial identifica erróneamente a las mujeres y las minorías y a una tasa mucho más alta que a los hombres blancos, lo que aumenta el riesgo de sesgo racial y de género*") [traducción propia]. Debe tenerse en cuenta que el Comité de Supervisión y Reforma es el principal comité de investigación de la Cámara de Representantes de los Estados Unidos.

que extrae plantillas biométricas de las imágenes faciales que captura de las personas que están en la vía o espacios públicos y que en tiempo real compara dichas plantillas biométricas con las existentes en una lista de vigilancia supone una injerencia en la vida privada de esas personas que están en la vía pública, conforme a lo previsto en el artículo 8 del Convenio Europeo de Derechos Humanos. La sentencia razona acertadamente que la tecnología de reconocimiento facial automático extrae información e identificadores únicos sobre un individuo que permiten su identificación con precisión en una amplia gama de circunstancias. A partir de ahí, con una aplicación a nuestro juicio excesivamente literal de la jurisprudencia del Tribunal Europeo de Derechos Humanos, fundamenta la injerencia en la vida privada en la existencia de un almacenamiento de esos datos, aunque sea exclusivamente por el brevísimo lapso de tiempo estrictamente necesario para identificar la imagen facial, extraer la plantilla biométrica y compararla con las plantillas biométricas existentes en la lista de vigilancia.

A nuestro juicio, dicha argumentación es poco contundente y conviene insistir en que las plantillas biométricas de las imágenes faciales captadas, haya o no coincidencia con las de la lista de vigilancia, no se retienen y son eliminadas de manera inmediata y automática por el sistema. Consideramos que existen otros argumentos más sólidos para sustentar esa injerencia en la vida privada conectados con la expectativa razonable de privacidad, con el carácter de los datos que se obtienen y con el uso de esos datos y el resultado. Además, aunque no fue objeto de debate en la sentencia, esa injerencia en la vida privada se produce no sólo con respecto a las personas cuyas imágenes faciales son captadas y procesadas, sino también con respecto a aquellas personas que están en la lista de vigilancia, aunque esa información se haya extraído de una base de datos policial.

Segunda. La apreciación de esa injerencia en la vida privada no significa por sí sola una vulneración de dicho derecho fundamental, sino que, conforme a lo exigido en el art. 8 CEDH, habrá que analizar si existe habilitación legal para emplear esta tecnología y si la misma es suficiente. A este respecto, el reconocimiento facial no es un método policial que suponga una intrusión física o interferencia con los derechos de la persona sobre su vivienda o sobre su integridad corporal. Más aún, ni siquiera exige colaboración por parte de la persona afectada. Estos argumentos llevan a la sentencia comentada a concluir que no es necesaria una habilitación legal específica para que los cuerpos policiales puedan hacer uso de esta técnica, bastando los poderes de *common law* que tienen los agentes de policía en el Reino Unido. En el caso de España y Perú, ante la ausencia de habilitaciones legales específicas, la traslación de esta argumentación, que entendemos razonable, permitiría admitir las habilitaciones legales genéricas, aunque las mismas deberían ser completadas con otros documentos, fundamentalmente, normas de carácter reglamentario, aunque en la sentencia incluso se admiten protocolos policiales, que ofrezcan una protección adecuada contra la arbitrariedad y hagan previsible la actuación administrativa policial.

Tercera. El reconocimiento facial automático también podrá ser conforme con la exigencia de proporcionalidad siempre que se trate de identificar a concretas personas sobre las que exista razones fundadas para pensar que puedan estar en la zona afectada por el despliegue del operativo y sobre las que haya un interés policial fundado, y concurran otras circunstancias vinculadas con el evento o espacio público en el que se pretenda utilizar (por ejemplo, altercados anteriores). A este respecto, a la hora de realizar el juicio de proporcionalidad, debe tenerse en cuenta que la injerencia en el derecho a la vida privada de las personas cuyas imágenes faciales se captan es muy reducida y, en el otro lado de la balanza, que la mera videovigilancia por circuitos cerrados de televisión no permite la consecución del objetivo de localizar personas que son buscadas por las fuerzas policiales. En cualquier caso, el juicio de la proporcionalidad habrá de efectuarse en cada caso concreto, pero la utilización de esta tecnología no supone en sí misma una conculcación de esta exigencia.

Cuarta. Los datos biométricos que se obtienen de las personas cuyas imágenes faciales son captadas por el dispositivo policial son información sobre una persona física, singulares de esa persona y distintos de todos los de las demás. Por tanto, son datos personales sometidos a la legislación de la Unión Europea sobre datos de carácter personal y, en particular, a las disposiciones específicas contenidas en la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, 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. Más aún, dentro de esa Directiva, el tratamiento de estos datos debe cumplir con el régimen específico y más exigente establecido para los datos biométricos que permiten "identificar de manera unívoca a una persona física".

Quinta. La sentencia rechaza que la utilización de estos sistemas suponga una conculcación del principio de no discriminación al que están sometidas las actuaciones de los poderes públicos. Existe una posición bastante extendida que afirma que los sistemas de reconocimiento facial tienen sesgos discriminatorios y que ello depende del conjunto de datos utilizado por la empresa desarrolladora del software para "entrenar" el sistema. No es que estos sistemas incluyan algoritmos directamente discriminatorios, sino que su tasa de acierto es considerablemente menor en el caso de tratarse la imagen facial de una mujer de piel oscura frente a la imagen de un hombre de piel blanca. Este sesgo sería especialmente preocupante si el sistema de reconocimiento facial se utilizara en procedimientos automatizados de toma de decisiones, pero en los dispositivos policiales que nos ocupan la decisión última siempre corresponde a un agente policial con base a todos los datos y circunstancias concurrentes. Además, en el proceso judicial no se aportó prueba alguna de ese sesgo discriminatorio y el cuerpo policial ofreció estadísticas que probaban lo contrario.

Referencias bibliográficas

Amann v. Suiza, application no. 27798/1995. (Tribunal Europeo de Derechos Humanos, de 16 de febrero de 2000).

Bank Mellat v. Tesoro de Su Majestad (No. 2). (Corte Suprema [Reino Unido], 19 de junio de 2013).

Committee on Oversight and Reform (Congress of the United States. House of Representatives) (2019). Memorandum Hearing on "Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties". Recuperado de https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and

František Ryneš v. Úřad pro ochranu osobních údajů, C-212/13. (Tribunal de Justicia de la Unión Europea, de 11 de diciembre de 2014).

Leander v. Suecia, application Nº 9248/1981. (Tribunal Europeo de Derechos Humanos, 26 de marzo de 1987).

Peck c. Reino Unido, application Nº 44647/98. (Tribunal Europeo de Derechos Humanos, sentencia de 28 de enero de 2003).

Pérez de los Cobos Orihuel, Francisco (2018). *El derecho al respeto de la vida privada: los retos digitales. Una perspectiva de Derecho Comparado*. Bruselas, Servicio de Estudios del Parlamento Europeo.

Perry v. United Kingdom, application Nº 63737/00. (Tribunal Europeo de Derechos Humanos, 17 de julio de 2003).

P.G. y J.H. v. United Kingdom, application Nº 44787/98. (Tribunal Europeo de Derechos Humanos, 25 de setiembre de 2001).

R (Bridges) v. CCSWP y SSHD, CO/4085/2018. (High Court of Justice, Queen's bench Division, Divisional Court [EE.UU.], 04 de setiembre de 2019).

R (Unison) v Lord Chancellor. (Corte Suprema [Reino Unido], 26 de julio 2017).

Rebollo Puig, Manuel (2019). "La actividad administrativa de limitación". En *Derecho Administrativo. Tomo III: Modos y medios de la actividad administrativa*. Coord. López Benítez e Izquierdo Carrasco. Madrid, Tecnos.

Romeo Casabona, Carlos María (2018). "Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad". En *Revista de Derecho, Empresa y Sociedad*, 13, p. 39-55.

S. and Marper v. United Kingdom, applications Nº 30562/04 y 30566/04. (Tribunal Europeo de Derechos Humanos, 4 de diciembre de 2008).

State of Wisconsin v. Loomis, Nº 2015AP157-CR. (Supreme Court of Wisconsin [EE.UU], 13 de julio de 2016).