TECNOLOGÍA BIOMÉTRICA Y DATOS BIOMÉTRICOS. BONDADES Y PELIGROS. NO TODO VALE

BIOMETRIC TECHNOLOGY AND BIOMETRIC DATA. BENEFITS AND DANGERS. NOT EVERYTHING IS FAIR

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 298-331

Silvia BARONA VILAR

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

RESUMEN: El desarrollo volcánico de la tecnología biométrica y la proliferación de técnicas de tratamiento de datos biométricos genera numerosos dilemas en el mundo jurídico. Los datos biométricos sirven para reconocer a las personas de acuerdo con sus características físicas, fisiológicas y parámetros conductuales y pueden ser explotados, manipulados y empleados para tomar decisiones en el sector privado, público y empresarial. Y no son infalibles, en absoluto. Es importante delimitar normas, fijar condiciones de determinación de su finalidad, de su necesidad y de su proporcionalidad. La investigación ahonda en supuestos que orillean las condiciones de legalidad y de ética y ponen en alerta ante su posible manipulación.

PALABRAS CLAVE: Sistemas biométricos; datos biométricos; protección de datos biométricos.

ABSTRACT: Many dilemmas arise in the legal world as a result of the volcanic development of biometric technology and the proliferation of biometric data processing techniques. Used to identify individuals by their physical, physiological and behavioural characteristics, biometric data can be exploited, manipulated and used to make decisions in the private, public and business sectors. And they are not infallible. It is important to delimit standards, to set conditions for determining their purpose, necessity and proportionality. This research examines in depth and critically the assumptions that circumvent the conditions of legality and ethics and alerts us to their possible manipulation.

KEY WORDS: Biometric systems; biometric data; biometric data protection.

SUMARIO.- I. LA APARICIÓN DE LA BIOMETRÍA COMO SISTEMA AUTOMATIZADO DE RECONOCIMIENTO.- II. LOS DATOS BIOMÉTRICOS.- 1. Noción, usos y aplicaciones.- 2. Tipología de las técnicas biométricas y su incidencia en el mundo jurídico.- *A) Huellas dactilares.- B) Reconocimiento del iris y escáner biométrico de la retina.- C) Geometría del árbol de venas del dedo o de las muñecas.- D) Reconocimiento de firma.- E) Reconocimiento de escritura de teclado o biometría del tecleo.- F) Reconocimiento de voz.- G) Análisis biométrico de movimientos corporales.- H) Reconocimiento biométrico de la palma de la mano.- I) Reconocimiento biométrico de orejas (otograma).- J) Biometría por ADN o huella genética.- K) Reconocimiento facial.*- III. AHORA BIEN...NO TODO VALE.- 1. Punto de partida: Protección jurídica de los datos biométricos.- 2. La teoría nos la sabemos, pero qué sucede en la práctica.- *A) Seguridad frente a la sofisticada criminalidad, derivada de la globalización.- B) Algunos Proyectos nacionales e internacionales en marcha con datos biométricos. Dudas.- C) "Worldcoin", el proyecto de escaneo del iris a cambio de criptomonedas; un negocio redondo a costa de datos biométricos.- D) Utilización biométrica en entradas y salidas empresariales y otros fines laborales.*

I. LA APARICIÓN DE LA BIOMETRÍA COMO SISTEMA AUTOMATIZADO DE RECONOCIMIENTO.

La biometría incluye medidas biológicas o características físicas que se pueden emplear para identificar a las personas, y se incardina en el nuevo paradigma algorítmico en el que vivimos; una sociedad con la hipervaloración de los datos, favoreciendo su obtención y explotación. Esta situación amerita regular la protección de los datos personales. Esta volcánica emergencia, como consecuencia en gran medida de la irrupción del dato como valor, como moneda de cambio, como petróleo del siglo XXI[1], como riqueza a la postre, ha encontrado un desarrollo perfecto en la biometría, al generar información especial, obtenida mediante estudios mensurativos o estadísticos de los fenómenos o procesos biológicos[2], que, aun cuando aplicable a otras especies, nos vamos a centrar en la diversidad de los datos biométricos que pueden extraerse de una sola persona humana.

Datos biométricos que están ofreciendo una multiplicidad de posibilidades de usabilidad, favoreciendo la construcción de la sociedad del control y de la vigilancia[3], especialmente a través de los sistemas de reconocimiento automatizado mediante sistemas biométricos; sistemas que han adquirido una valorización espectacular

1 Esta frase se reitera *como si se tratara de un mantra*, tal como apunta Desireé Jaimovich, en la entrevista con Infobae que realizó a Juan Carlos Gutiérrez, director de IBM Storage para América Latina, https://www.infobae.com/america/tecno/2018/07/13/juan-carlos-gutierrez-los-datos-se-estan-convirtiendo-en-el-nuevo-petroleo-de-las-empresas/.

2 Abs, M.: "Biometrik", en *Historisches Wörterbuch der Philosophie,* online version, (ed. por J. Ritter, J.; K Gründer.; G. Schwabe,), AG Verlag, Basel, 1971, pp. 945-946. Y en el mismo sentido, Real academia española de la lengua, que considera que bajo el término "Biometría" se entiende "el estudio mensurativo o estadístico de los fenómenos o procesos biológicos".

3 Barona Vilar,baroBbb S.: *Algoritmización del derecho y de la justicia: de la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021, especialmente pp. 235-248.

• Silvia Barona Vilar
Catedrática de Derecho Procesal, Universitat de València.
Correo electrónico: silvia.barona@uv.es

en momentos en que la globalización abrió fronteras, se difuminaron, se permitió flujos de población, la movilidad comercial, personal, laboral, con efectos positivos, pero también negativos.

La irrupción de los sistemas tecnológicos favoreció un nuevo modelo de frontera, exigible ante el flujo humano, económico y laboral, incorporando medios que permitieran garantizar la seguridad nacional e internacional. No debe olvidarse que el modelo de "frontera" como delimitadora geográfica respondía a la fijación de la zona territorial en sentido político y administrativo, integrando cuestiones como soberanía (que incide en lindes, titularidades, propiedades y explotaciones de tierra, agua y aire) y que llevó a que fueran materializadas con un sistema de control especialmente en puertos y aeropuertos, con exigencias de pasaportes y visados o documentos identificatorios, para la entrada y salida del país. Este modelo ha permitido, como apunta Escajedo San Epifanio[4], soluciones frente al crecimiento de manipulaciones (robos y usurpaciones de identidad), de terrorismo internacional, de delincuencia organizada y las amenazas a la salud pública. El interés que despierta esta aparición de la biometría en el mundo jurídico se debe esencialmente al desarrollo que la misma ha propulsado en la aparición de los denominados sistemas automatizados de reconocimiento e identificación de seres humanos.

Se ha venido sosteniendo que el origen de la biometría como ciencia se debe fundamentalmente a Francis Galton[5] (aun considerándose que anteriormente hubo quien empleó este *nomen iuris*), quien, junto a Karl Pearson, fundaron la revista "Biometrika" (su primer número en 1901). En ella confluyen aportes de las matemáticas, estadística, antropología, zoología, botánica, estadística económica, etc.., dirigida a la búsqueda del conocimiento biológico por medios cuantitativos, independientemente de los fines - biomédicos, biocientíficos o de otra naturaleza[6]-. Se creó en 1947 la Sociedad internacional de Biometría, cuyo objetivo ha sido promover el "desarrollo y aplicación de la teoría y los métodos matemáticos y estadísticos a las Biociencias, incluyendo la agricultura, las ciencias biomédicas y la salud pública, la ecología, las ciencias ambientales forestales y disciplinas afines"[7].

Sus desarrollos posteriores han alcanzado al Derecho, siendo aceptadas con fascinación en ciertos sectores y con poca mirada crítica. En el siglo XIX se

4 Escajedo San Epifanio, L.: *Reconocimiento e Identificación de las personas mediante Biometrías estáticas y dinámicas,* Tesis Doctoral, Alicante, diciembre 2015, *open access*, p. 40, quien explica los diversos sistemas de registro de los habitantes y los documentos de identificación que se emitían especialmente a lo largo del siglo XX con la movilidad fronteriza y cómo se ha impulsado el sistema automatizado de reconocimiento biométrico en estos últimos tiempos, en gran medida favorecidos por el crecimiento poblacional y la movilidad.

5 Galton, F.: " Spirit of Biometrika", editorial del número primero de la Revista *Biometrika*, 1901.

6 Stigler, S.M.: "The Problematic Unity of Biometrics", Revista *Biometrics*, 2000, p. 654.

7 http://www.biometricsociety.org/about/

vinculó la biometría con las características psíquicas de las personas, el carácter y la capacidad con el cerebro (craneoscopia o frenología), con determinaciones referidas a las facultades mentales y morales derivadas de la estructura del cráneo. Fundamentaron las teorías de Lombroso, que fueron seguidas por Garofalo y Ferri, acerca de la vinculación de la delincuencia con los rasgos biológicos y psíquicos[8], esto es, considerando que el delincuente nace como tal, no se hace, de modo que defendían el determinismo biológico criminal. Posición doctrinal afortunadamente superada, pero que permitió su manipulación por gobiernos totalitarios para fundamentar crímenes contra la humanidad.

En la actualidad la biometría se vincula a los sistemas automatizados de identificación -entendida como el proceso de reconocimiento de un individuo particular entre un grupo- y autenticación -el proceso de probar que es cierta la identidad reclamada por el individuo-[9]. Estos sistemas pueden servir para identificar colectividades, en atención a rasgos identitarios de grupos, o referirse tan solo a datos biométricos de personas individualmente consideradas, siendo esta última la que ha impulsado especialmente los desarrollos biométricos informáticos, desde los que se trabaja con los datos almacenados en soporte informático para ofrecer respuestas de reconocimiento e identificación individual.

II. LOS DATOS BIOMÉTRICOS.

Los datos biométricos en la actualidad se utilizan en procedimientos automatizados de autenticación, comprobación e identificación. Inicialmente, el uso de la biometría se limitó al ADN y a la comprobación de las huellas digitales, especialmente en materia criminal, con una enorme incidencia en la investigación (penal y civil) y en la prueba. La proliferación de adquisición de estos datos ha emergido, ante una suerte de inconsciencia acrítica inicial en torno a los riesgos que supone la conservación de los datos ante la ausencia de protección jurídica de su tratamiento. En las últimas décadas se ha impulsado la legislacion para la protección de datos biométricos, nacional y supranacionalmente.

1. Noción, usos y aplicaciones.

Los datos biométricos sirven para reconocer a las personas de acuerdo con sus características físicas, fisiológicas o parámetros conductuales[10]. Estos datos

8 Garófalo, R.: *La criminología. Estudio sobre el delito y sobre la teoría de la represión,* Analecta editorial, 1900, pp. 142 y siguientes; Ferri, E.: *Principios de Derecho Criminal,* Ed. Reus, Madrid, 1933, pp. 45 y siguientes.

9 Agencia española de protección de datos: *14 equívocos en relación con la identificación y autenticación biométrica,* 2020, https://www.aepd.es/guias/nota-equivocos-biometria.pdf.

10 El artículo 3. 34) del Reglamento de Inteligencia Artificial, en virtud de la Resolución del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento (P9_TA (2024)0138, dispone que son "datos biométricos", "los datos personales obtenidos a partir de un tratamiento técnico específico,

biométricos que se obtienen pueden ser el resultado del análisis de un elemento biométrico de naturaleza universal, a saber, que existe en todas las personas, o bien algo identitario y distintivo de la persona, de forma permanente o temporal. No todos los elementos biométricos son equivalentes y el índice de diferenciación de una persona frente a otra es diverso en función del tipo de biometría utilizada. Así, de acuerdo con el objetivo de los sistemas biométricos (identificar o reconocer, oautenticar o verificar las personas a partir de algunas características fisiológicas o morfológicas) se utiliza el sistema más adecuado[11]. En este sentido, los sistemas biométricos de reconocimiento utilizan un dato y lo comparan con una lista o base de datos, como sucede con las bases de datos criminales, mientras que los sistemas biométricos de verificación sólo utilizan un dato comparándolo con el mismo dato previamente almacenado, como es el caso de las bases migratorias[12]. Cada vez más se emplean sistemas biométricos de reconocimiento o autenticación con dos o más datos biométricos, que se denominan "sistemas de combinación biométrica", en los que pueden valorarse el peso, la altura, el tipo de sangre, factor sanguíneo, etc..

Si bien inicialmente las técnicas biométricas funcionaban a través de la instalación de sensores en edificios o salas, su desarrollo y polimorfa multifuncionalidad ha permitido que se integren sensores biométricos en los ordenadores corporativos, para gestionar la identificación con reconocimiento y autenticidad a las personas, a través de sistemas y aplicaciones con tecnologías biométricas. Se trabaja con la biometría bimodal, combinando factores de identificación de quién o cómo es y de lo que se sabe o se tiene[13]. Podemos considerar que a través de estos sistemas se puede[14]:

1.- Llevar a cabo el control de presencia, registrando horarios de trabajo (llegada y salida de los trabajadores), pudiendo emplearse la huella dactilar o la planta o la geometría de la mano, entre otras, siempre con el consentimiento de estos, en relación con la usabilidad de los datos biométricos.

relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos".

11 Boulgouris, N. V. et al.: *Biometrics, Theory, Methods, and Applications*, IEEE and WILEY, Estados Unidos, 2010.

12 Díaz Rodríguez, V.: "Sistemas biométricos en materia criminal: un estudio comparado", *Revista IUS vol. 7, núm. 31*, Puebla, enero-junio 2013, en http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100003.

13 Instituto nacional de ciberseguridad (incibe): *Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario,* 2016, en https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf, p. 14.

14 Instituto nacional de ciberseguridad (incibe): *Tecnologías biométricas aplicadas a la ciberseguridad*, cit., pp. 14-15.

2.- Permite ser un instrumento de lucha contra el fraude, especialmente en el sector bancario (por ejemplo, para realizar transferencias bancarias) o en el ámbito del fraude a otras entidades privadas o incluso la Administración Pública.

3.- Conformar centros de atención de llamadas, esto es, los *Call-centers*, incorporando técnicas biométricas de reconocimiento de la voz, por ejemplo, otorgando mayor seguridad y eficiencia al comprobar la identidad del cliente interlocutor de forma más segura y con menos tiempo.

4.- Pueden igualmente favorecer el control de navegación como vía para acceder o negar redes sociales o a determinados sitios web, filtrar contenidos, etc.

5.- Para realizar vigilancia general o predictiva policial, ganando protagonismo el reconocimiento facial y el reconocimiento de la manera de andar (movimientos). Esta función está siendo contestada en el seno de la UE, y son numerosos los instrumentos que la limitan; recientemente, el texto de futuro Reglamento de Inteligencia Artificial UE (Artificial Intelligence Act).

6.- En los últimos años se ha venido empleando la denominada combinación biométrica con NFC, a saber, un sistema que permite proteger determinadas aplicaciones, autenticarse, realizar pagos o gestionar contraseñas en el ejercicio de las funciones de los dispositivos móviles. Ejemplo más común es la tecnología *Near Field Communication (NFC)* en los móviles, que permite realizar pagos desde el móvil con un sistema que permite identificar al usuario antes de validar la operación.

Si bien la aplicación general de estos sistemas biométricos es la de identificar a una persona, deben considerarse otras aplicaciones, de manera que es posible hablar: 1º) de medio de autenticación o verificación biométrica, comparando plantillas biométricas (que están en fichero) que pertenecen supuestamente a la misma persona para determinar que la persona es la misma en ambas, lo que el art. 3.36) del Reglamento IA considera como "verificación automatizada y uno-a-uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente"; 2º) de medio de identificación biométrica (art. 3. 35): "el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos") ; y 3º) de medio de categorización o segregación biométrica, cuya finalidad no es identificar o verificar a la persona, sino categorizarla (por edad, sexo, raza...), exigiéndose en el Reglamento IA de la UE, de forma conjunta con los sistemas de reconocimiento de emociones, normas armonizadas de transparencia aplicables, de manera que se informe del

funcionamiento del sistema a las personas expuestas a este. Esta última modalidad es altamente riesgosa, dado que puede generar efectos discriminatorios que están proscritos por el art. 21 de la Carta de Derechos de la UE[15].

2. Tipología de las técnicas biométricas y su incidencia en el mundo jurídico.

Estas técnicas biométricas variarán según sean fisiológicas, comportamentales o ambas, y según se utilicen datos estáticos o datos dinámicos sobre el comportamiento[16]. Por un lado, entre las técnicas que inciden en los aspectos físicos y fisiológicos caracterizadores de una persona se hallan: huellas dactilares, análisis de la imagen del dedo, reconocimiento del iris, análisis de la retina, geometría de las manos, otogramas de las orejas, reconocimiento facial, de la voz, análisis de ADN, análisis de poros de la piel o incluso detección de olor corporal. Por otro lado, es posible trabajar con técnicas que analizan el comportamiento de una persona a través de la comprobación de la firma (figura, trazo, presión, velocidad, etc.), el análisis de la pulsación de las teclas, análisis de movimientos o forma de caminar, etc.. Y, además, la integración de ambos sistemas, a saber, aquellos que combinan las características biométricas del usuario con otras tecnologías de identificación o autenticación (contraseña y número de identificación personal, o huella dactilar, por ejemplo); es lo que se denomina la biometría multimodal o de segunda generación[17].

Los avances en biometría no cesan, presentándose como una respuesta a los peligros y riesgos que se están generando cada vez más en materia de ciberseguridad, de modo que frente a las contraseñas tradicionales -punto débil de los sistemas de seguridad desde hace tiempo- la biometría se presenta como la vía de garantía de la ciberseguridad, al combinar elementos identitarios corpóreos con patrones de comportamiento, otorgando una gran versatilidad al poder ser empleados en múltiples áreas y para una enorme multifuncionalidad. Vamos a referenciar algunas de estas modalidades.

A) Huellas dactilares.

Las huellas dactilares son los datos biométricos más usados, en gran medida por su sencillo acondicionamiento (podemos pensar que en la actualidad está siendo usada en dispositivos móviles y portátiles, como vía de autenticación sencilla de

15 En el mismo sentido, Etxeberría Guridi, J.F.: "Sistemas biométricos (el reconocimiento facial en particular) y sus aplicaciones", AAVV.: *Inteligencia Artificial y Administración de Justicia*, (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Thomson Reuters-Aranzadi, Cizur Menor (Navarra), 2022, pp. 170-171.

16 Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales (markt/12168/02/es wp 80): *Documento de trabajo sobre biometría*, adoptado el 1 de agosto de 2003, https://www.informatica-juridica.com/documento-trabajo/documento-trabajo-biometria/

17 Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales: Agencia espanola de protección de datos, *Dictamen 3/2012 sobre la evolución de las tecnologías biométricas* de 27 de abril de 2012 (WP193), https://www.aepd.es/documento/wp193_es.pdf.

los usuarios), que se integran fácilmente, amén de su bajo coste y su consideración de alta precisión[18]. Fue a finales del siglo XX cuando se desarrollaron los sistemas de reconocimiento mediante huellas dactilares, aun cuando la ficha decadactilar se creó en 1891 por el croata Iván Vucetich.

Puede haber dos maneras de recoger las huellas dactilares, bien a través del "basado de minucias", que consiste en identificar formas de la huella dactilar y su posición dentro de la misma; o bien a través del denominado "basado en correlación", o análisis de la huella dactilar de forma global. La huella dactilar ya fue desde hace tiempo un análisis que se realizaba y al que se otorgaba una importante validez en determinados sectores, inclusive permitía sustituirla por la firma cuando no se supiera escribir. Ahora bien en la última década se ha investigado que, aun cuando es difícil, no resulta imposible falsificar huellas dactilares, pudiendo defraudar a través de la entrada en espacios virtuales; inicialmente, estas falsificaciones permitieron desbloquear candados inteligencias y unidades USB protegidas con sensores de huellas dactilares, lo que constata su falibilidad.

B) Reconocimiento del iris y escáner biométrico de la retina.

El reconocimiento del iris se materializa a través de una cámara de infrarrojos, que realiza una fotografía del ojo, y permite identificar a la persona, en cuanto la información referida al iris no es variable (al menos no lo es hasta el momento). Son numerosas las aplicaciones que se realizan en la actualidad con este medio, tanto como medio de acceso propio a instrumentos personales (como el móvil o la Tablet), como para acceso colectivo (para entrar en un lugar de trabajo o para entrar en un país a través de la aduana electrónica, por ejemplo). Existen proyectos dudosos de escaneo de iris, como el "Worldcoin", al que nos referimos *infra*.

Igualmente es posible hacer referencia al escáner biométrico de la retina, que se basa en la utilización del patrón de los vasos sanguíneos contenidos en la misma; se considera una técnica idónea para entornos de alta seguridad por su alto grado de fiabilidad, si bien se requiere que el usuario voluntariamente acepte que se le realice la muestra, manteniéndose inmóvil y muy cerca del sensor durante la captura de la imagen[19], lo que se presenta como inconveniente.

C) Geometría del árbol de venas del dedo o de las muñecas.

El reconocimiento vascular es un dato biométrico que permite el estudio de la geometría del árbol de venas del dedo o de las muñecas. Es probablemente

18 Ferrer, C.: "¿Cómo cumplir el RGPD si manejas datos biométricos?", en *https://protecciódatos-lopd.com/empresas/datos-biometricos-rgpd/,* 9 de julio 2018. Puede verse igualmente, Instituto nacional de ciberseguridad (incibe): *Tecnologías biométricas aplicadas a la ciberseguridad,* p. 8.

19 Instituto nacional de ciberseguridad (incibe): *Tecnologías...*, cit., p. 9.

menos conocido que otros. Se capta, como si fuere una cámara de circuito cerrado de televisión para visualizar ambientes sin luz visible, lo que se denomina la "transmitancia" en la imagen, un proceso que permite diferenciar entre tejido muscular y lo que son venas y capilares, por tanto, el formato de las venas a través de la biometría vascular. Su incorporación a la Biometría arroja mejores resultados que la huella digital (que puede fallar en ciertos casos por falta de impresión en personas con diabetes o de edad avanzada o en quienes manejan productos químicos, o bien por suciedad en la impresión por polvo, cremas, etc, o incluso por cambios en la impresión debido, por ejemplo, a cortes, quemaduras, etc). Se considera, por tanto, que es un sistema biométrico de mayor fiabilidad y que surge como mecanismo de mejora de la biometría digital[20].

D) Reconocimiento biométrico de la palma de la mano.

El reconocimiento biométrico de la palma de la mano gracias a la aplicación de diversos algoritmos, como método de identificación. Fue Samsung quien patentó esta técnica, en la que se conjugan aprendizaje profundo, tecnología de visión computadora y redes neuronales, para reconocer las venas y los patrones de impresión de la palma de la mano, que singularizan las persona, obstaculizando posibles duplicidades. Funciona como una suerte de escaneo de la palma y comenzó inicialmente a emplearse para facilitar a las personas la recuperación de credenciales, ante la complicación que existe en muchos casos de tener que llamar a operadoras, utilizar el correo electrónico, etc. Una manera mucho más sencilla de conseguir el desbloqueo de algunos de nuestros instrumentos cotidianos personales y profesionales.

E) Reconocimiento de firma.

El reconocimiento de firma se presenta como otro de los parámetros biométricos de identificación de la persona. Es una forma de asociar la identidad del que firma un documento electrónico, gracias a la captación de datos biométricos asociados a la firma manuscrita sobre dispositivos electrónicos adecuados. Los datos biométricos que se capturan en la firma son la presión del instrumento con el que se firma (lápiz, bolígrafo), la velocidad de la escritura y la aceleración. Son de gran utilidad como sistemas de identificación en las gestiones bancarias, o en el ámbito laboral. Es una técnica diversa al reconocimiento de la firma manuscrita tradicional, dado que en ésta lo que importa es la firma en sí, las características de la misma, mientras que en la firma biométrica lo que importa es el cómo se realizó la firma para fijar criterios conductuales.

20 Puede verse más detalles en "Biometría vascular: ¿es el futuro?", en https://www.anixter.com/es_la/about-us/news-and-events/news/vascular-biometrics-is-it-the-future.html.

Igualmente, el del reconocimiento del escrito, que se realizará a través de un reconocimiento óptico de los caracteres del texto por medio de un software específicamente determinado.

F) Reconocimiento de escritura de teclado o biometría del tecleo.

El reconocimiento de escritura de teclado es un sistema que incide en un componente conductual - manera de escribir en un teclado-. Se denomina biometría del tecleo, y se analiza la manera y los tiempos en que una persona presiona una tecla y la suelta cuando escribe en una computadora. Aun cuando es técnica moderna, tiene antecedentes en el trabajo que la inteligencia militar en la II Guerra Mundial realizaba con el sistema de valoración de ritmos de transmisión de mensajes emitidos a través del "código morse", según la forma, ritmo de teclear, valorando cómo introducían puntos, comas, guiones en el mensaje, para detectar quienes eran amigos y quienes enemigos.

En la actualidad se trabaja a través de algoritmos, que crean patrones de dinámicas de escritura para efectuar las autentificaciones en su caso. Básicamente los parámetros que se emplean para llevar a cabo la medición, entre otros, son la fuerza con la que se teclea, el tiempo de pulsación y el plazo transcurrido entre las pulsaciones de teclado.

G) Reconocimiento de voz.

En el desarrollo de la investigación penal puede emplearse el reconocimiento de voz a través de aplicaciones algorítmicas que realizan una medición de muestras de voz y devuelven el resultado con la identificación o no de la persona. La voz es una de las características que singularizan a las personas de manera que con escuchar alguna palabra es posible distinguir e identificarla. Hay, empero, factores que pueden alterar la exteriorización de la voz, como el momento del día o alteraciones debido a catarro, faringitis, afonía, etc. Estos elementos permiten afirmar que la biometría de voz es más compleja que la de la huella dactilar, por ejemplo. Se trabaja sobre la parte de la voz que siempre es fija, como las ondas sonoras que se exteriorizan y vienen condicionadas por determinados parámetros fisiológicos como la posición de los dientes o la longitud del cuello entre otras, lo que permite la singularidad de la voz.

La biometría de la voz se despliega a través de varias etapas: por un lado, el registro que permite tomar varias muestras de voz de la persona (por ejemplo, diciendo un código o una frase), configurando la huella vocal; y en segundo lugar, en la fase de test se compara la huella vocal con la voz de quien habla, verificando

si corresponden o no a la misma persona[21]. En cualquier caso, se considera que pueden incidir factores externos que alteren el resultado, como la posible existencia de ruido de fondo que impidiera realizar de forma fiable esa identificación.

Recientemente, están surgiendo herramientas de audio capaces de clonar las voces humanas, a partir de una muestra de 15 segundos para desarrollar su creación. Un ejemplo de ello es el modelo "Voice Engine de Open AI", que utiliza texto y muestra de los 15 segundos para generar un habla natural que se asemeja mucho al hablante original, inclusive en otro idioma diverso al original. De momento es un ensayo, si bien genera no pocas dudas acerca de los riesgos de suplantación de identidad que pueden provocarse como consecuencia de estos resultados algorítmicos[22].

H) Análisis biométrico de movimientos corporales.

Como componente conductual de las personas también existe el análisis biométrico respecto de los movimientos de la persona o forma de caminar. Utilizar el andar humano como característica biométrica es algo relativamente novedoso, aun cuando su estudio ciertamente ha cobrado un enorme interés especialmente por su aplicación al ámbito de la vigilancia y seguridad. Cada persona tiene una manera diferente de caminar.

Lo que se pretende con la biometría es tomar este lenguaje corporal y traducirlo a un conjunto de datos que puede ser interpretado por una computadora. La diferencia con otros sistemas biométricos es que se puede realizar a distancia o incluso con imágenes de baja resolución, de manera que no depende de factores como el color, la textura o la iluminación. En este reconocimiento del andar humano se procesan imágenes extraídas de un video para obtener datos que permitan reconocer al sujeto que está caminando[23]. Su uso en la actualidad es extenso, en bancos, instalaciones militares, hoteles, aeropuertos, estaciones de tren, donde se justifica la posible existente de amenazas, siendo éste un medio para detectarlas de forma rápida[24].

21 "¿Cómo funciona la biometría de voz?", 8 de diciembre de 2015, en https://biometricvox.com/blog/biometria-de-voz/como-funciona-la-biometria-de-voz/.

22 Jiménez, M.: "Open AI lanza una herramienta de audio capaz de clonar las voces humanas", El País 30 de marzo de 2024.

23 Romero Moreno, M.: *Reconocimiento del Andar Humano basado en ensamble de clasificadores utilizando silueta y contorno*, Tesis de Maestría, Instituto Nacional de Astrofísica, Óptica y Electrónica, Tonantzinla, Puebla, 2008, en https://inaoe.repositorioinstitucional.mx/jspui/bitstream/1009/558/1/RomeroMM.pdf, pp. 2-3.

24 Ruane Dawson, M.: *Gait Recognition. Final Report,* Department of Computing Imperial College of Science, Technology and Medicine, Londres, 2002, 4-25.

l) Reconocimiento biométrico de orejas (otograma).

El reconocimiento biométrico de las orejas es el modelo avanzado de lo que históricamente se empleó hace ya algún tiempo en el campo forense, a los efectos de su utilización para la identificación de sospechosos. Era lo que se denominaba como otograma, otohuella o huella auricular[25], una prueba antropomórfica.

Se considera que el análisis del pabellón auricular es uno de los rasgos más fiables y significativos en el reconocimiento biométrico, dado su carácter individualizante y que, a diferencia de las huellas dactilares, no suele tener cambios a lo largo de la vida de la persona. Alphonse Bertillon fue el primer autor que consideró que la oreja era una de los elementos más importantes en la descripción de una persona, manteniendo que es casi imposible que dos orejas sean idénticas. Este autor desarrolló lo que se denominó la "fotografía métrica", en la que se estandarizaban las fotografías de identificación e imágenes visuales de las escenas de crímenes, aplicándolas en la ciencia forense[26]. Todo ello sin olvidar que este discurso permitió trabajar con la genética a Lombroso y sus discípulos creando su teoría antropológica criminal[27]. Ahora bien, si la irrupción de estas ideas se gestó en el Siglo XIX, fue en 1964 cuando el policía californiano Alfred Victor Lannarelli confirmó que en ese momento la huella dactilar y la oreja humana debían considerarse como los medios más adecuados para identificar a una persona[28].

La utilización de la oreja como característica biométrica del individuo viene marcada por ciertas ventajas: por un lado, las orejas son parte del cuerpo visible, elementos externos corpóreos y, por otro, es más sencillo llevar a cabo un reconocimiento biométrico teóricamente sin la percepción ni el consentimiento del sujeto pasivo. Incluso, se ha afirmado por González Sánchez[29], la biometría de la oreja también se puede utilizar para acentuar la efectividad de otras biometrías como la voz, geometría de la mano o identificación de rostros, favoreciendo con ello la implementación de sistemas biométricos multimodales o híbridos.

25 Gargantilla, P.: "Puedes acabar en la cárcel por la huella de tu oreja", publicado el 26 de mayo de 2019 en https://www.abc.es/ciencia/abci-puedes-acabar-carcel-huella-oreja-201905260149_noticia.html, quien explica: "el pabellón auricular está constituido por un esqueleto cartilaginoso, que se pliega sobre sí mismo formando relieves y depresiones, que en su conjunto configuran al pabellón una forma característica. La otohuella es la representación bidimensional del pabellón auricular".

26 "Bertillon system", en http://www.britannica.com/EBchecked/topic/62832/Bertillon-system.

27 Clouston, T. S.: "The Developmental Aspects of Criminal Anthropology", *The Journal of the Antropological Institute of Great Britain and Ireland*, vol. 23, pp. 215-225.

28 Gargantilla, P.: "Puedes acabar en la cárcel por la huella de tu oreja", cit., quien atribuye a Iannarelli el empleo de una denominación que se refiere al reconocimiento de la oreja, *Earology.*

29 González Sánchez, M.E.: *Análisis biométrico de las orejas,* Tesis Doctoral, Departamento de Informática y Sistemas, Universidad de Las Palmas de Gran Canaria, 2008, p. 6, en https://accedacris.ulpgc.es/bitstream/10553/3435/1/Analisis_biometrico_orejas.pdf. Esta autora insiste en la necesidad de aplicar un método robusto de extracción de características, a partir de las imágenes tomadas de la oreja, que se pueda usar para determinar la identidad de algunos individuos.

J) Biometría por ADN o huella genética.

Existe, igualmente, la biometría por ADN o huella genética (son datos genéticos[30]). La técnica atiende a una premisa: dos seres humanos tienen una gran parte de su secuencia de ADN en común y para distinguir a dos individuos se puede explotar la repetición de secuencias altamente variables llamada "microsatélites". Será poco probable que dos seres humanos no relacionados tengan el mismo número de microsatélites en un determinado locus; de ahí que es factible establecer una selección que raramente ha surgido por casualidad, salvo en el caso de gemelos idénticos, que tendrán idénticos perfiles genéticos pero no las huellas dactilares[31].

Esta técnica comenzó en la década de los años ochenta mediante la comparación de muestras genéticas con los perfiles genéticos que obran en las diversas bases de datos, y que puede llevar tanto a la identificación de posibles delincuentes como a la exculpación de quien ha quedado afectado a un proceso penal. Desde la década de los años ochenta hasta la actualidad la inteligencia artificial ha permitido perfeccionar lo que se denominan "Modelos de Inteligencia Forense" que se dirigen a la investigación criminal, empero tratar de equilibrarse en el marco de los derechos y las garantías de quienes son objeto de investigación[32].

Esta técnica de identificación de la huella genética se ha venido utilizando en las investigaciones criminales para identificar a los sospechosos con muestras de sangre, cabello, saliva o semen, o para fundamentar una absolución. Igualmente se utiliza en aplicaciones como la identificación de los restos humanos, pruebas de paternidad, la compatibilidad en la donación de órganos, el estudio de las poblaciones de animales silvestres, y el establecimiento del origen o la composición de alimentos. También se ha utilizado para generar hipótesis sobre las migraciones de los seres humanos en la prehistoria[33].

Para realizar un análisis genético de obtención de un perfil de ADN se requiere de la existencia de material biológico, que puede obtenerse de dos maneras diversas: por un lado, sin intervención corporal alguna, recogiendo dicho material, o bien mediante la intervención corporal para obtener las muestras o vestigios que permitan obtener el perfil de ADN. La injerencia en una serie de derechos

30 El Reglamento de Protección de Datos y la Directiva 2016/680 consideran los datos genéticos como una categoría autónoma y diversa respecto de los datos biométricos, si bien los diversos documentos de trabajo sobre biometría de la Agencia de Protección de Datos (WP80 y GT29) han venido a pronunciarse acerca de las técnicas de elaboración de perfiles de ADN, considerando una posibilidad de su usabilidad para generar sistemas de autenticación o identificación biométrica del ADN.

31 Ecured: "Biometría por ADN", en https://www.ecured.cu/Biometr%C3%ADa_por_ADN.

32 Caneppele, S., Ribeaux, O.: "Forensic intelligence", *"The Routledge International Handbook of Forensic Intelligence and Criminology",* Routledge, 2017, pp. 136-148.

33 Ecured: "Biometría por ADN", en https://www.ecured.cu/Biometr%C3%ADa_por_ADN.

fundamentales se traduce en que la práctica de las intervenciones corporales deberá efectuarse con el debido respeto a un régimen de garantías, máxime cuando estos resultados alcanzados puedan tener una influencia en la persecución de hechos delictivos[34].

K) Reconocimiento facial.

La técnica del reconocimiento facial permite el tratamiento automático de imágenes digitales que contienen las caras de personas con fines de identificación, autenticación o verificación y categorización de las personas empleando algoritmos, a través de "búsqueda de la apariencia". Este sistema algorítmico analiza las facciones del rostro de la persona y las compara con el resto de personas que se hallan incluidas en la base de datos; no es una mera captación de imágenes. Son cada vez más numerosas y más sofisticadas las aplicaciones y programas que permiten identificar a una persona por los rasgos de su cara. Se afirma que el rostro es la identidad visual más importante de un ser humano[35].

El reconocimiento facial se ha convertido en una herramienta efectiva y de gran usabilidad en los últimos tiempos, tanto en ámbitos públicos como privados, basada en un desarrollo tecnológico de *deep learning*, que ha logrado que el sistema computacional interprete con gran acierto la imagen, tras una acumulación masiva de datos biométricos faciales. Gobiernos[36] y empresas se han lanzado a trabajar con estas técnicas de reconocimiento facial, que permiten una vigilancia y seguridad de lugares de trabajo, de aeropuertos, de centros comerciales, de colegios, universidades[37], etc.

Pese a las posibles mermas de capacidad identificadora de los modelos concurrentes, debido a circunstancias como el ángulo de la cámara, el cambio de tono de piel o por cambios estéticos de la cara, en los últimos tiempos las empresas destinadas al diseño y perfeccionamiento de estos softwares han incorporado tecnología de última generación, saltando obstáculos. Los avances en esta técnica biométrica han sido espectaculares, debido a los desarrollos algorítmicos, a la cada

34 Etxeberría Guridi, J.F.: "Obtención de perfiles de ADN a la luz de la nueva Orden Europea de Investigación (OEI): diversas alternativas", AAVV.: *Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad*, (ed. por S. Barona Vilar). Tirant lo Blanch, Valencia, 2019, p. 379.

35 Prasanthi Jasmine, K.; Naga Prakash, K.: *Reconocimiento de emociones humanas a partir de imágenes de rostros*, Ed. Nuestro Conocimiento, 2021, p. 6.

36 Fue EEUU en la década de los noventa cuando desarrolló algunos programas de reconocimiento automatizado de rostros (FERET -*Face Recognition Technmology*-, FRVT -*Face Recognition Vendor Test*-), conm una fiabilidad diversa en función del entorno controlado o no. Puede verse, Escajedo San Epifanio, L.: *Reconocimiento e Identificación de las personas mediante Biometrías estáticas y dinámicas,* cit., p. 90.

37 Con motivo de la realización de pruebas de evaluación on line de estudiantes, ante la situación de crisis sanitaria del COVID-19, la Agencia Española de Protección de Datos (AEDP) realizó un Informe sobre el posible uso del reconocimiento facial a los alumnos que realizan los exámenes universitarios, debiendo concurrir consentimiento libre del afectado, y legitimándose en la existencia de un interés público que debe ser "esencial" para que pueda ser legítimo, que debería justificarse en una norma con rango de ley, que no existía, https://www.aepd.es/es/documento/2020-0036.pdf.

vez mayor disponibilidad de grandes bases de datos de imágenes faciales y método para evaluar el rendimiento y la fiabilidad de los algoritmos de reconocimiento facial[38]. Paradigmático fue la identificación a través de estos datos biométricos del rostro a una persona aun cuando esté usando mascarilla por causa del COVID-19. La tecnología se renovó y se aceleró el entrenamiento de algoritmos para identificar a personas con mascarillas[39].

La experiencia del empleo de las técnicas biométricas de reconocimiento facial en China, Japón, Corea del Sur, Singapur, en parte de EEUU, es larga. Los condicionantes en cada país y sus límites legales son diversos. Si bien es cierto que su empleo en el control de acceso a determinados espacios físicos o virtuales se ha generalizado, en Europa sigue manteniéndose una posición resistente, por los falsos positivos o negativos producidos, que han cobrado especial relevancia, sobre todo cuando se usa como sistema de identificación remota en la prevención, la investigación, el enjuiciamiento y la ejecución de infracciones penales, dada la afectación de derechos fundamentales.

En Europa en general se cuestiona su fiabilidad, su funcionalidad, planteando cuestiones éticas y de afectación de derechos fundamentales, y muy especialmente también del derecho de protección de datos, que tan celosamente ha querido tutelarse por las instituciones europeas. Pese a esta resistencia, hay ya diversas manifestaciones, refiriéndonos a algunos proyectos piloto[40].

En España, a título de ejemplo, Marbella, Ceuta, La Nucía, Las Rozas o Vaciamadrid poseen cámaras que incorporan la técnica biométrica del reconocimiento facial, en la lucha contra determinada delincuencia. La potencia del software marbellí busca por apariencia, que incluye rasgos del rostro, color de ropa, edad, género, color de pelo y aspecto. Frente a los detractores de estos sistemas, se argumenta que se trata de un modelo de inteligencia artificial capaz de observar miles de horas de video para acelerar o concentrar las búsquedas, permitiendo hallar personas y objetos, por ejemplo, automóviles[41]. Y se presenta como la tensión cada vez más íntima o carnal entre las anatomías humanas y los objetos técnicos[42]. No obstante,

38 Prasanthi Jasmine, K.; Naga Prakash, K.: *Reconocimiento de emociones humanas* …, cit., p. 7.

39 García, J.G.: "El reconocimiento facial aprende a identificar mascarillas", *Retina, El País Economía,* mayo 2020. Este autor se refiere precisamente a HERTA, compañía dedicada a conseguir estos avances de forma acelerada.

40 Barona Vilar, S.: *Algoritmización del derecho y de la justicia,* cit., pp. 489-490.

41 A través del software se pretende hacer seguimiento del vehículo, dado que precisamente en Marbella el robo de coches de alta gama se da con mucha asiduidad. Pérez Colomé, J.: "Marbella, el mayor laboratorio de videovigilancia de España", *El País, 22 de noviembre de 2019*, https://elpais.com/tecnologia/2019/11/21/actualidad/1574348695_231540.html, considera que el gran peligro es avanzar poco a poco este software de reconocimiento facial, permitiéndose la búsqueda indiscriminada de la cara de algún sospechoso. La situación no está exenta de dudas, y prueba de ello son las sanciones desde la UE, como la impuesta por empleo de reconocimiento facial en un colegio sueco, pese a tener el consentimiento de los alumnos; y la otra, en Londres, que en la zona de King's Cross estuvo usando durante dos años esta tecnología.

42 Sadin, E.: *La humanidad aumentada,* Ed Caja Negra, 2017, p. 82.

amén de los falsos positivos y negativos, concurre todavía la posibilidad de incurrir en discriminación, en parte por los sesgos y en parte por la calidad de los datos. Precisamente, la Agencia de los Derechos Fundamentales de la Unión Europea (FRA European Union Agency for Fundamentals Rights), refiriéndose a la calidad de los datos, apunta la necesidad de que el software de reconocimiento facial sea alimentado de grandes cantidades de imágenes faciales (debe entenderse, representativas de los diferentes grupos étnicos y de género), dado que, a mayor cantidad de imágenes, mayor precisión en las predicciones[43].

De hecho, cada vez más asistimos a una evolución de esta técnica, combinando características físicas con psicológicas que entroncan con origen, emociones y bienestar y cada vez más están comenzando a emplearse para detectar si las personas mienten o dicen la verdad (inclusive en el ámbito laboral a efectos de productividad). Esto va más allá de la mera identificación.

Así, el Reglamento de la IA (AI Act, P9_TA(2024)0138)[44] incorpora la referencia a los "sistemas de reconocimiento de emociones", entendiendo que se trata de un "sistema de IA destinado a detectar o deducir las emociones o las intenciones de personas físicas a partir de sus datos biométricos" (art. 3.34). Ejemplo de este sistema de reconocimiento de emociones fue el Proyecto iBorderCtrl que se establece en la UE para la detección de mentiras en las fronteras, en el que intervenían Luxemburgo, Chipre, Reino Unido, Polonia, España, Hungría, Alemania y Letonia[45], que provocó reacciones en contra, como el Informe de 13 de julio de 2021 de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (A9-0232/2021), que insta a la Comisión para que deje de financiar investigaciones, aplicaciones o programas biométricos que puedan concluir probablemente en una vigilancia masiva e indiscriminada en espacios públicos. El Parlamento Europeo se ha mostrado muy preocupado, especialmente por los efectos de la utilización de los sistemas de reconocimiento facial en sectores como la prevención, investigación, enjuiciamiento y ejecución en materia penal, si bien se recogen como posibles en el texto del reglamento IA.

En algunos países europeos se han dado situaciones específicas con respuestas *ad hoc*. Francia, a través de su regulador de la privacidad en internet (CNIL) propone distinguir cuándo un reconocimiento facial es necesario y cuándo no, para evitar la situación desmedida en una sociedad que se asienta en el reconocimiento de los derechos y las libertades de las personas. Por su parte, Suecia, a través de su Agencia de Protección de Datos, ha multado con 18.500 euros a una escuela secundaria de Skelleftea por adoptar la tecnología de reconocimiento facial para

43 *Facial recognition technology: fundamental rights considerations in the context of law enforcement (2020)*, p. 27.

44 https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf.

45 https://ec.europa.eu/research/infocentre/article_en.cfm?artid=49726.

controlar la asistencia de los alumnos al aula, entendiendo que este proyecto vulnera varios artículos del Reglamento de Protección de Datos, de obligado cumplimiento para empresas y ciudadanos. Fuera de Europa, San Francisco fue la primera ciudad en EEUU que prohibió el uso de la tecnología de reconocimiento facial –debido al movimiento de las organizaciones pro derechos humanos que se manifestaron en contra-, a las que han seguido Oakland, Berkley (California) y Somerville (Massachusetts), en las que se consideró la posible prohibición de la vigilancia facial por el Gobierno. Ahora bien, Nueva York, Chicago, Detroit y Washington tienen programas piloto para implementar estos sistemas. En Gran Bretaña la policía de Gales del Sur lo probó como sistema de vigilancia y en Londres (Scotland Yard), un sistema de cámaras de reconocimiento facial en vivo (LFR), con el objetivo de identificar delincuentes en las calles de la ciudad. Es un sistema capaz de hacer identificación de caras a través del procesamiento de imágenes de caras de gente que pasa por la calle, de forma indiscriminada, detectando si alguna coincide con la lista almacenada de personas sospechosas de haber cometido un hecho delictivo. Durante tres años se han venido realizando pruebas preliminares, arrojando un resultado que para la policía es satisfactorio, en cuanto el sistema ha registrado aciertos en un 70 por cien de los casos (lo que es altamente peligroso si pensamos en el 30% restante), con voces críticas que han presentado un estudio independiente de la policía en el que se demostró un 81% de falsos positivos, lo que incitó que organizaciones civiles (como *Big Brother Watch*) se posicionaran contra su uso de forma indiscriminada[46], considerando que supone un ataque a los derechos de las personas[47].

La posición cautelosa de la UE ha sido constante, por los riesgos e injerencias desmedidas en los derechos fundamentales de las personas. El Reglamento IA (2024) establece en el artículo 5 las prácticas prohibidas de IA, refiriéndose en la letra h) a los sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público con fines de aplicación de la ley, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar algunos de los tres objetivos que se exponen, como excepción a la prohibición: 1°) cuando se trate de una búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas; 2°) para la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista; y 3°) para localizar o identificar a una persona sospechosa de haber cometido una infracción penal, con fines de investigación o enjuiciamiento penales o de ejecución de una sanción penal por alguno de los delitos (anexo II) que el Estado castigue con una

46 Barona Vilar, S.: *Algoritmización del derecho y de la justicia,* cit., pp. 491-492.

47 De Miguel, R.; Victoria, M.; Nadal, S.: "Londres instalará cámaras de reconocimiento facial", en El País, sábado 25 de enero de 2020, p. 3.

pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

Se exige en el Reglamento que solo se emplee para los fines expuestos, y bajo las siguientes condiciones: a) la naturaleza de la situación que permite su uso (gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema); b) las consecuencias que tendría en los derechos y libertades de las personas implicadas y, en particular, la gravedad, probabilidad y magnitud de dichas consecuencias. Además, se exige que se realice en condiciones de necesidad y proporcionalidad, de acuerdo con la legislación nacional que lo autorice, y si la autoridad encargada de la aplicación de la ley ha completado una evaluación de impacto relativa a los derechos fundamentales (en casos de urgencia cabe la utilización de estos sistemas sin registro en la base de datos de la UE, si bien se llevará a cabo sin demora). El uso de estos sistemas de identificación biométrica remota en tiempo real estará supeditado a la concesión de una autorización previa por parte de la autoridad judicial o administrativa independiente, salvo urgencia justificada, solicitándola sin demora debida, a más tardar en un plazo de 24 horas. Rechazada la autorización, se producirá la interrupción de inmediato desechándose todos los datos.

En numerosos países asiáticos[48] se ha acometido un desarrollo tecnológico para favorecer este control a través del reconocimiento facial masivo. Se dice que China es el principal banco de pruebas de esta tecnología, no solo para controlar criminales, sino para llevar a cabo una monitorización (laboral, en las escuelas, universidades, etc), para vigilar a minorías étnicas o para efectuar seguimiento de disidentes políticos. En suma, se muestra como un cauce para implementar un sistema de vigilancia policial predictiva, una monitorización de los ciudadanos, de dónde van, con quién van, qué compran, con quién hablan, si hacen deporte, si viajan mucho, y un largo etcétera. Así, con la tecnología biométrica de identificación facial se permite realizar, como ha sucedido en China, una clasificación ciudadana que, allende la funcionalidad de seguridad ciudadana, convierte a las personas en un número, un color, se le cosifica, y todo ello con ineludibles consecuencias jurídicas.

Uno de los proyectos pioneros fue el desplegado en la región china de Xinjang, en la ciudad de Tumxuk, donde los funcionarios han recogido sin consentimiento muestras de sangre de cientos de uigures como parte de una campaña de recolección masiva de ADN, siendo el objetivo de ello crear imágenes faciales exactas con la información de las muestras de ADN, una tecnología que podría emplearse contra la minoría uigur –son cerca de 11 millones de uigures los que viven en la citada región china y son una minoría predominantemente

48 Barona Vilar, S.: *Algoritmización del derecho y de la justicia,* cit., p. 493.

musulmana- así como respecto de opositores disidentes políticos. El desarrollo tecnológico se realiza en laboratorios dependientes del Ministerio de Sanidad chino con la intervención de dos científicos chinos del Ministerio financiados por la Max-Planck Society y la Erasmus University Medical Center de Holanda. Ha provocado campañas de represión gubernamental contra esta y otras minorías de la provincia, con detenciones masivas, con argumentos de lucha preventiva terrorista y del extremismo islámico. Con el sistema tecnológico chino se aúnan las bases de datos de ADN (la más grande del mundo, con más de 80 perfiles, según medios chinos), que podrían alimentar los sistemas de vigilancia masiva y reconocimiento facial simultáneamente, de manera que se mantendría un férreo control sobre la sociedad civil al permitir no solo rastrear a delincuentes, sino también a manifestantes o a disidentes, con el fin de garantizar las políticas de segregación.

La cuestión es, en suma, para qué el uso de este software que permite etiquetar a las personas, máxime cuando existe el riesgo de que el mismo sistema computacional venga inoculado de sesgos, con niveles de error que ya han sido constatados, como la confusión de 28 congresistas con sospechosos de la policía por un reconocimiento facial hecho por Amazón en 2018[49], lo que cuestiona su fiabilidad[50].

III. AHORA BIEN...NO TODO VALE.

Los desarrollos científicos y tecnológicos y su aplicación a los sistemas biométricos están empleándose en espacios privados y públicos con consecuencias más que palmarias en los derechos y libertades fundamentales. La obtención masiva de datos (excepcional o sin excepción, según el espacio geográfico del planeta), la identificación, la autenticación, la explotación de la información conductual, la clasificación o perfiles que se crean, están permitiendo construir un mundo en el que la manipulación está presente, favoreciendo la alteración de comportamientos de las personas (por ejemplo, en la toma de decisión en las elecciones políticas, en el consumo, en la cultura, etc.), la adopción de políticas represivas frente a minorías, o grupos raciales, o para pervertir políticas igualitarias, a emplear los datos alcanzados para ofrecer respuestas predictivas de riesgos (cometerá delito o reincidirá), para interferir en emociones en el lugar de trabajo, para clasificar y etiquetar a las personas -perfiles- (por raza, sexo, ideología, etc)... Son numerosas

49 Rubio, I.: "Reconocimiento facial: la tecnología que lo sabe todo", en *El País, 25 de mayo de 2019, https://elpais.com/tecnologia/2019/05/21/actualidad/1558455279_966010.html?rel=mas*. Por ejemplo, en EEUU, Amazon ensaya una aplicación de reparto que obliga al mensajero a hacerse una foto cuando entrega el paquete para cotejarla con un programa de reconocimiento facial.

50 Un estudio del Centro de Georgetown para la Privacidad y la Tecnología asegura que el reconocimiento facial utilizado por varios departamentos norteamericanos tiene mucho más margen de error con afroamericanos. Rubio, I.: "Reconocimiento facial: la tecnología que lo sabe todo", en *El País, 25 de mayo de 2019, https://elpais.com/tecnologia/2019/05/21/actualidad/1558455279_966010.html?rel=mas*.

las situaciones que van propulsando lo que Byung-Chul Han denomina como *psicopolítica digital*, que se apodera de la conducta social de las masas, o dicho de otro modo, la sociedad de la vigilancia digital, como le llama este autor, tiene acceso al inconsciente colectivo, controla y manipula posibles futuros comportamientos sociales, lo que irrefutablemente nos está llevando a sistemas totalitarios, en cuanto somos programados y controlados por una ideología que nos viene impuesta, tanto política como social[51]. Es por ello que considera que "el mercado de vigilancia en el Estado democrático se acerca peligrosamente al estado de vigilancia digital". En él vigilancia y control son una parte de la comunicación digital, si bien ese *Big Brother* lleva a que no solo sea el servicio secreto del Estado el que vigile, sino que Facebook, Apple, Amazon, Google, Huawei, los bancos, etc., actúen de espías de sus trabajadores, de sus usuarios, de sus consumidores[52]. Y mientras tanto, los habitantes del panóptico benthiano digital que somos todos vivimos con la ilusión de alimentar con más y más información, renunciando a nuestra esfera privada e íntima y exponiéndola a cambio de una ilusión de seguridad que desde luego no existe[53]. Muy probablemente concurre una suerte de inconsciencia que nos lleva a regalar datos, con un coste impredecible en los momentos en que vivimos.

Ante esta real y perturbadora situación, estamos asistiendo, por un lado, a la necesidad de un marco normativo que permita fijar límites de actuación (qué se puede hacer, hasta dónde llegar y por qué), que exige una reflexión sobre el equilibrio entre la realidad y el deseo, entre qué se puede, por qué se puede y en qué condiciones. El Reglamento de IA, en su última versión de 2024, es el que nos ofrece esa búsqueda del equilibrio entre lo prohibido y lo permitido, siempre con el debido respeto al equilibrio con los derechos y libertades fundamentales. Por otro lado, la importante labor jurisprudencial, que proviene de los tribunales (tanto el TJUE como los tribunales nacionales), así como de las autoridades administrativas de control (agencias de protección de datos en particular) está permitiendo, en tiempos de tránsito en una sociedad digital que cabalga velozmente hacia desarrollos cada vez más disruptivos, responder ante situaciones de "exceso" que truncan los límites de un modelo jurídico de derechos.

1. Punto de partida: Protección jurídica de los datos biométricos.

La necesidad de determinar que no todo vale es lo que llevó a la Unión Europea a preocuparse por establecer normativamente el equilibrio entre la seguridad y los derechos, y muy especialmente la privacidad de las personas. Así, el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea (2000/C364/01) de 18 de diciembre, otorga ese reconocimiento de derecho fundamental a la protección de

51 Han, B-CH: *En el enjambre*, Herder, 2014, pp. 108-109.

52 Han, B-CH: *En el enjambre*, cit., pp. 100-101.

53 Barona Vilar, S.: *Algoritmización del derecho y de la justicia,* cit., p. 495.

datos personales; e igualmente, el art. 16 del Tratado de Lisboa (de Funcionamiento de la UE, TFUE), defendiendo a las personas frente a posibles amenazas de la era digital, fruto de los avances científicos y tecnológicos[54]. El camino tuitivo de protección de datos proviene de la Directiva 95/46/CE, de 24 de octubre, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como en la Decisión Marco 2008/977/JAI, de noviembre de 2008, para la protección de datos personales en la cooperación policial y judicial en materia penal; derogados por el Reglamento (UE) 2016/679, de 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOUE, de 4 de mayo de 2016), que introduce reglas generales uniformes en el Derecho de la Unión[55] y la Directiva (UE) 2016/680, que rige para la protección de datos en relación con la cooperación policial y judicial al prevenir, investigar, detectar o enjuiciar delitos[56]. Sin perjuicio de otras normas que los complementan, así como la jurisprudencia del TJUE, verdadero impulsor e interpretador fundamental del derecho a la protección de datos[57], la UE garantiza el derecho a la protección de los datos personales en la UE.

Si bien inicialmente el tratamiento jurídico de los datos biométricos era el mismo que el de datos de carácter personal, la situación cambia con el Reglamento Europeo de Protección de Datos 2016/679, de 27 de abril, que los considera como "datos de carácter sensible". El art. 4.14 define los datos biométricos como "datos personales obtenidos a partir de un tratamiento técnico específico, relativo a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos". Además, los datos no personales se regulan por el Reglamento 2018/1807, relativo al marco para la libre circulación de datos no personales en la UE, aplicable desde 28 de mayo de 2018, que habrá que considerar en todo caso, máxime con difuminación entre datos personales y los no personales, debido a los

54 Sobre la incidencia de estos desarrollos puede verse: Barona Vilar,baroBbb S.: *Algoritmización del derecho y de la justicia*, cit., pp. 42-76, así como Planchadell Gargallo, A.: "Inteligencia Artificial y medidas cautelares", AAVV, *Justicia algorítmica y neuroderecho: una mirada multidisciplinar*, (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 389-419.

55 Este Reglamento deroga la Directiva 95/46/CE (RGPD) y propulsó la promulgación española de la L.O 3/2018, de 5 de diciembre, de Protección de Datos personales y garantías de los y garantía de los derechos digitales.

56 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 (DOUE, de 4 de mayo de 2016).

57 Rallo Lombarte, A.: "El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en Internet", *UNED. Teoría y Realidad Constitucional*, núm. 39, 2017, p. 584; http://revistas.uned.es/index.php/TRC/article/view/19150; y también, Piñar Mañas, J.L.; Recio Gayo, M.: *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Wolters Kluwer-La Ley, Madrid, 2018, p. 300.

desarrollos tecnológicos que nos invaden[58], que están propulsando la distinción entre datos biométricos de primera y de segunda generación. Y propicia que en ciertos casos el tratamiento de estos datos se puede hacer perfectamente sin que el titular de los datos lo perciba, lo que a su vez complica la verificación de la actuación de los responsables del tratamiento de acuerdo con la normativa de protección de datos. Este riesgo se retroalimenta con otro, la posible elaboración de perfiles, que pueden favorecer categorías o clasificaciones, camino perfecto para propiciar un estigma social.

En consecuencia, el tratamiento de los datos biométricos no será en todos los casos igual (así se pronunció también el TEDH en la Sentencia de 4 de diciembre de 2008, caso "Marper"), de modo que habrá que estar al grado de injerencia de cada uno. En todo caso, habrá que respetar los principios de necesidad, idoneidad y proporcionalidad en el tratamiento, así como la adopción de determinadas medidas de seguridad basadas en cifrado y en control de acceso de acuerdo con la finalidad de obtención de los datos biométricos: control de presencia, identificación, control de la información o control de acceso. Se establece la necesidad de medidas concretas en caso de datos sensibles, almacenándose en plantillas biométricas, no almacenamiento centralizado de los datos, sino en dispositivos cifrados, recomendándose que se supriman los datos biométricos de forma automática cuando se cumpla el tiempo necesario para el fin por el que se recogieron. Y se establece la obligación del responsable del tratamiento de establecer un protocolo de control de acceso que registre qué persona ha accedido a los datos, fecha y hora en que se accedió y los datos a los que se ha accedido.

Por su parte, el art. 9 del Reglamento configura unos requisitos, como son la necesidad de que exista consentimiento explícito en un documento donde se especifique la finalidad para la que se obtienen esos datos biométricos, así como la evaluación de impacto sobre los datos y, por supuesto, el debido registro de actividades de tratamiento (como mínimo: nombre y datos de contacto – responsable, corresponsable, representante del responsable, delegado de protección de datos-, fines del tratamiento, descripción de las categorías interesados y de las categorías de datos personales, así como de los plazos previstos para la supresión de las diferentes categorías de datos).

El gran dilema que se nos presenta como sociedad es manejar adecuadamente las excepciones que permiten la injerencia en los derechos y libertades de las personas a través de sus datos (biométricos). El entorno que nos rodea, en el que hay una clara cesión de garantías y derechos como respuesta "necesaria(?)" para

58 Muñoz ruiz, A.B.: *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones jurídico-laborales,* Ed. Tirant lo Blanch, Valencia, 2023, p. 25.

garantizar la "seguridad", nacional e internacional, del Estado, el interés público, el orden público (conceptos indeterminados que exigen concreción), nos lleva al punto de partida, generado con la irrupción de la tecnología disruptiva, el albor algorítmico y la inteligencia artificial, que no es otro que el "humanismo está en retirada", como señala Lasalle[59], fruto de esa fascinante servidumbre maquínica, que nos convierte en proletariado digital. Es imprescindible configurar contrapesos a esa atractiva y fascinante emergencia tecnológica. Los medios existen: los límites legales y éticos, nacionales y supranacionales, la función tuitiva de los tribunales, y la mirada crítica de los investigadores.

2. La teoría nos la sabemos, pero qué sucede en la práctica.

El equilibrio entre lo posible y lo refutable lo tenemos claro y la Unión Europea y los diversos Estados miembros han hecho un gran esfuerzo por fijar un marco de permisibilidad versus restricción de la utilidad de los datos biométricos. Los tribunales están velando igualmente por mantener ese equilibrio. Sin embargo, los desafíos son enormes y la expansión de su usabilidad ha venido aflorando situaciones alarmantes. Si bien es palmario que el marco normativo ha esclarecido con carácter general los límites inquebrantables cuando de datos biométricos se trata, la práctica nos ofrece algunos casos que merecen tomarse en consideración.

A) Seguridad frente a la sofisticada criminalidad, derivada de la globalización.

En los albores del siglo XXI asistimos a una metamorfosis del planeta, de la mano de la globalización, que propulsó una transformación social, económica, cultural, social, sociológica, ideológica, etc., alterando los modelos de Estado configurados a lo largo del siglo XX. La globalización cambió los Estados (minimizados ante una economía que devora la política) y el significado de las fronteras. Esta mutación favoreció la movilidad para lo bueno y para lo malo, favoreciendo igualmente una proliferación de la criminalidad, también en cuanto a su sofisticación, aflorando la delincuencia organizada y el terrorismo internacional. Surgieron motivos de seguridad y orden público que desequilibran la balanza en desfavor de los derechos de la persona y, por supuesto, del derecho a la protección de datos personales. Comenzó el tratamiento masivo de los datos para favorecer el intercambio de información en materia de cooperación entre autoridades policiales y judiciales europeas y su transferencia a terceros países[60].

59 Lasalle, J.M.: *Ciberleviatán*, Barcelona, Ed Arpa, 2019, p. 50.

60 Sobre estas cuestiones Gutiérrez Zarza, A.: "Terrorismo yihadista, crisis migratorias, fronteras, prueba electrónica, encriptado, referéndum y otras palabras clave del espacio LSJ", en *Diario La Ley, Sección Tribuna*, núm. 8904, 2016, http://diariolaley.laley.es/home/DT0000240761/20170111/Terrorismo-yihadista-crisis-migratorias-fronteras- prueba-electronica-encriptado-, acceso el 3 de febrero de 2024.

Son ya múltiples las herramientas "asimétricas" y "heterogéneas" que desequilibran esa protección de datos enmarcada en las normas expuestas: SIS (Sistema de Información de Schengen) y SIS II (Sistema de Información de Schengen de segunda generación); EURODAC; VIS (Sistema de Información de Visados); API (Información Previa sobre Pasajeros); SIA (Sistema de Información Aduanero); PRÜM I y II[61] (Instrumentos de la UE para prevenir y combatir el terrorismo y otras formas graves de delincuencia transfronteriza, que intercambian ADN, datos dáctiloscópicos, registros de matriculación de vehículos y datos personales y no personales relacionados con la cooperación policial transfronteriza); ECRIS (Sistema de Información Europeo de Antecedentes Penales[62]); Registro de Nombres de Pasajeros (PNR)[63]; Programa de seguimiento de la financiación del terrorismo, además de generar Unidades y Organismos (de Información Financiera; de Recuperación de Activos; Europol; Eurojust para cooperación en investigaciones y actuaciones relativas a la delincuencia grave que afecta al menos a dos Estados miembros).

El equilibrio entre la protección de los datos, como derecho fundamental, y la lucha contra la criminalidad, por otro, está propulsando en el seno de la UE acciones que comportan la necesidad de actuar por motivos de interés público y en deterimento del interés individual o colectivo de la ciudadanía. Hay excepciones por motivos de "seguridad", bajo el debido respeto a la proporcionalidad, amén de-según la Directiva de protección de datos en el ámbito penal- una necesidad indiscutible y autorización, ora de las autoridades nacionales ora de las europeas, además de concurrir en su tratamiento y uso las garantías adecuadas. Esa naturalización de "excepcionalidad" es lo que se otorga en el Reglamento IA (AI Act 2024), delimitando las prohibiciones y sobre todo configurando los supuestos en que de forma excepcional y bajo determinadas condiciones, podría justificarse el empleo de sistemas algorítmicos y de inteligencia artificial que traspasen las barreras de la protección de datos configurada en la UE y reforzada por la Carta de Derechos Fundamentales de la UE. En todo caso, la excepcionalidad debe interpretarse restrictivamente, siendo un habitat adecuado cuando se pretende luchar contra la delincuencia organizada y el terrorismo.

61 Reglamento (UE) 2024/9823 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, relativo a la búsqueda y al intercambio automatizado de datos para la cooperación policial, y por el que se modifican las decisiones 2008/615/JAI y 2008/616/JAI del Consejo y los reglamentos (UE) 2018/1726 (UE) 2019/817 y (UE) 2019/818 del Parlamento Europeo y del Consejo (Reglamento Prüm II).

62 ECRIS permite el intercambio de información, a través de una red segura, sobre las condenas pronunciadas contra una persona determinada por los órganos jurisdiccionales penales en la Unión Europea; información de identificación alfanumérica, aunque es posible el intercambio de datos biométricos. Comisión Europea: "Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad", COM (2016) 205 final, de 14 de septiembre de 2016.

63 Catalina Benavente, M.A.: "La recogida y tratamiento masivo de los datos PNR: algunas cuestiones para preocuparse", en AAVV, *Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad, (*ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2019, pp. 279-295.

El Parlamento Europeo ha aprobado la creación de una base de datos biométricos de huella dactilar o de la cara del usuario de los más de 500 millones de habitantes de la UE; una base de datos centralizada que incluirá la información habitual (nombre, dirección, fecha de nacimiento y número de identidad) y datos biométricos de la huella dactilar o de la cara del usuario (con foto incluida), y escaneos faciales. Esta nueva base de datos se denomina *Common Identity Repository (CIR)*[64], que unificará los registros de 500 millones de ciudadanos de la UE, estando a disposición de las fuerzas de seguridad, incluidas las responsables de los pasos fronterizos de los países miembros[65].

B) Algunos Proyectos nacionales e internacionales en marcha con datos biométricos. Dudas.

Existe igualmente un proyecto piloto en Menorca en virtud del cual se permite (Aena así lo ha aprobado con Air Europa) subirse al avión mediante reconocimiento facial utilizando detectores biométricos. Es un sistema que pretende, por un lado, de forma más ágil y rápida identificar la persona física que quiere subir al avión con el que es portador del billete. Si su empleo fuere solo para identificar al pasajero, podría aceptarse como medida piloto, empero plantea dudas cuando el sistema va más allá, detectando estados de ánimo, de salud, ADN del pasajero y un largo etcétera que vienen a generar información sensible de las personas que no deben ni pueden ser almacenadas, clasificadas, y explotadas. Para que se tratara de una finalidad lícita se requiere el consentimiento del viajero[66]. Y, en todo caso, debe evitarse el sistema de tarjeta o crédito social, prohibido en el art. 5 Reglamento IA.

La discusión está en la explotación que puede efectuarse de los datos sensibles que se obtienen a través de estas tecnologías biométricas, o si se quiere, los fines pretendidos por quienes realizan estas acciones. En China, por ejemplo, se permite el uso de gafas con reconocimiento facial y ADN, piel, comportamiento de movilidad, etc., para identificar sospechosos (no necesariamente de delitos, sino también de acciones políticamente inapropiadas o contrarias al régimen). En China existe el sistema de crédito social, denominado *scoring,* que es un instrumento que utiliza el *big data* para calificar el comportamiento de los usuarios, de manera que las personas con bajo crédito social tienen prohibido adquirir billetes de tren y de avión; o permiten detectar en las escuelas el absentismo escolar, y en Shangai se habla de incorporar en los autobuses un sistema de reconocimiento facial

64 "EU Interoperability framework for border management systems. Secure, Safe and Resilient Societies", 5 junio 2018, Brussels, European Commission, https://www.securityresearch-cou.eu/sites/default/files/02.Rinkens.Secure%20safe%20societies_EU%20interoperability_4-3_v1.0.pdf. El CIR unificará la información contenida en sistemas como Schengen Information System, Eurodac, Visa Information System (VIS), European Criminal récords System (ECRIS-TCN), Entry/Exit System (EES) y European Travel Information and Authorisation System (ETIAS).

65 Una medida que ya funciona en los principales aeropuertos de EEUU, China, India.

66 Barona Vilar,baroBbb S.: *Algoritmización del derecho y de la justicia*, cit., p. 498.

que detecte la fatiga de los conductores (en algunos automóviles de tecnología avanzada ya existe en Europa). O, en los baños públicos del Cielo de Pekín, se usa una máquina que escanea el rostro del usuario, le dispensa de un trozo de papel higiénico de 60 centímetros de longitud y no le permite volver a usar más hasta que han pasado nueve minutos[67].

En ciertos casos, la vulneración de derechos por el uso de reconocimiento facial sin consentimiento podría justificarse por razones de interés o seguridad públicos, por ejemplo, para la detención de terroristas, como sucedió durante la marathon de Boston en 2013, o en supuestos como, por ejemplo, la búsqueda de desaparecidos[68]. Además, desde el punto de vista de salud, desde el Instituto de Genoma Humano se están utilizando estas técnicas para detectar algunas enfermedades genéticas raras[69].

C) Worldcoin, el proyecto de escaneo del iris a cambio de criptomonedas; un negocio redondo a costa de datos biométricos.

La situación de nebulosa en la que transitamos, a pesar del marco normativo, ha llevado a algunas empresas tecnológicas a aprovechar la coyuntura para "negociar" con los datos biométricos, todo y que amparadas en el "consentimiento". Un ejemplo paradigmático reciente es la prohibición por la Agencia de Protección de datos del denominado Proyecto "Worldcoin" de escaneo del iris. Más de 300.000 personas en nuestro país han participado en el mismo, con la finalidad de crear una identidad digital única, siendo su contraprestación otorgar, por la entidad "Tools for Humanity", "tokens" o criptomonedas WLD, que pueden almacenarse o intercambiarse por dinero u otras criptomonedas a través de Internet. Esta entidad, con sede en San Francisco y en Berlín, fue fundada por el CEO de OpenAI, Sam Altman.

Worldcoin utiliza "orbes" esféricos para escanear el iris de los usuarios, proporcionándoles una identidad digital registrada en la blockchain de Worldcoin, actuando como un registro en el que se almacenan todas las transacciones, saldos e intercambios dentro de la red "Worldcoin"; transacciones que se agrupan en bloques (es algo similar a Bitcoin o Ethereum). Con este sistema se garantiza que en las operaciones económicas hay un humano y no un robot realizando las transacciones.

67 Rubio, I.: "Reconocimiento facial: la tecnología que lo sabe todo", en *El País, 25 de mayo de 2019,* https://elpais.com/tecnologia/2019/05/21/actualidad/1558455279_966010.html?rel=mas.

68 "Indian Police trace 3.000 missing children in just four days using facial recognition Technology", en *Independent, 24 de abril de 2018,* https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html. O también en relación con niños desparecidos puede verse http://missingchildreneurope.eu/facts&figures.

69 Barona Vilar,baroBbb S.: *Algoritmización del derecho y de la justicia*, cit., p. 499.

Las dudas éticas y de transparencia del consentimiento han llevado a cuestionar esta acción empresarial, que comporta la recopilación de datos biométricos sensibles, sin garantías respecto de un posible uso indebido y la protección de la información personal, amén del carácter irreversible del intercambio de datos a cambio de criptomonedas, aun cuando la empresa ha manfiestado en diversos momentos que cualquier persona puede revocar el consentimiento sobre sus datos biométricos. A mayor abundamiento, se ha detectado una alta participación de menores de edad en el proyecto sin la debida autorización. Y en muchos casos, los usuarios no tienen claro en qué consiste esa cesión de datos biométricos a partir del escaner del iris (Orb), interesándose tan solo por la contraprestación que se obtiene.

Las derivaciones de esta cesión de datos biométricos, en este caso a través del iris, puede integrar incluso datos acerca de la salud de una persona, lo que podría, si se explotaren o vendieren los datos, derivar en consecuencias tales como no asegurar a la persona por padecer alguna enfermedad o denegarle un transplante por esta misma razón, entre otras.

Se trata, en suma, de la posible obtención de datos biométricos sensibles, con apariencia de consentimiento del donante, todo y que en muchos casos sin que se tenga conocimiento de las consecuencias que pueden derivarse, con enormes líneas rojas que no pueden ni deben traspasarse.

Ante la situación descrita, la Agencia Espanola de Protección de datos ha exigido en marzo de 2024 el cese en la recogida y tratamiento de categorías especiales de datos personales así como el bloqueo de los recopilados. Decisión que fundamenta en el consentimiento insuficiente, la imposibilidad de retirar el consentimiento y en la captación de menores, por lo que solicita el cese inmediato del tratamiento, para prevenir la cesión de datos a terceros y la salvaguarda del derecho funbdamental a la protección de datos personales. Esta prohibición temporal de la actividad en Espana tiene un periodo de validez máximo de tres meses. La medida cautelar se fundamenta en el Reglamento General de Protección de Datos, que considera el tratamiento de los datos biométricos como de especial protección, dados los riesgos y potenciales daños irreparables que conlleva para los derechos de las personas. La decisión de la AEPD fue recurrida a la Audiencia Nacional, quien ha rechazado el recurso, sosteniendo que "ateniendo a la ponderación de los intereses en conflicto y, a la vista de las circunstancias concurrentes, debe prevalecer la salvaguarda del interés general que consiste en la protección de datos personales de los interesados frente al interés particular de la empresa recurrente de contenido fundamentalmente económico"[70].

70 https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Audiencia-Nacional/Oficina-de-Comunicacion/Notas-de-prensa/La-Audiencia-Nacional-avala-el-cese-cautelar-de-la-recopilacion-de-datos-a-traves-del-iris-de-Worldcoin-acordado-por-la-Agencia-de-Proteccion-de-datos.

D) Utilización biométrica en entradas y salidas empresariales y otros fines laborales.

Hemos venido reiterando que los datos biométricos pueden utilizarse solo si son adecuados, pertinentes y no excesivos, ateniendo a la necesidad, propocionalidad de los datos tratados y si la finalidad prevista podría alcanzarse mediante un medio menos intrusivo. Y hemos encontrado exponentes en diversos ámbitos en los que el desarrollo tecnológico, en sentido maximalista, ha ido convirtiendo también el cuerpo humano en una suerte de espacio de computación, lo que favorece e impulsa las posibilidades de control. Precisamente, en el ámbito laboral surgen situaciones cada vez más sofisticadas, en las que la integración de algoritmos, inteligencia artificial y robótica inciden cada vez más, favoreciendo el uso de sistemas biométricos en el mundo del trabajo. En unas ocasiones, para favorecer los registros de la jornada laboral (en el primer estadio se empleaba la huella digital), para ir poco a poco incorporando sistemas de biometría vocal (especialmente en los supuestos de teletrabajo), el control a través de retina o iris o el reconocimiento facial. Incluso se habla en los últimos tiempos del uso de los latidos del corazón como herramienta biométrica. Todos ellos como sistemas de individualización y también de control (por ejemplo, para verificar el cumplimiento de la prestación laboral o incluso para implantar medidas de seguridad frente a riesgos graves)[71].

También en el ámbito laboral el uso o mal uso por el empresario de los sistemas biométricos puede traer consecuencias diversas, y sobre todo debe tomarse en consideración cuanto se ha venido exponiendo sobre la necesidad, proporcionalidad y fines pretendidos. Curiosa es la reciente Sentencia del Juzgado de lo Social n 2 de Alicante 190/2023, de 15 de septiembre (REC 489/2023), que declaró la vulneración del derecho a la intimidad personal y familiar y a la propia imagen del trabajador por la utilización de su información biométrica sin su consentimiento para el fichaje de entrada y salida, condenando a la empresa a una indemnización moral de más de seis mil euros. El trabajador solo había autorizado a la empresa el uso de sus derechos de imagen para publicaciones en páginas web y redes sociales, propiedad de la empresa, campañas, revistas, publicaciones, folletos, publicidad corporativa y demás materiales de apoyo, pertinentes para la difusión y promoción de la actividad de la empresa, pero no había autorizado que la empresa realizara una fotografía de la cara de los empleados desde un dispositivo de "entrea" y que esa imagen fuera usada para fichar la entrada y la salida en el puesto de trabajo; de hecho, el trabajador manifiesta que ni siquiera fue informado del uso de los datos biométricos.

71 Un desarrollo *ad extensum* acerca del uso de estso sistemas biométricos en el mundo laboral y el posible control del empresario, puede verse en Muñoz ruiz, A.B.: *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones jurídico-laborales,* Tirant lo Blanch, Valencia, 2023.

En suma, hemos venido reiterando que la tecnología no es buena ni mala, pero es palmario que no es neutra, y el uso de los sistemas biométricos tampoco lo es. El gran dilema de la sociedad actual se halla en ese proletariado digital que nos asiste, en el que hemos aceptado sin resistencia el cambio de moneda: los datos, nuestros datos, personales y no personales, físicos, fisiológicos y conductuales, que concedemos, en muchas ocasiones de forma inconsciente o irreflexiva, a cambio de información, de comodidad, de bienes o de seguridad. Forma parte de la herencia de la globalización, que nos ha venido inoculando *un modus operandi* de masas, acrítico, en el que aceptamos el control, la categorización, los perfiles, la vigilancia predictiva masiva, la efectividad, la inmediatez, a cambio de "nosotros". El uso de este *Big data* se expande a todo, al sector público, al sector privado y al sector empresarial, y muy especialmente con consecuencias en la Justicia, en los principios procesales, en la prueba y en la decisión judicial; Biometría, algoritmos e inteligencia artificial se convierten en un magnífico coctel del eficientismo, si bien... No todo vale.

BIBLIOGRAFÍA

Abs, M.: "Biometrik", en *Historisches Wörterbuch der Philosophie,* (ed. por J. Ritter, J.; K. Gründer; G. Schwabe), AG Verlag, Basel, 1971.

Agencia española de protección de datos: *14 equívocos en relación con la identificación y autenticación biométrica,* 2020, https://www.aepd.es/guias/nota-equivocos-biometria.pdf.

Barona Vilar,baroBbb S.: *Algoritmización del derecho y de la justicia: de la Inteligencia Artificial a la Smart Justic*e, Tirant lo Blanch, Valencia, 2021.

Boulgouris, N. V. et alt.: *Biometrics, Theory, Methods, and Applications*, IEEE and WILEY, Estados Unidos, 2010.

Caneppele, S.; Ribeaux, O.: "Forensic intelligence", *"The Routledge International Handbook of Forensic Intelligence and Criminology",* Routledge, 2017.

Catalina Benavente, M.A.: "La recogida y tratamiento masivo de los datos PNR: algunas cuestiones para preocuparse", en AA.VV.: *Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad, (*ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2019.

Clouston, T. S: "The Developmental Aspects of Criminal Anthropology", *The Journal of the Antropological Institute of Great Britain and Ireland*, vol. 23.

De Miguel, R.; Victoria, M.; Nadal, S.: "Londres instalará cámaras de reconocimiento facial", El País, sábado 25 de enero de 2020.

Díaz Rodríguez, V.: "Sistemas biométricos en materia criminal: un estudio comparado", *Revista IUS vol. 7, núm. 31,* Puebla, enero-junio 2013, en http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100003.

Ecured: "Biometría por ADN", en https://www.ecured.cu/Biometr%C3%ADa_por_ADN

Escajedo San Epifanio, L.: *Reconocimiento e Identificación de las personas mediante Biometrías estáticas y dinámicas,* Tesis Doctoral, Alicante, diciembre 2015, *open Access*.

Etxeberría Guridi, J.F.: "Obtención de perfiles de ADN a la luz de la nueva Orden Europea de Investigación (OEI): diversas alternativas", AAVV, *Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad*, (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2019.

Etxeberría Guridi, J.F.: "Sistemas biométricos (el reconocimiento facial en particular) y sus aplicaciones", AAVV *Inteligencia Artificial y Administración de Justicia*, (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Thomson Reuters-Aranzadi, Cizur Menor (Navarra), 2022.

Ferrer, C.: "¿Cómo cumplir el RGPD si manejas datos biométricos?", en *https://protecciónd atos-lopd.com/empresas/datos-biometricos-rgpd/,* 9 de julio 2018.

Ferri, E.: *Principios de Derecho Criminal,* Ed. Reus, Madrid, 1933.

Galton, F.: " Spirit of Biometrika", editorial del número primero de la Revista *Biometrika*, 1901.

García, J.G.: "El reconocimiento facial aprende a identificar mascarillas", *Retina, El País Economía,* mayo 2020.

Gargantilla, P.: "Puedes acabar en la cárcel por la huella de tu oreja", publicado el 26 de mayo de 2019 en https://www.abc.es/ciencia/abci-puedes-acabar-carcel-huella-oreja-201905260149_noticia.html

Garófalo, R.: *La criminología. Estudio sobre el delito y sobre la teoría de la represión,* Analecta Editorial, 1900.

González Sánchez, M.E.: *Análisis biométrico de las orejas,* Tesis Doctoral, Departamento de Informática y Sistemas, Universidad de Las Palmas de Gran Canaria, 2008, p. 6, en https://accedacris.ulpgc.es/bitstream/10553/3435/1/Analisis_biometrico_orejas.pdf

Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales (markt/12168/02/es wp 80): *Documento de trabajo sobre biometría*, adoptado el 1 de agosto de 2003, https://www.informatica-juridica.com/documento-trabajo/documento-trabajo-biometria/.

Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales: Agencia espanola de protección de datos, *Dictamen 3/2012 sobre la evolución de las tecnologías biométricas* de 27 de abril de 2012 (WP193), https://www.aepd.es/documento/wp193_es.pdf.

Gutiérrez Zarza, A.: "Terrorismo yihadista, crisis migratorias, fronteras, prueba electrónica, encriptado, referéndum y otras palabras clave del espacio LSJ", *Diario La Ley, Sección Tribuna*, núm. 8904, 2016, http://diariolaley.laley.es/home/DT0000240761/20170111/Terrorismo-yihadista-crisis-migratorias-fronteras-prueba-electronica-encriptado-.

Han, B-CH: *En el enjambre,* Herder, Barcelona, 2014.

Instituto nacional de ciberseguridad (incibe): *Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario,* 2016, en https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

Jiménez, M.: "Open AI lanza una herramienta de audio capaz de clonar las voces humanas", *El País* 30 de marzo de 2024.

Lasalle, J.M.: *Ciberleviatán*, Ed Arpa, Barcelona, 2019.

Muñoz ruiz, A.B.: *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones jurídico-laborales,* Ed. Tirant lo Blanch, Valencia, 2023.

Pérez Colomé, J.: "Marbella, el mayor laboratorio de videovigilancia de España", *El País, 22 de noviembre de 2019*, https://elpais.com/tecnologia/2019/11/21/actualidad/1574348695_231540.html.

Piñar Mañas, J.L.: Recio Gayo, M.: *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Wolters Kluwer-La Ley, Madrid, 2018.

Planchadell Gargallo, A.: "Inteligencia Artificial y medidas cautelares", en AA.VV.:*Justicia algorítmica y neuroderecho: una mirada multidisciplinar,* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021.

Prasanthi Jasmine, K.; Naga Prakash, K.: *Reconocimiento de emociones humanas a partir de imágenes de rostros*, Ed. Nuestro Conocimiento, 2021.

Rallo Lombarte, A.: "El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en Internet", *UNED. Teoría y Realidad Constitucional*, núm. 39, 2017.

Romero Moreno, M.: *Reconocimiento del Andar Humano basado en ensamble de clasificadores utilizando silueta y contorno*, Tesis de Maestría, Instituto Nacional de Astrofísica, Óptica y Electrónica, Tonantzinla, Puebla, 2008, en https://inaoe.repositorioinstitucional.mx/jspui/bitstream/1009/558/1/RomeroMM.pdf.

Ruane Dawson, M.: *Gait Recognition. Final Report,* Department of Computing Imperial College of Science, Technology and Medicine, Londres, 2002.

RUBIO, I.: "Reconocimiento facial: la tecnología que lo sabe todo", *El País, 25 de mayo de 2019, https://elpais.com/tecnologia/2019/05/21/actualidad/1558455279_966010.html?rel=mas.*

SADIN, E.: *La humanidad aumentada,* Ed Caja Negra, 2017.

STIGLER, S.M.: "The Problematic Unity of Biometrics", Revista *Biometrics*, 2000.