Revista de Derecho UNED, núm. 28, 2021

RECONOCIMIENTO FACIAL Y PROTECCIÓN DE DATOS: UNA RESPUESTA PROVISIONAL A UN PROBLEMA PENDIENTE

FACIAL RECOGNITION AND DATA PROTECTION: A PROVISIONAL ANSWER TO A PENDING ISSUE

Mario Santisteban Galarza

Investigador predoctoral UPV/EHU

Sumario: *I. Los riesgos del reconocimiento facial para el sistema de derechos y libertades. II. El reconocimiento facial: un tratamiento de una categoría especial de datos. II.1. Los sistemas de reconocimiento facial. II.2. Los sistemas de reconocimiento facial implican un tratamiento de datos biométricos. III. Las bases jurídicas para el tratamiento de datos que utilice técnicas de reconocimiento facial. III.1. Fuera del RGPD: el uso del reconocimiento facial para la prevención, investigación, detección o enjuiciamiento de infracciones penales. III.2. El consentimiento explícito del interesado. III.3. El interés público esencial. III.4. Una puerta abierta: El reconocimiento facial como medida para garantizar el cumplimiento de las obligaciones laborales. IV. Conclusiones.*

Resumen: *Las técnicas de reconocimiento facial se están expandiendo, y además de suponer importantes avances en la seguridad y la comodidad en el acceso a bienes y servicios, pueden poner en peligro derechos y libertades. Hasta el momento, a la espera de una regulación europea del uso de la Inteligencia Artificial, la normativa de protección de datos es el principal límite legal a la implementación de esta tecnología. El presente estudio pretende analizar las implicaciones que tiene el reconocimiento facial como un tratamiento biométrico de datos. En*

particular, trata de analizar los supuestos en los que el Reglamento General de Datos permite el uso de estas tecnologías, haciendo hincapié en las bases jurídicas que fundamentan el tratamiento de datos.

Abstract: Facial recognition technologies are expanding, and even though they could benefit law enforcement authorities and make the access to goods and services more comfortable, they might put at stake certain democratic freedoms. At the moment, the European data protection framework is the main legislation that can restrain the use of facial recognition. This paper aims to analyse the implications of facial recognition as a category of biometric data processing. Particularly, it attempts to clarify which legal basis of the European Data Protection Regulation could allow the use of these technologies.

Palabras clave: Reconocimiento facial, Protección de datos, Inteligencia Artificial.

Keywords: Facial recognition, Data Protection, Artificial Intelligence.

Recepción original:05-07-2021

Aceptación original:28-07-2021

I. LOS RIESGOS DEL RECONOCIMIENTO FACIAL PARA EL SISTEMA DE DERECHOS Y LIBERTADES

En junio de 2020 el medio estadounidense The New York Times reveló que la empresa Clearview posee una base de datos en las que se almacenan alrededor de tres billones de fotografías. Esa información, extraída de redes sociales como Twitter, Facebook o YouTube es utilizada por Clearview para su tecnología de reconocimiento facial. El funcionamiento de la aplicación es bastante sencillo desde la perspectiva del usuario: al introducir la imagen de una persona Clearview IA identifica las fotos públicas que asocia a ella, y los links a los dominios web de donde se extrayeron esas fotos. De esta forma, Clearview permite identificar a cualquier persona cuya imagen se encuentre almacenada en la base de datos de la aplicación[1].

[1] KASHMIR, H., "The Secretive Company That Might End Privacy as We Know It" *The New York Times*, 18 de junio 2020. Disponible en: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (última consulta 2 de julio de 2021).

Según los desarrolladores de aplicación, esta solo puede utilizarse por autoridades policiales con el objetivo de promover la seguridad pública, reducir el crimen y el fraude[2]. Actualmente, Clearview ha sido usada por el FBI, el US Department of Homeland Security y alrededor de 600 fuerzas policiales alrededor del mundo[3]. En Europa, la Autoridad Sueca de protección de datos ha constatado que Clearview ha sido utilizada con propósitos policiales en dicho país[4].

Que una pequeña *start-up* pueda implementar esta tecnología pone en evidencia lo extendida que se encuentra. En EE. UU., se ha utilizado el reconocimiento facial desde 2001, y para 2016, una cuarta parte de las casi dieciocho mil agencias en todo el país tuvieron acceso a un sistema de reconocimiento facial[5]. La respuesta normativa ha variado mucho entre los distintos de la federación[6], pasando de la prohibición absoluta, moratorias temporales en algunos Estados o a normativas que avalan su uso en determinadas condiciones[7]. Dentro de este espectro destaca la prohibición de su uso por las autoridades policiales en el Estado de California debido a sus implicaciones negativas para los derechos y libertades[8].

En Rusia el reconocimiento facial ha sido usado en las calles de Moscú para controlar el confinamiento, y también individuos calificados como peligrosos[9]. En China, desde 2018 el sistema *Dragon Fly* compara imágenes en vivo de los usuarios del metro con los archivos

---

[2] CLEARVIEW, "Clearview AI - Code of Conduct" https://staticfiles.clearview.ai/code_of_conduct.html

[3] "Twitter tells Clearview: stop taking our images", *Biometric Technology Today*, Volume 2020, Issue 2, February 2020, pág. 2.

[4] EDPB, "Swedish DPA: Police unlawfully used facial recognition app" EDPW news, 12 de Febrero de 2021. Disponible en: https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en (última consulta 11 de junio de 2021).

[5] SPIVACK J. and GARVIE, C, "Taxonomy of Legislative Approaches to Face Recognition in the United States, en *Regulating Biometrics: Global Approaches and Urgent Questions*, KAK, A. (ed.) 2020, pág. 82.

[6] Un ejemplo regulatorio es la BIPA (The Illinois Biometric Information Privacy Act) que si bien no veda el uso de estas tecnologías, supedita su uso por parte de entidades privadas al consentimiento informado del sujeto, prohibiendo comerciar o revelar su información biométrica. s

[7] SPIVACK J. and GARVIE, C, o.c, pág.83.

[8] Texto legislativo disponible en: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1215

[9] Véase, para entender las implicaciones éticas de esta tecnología ROUSSI, A., "Resisting the rise of facial recognition. Growing use of surveillance technology has prompted calls for bans and stricter regulation" *Nature*, Vol. 587, 2020, págs. 350-353.

policiales, propiciándose procesos de detención cuando el algoritmo identifica un positivo en el sistema[10].

La aplicación del reconocimiento facial también se ha sugerido en España, para vigilar exámenes online, y para el control de instalaciones por la seguridad privada. Recientemente la empresa Mercadona ha implementado un sistema de reconocimiento facial que pretende identificar aquellas personas que han cometido delitos de hurto en sus instalaciones[11]. Mientras se escriben estas líneas se espera una resolución de la AEPD (Agencia Española de Protección de Datos) que enjuicie este sistema, si bien determinadas decisiones judiciales ya han planteado dudas sobre su adecuación a la normativa de protección de datos[12].

La preocupación por los riesgos que implica el reconocimiento facial también se ha hecho eco en la propuesta de Reglamento Europeo para establecer reglas armonizadas en la regulación de la Inteligencia Artificial (en lo que sigue IA)[13]. La propuesta parte de los beneficios del uso de técnicas de IA para empresas y servicios, pero también de sus riesgos para los derechos de sus usuarios (Considerandos 4 y 5). En atención a dichos riesgos se diferencia entre sistemas que deben ser prohibidos tajantemente por atentar contra los valores de la Unión (artículo 5)[14], de aquellos que pueden ser

[10] ALDAMA Z.," Videovigilancia: China se queda con tu cara" *ELPASIS*, 27 de abril de 2018, Disponible en: https://elpais.com/retina/2018/04/25/tendencias/1524640135_207540.html (última consulta 2 de julio de 2021).

[11] RUBIO, I., "Las claves de la polémica por el uso de reconocimiento facial en los supermercados de Mercadona" *ELPAIS*, 7 de julio de 2020. Disponible online en: https://elpais.com/tecnologia/2020-07-06/las-claves-de-la-polemica-por-el-uso-de-reconocimiento-facial-en-los-supermercados-de-mercadona.html (última consulta 2 de julio de 2021).

[12] Véase el auto Auto 72/2021 de 15 Feb de la Audiencia Provincial de Barcelona, Sección 9ª, que deniega el uso del sistema de reconocimiento facial de la empresa Mercadona para garantizar el cumplimiento de la condena accesoria de prohibición de acceso a las instalaciones del supermercado. Disponible en: https://diariolaley.laleynext.es/content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbH1CjUwMDCzNDUwtzRVK0stKs7Mz7Mty0xPzStJBfEz0ypd8pNDKgtSbdMSc4pT1RKTivNzSktSQ4sybUOKSlMBe81L1EUAAAA=WKE (última consulta 2 de julio de 2021).

[13] EUROPEAN COMMISION, "Proposal for a Regulation laying down harmonised rules on artificial intelligence" de 26 de abril de 2021. Documento disponible en: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence (última consulta 2 de julio de 2021).

[14] Entre estos se encuentran aquellos sistemas que utilizan técnicas subliminales para distorsionar el comportamiento de personas con efectos dañinos; sistemas de calificación social utilizados por el poder público con efectos perjudiciales

admitidos, siempre que observen determinadas garantías en función de su grado de peligrosidad.

La propuesta no se refiere al reconocimiento facial en específico, pero el mismo queda integrado dentro de las tecnologías biométricas de identificación remota[15]. En un principio, estas tecnologías se incardinan dentro de este primer grupo de usos de la IA que se encuentran prohibidos. No obstante, esta prohibición abarca únicamente aquellos sistemas de identificación a tiempo en real, en espacios públicos y con propósitos de aplicación de la ley penal (artículo 5.1 d)).

Como prematuramente apuntó el EDPS (European Data Protection Supervisor), si bien la propuesta es un paso adelante, quedan fuera de la "lista negra" muchos sistemas de reconocimiento biométrico que merecerían idéntico tratamiento[16]. Por ejemplo, el caso de Clearview no entraría dentro de esta prohibición en la medida en que el reconocimiento facial no opera a tiempo real. Tampoco las propuestas de muchos actores privados que ya están utilizando esta tecnología y que pueden tener consecuencias igual de dañinas para los derechos y libertades[17].

Asimismo, la propuesta ofrece la posibilidad a los Estados Miembros de levantar esta prohibición, ya de por sí escueta. Esto será posible cuando el reconocimiento biométrico se utilice para cumplir determinados objetivos de interés público y se observen determinadas garantías. Ateniendo a la flexibilidad de la propuesta, el EDPB y el EDPS emitieron una opinión conjunta que abogaba por una prohibición más amplia del uso de tecnologías de identificación biométrica en el espacio público. Concretamente, ambas autoridades apuestan por una prohibición general del uso de tecnologías

---

y sistemas de reconocimiento biométrico a tiempo real y por las autoridades públicos con las precisiones que se hacen notar en el cuerpo del trabajo.

[15] La propuesta define estos sistemas como "AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used" (considerando 89).

[16] EDPS, "Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary" EPDS News, 23 de abril de 2021, Disponible en: https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en (última consulta 2 de julio de 2021).

[17] Por ejemplo, el club deportivo Brøndby IF, que utiliza técnicas de reconocimiento facial a tiempo real en su estadio para identificar a personas que han sido sancionadas e inhabilitadas para asistir a partidos del equipo.

biométricas que automáticamente capten datos sensibles (no solo el rostro, sino también la voz, el ADN, o huellas dactilares) en el espacio público y "a gran escala"[18].

El reconocimiento facial puede ofrecernos avances en comodidad y en seguridad. Como señala el Libro Blanco de IA de la Comisión Europea, la inteligencia artificial aumentará la seguridad de los europeos y "nos aportará otros muchos cambios que de momento solo podemos intuir"[19]. Nos permite acceder a servicios y a instalaciones con rapidez, evitando costosos controles. Asimismo, puede ayudar a las autoridades policiales y judiciales en su misión de garantizar cumplimiento de la ley y en la detección del delito. No obstante, también implica riesgos considerables que una sociedad democrática debe de mitigar.

El primero de ellos es la existencia de una tasa de error, de falsos positivos o falsos negativos. En el caso de sistemas que se basan en el reconocimiento de imágenes en vivo, en lugares que son visitados por millones de personas, una tasa de error muy reducida puede suponer la identificación incorrecta de cientos de personas[20]. Es conocido que estas tasas de error son más elevadas en mujeres u afroamericanos[21]. Esto se explica por los datos utilizados en el proceso de entrenamiento de la IA, en los que frecuentemente estos colectivos

[18] El EDPB y el EDPS han señalado en concreto "the EDPB and the EDPS call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioral signals - in any context. The current approach of the Proposal is to identify and list all AI systems that should be prohibited. Thus, for consistency reasons, AI systems for large-scale remote identification in online spaces should be prohibited under Article 5 of the Proposal. Taking into account the LED, the EUDPR and GDPR, the EDPS and EDPB cannot discern how this type of practice would be able to meet the necessity and proportionality requirements, and that ultimately derives from what are considered acceptable interferences of fundamental rights by the CJEU and ECtHR". EDPB-EDPS, "Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)" 18 de junio de 2021. apdos 30-32.

[19] COMISIÓN EUROPEA "Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza" adoptado el 19 de febrero de 2020, pág. 3.

[20] FRA FOCUS, "Facial recognition technology: fundamental rights considerations in the context of law enforcement" adoptado el 21 de noviembre de 2019. pág. 7. Disponible online en: https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law (última consulta 2 de julio de 2021).

[21] RUBIO I., "Reconocimiento facial: la tecnología que lo sabe todo" *ELPAÍS*, 25 de mayo de 2019. Disponible en: https://elpais.com/tecnologia/2019/05/21/actualidad/1558455279_966010.html (última consulta 2 de julio de 2021).

se encuentran infrarrepresentados. No obstante, que los algoritmos de reconocimiento facial presenten sesgos es una cuestión que el desarrollo técnico puede paliar: el verdadero problema es que esta tecnología sea precisa[22].

Distintos autores e instituciones nos han alertado que naturalizar estos sistemas podría implicar normalizar la vigilancia masiva de la población. Por ejemplo, SELINGER y HARTZOG escriben "Biometric surveillance powered by artificial intelligence is categorically different than any surveillance we have seen before. It enables real-time location tracking and behaviour policing of an entire population at a previously impossible scale. The technology can be used to create chill that routinely prevents citizens from engaging in First Amendment protected activities, such as free association and free expression"[23].

El derecho a la privacidad constituye un presupuesto de otros derechos, como la libertad de expresión. Este razonamiento parte de la necesidad de garantizar cierto anonimato en el espacio público, pues ya sea físico o digital, es un lugar en el que muchas personas ejercen libertades individuales con una enorme trascendencia para el sistema democrático[24]. Al permitir identificar a dichas personas y seguir sus movimientos se corre el riesgo de que no se sientan libres a la hora de expresar sus ideas y que en último término se produzca un efecto desaliento (*chilling effect*).

Un razonamiento similar es el seguido por el TJUE (Tribunal de Justicia de la Unión Europea) en el asunto *Digital Rights*, en el que se estudió la adecuación con el derecho a la protección de datos y la libertad de expresión el sistema de conservación de datos que imponía la Directiva 2006/24. El Alto Tribunal apuntó que "la circunstancia de que la conservación de los datos y su posterior utilización se efectúen sin que el abonado o el usuario registrado hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante"[25], pudiendo tener implicaciones negativas para el ejercicio de la libertad de expresión de los individuos.

---

[22] SELINGER E., HARTZOG W., "The inconsentability of facial surveillance", *Loyola Law Review*, Vol. 66, 2020, pág.110.

[23] Ibídem pág. 111.

[24] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS "Reconnaissance faciale pour un debat à la hauteur des enjeux" 15 de noviembre de 2019. Disponible online en: https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

[25] SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala) de 8 de abril de 2014 asuntos acumulados C-293/12 y C-594/12, Apdos 34-37.

Finalmente, el uso de esta tecnología supone un tratamiento de datos especialmente sensibles como es el rostro de una persona. Ello puede llevar a revelar otros datos como la etnia, o el estado de salud. Asimismo, el reconocimiento facial puede ser utilizado para inferir el estado anímico de una persona con fines publicitarios, si bien con resultados de dudosa exactitud[26].

Hasta el momento que se apruebe el Reglamento de IA Europeo, son el Reglamento General de Protección de Datos (RGPD) y en el caso español la Ley Orgánica de Protección de Datos Personales y Darantía de los Derechos Digitales (LOPDGDD) las normativas que pueden protegernos de usos dañinos de esta tecnología. Así, en interpretación de estas normativas y las directrices del EDPB y el Tribunal Constitucional, la Agencia Española de Protección de Datos ha puesto serios obstáculos para que estas tecnologías se extiendan en nuestro país.

II. EL RECONOCIMIENTO FACIAL: UN TRATAMIENTO DE UNA CATEGORÍA ESPECIAL DE DATOS.

II.1. Los sistemas de reconocimiento facial

Al igual que el resto de las técnicas de identificación biométricas, el reconocimiento facial se basa en una comparación de plantillas biométricas. Las plantillas biométricas, tal como las define el Grupo de Trabajo del art 29[27], son características claves de los datos biométricos puros que permiten identificar al interesado sin necesidad de acudir a la fuente de la que se extraen. En el caso del reconocimiento facial nos referiremos a determinadas particularidades de nuestro rostro; la ubicación de los ojos, o las cejas, cuyo análisis conjunto permiten identificar a una persona.

Para que pueda operar esta identificación, la información gráfica, resumida en una plantilla biométrica, debe ser recogida en dos momentos. Un primero, conocido como fase de registro, en el que el sistema almacena la plantilla para una identificación posterior. Pensemos en el rostro de una persona, cuya identidad es desconocida, pero sospechosa de haber cometidos actos delictivos y cuya imagen

[26] Véase ALMONACID DÍAZ, C., "Consideraciones teóricas y éticas del reconocimiento facial de las emociones en contexto de pandemia", *VERITAS*, Núm. 46, 2020, págs. 55-75.

[27] GRUPO DE TRABAJO DEL ARTÍCULO 29, "Dictamen 3/2012 sobre la evolución de las tecnologías biométricas" pág. 5.

ha sido captada por la policía y almacenada en una base de datos. Posteriormente se dará una segunda captación de la imagen de esa persona que se compara con la plantilla inicial; el sospechoso es fotografiado en la multitud de una ciudad e identificado por el sistema de reconocimiento facial.

Los algoritmos de reconocimiento facial, en función de las coincidencias entre las plantillas examinadas, establecen un porcentaje de similitud entre ambas plantillas. Superado un determinado umbral el sistema notifica un caso positivo, esto es, una alta probabilidad de que las plantillas pertenezcan a un mismo sujeto. En caso contrario el sistema notifica un negativo. De ello podemos inferir, que las técnicas de reconocimiento facial suponen un tratamiento de datos personales. Esto es así pues la comparación entre plantillas biométricas requiere captar, al menos en dos momentos distintos, la imagen del rostro de una persona, información sobre una persona física identificable.

En función del lugar dónde se almacenan las plantillas podemos distinguir dos sistemas biométricos: sistemas de autentificación o verificación y sistemas de identificación. La autentificación implica un sistema de comparación uno a uno, en el que se capta el rostro del interesado y se compara con una única plantilla biométrica, generalmente ubicada en un dispositivo que porta el propio interesado. Piénsese un sistema de fichaje en el centro de trabajo, en el que el sujeto pasa una tarjeta por un lector y la tecnología de reconocimiento facial compara una imagen tomada en tiempo real con la información biométrica previamente almacenada en la tarjeta. Los sistemas de identificación, por el contrario, comparan el rostro del interesado con una base de datos en la que se almacenan plantillas biométricas de un conjunto de personas.

Los sistemas de autenticación se consideran por norma general mucho menos invasivos en la privacidad[28]. Uno de sus aspectos más positivos es que pueden impedir fácilmente el tratamiento de datos biométricos de terceras personas. El tratamiento se adscribe a la persona que ha introducido la tarjeta donde se almacena la plantilla biométrica, en comparación a un sistema de identificación basado en un circuito cerrado de televisión, en la que se captan y

[28] En el mencionado libro blanco sobre Inteligencia artificial la Comisión hace una distinción entre la peligrosidad de ambas tecnologías "El uso de aplicaciones de IA para la identificación biométrica remota y otras tecnologías de vigilancia intrusiva deben considerarse siempre de riesgo elevado", diferenciándolas de la autenticación biométrica, pág. 22.

tratan los datos de todos los rostros que se muestran ante las cámaras. Por otra parte, desde el punto de vista de la seguridad, sistemas que combinan biometría y tarjetas inteligentes (*mach on card*) se consideran más fiables[29] pues proporcionan una autenticación de doble factor (algo que tienes y algo que eres)[30].

En cambio, los sistemas de identificación solo pueden operar con una base centralizada de datos pues "con objeto de averiguar la identidad del interesado, el sistema debe comparar sus plantillas o datos brutos (imagen) con las plantillas o datos brutos de todas las personas cuyos datos ya están almacenados de forma centralizada"[31]. El almacenamiento de los datos de las plantillas en el sistema centralizado presenta riesgos: el uso indebido de los datos para una finalidad incompatible y/o el acceso indebido a la información. Muchos tratamientos basados en el reconocimiento facial, piénsese en un sistema de videovigilancia, pueden tratar datos terceros sin su consentimiento, o sin que tan siquiera sean conocedores de que su imagen está siendo capturada para ser utilizada por un sistema de reconocimiento facial.

Para evitar el acceso no autorizado de esos datos a terceros, los sistemas de reconocimiento facial que se aplican a numerosos individuos en tiempo real suelen eliminan rápidamente los datos tratados, una vez que se ha constatado que la plantilla del sujeto no concuerda con la plantilla almacenada en la base de datos. Ese es el caso AFR Locate, un sistema de reconocimiento facial utilizado por la policía de Gales del Sur y que fue enjuiciado por el Alto Tribunal de Justicia de Inglaterra y Gales[32]. AFR Locate no retiene la información de las personas cuyas caras han sido escaneadas, que es

[29] Como recuerda la AEPD en su documento de 14 equívocos de la biometría "Por definición, un sistema de autenticación fuerte es aquel que exige que se proporcione, al menos, dos de los siguientes: algo que se sabe, algo que se tiene o algo que se es (biometría). Por definición, sólo utilizar biometría es un proceso de autenticación débil, mientras que utilizar una tarjeta de acceso y contraseña es fuerte. Aunque la autenticación biométrica muchas veces exige un proceso previo de registro o identificación en el que, por ejemplo, en reconocimiento facial, hay que comparar con la foto en el DNI, si, después del proceso de identificación, el proceso de autenticación sólo es biométrico, sigue siendo un sistema débil".

[30] INSTITUTO NACIONAL DE CIBERSEGURIDAD "Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario", publicado el 21 de septiembre de 2016, pág. 15.

[31] GRUPO DE TRABAJO DEL ARTÍCULO 29 "Documento de trabajo sobre biometría", Adoptado el 1 de agosto de 2003, pág. 5.

[32] Para un interesantísimo estudio de la sentencia Véase CARRASCO IZQUIERDO, M. "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", *Ius Et Veritas*, Núm. 60, 2020, pp. 86-103

inmediatamente eliminada, salvo en el supuesto que identifique un positivo. De esta forma los datos biométricos de terceros no están al alcance de quien opera el sistema ni de la policía[33].

No obstante, como el Tribunal de Gales hizo notar, el hecho de que la información personal se capte durante un brevísimo periodo de tiempo no impide que exista también un tratamiento de datos de los terceros no sospechosos[34]. Esto es lógico desde el punto de vista de las garantías que ofrece el derecho a la protección de datos, que otorga el "derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención" (STC 292/2000 FJ 5). Un tratamiento de datos, aunque sea breve en el tiempo supone un poder del responsable frente al interesado. Impedir la fiscalización de ese poder, por ejemplo, constatar si el tratamiento se ha basado en una base legítima, vaciaría el contenido del derecho a la protección de datos.

La rápida eliminación de los datos cumple las exigencias del principio de limitación de la conservación de datos, que implica que los datos deban ser "mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales" (art. 5.1 e) RGPD. A pesar de ello ha existido un tratamiento de datos, y dicha recogida de datos debe haber operado con fines determinados, explícitos y legítimos.

II.2. Los sistemas de reconocimiento facial implican un tratamiento de datos biométricos

El mencionado poder de control que se pone en manos del interesado debe acentuarse en el caso del reconocimiento facial, pues estas técnicas implican un tratamiento de datos biométricos. El RGPD define los datos biométricos como aquellos "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" (art 4. 14).

[33] Sentencia del Alto Tribunal de Justicia de Inglaterra y Gales de 4 de septiembre de 2019. Apdo 17.

[34] Ibídem, Apdo 133.

Por tanto, para atender si estamos ante un dato biométrico debemos tener en cuenta tres factores: La naturaleza de los datos (datos relativos a las características físicas, fisiológicas o conductuales de una persona física); los medios y las formas de tratamiento (datos obtenidos a partir de un tratamiento técnico específico) y la finalidad del tratamiento (los datos se deben utilizar para la finalidad de identificar de manera unívoca a una persona física)[35].

Bajo el régimen de la Directiva 95/46/CE los datos biométricos no se consideraban categorías sensibles de datos por norma general. Eso solo ocurría cuando dicho tratamiento revelaba datos sensibles que la Directiva enumeraba "el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad" (art. 8.1). Así, como señaló el Grupo del artículo 29 en su mencionado informe del año 2003 sobre biometría "Si un tratamiento contiene datos sensibles es una cuestión de apreciación vinculada con la característica biométrica específica utilizada y la aplicación biométrica en sí".

Los datos biométricos pueden revelar información muy sensible de la vida de una persona. En el caso de la huella dactilar, se ha demostrado que de ella se puede inferir el consumo de drogas o medicamentos[36]. Dependiendo del concreto sistema biométrico que se utilice, no siempre existe riesgo de que dichos datos puedan ser revelados de los datos brutos, pero es de agradecer que el RGPD haya extendido el concepto de datos sensibles (ahora categorías especiales de datos) a los datos biométricos, siempre que estén "dirigidos a identificar de manera unívoca a una persona física" (art. 9.1).

Ahora bien, como hemos señalado más arriba un tratamiento biométrico requiere el uso de un medio técnico dirigido a la identificación de la persona. En este sentido el EDPB ha señalado recientemente que "Para considerarse datos biométricos en el sentido del RGPD, el tratamiento de datos sin procesar, como las características físicas, fisiológicas o conductuales de una persona física deben implicar una medición de dichas características"[37].

---

[35] EDPB "Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo" adoptado el 29 de enero de 2020, págs. 19-20.

[36] BAILEY, M. "The hidden data in your fingerprints" *The Coversation US*, 27 de abril de 2018. https://www.scientificamerican.com/article/the-hidden-data-in-your-fingerprints/

[37] EDPB "Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de video" adoptado el 20 de enero de 2020, apdo. 74.

La AEPD ha sugerido, basándose en esa distinción señalada por el Grupo del art. 29 que, "puede interpretarse que, de acuerdo con el artículo 4 del RGPD, el concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación/autenticación. Sin embargo, y con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno—a varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno)"[38].

Desde mi punto de vista esta distinción no se sostiene. Piénsese en un sistema de reconocimiento facial instalado en el hogar, que permite el acceso a la vivienda, o a una de sus partes mediante la comparación del rostro del individuo con una plantilla biométrica que él porta en una tarjeta. El objetivo del sistema sigue siendo identificar unívocamente al propietario de la vivienda, y utilizará medios técnicos para ello. Cosa distinta es que este tratamiento sea especialmente seguro al utilizarse un sistema descentralizado. Incluso podría argumentarse, dependiendo de sus características, que estos sistemas se benefician de la exención doméstica del art. 2.2 del RGPD, en la medida en que únicamente tratan datos en un contexto doméstico y terceras personas no se verán afectadas.

A mi juicio, el requisito de que se utilicen medios técnicos persigue impedir que el almacenamiento del dato bruto, una fotografía o un video, implique *per se* un tratamiento de una categoría especial de datos. Así lo aclara el Considerando 51 del RGPD "El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física".

Este criterio, acertado para no elevar la dificultad de justificar tratamientos que entrañan menor grado de peligro para las libertades individuales, presentan un gran problema desde el punto de vista del reconocimiento facial. Una vez almacenadas las fotografías o videos, el responsable ya dispone de los datos brutos sobre los que utilizar sus tecnologías de reconocimiento facial. En el momento de la creación de la plantilla existirá un nuevo tratamiento datos, que en este caso sí se considerará como un tratamiento de una categoría especial de datos (art 9.2 RGPD). No obstante, para entonces el

[38] AEPD, "Informe de Gabinete Jurídico N/Ref: 0036/2020" pág. 19.

sujeto ya ha perdido la oportunidad real de fiscalizar dicho tratamiento en la medida en que desconoce que puede haber operado. Como señala el FRA FOCUS, "Facial images are also easy to capture: in contrast to other biometric identifiers, such as fingerprints or DNA, a person is typically unable to avoid having their facial image captured and monitored in public".[39]

La confidencialidad de los datos es un principio fundamental en el RGPD, que comprende "la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiada" (art. 5.1 f)). El grupo de Trabajo del art 29 identificó tres riesgos fundamentales que implicaban las tecnologías biométricas: La suplantación, la violación de los datos y la desviación de la finalidad. A mí parecer actualmente es la desviación de la finalidad, es decir, que la información biométrica sea utilizada para un propósito incompatible con el original, el principal riesgo que presenta el reconocimiento facial.

La información biométrica es fácil de capturar una vez que se dispone de información gráfica del sujeto y el software correspondiente. Piénsese en el caso de Clearview, en el que una modesta compañía ha creado plantillas biométricas de millones de personas adquiriéndolos de la internet abierta. Nuestra información biométrica ya se encuentra al alcance de muchas personas; impedir brechas de seguridad seguramente facilite que nuestros datos no sean utilizados por terceros con propósitos ilícitos, pero si Clearview ha conseguido obtener esa información de la Internet abierta nada impide que otra empresa esté haciendo lo mismo. De ahí que, a la hora de enfrentarnos a la regulación del reconocimiento facial, lo relevante sea determinar en qué supuestos dicha información puede ser utilizada, especialmente cuando puede serlo en nuestra contra.

III. LAS BASES JURÍDICAS PARA EL TRATAMIENTO DE DATOS QUE UTILICE TÉCNICAS DE RECONOCIMIENTO FACIAL

Ya hemos señalado que el reconocimiento facial implica un tratamiento de una categoría especial de datos. Ello tiene varias consecuencias, por ejemplo, que antes de realizar un tratamiento de datos que utilice esta tecnología sea necesario realizar una evaluación

[39] FRA Focus, "Facial recognition technology: fundamental rights considerations in the context of law enforcement" adoptado el 29 de noviembre de 2021, p. 5.

de impacto[40]. Así lo ha señalado la AEPD, respecto al tratamiento de categorías especiales de datos, tal como preceptúa el art. 35.4 del RGPD[41]. No obstante, la principal característica que presentan las categorías especiales de datos es que, para ser tratados, requieren una base jurídica adicional a las previstas en el art. 6 del RGPD.

El artículo 9.1 establece un principio general de prohibición, señalando "Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física". Esa prohibición general puede ser levantada si se da alguna de las condiciones a las que se refiere el apartado segundo de este precepto. Acto seguido nos centraremos en el estudio de estas condiciones, concretamente en las letras a), b) y g), que son las que ofrecen mayor posibilidad de ser aplicados o más dudas, como el caso del consentimiento. No obstante, antes de centrarnos en cada una de estas bases merece la pena hacer alguna precisión entorno al tratamiento de datos biométricos con la finalidad de prevenir o detectar infracciones penales.

III.1. Fuera del RGPD: el uso del reconocimiento facial para la prevención, investigación, detección o enjuiciamiento de infracciones penales

No toda técnica de reconocimiento facial está necesariamente sujeta al RGPD. Cuando esta se utilice "por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales", habrá que atender a las disposiciones de la Directiva 2016/680 del Parlamento europeo y del Consejo de 27 de abril

[40] El art. 35.1 del RGPD señala que "Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares".

[41] AEPD "listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4)" documento disponible en: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf (última consulta 2 de julio de 2021).

de 2016 (art. 2.2 d RGPD)). Respecto a su ámbito de aplicación, esta normativa es aplicable tanto a las personas investigadas, como a los terceros cuyos rostros son captados por el sistema, en la media en que el ámbito de aplicación de la Directiva depende de la finalidad del tratamiento (la detección y prevención de infracciones penales) y no de la cualidad de los interesados implicados. Eso no quiere decir, que dicho ámbito de aplicación deba extenderse indebidamente. Por ejemplo, la AEPD ha entendido que la Directiva no desplaza al RGPD cuando el responsable de tratamiento de datos es una entidad privada como empresas de seguridad, o detectives privados[42].

Dicho instrumento normativo estable una regulación específica para las categorías especiales de datos, entre las que también se encuentran los datos biométricos. Su artículo 10 establece que su tratamiento solo será procedente cuando sea estrictamente necesario, "con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado" y siempre que así lo autorice el Derecho de la Unión o del Estado miembro; sea necesario para proteger los intereses vitales del interesado o de otra persona física, o dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos. Por lo tanto, para autorizar el tratamiento de datos biométricos en el ámbito de la detección del delito es necesario la concurrencia de cualquiera de los mencionados tres requisitos y que el tratamiento de datos se sujete a los principios generales de protección de datos que inspiran la Directiva 2016/680 y el RGPD.

La reciente Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales se ha ocupado de la trasposición de dicha normativa europea en España. Su artículo 13, tras reproducir íntegramente lo dispuesto en la Directiva Europea, preceptúa que "Las autoridades competentes, en el marco de sus respectivas funciones y competencias, podrán tratar datos biométricos dirigidos a identificar de manera unívoca a una persona física con los fines de prevención, investigación, detección de infracciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública". De esta forma, se cumple con uno de los tres requisitos alternativos previstos para permitir dicho tratamiento biométrico de

[42] AEPD, "Informe sobre el uso de sistemas de reconocimiento facial por parte de las empresas de seguridad privada". N/REF: 010308/2019 pág. 10. Disponible online en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/AEPD-informe-sistemas-reconocimiento-facial-empresas-seguridad-privada

de datos, tanto en la Directiva como en la propia Ley Orgánica, "que así lo autorice el Derecho de la Unión o del Estado miembro".

Teniendo en cuenta lo anterior, las autoridades policiales podrían hacer uso de sistemas de reconocimiento facial siempre que observen las salvaguardas establecidas en el resto de la Ley Orgánica. Al tratarse de tratamiento de datos que se valgan de nuevas tecnologías y que podemos presuponer que impliquen "un alto riesgo para los derechos y libertades de las personas físicas", el responsable del tratamiento deberá realizar con carácter previo una evaluación de impacto del sistema que deberá de incluir una evaluación de riesgos para los derechos y libertades de los interesados (art 35.1 y 2 de la LO). Por otra parte, atendiendo a los peligros expuestos, es probable que estos sistemas deban de someterse a la consulta previa de la AEPD antes de ser implementados (art 36.1).

Dicho esto, no quedan despejadas las dudas sobre la posible legalidad de un sistema de reconocimiento facial para usos de detección o prevención de infracciones penales. La mencionada Ley Orgánica se refiere a tecnologías biométricas, pero no especifica cuáles, ni sus características. Serán justamente estas especificidades técnicas del sistema y su uso (si el reconocimiento opera a tiempo real o en diferido, su ámbito geográfico o temporal) las que determinen la legalidad del sistema desde la perspectiva de la proporcionalidad y necesidad del tratamiento de datos (art. 4. c) Directiva 2016/680 del Parlamento Europeo Y del Consejo de 27 de abril de 2016).

El EDPB en contestación a las preocupaciones de varios Parlamentarios europeos por el caso de Clearview, no se cerró tajantemente al uso de técnicas de reconocimiento facial por parte de las autoridades policiales. Concretamente ha señalado "EU law enforcement authorities may under certain circumstances process certain biometric data, including biometric templates from photos and check these against biometric templates in databases that are under the control of the official authorities and that have been established under Union or Member State law"[43]. Por tanto, en este comunicado "informal" no se opuso a un sistema de reconocimiento facial que operara en diferido y basado en datos policiales. No obstante, dudó de la legalidad del uso policial de una base de datos privada como Clearview IA por parte de estas autoridades. En la misma línea la autoridad sueca de protección de datos también consideró que utilizar Clearview IA exigía una especial justificación de la necesidad

[43] EDPB, OUT 2020-0052, 10 de junio de 2020. Disponible en: https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf

de la medida, y que en todo caso requería de una evaluación de impacto previa para su uso, multando a la autoridad policial que hizo uso de Clearview por desoír tales garantías[44].

Desde mi punto de vista es discutible la proporcionalidad de sistemas de reconocimiento facial que trabajen con grandes bases de datos, y que contengan información de personas del todo ajenas a la investigación criminal. Tal como ha señalado el TJUE, para apreciar la necesidad de una medida limitativa del derecho fundamental a la protección de datos ha tenido en cuenta el ámbito de aplicación de esta en relación con los fines perseguidos. Así, en el ya citado caso *Digital Rights* declaró la no conformidad con el derecho fundamental a la protección de datos un sistema como el impuesto por la Directiva 2006/24 que afecte a la conservación de los datos referidos "a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves"[45]. Idéntico planteamiento podría extrapolarse a un sistema de reconocimiento facial, ya opere en tiempo real o en diferido, que resulte por su ámbito de aplicación temporal, espacial o personal desproporcionado con los fines perseguidos.

III.2. El consentimiento explícito del interesado

De vuelta al RGPD, el primer supuesto al que se refiere el art. 9.2 para levantar la prohibición de procesamiento de categorías especiales de datos es el consentimiento explícito del interesado. El precepto matiza que esto no será posible "cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado".

A este respecto debe de recordarse que en nuestro ordenamiento jurídico "el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico" (art. 9.1 de la LOPDGDD). Los datos biométricos no se encuentran dentro de dicho listado, por lo que, en un principio, el consentimiento explícito del interesado puede ser base para el tratamiento de dichos datos. Dicho eso,

[44] Resolución en sueco disponible en: https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-polismyndigheten-cvai.pdf (última consulta 11 de junio de 2021).

[45] SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala) de 8 de abril de 2014 asuntos acumulados C-293/12 y C-594/12 apdo 57.

hay que tener en cuenta que el reconocimiento facial puede permitir identificar la raza de una persona, y seguramente aquellos sistemas que tratan de inferir las emociones puedan también descubrir otros datos históricamente considerados como sensibles. De esta forma, dependiendo de las características del sistema y sus usos podrá concluirse que se están tratando otros datos sensibles que el interesado con su consentimiento no puede autorizar.

El consentimiento es definido por el RGPD como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen" (art. 4. 11)). Por tanto, una nota esencial para que el consentimiento sea válido como base de legitimación es que este sea libre. El EDPB señala al respecto "According to the EDPB this means that consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences"[46]. Desde este punto de vista, el consentimiento solo es posible cuando se ofrece una alternativa al interesado, una opción real que no implique un tratamiento tan invasivo de sus datos

Piénsese en una compañía aérea que ofrece a sus clientes un sistema de reconocimiento facial para verificar su identidad antes de subir al avión. Dicho sistema sería valido siempre que se ofreciera al consumidor la opción de optar por otra técnica de identificación que no fuera menos gravosa. De esta forma, sería necesario compaginar el reconocimiento facial con la identificación realizada manualmente por el personal de la compañía, sin que este segundo tipo de identificación pueda suponer mayores costes para el consumidor.

Puede entreverse rápidamente que la oferta de esta opción, preceptiva bajo el RGPD, limitaría en la práctica el uso comercial del reconocimiento facial. Su uso es beneficioso para los clientes pues pueden resultar más cómodas, al eliminar trámites en el acceso a determinados servicios o instalaciones. En el caso de las compañías el beneficio puede consistir en automatizar tareas llevadas antes por el personal y por tanto en la reducción del coste. Mantener un doble sistema de reconocimiento, automático y otro manual reduciría notablemente los incentivos económicos que hay detrás de la implementación de esta tecnología.

[46] The European Data Protection Board "Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1", 4 de mayo de 2020, P. 9.

A dicho impedimento práctico hay que sumarle el hecho de que para que el consentimiento deba considerarse otorgado en libertad no puede existir una relación de subordinación o dependencia entre interesado y responsable. El Considerando 43 del RGPD aclara al respecto que "Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular".

Esta situación de desbalance de poder también se da entre empleado y empresario, en la medida en que el empleado puede temer una represalia en caso de que se niegue al tratamiento de sus datos[47]. Asimismo, se ha dudado de que el consentimiento pueda servir como base legítima en un contexto de ayuda humanitaria, en el que la situación de desamparo del interesado no le permite ejercer una verdadera opción para consentir el uso de sus datos[48]. Todo ello hace que el número de supuestos prácticos en el que el consentimiento pueda servir como base para el tratamiento de datos que venimos analizando se reduzca considerablemente.

III.3. El interés público esencial

La AEPD ha conocido sobre la legalidad del uso de tecnologías de reconocimiento facial en dos supuestos. El primero de ellos ha sido en el ámbito educativo, en el que se barajaba su uso para controlar exámenes online. Siguiendo los criterios asentados, la AEPD también se ha pronunciado sobre su implementación por parte de una empresa de seguridad privada, que preguntaba por "la licitud de la incorporación de sistemas de reconocimiento facial en los servicios de videovigilancia al amparo del artículo 42 de la Ley de Seguridad Privada"[49].

[47] Ibídem, pág. 9.

[48] Véase BEN HAYES B., MARELLI M., "Reflecting on the International Committee of the Red Cross's Biometric Policy: Minimizing Centralized Databases" en *Regulating Biometrics,* págs. 70-77, 2020.

[49] AEPD, "Informe Gabinete jurídico 010308/2019", pág. 1. Disponible en: https://www.aepd.es/es/documento/2019-0031.pdf

Ambos supuestos han sido enjuiciados bajo la óptica del art. 9.2 g) del RGPD. Este precepto legitima el tratamiento de categorías especiales de datos cuando sea necesario "por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

La LOPDGDD añade que "Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad". Por tanto, para que sea de aplicación esta base jurídica deben de darse tres requisitos: el tratamiento debe estar amparado en un interés público esencial; previsto en una norma con rango de ley, que además debe de ofrecer garantías suficientes y por último debe superar el test de proporcionalidad[50].

Respecto al primero de los requisitos, el interés público esencial, dicho nota de esencialidad, da una nueva dimensión al problema. Como apunta la AEPD "tratándose de categorías especiales de datos, el supuesto contemplado en la letra g) del artículo 9.2. no se refiere solo a la existencia de un interés público, tal y como hace en muchos otros de sus preceptos el RGPD, sino que es el único precepto del RGPD que requiere que el mismo sea "esencial", adjetivo que viene a cualificar dicho interés público, habida cuenta de la importancia y necesidad de mayor protección de los datos tratados"[51].

A pesar de ello, la AEPD, tanto el Tribunal Constitucional han apostado por la concreción de tal interés más que por su "cualidad". Ambos citan en sus resoluciones la STC 292/2000, que versaba sobre la constitucionalidad de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En ella se hacía hincapié que era el legislador quién debía de concretar los límites al derecho de protección de datos y la finalidad que persigue esa restricción. El TC, apoyándose en la misma demanda de concreción ha señalado en su STC 79/2019 que "Es suficiente con constatar que, al no poderse identificar con la suficiente precisión la finalidad del tratamiento de datos, tampoco

[50] Este último ha sido añadido por la AEPD apoyándose en la jurisprudencia del Tribunal Constitucional como veremos.

[51] AEPD, "Informe Gabinete jurídico N/REF: 0036/2020, pág. 25.

puede enjuiciarse el carácter constitucionalmente legítimo de esa finalidad, ni, en su caso, la proporcionalidad de la medida prevista de acuerdo con los principios de idoneidad, necesidad y proporcionalidad en sentido estricto". Dicho esto, qué debe entenderse por interés público esencial, frente a un "interés público" menos cualificado sigue sin haberse esclarecido.

En un segundo estadio, es necesario que dicho tratamiento biométrico de datos debe estar previsto en una norma con rango de ley. Debe de advertirse que la reserva de ley a que se refiere el Tribunal Constitucional es la del art. 53.1 de la CE, esto es, una reserva de ley ordinaria, y por tanto deben descartarse otras fuentes como la ley orgánica o el decreto ley que pese a tener idéntico rango tienen un ámbito material distinto.

Esta norma no solo debe amparar el tratamiento de datos biométricos, sino que también debe incluir las garantías que velen por los derechos del interesado. Así lo ha señalado el TC en la citada STC 79/2019, "La previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado" (FJ 8).

La AEPD ha entendido incumplido este requisito en los dos supuestos enjuiciados. En el caso de los exámenes online, el precepto que se alegaba como base legal para adoptar la medida era el artículo 46.3. de la LO de Universidades[52]. La AEPD señaló que el precepto era insuficiente para amparar dicho tratamiento pues no precisaba "en qué medida y en qué supuestos, la identificación de los alumnos mediante el empleo de la biometría respondería a un interés público esencial"[53]. Al analizar el supuesto del reconocimiento facial en una empresa de seguridad privada, la AEPD llega a la misma conclusión "los tratamientos de videovigilancia regulados en la LOPDGDD y en la LSP, se refieren exclusivamente a los tratamientos dirigidos a captar y grabar imágenes y sonidos, pero no

[52] "Las Universidades establecerán los procedimientos de verificación de los conocimientos de los estudiantes. En las Universidades públicas, el Consejo Social, previo informe del Consejo de Universidades, aprobará las normas que regulen el progreso y la permanencia en la Universidad de los estudiantes, de acuerdo con las características de los respectivos estudios".

[53] AEPD, "Informe Gabinete jurídico N/REF: 0036/2020", pág. 35,

incluyen los tratamientos de reconocimiento facial, que es un tratamiento radicalmente distinto al incorporar un dato biométrico"[54].

De ambos pronunciamientos se deriva que la ley que prevea el tratamiento necesariamente debe de hacer una alusión específica a las técnicas de reconocimiento facial y a las garantías que pretendan limitar abusos de esta tecnología. Puede concluirse que hasta que no haya un esfuerzo regulatorio se cierra la puerta al uso de esta tecnología, al menos al amparo del art 9.2 g) del RGPD.

Finalmente, el último de los requisitos se refiere a que el tratamiento debe ser proporcional al fin perseguido, lo que nos coloca en la valoración del reconocimiento facial dentro del test de proporcionalidad, estándar seguido para enjuiciar la validez de los límites a los derechos fundamentales. El propio RGPD se refiere a la proporcionalidad, que implica que los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios (Considerando 39). Por norma general, este requisito de la necesidad de la medida, dentro del juicio de proporcionalidad en sentido amplio, conlleva que para adoptar un acto restrictivo de derechos deben valorarse otras medidas alternativas menos gravosas para los intereses en juego.

Al respecto debe advertirse que el principio de necesidad no convive fácilmente con la adopción de nuevas tecnologías, como la que aquí se analiza. Esto es así, puesto que antes de que se diese el avance tecnológico en cuestión ya existía una alternativa que por norma general puede considerarse como menos gravosa. Por ejemplo, la junta escolar de un colegio en Bélgica un utilizó software de reconocimiento facial a través de la cámara para capturar y registrar la participación de 22 estudiantes en la clase. El propósito había sido agilizar aún las operaciones de registro de clases, una tarea que generalmente tomaba 10 minutos. De esta forma se esperaba que automatizar la toma del registro de clases ahorraría 17.280 horas de trabajo cada año en la escuela. No obstante, la Autoridad Sueca en materia de protección de datos sancionó a la escuela, entre otros motivos, porque existían medios menos invasivos para realizar el control de asistencia, dando lugar a que el tratamiento de datos fuera desproporcionado[55].

---

[54] AEPD, "Informe Gabinéte jurídico N/REF: 010308/2019" pág. 27.

[55] Véase EDVARDSEN, S., "How to interpret Sweden's first GDPR fine on facial recognition in school" *IAPP*, Agosto de 2019. Disponible en: https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school/

En idéntico sentido se ha pronunciado la AEPD, que exige que las medidas alternativas propuestas se hayan mostrado tanto ineficaces como ineficientes para la finalidad perseguida, siendo la alternativa que implique el tratamiento más invasivo la única opción viable[56]. En el informe referente al control de los exámenes online la AEPD ya ha adelantado sus reservas de cara a este requisito. La Agencia ha entendido que solo se podrá acudir al reconocimiento facial, aun cuando este previsto por una norma con rango de ley, cuando "no exista otra medida más moderada para la consecución de tal propósito con igual eficacia", y que en todo caso requerirá una especial justificación[57].

La AEPD no ha vedado complemente el uso del reconocimiento facial en el ámbito educativo, como tampoco el uso de otras tecnologías biométricas como la identificación por huella dactilar. No obstante, sí que ha insistido en su carácter extraordinario y subsidiario, incluso en un contexto en el de una pandemia como la propiciada por la Covid-19, en el que debe quedar limitado a "a aquellas enseñanzas y asignaturas concretas que, por su importancia, complejidad u otras circunstancias de especial incidencia, no aconsejaran acudir a otras opciones, como la evaluación continua, o hicieran excesivamente gravoso la adopción de otros medios como el control por videocámara o la realización de exámenes orales". Como apunta MARTINEZ MARTINEZ "El mensaje del regulador resulta claramente entendible: siempre que el profesor pueda reconocer visualmente a cada estudiante no se aplicarán tecnologías de reconocimiento facial"[58].

III.4. Una puerta abierta: El reconocimiento facial como medida para garantizar el cumplimiento de las obligaciones laborales

La letra b) del art. 9.2 del RGPD señala que el tratamiento de una categoría especial de datos será válido siempre que sea "necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados

[56] AEPD, "Informe gabinete jurídico 0065/2015", pág. 5.
[57] AEPD, "Informe gabinete jurídico 0036/2020", pág. 35.
[58] MARTÍNEZ MARTÍNEZ, R,. "Tecnología de verificación de identidad y control en exámenes online», *Revista de educación y derecho*, Núm. 22, 2020. pág. 26.

miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado".

El primer requisito para que dicho tratamiento sea posible es que así lo reconozca una norma del Derecho de la Unión o de los Estados Miembros. La AEPD ha entendido que el Estatuto de los Trabajadores, concretamente su artículo 20, ofrece una cobertura legal suficiente para establecer un sistema de reconocimiento biométrico del trabajador[59]. Este precepto dispone que "El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad".

En aplicación del mencionado precepto se ha concluido que es posible el tratamiento de datos biométricos del empleado en un sistema de identificación por huella dactilar. Esta forma de verificar la identidad del trabajador se ha entendido como necesaria, especialmente tras el Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, que modifica el Estatuto de los trabajadores para hacer el registro de la jornada obligatorio.

Dicho eso, sorprende el estándar manejado por la AEPD en comparación con el seguido en sus resoluciones sobre el interés público esencial. El art. 20.3 del ET reconoce un poder de control genérico para el cumplimiento de las obligaciones laborales por parte del empresario, pero no especifica qué tecnologías van a utilizarse en ejercicio de ese control ni qué obligaciones del trabajador están destinadas específicamente a ser fiscalizadas por dichos medios. A pesar de ello la AEPD ha admitido que dicho precepto ampara el uso del reconocimiento por huella dactilar en el trabajo.

Es cierto que estamos ante bases jurídicas distintas, la letra b) y la letra de g) del artículo 9.2 del RGPD. No obstante, la consecuencia inmediata es que en el ámbito laboral el uso del reconocimiento facial, como el resto de las tecnologías biométricas, no deben estar previstos específicamente en una norma con rango de ley. Tampoco deberán de serlo las garantías para respetar los derechos y libertades del interesado, lo cual presenta problemas con la literalidad del art. 9.2 b) del RGPD. Según la Agencia, el reconocimiento en el

[59] Véase AEPD "procedimiento Nº: E/03925/2020".

art. 20.3 del ET del poder de control y vigilancia del empresario suple esa necesidad.

Seguramente esta doble vara de medir se justifica por las garantías que pueden darse en un sistema de fichado por huella dactilar: el sistema debe pasar por una evaluación de impacto, y frecuentemente estos sistemas se basan en técnicas de autentificación y no identificación[60]. Lo cierto es que el uso del reconocimiento facial, en idénticas condiciones, no presentaría especiales problemas para los derechos y libertades del trabajador.

No obstante, si el reconocimiento facial no se circunscribe únicamente al lugar donde se controla el fichaje, sino que pretende afectar a otras partes del centro de trabajo podrían derivarse verdaderos peligros para los derechos del trabajador. Piénsese en sistemas que permitan que el empleado se encuentre continuamente localizado o incluso realicen un reconocimiento de sus emociones con la finalidad de medir su rendimiento. El Grupo de trabajo del artículo 29 ya advirtió que "Con las capacidades que ofrecen los análisis de vídeo, es posible que un empresario observe las expresiones faciales del trabajador por medios automatizados, identifique desviaciones con respecto a los patrones de movimiento predefinidos"[61].

A mi juicio, un primer límite a estas tecnologías derivaría de las propias normas y principios que guían el uso de cámaras de seguridad en el centro de trabajo. Quedaría su uso prohibido en "lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos" (art. 89.2 LOPDGDD). Asimismo, habrá que tener en cuenta los criterios establecidos en la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de

[60] En su reciente documento sobre "la protección de datos en las relaciones laborales" la AEPD ha apuntado "En caso de que se traten datos biométricos, la AEPD recomienda optar por sistemas de verificación o autenticación biométrica, siendo aconsejable que los sistemas biométricos se basen en la lectura de los datos biométricos almacenados como plantillas cifradas en soportes que puedan ser conservados exclusivamente por las personas trabajadoras (por ejemplo, tarjetas inteligentes o dispositivos similares). Por ejemplo, en el caso del tratamiento de datos biométricos para el fichaje en el momento de acceso al edificio, se utilizarán por la persona trabajadora terminales en los que será necesario tanto la aproximación de la tarjeta como la lectura de la huella. Es decir, el lector generará el identificador numérico de la huella que habrá de corresponderse con el de la tarjeta, entendiéndose que se ha producido el acceso al puesto de trabajo como consecuencia de la coincidencia entre el identificador generado y el que consta en la huella" pág. 31.

[61] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, "Dictamen 2/2017 sobre el tratamiento de datos en el trabajo" adoptado el 8 de junio de 2017, pág. 21.

datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. En ellas se establece que "Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal". Dicho requisito engarza con la proporcionalidad y necesidad que exige la justificación de todo tratamiento de datos, así como en la "modulación" de los derechos del trabajador en el contexto de la relación laboral, que debe ser en todo caso proporcionada (STC 99/1994 FJ 4).

Siguiendo esa línea la AEPD considera que el control audiovisual del empleado en el centro de trabajo "ha de respetar los derechos fundamentales de la persona trabajadora, especialmente el derecho a la intimidad personal"[62]. Ello le hace concluir, si bien sin entrar en un análisis exhaustivo, que la combinación de la videovigilancia con otras tecnologías como el reconocimiento facial sería una injerencia desproporcionada en los derechos del trabajador. El Grupo del art. 29 también señaló que "los empresarios deben abstenerse de utilizar tecnologías de reconocimiento facial" si bien matizó que "puede haber algunas excepciones marginales a esta regla, pero tales escenarios no pueden utilizarse para invocar una legitimación general del uso de esta tecnología"[63].

Por tanto, el debate del uso del reconocimiento facial en el entorno de trabajo parte de enjuiciar su necesidad y las garantías previstas para mitigar sus efectos adversos para el trabajador. De nuevo entramos en el terreno de la ponderación jurídica, y sería precipitado aventurar una solución sin tener en cuenta las características concretas de la tecnología de reconocimiento facial enjuiciada y sus usos en el entorno de trabajo.

IV. CONCLUSIONES

La tecnología de reconocimiento facial llama a nuestras puertas con fuerza. Podemos entrever sus beneficios, pero también sus riesgos, sin que pueda hacerse una valoración negativa o positiva para

[62] AEPD, "la protección de datos en las relaciones laborales" adoptado en mayo de 2021, pág. 52.

[63] Grupo de Trabajo sobre Protección de Datos del Artículo 29, "Dictamen 2/2017 sobre el tratamiento de datos en el trabajo" adoptado el 8 de junio de 2017, p. 21.

nuestras sociedades de este "avance" tecnológico, sin detenernos en el concreto análisis de cada sistema propuesto. La propuesta de Reglamento de Inteligencia Artificial Europeo, pese a las críticas que pueda merecer, creo que avanza en este sentido. En el caso de su aprobación tendremos una herramienta más para evaluar las características técnicas y finalidades de cada sistema de reconocimiento facial y dar una respuesta jurídica acorde con los peligros asociados al mismo.

Hasta entonces el RGPD, y su desarrollo en la LOPDGDD, nos ofrece, y seguirá ofreciéndonos[64] garantías frente a aquellos sistemas de reconocimiento facial que superen este umbral de riesgo inadmisible para nuestros derechos, concretamente para nuestra privacidad y el poder de disposición sobre nuestra información personal. Dicho eso, la normativa de protección de datos sigue presentándose demasiado abierta con respecto al uso de las tecnologías biométricas. Se echa en falta que los principios de necesidad y proporcionalidad enunciados abstractamente sean concretados en normativas como la LOPDGDD o la reciente Ley Orgánica 7/2021, de 26 de mayo.

Como hemos tenido ocasión de señalar, existen distintos ámbitos (en el seno de una investigación penal o en el cumplimiento de las obligaciones laborales) donde el actual marco legal deja la puerta abierta al uso del reconocimiento facial. Esto es debido a que la legislación no establece distinciones entre las distintas técnicas de identificación biométricas existentes. Eso contrasta con el criterio de la AEPD, en cuyas resoluciones y opiniones se ha mostrado reacia al uso del reconocimiento facial, en contraste con otros sistemas biométricos como la identificación por huella dactilar. Dicha actitud coincide con los temores de distintos autores e instituciones que ven en el reconocimiento facial el riesgo de una vigilancia masiva de la población.

Todo lo anterior me hace creer que una mención específica en nuestra legislación al reconocimiento facial o a las tecnologías biométricas de identificación a distancia sería deseable. Dicha alusión, que debería hacerse en una norma con rango de ley, debería de especificar qué salvaguardas deben ser observadas para protegernos de un uso desproporcionado de esta tecnología, sin cerrar la puerta a su uso cuando los riesgos existentes sean verdaderamente mitigados.

[64] Debe de advertirse que la Regulación de la Inteligencia Artificial que propone la Comisión es adicional a la prevista por el RGPD. Ello dará lugar a que sistemas que bajo la óptica de dicha norma sean admisibles, pero que no pasen los filtros de la actual normativa de protección de datos personales.