TESIS DOCTORAL

2019

“DATOS PERSONALES BIOMÉTRICOS DACTILOSCÓPICOS Y DERECHOS FUNDAMENTALES: NUEVOS RETOS PARA EL LEGISLADOR”

JUANA MARÍA DOMAICA MAROTO

PROGRAMA DE DOCTORADO EN DERECHO Y CIENCIAS SOCIALES

DIRECTORA: DÑA. ELENA GARCÍA-CUEVAS ROQUE

AGRADECIMIENTOS

A mi directora, Dña. Elena García-Cuevas, por su apoyo y ayuda constante a lo largo de todo el trabajo; sin ella no hubiera sido posible concluirlo en modo alguno. A Dña. Remedios Morán, por su comprensión y generosidad en este largo camino hacia el Doctorado.

A mis compañeras y amigas de la Facultad de Ciencias Económicas y Empresariales de la Universidad CEU-San Pablo, que siempre han estado conmigo: las profesoras Cristina Aguirre, M. Carmen García Centeno, Elena Inchausti, Virginia Ruiz y Marta Gutiérrez.

Y muy especialmente a mi madre, porque, sin ella, no sería posible la vida.

DATOS PERSONALES BIOMÉTRICOS DACTILOSCÓPICOS Y DERECHOS FUNDAMENTALES: NUEVOS RETOS PARA EL LEGISLADOR

ÍNDICE

Índice Abreviaturas

AEPD	Agencia Española de Protección de Datos.
CDFUE	Carta de Derechos Fundamentales de la UE.
CEDH	Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales hecho en Roma el 4 de noviembre de 1950.
CNIL	Commission nationale de l'informatique et des libertés.
ET	Estatuto de los Trabajadores.
GPD 29	Grupo de Protección de Datos del artículo 29.
IO	Internet de los Objetos, Internet de las cosas.
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE núm. 298, de 14 de diciembre de 1999.
LORTAD	Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal.
PRGPD	Propuesta de Reglamento del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, de 25 de enero de 2012.
RGPD	REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOUE 04/05/2016 L 119.
RLOPD	Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.
STC	Sentencia del Tribunal Constitucional
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TJUE	Tribunal de Justicia de la Unión Europea

T-PD	Comité Consultivo de la Convención para la protección de las personas respecto al proceso automatizado de los datos de carácter personal del Consejo de Europa.
TSJ	Tribunal Superior de Justicia
UE	Unión Europea.
WP-DP	*Working Party on Data Protection* (Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales del artículo 29).

Introducción

Vivimos en un mundo globalizado, tan extenso como sus propios confines, donde todos podemos establecer relaciones públicas o privadas en cualquier punto del planeta. Podemos, incluso, hablar de una internacionalización de nuestra vida de relación. El intercambio o flujo de información es global, mundial, y reiteradamente así lo han manifestado los Comisarios de Protección de Datos en distintas conferencias internacionales como, por ejemplo, en la 27 Conferencia Internacional de Montreaux donde expresamente reconocen que "[…] el desarrollo de la sociedad de la información está dominado por la globalización del intercambio de información, el uso de tecnologías de procesamiento de datos progresivamente intrusivas y el incremento de medidas de seguridad"[1]. En este contexto parece evidente que la necesidad de identificación fiable de las personas se hace imprescindible; necesidad de identificación que tanto se hace ineludible en el ámbito público como en el privado, donde la persona desarrolla los distintos aspectos de su vida, como se verá más adelante. En este contexto, la biometría aporta una tecnología que permite la verificación masiva y fiable de individuos, pero, al mismo tiempo, el uso de esas tecnologías "progresivamente intrusistas*"*, de las que habla la declaración de Montreaux, abre un abanico de implicaciones para los derechos individuales, que debe ser analizado con la suficiente profundidad.

I. Delimitación y planteamiento del problema.

Lo anteriormente expuesto queda claramente recogido en el informe de situación elaborado por el Comité Consultivo[2] (en adelante, T-PD) creado por el Convenio 108

[1] Declaración de Montreux "La protección de datos personales y de la intimidad en un mundo globalizado: un derecho universal que respeta diversidades". 27th International Conference of Data Protection and Privacy Commissioners. 14-16 septiembre de 2005. Texto disponible en la URL: http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_s.pdf. [Fecha de consulta: 12/03/2017].

[2] Consejo de Europa. Comité Consultivo de la Convención para la protección de las personas respecto al proceso automatizado de los datos de carácter personal (T-PD). Informe de Situación relativo a la aplicación de los Principios de la Convención 108 a la recogida y al proceso de los datos biométricos. Elaborado por el T-PD en su 21ª reunión (Estrasburgo, 2-4 de febrero de 2005). T-PD (2005) BIOM F. http://www.agpd.es/portalwebAGPD/canaldocumentacion/textos_interes/common/pdfs/informe-principios-convencion-108.pdf [Fecha de consulta: 12/03/2017]. El Comité está formado por un representante de cada uno de los Estados que ratifica el Convenio. Así mismo, este Comité carece de competencias ejecutivas y/o de control siendo su función primordial presentar propuestas de mejora en la aplicación del Convenio 108. Muchas de las competencias de este Comité se han trasladado a las

para la protección de las personas respecto al proceso automatizado de los datos de carácter personal del Consejo de Europa de 28 enero 1981.

Es fácil imaginar las necesidades de identificación que se plantean, en el ámbito público y de seguridad del ciudadano, por ejemplo, en la lucha contra el terrorismo internacional y la importante ayuda que pueden proporcionar los sistemas biométricos de identificación y/o verificación[3].

Todos los ciudadanos tenemos derecho a la seguridad (artículo 17.1 CE) y las Fuerzas y Cuerpos de Seguridad del Estado tienen como labor fundamental la garantía de dicho derecho. En el desarrollo de esta labor, es indudable que es fundamental disponer de información[4]. Ésta, y como resultado de una investigación o de una elaboración, es imprescindible para el desarrollo de las tareas de seguridad[5].

Como consecuencia de lo dispuesto en el artículo 3.2 del Tratado de la Unión Europea ya se han creado en el seno de la Unión Europea (en adelante UE) distintos organismos y sistemas (Europol, Eurodac, sistema VIS, Sistema de Información Schengen, etc.) que tienen como objetivo agilizar y propiciar un mayor flujo de información dentro del ámbito territorial de la aquélla, garantizando así un espacio de libertad, seguridad y

autoridades de control nacionales y a otros órganos de la Unión Europea. Cfr. REBOLLO DELGADO, L., *Vida Privada y Protección de datos en la Unión Europea*, Madrid, Dykinson, 2008, pp.149-150.

[3] En este sentido deseamos reproducir parte del Preámbulo de la LO 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN: "La sociedad viene exigiendo que las autoridades, judiciales y policiales, encargadas de la persecución de los delitos, cuenten con los instrumentos de investigación más eficientes posibles, especialmente en la lucha contra aquellos crímenes que generan mayor alarma social. Finalmente, no puede olvidarse que la creciente globalización de los delitos y la paralela asunción por parte de España de una serie de obligaciones recíprocas con otros países para compartir la información disponible en los respectivos ficheros y bases de datos exigen la adopción de las medidas materiales y jurídicas adecuadas".

[4] ÁLVAREZ GARCÍA, F. J., *El acceso por parte de las fuerzas y cuerpos de seguridad del Estado a ficheros de datos personales. Protección de Datos y proceso penal*, Madrid, La Ley, 2010, pp. 53 y ss. Debemos distinguir entre dato e información; se puede considerar los datos como el antecedente o noticia previa que sirve de punto de partida de la investigación de la verdad. Un concepto distinto es el de información en el sentido de dato o datos estructurados para responder a determinados fines, para la orientación de la solución de un problema concreto. Ese dato estructurado y orientado a un fin determinado ya se ha convertido en información. Vid. DAVARA RODRÍGUEZ, M.A., *Manual de Derecho Informático*, Pamplona, Aranzadi, 1997.

[5] En el ámbito de la Unión Europea ya se ha planteado de manera explícita la necesidad de cooperación internacional en el control de fronteras exteriores y en materia de asilo y todo ello partiendo de lo dispuesto en el artículo 3.2 del Tratado de la Unión Europea: "La Unión ofrecerá a sus ciudadanos un espacio de libertad, seguridad y justicia sin fronteras interiores, en el que esté garantizada la libre circulación de personas conjuntamente con medidas adecuadas en materia de control de fronteras exteriores, asilo, inmigración y de prevención y lucha contra la delincuencia". Versión consolidada del Tratado de la Unión Europea. Diario Oficial de la Unión Europea (DOCE) 30.3.2010. C83/13-45. https://www.boe.es/doue/2010/083/Z00013-00046.pdf [Fecha de consulta: 12/03/2017].

justicia. Y es dentro de alguno de estos sistemas donde la obtención y tratamiento de muestras y datos biométricos se está revelando como un coadyuvante esencial a dichos fines[6].

Pero también es cierto que la elección, en el sentido de incorporación, de la biometría en un sistema de información no es una elección intranscendente, sino muy al contrario plantea importantes cuestiones de orden técnico y jurídico. Ya el Supervisor Europeo de Protección de Datos, en el año 2006, advirtió que el uso de la biometría en un sistema de información cambia definitivamente la relación entre cuerpo e identidad, de tal forma que las características del cuerpo humano pasan a ser objetos legibles susceptibles de uso posterior[7]. En el orden jurídico son de trascendental importancia las cuestiones relacionadas con los derechos de la personalidad, derechos humanos o derechos fundamentales, desde una perspectiva constitucional, que pueden verse afectados.

---

[6] Piñar Mañas, en comparecencia ante las Cortes Generales en septiembre de 2005, ya manifestó expresamente la relevancia práctica del uso de datos biométricos y, así mismo, apuntó riesgos para los derechos individuales: "El tratamiento de datos biométricos ha constituido una de las preocupaciones más importantes de las autoridades de protección de datos personales. Desde el año 2003, año en que el grupo de trabajo del artículo 29 adoptó un documento sobre biometría se ha mantenido una reflexión permanente sobre esta materia cuya última manifestación ha tenido lugar en la reiteradamente citada 27 Conferencia Internacional de Montreaux. En ella se aprobó una propuesta de resolución que hace especial hincapié en el uso de los datos biométricos en pasaportes, documentos de identidad y documentos de viaje. La resolución advierte sobre los riesgos de que los datos biométricos puedan llegar a ser recabados sin que el ciudadano se dé cuenta de ello, de que tales datos posibiliten que el cuerpo humano sea legible por una máquina y de que la información biométrica pueda ser utilizada como identificador único. Por ello, se exige: Primero, la implantación de garantías efectivas, desde el inicio, para limitar los riesgos inherentes a la naturaleza de la biometría; segundo, la estricta distinción entre datos biométricos recabados y almacenados con fines públicos —por ejemplo, control fronterizo—, de acuerdo con imperativos legales, y datos biométricos recabados con fines contractuales, con obtención del consentimiento; tercero, la restricción técnica del uso de la biometría en pasaportes y tarjetas de identidad, con fines de control, comparando los datos del documento con los datos proporcionados por el titular en la presentación del documento". Cfr. Cortes Generales, Diario de Sesiones del Congreso de los Diputados. Comisiones. Año 2005 VIII Legislatura Núm. 353 Constitucional. Presidencia del Excmo. Sr. D. Alfonso Guerra González. Sesión núm. 10 celebrada el miércoles, 28 de septiembre de 2005. Comparecencia a petición propia del Señor Director de la Agencia Española de Protección de Datos (Piñar Mañas), para informar sobre la memoria de la Agencia Española de Protección de datos correspondiente al año 2004, (número de expediente 212/000674).

[7] Literalmente el Supervisor Europeo en Protección de Datos afirma: "*Using biometrics in information systems is never an insignificant choice, especially when the system in question concerns such a huge number of individuals. Biometrics (...) change irrevocably the relation between body and identity, in that they make the characteristics of the human body "machine-readable" and subject to furher use. Even if the biometric characteristics of the human eye, they can be read and used by appropriate tools, forever, wherever the person goes*". *Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the Eupean Parliament and the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications* (COM (2006) 269 final)-2006/0088 (COD).

Algunos sistemas de lectura y posterior tratamiento de datos biométricos, ¿podrían afectar a la integridad del cuerpo humano y, por ende, a la dignidad humana?

Por otra parte, en el ámbito privado la suplantación de personalidad ha sido, y es, un medio habitual de comisión de fraudes o defraudaciones patrimoniales y malversaciones de fondos en general. En este punto, puede proporcionar una inestimable ayuda la biometría en base a las características que reúne un dato biométrico; siguiendo el análisis del Grupo de Protección de Datos del artículo 29 (en adelante GPD 29) en su documento de trabajo sobre biometría[8], todo elemento biométrico tiene tres propiedades o características: universal, único y permanente. Efectivamente, puede predicarse el carácter universal del elemento biométrico puesto que está presente en todas las personas. A la vez es único[9], porque es distinto en cada persona, y es permanente[10], puesto que permanece inalterable en cada persona a lo largo del tiempo.

El dato biométrico es un dato de naturaleza especial; en este sentido, el GPD 29[11] manifiesta que tiene que ver con las características comportamentales, es decir, del comportamiento y fisiológicas de una persona y, lo que es fundamental, puede permitir la identificación inequívoca de esta persona. Pero, como ya hemos apuntado, hay que tener en cuenta que la biometría plantea cuestiones en relación con los derechos humanos, pues el dato biométrico forma parte del cuerpo humano, de la integridad física del individuo, se obtiene directamente de aquél y todo ello está relacionado con la dignidad de la persona. Igualmente, otros derechos individuales pueden resultar afectados tanto en la fase inicial de obtención como en la posterior de tratamiento del dato extraído.

---

[8] Documento del GPD 29 Directiva 95/46/CE. "Documento de trabajo sobre biometría". Adoptado el 1 de agosto de 2003. WP 80 12168/02/ES. http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2003_en.htm [Fecha de consulta: 20/03/2017].

[9] Este carácter único es destacado por OLÓRIZ al referirse al método dactiloscópico como el "nombre natural propio, no compartido con ningún otro ser humano", citado por RICO PÉREZ, F., "La individualización de la persona humana en el Derecho Civil", *Revista General de Legislación y Jurisprudencia*, enero 1975, Reus, Separata, p. 13.

[10] En este sentido el Informe de Situación T-PD (2005) BIOM F, cit. pone de manifiesto que la biometría puede permitir una identificación permanente de una persona, pero también caben excepciones ya que las características biométricas de una persona pueden variar a lo largo de su vida debido, por ejemplo, al envejecimiento, una intervención quirúrgica o un accidente.

[11] WP 80. *Documento de trabajo sobre biometría*, adoptado el 1 de agosto de 2003. WP 80 12168/02/ES, pp. 3 y ss. Disponible en http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2003_en.htm [Fecha de consulta: 15/04/2017].

El T-PD, en el informe de situación aludido, destaca la importancia que el artículo 8 de la Convención europea de Derechos Humanos[12] tiene en el campo de las aplicaciones de la biometría en relación a la vida privada y al cuerpo humano. La tensión entre, por una parte, el respeto a la vida privada y familiar, el respeto a la integridad física del individuo y, por otra, la seguridad nacional y pública, la prevención de infracciones penales y, en general, los derechos y libertades del resto de miembros de la sociedad, plantea arduos debates técnicos y jurídicos. En este mismo sentido el GPD 29, en su Dictamen 3/2012[13], interpretando el citado artículo 8 "[…] subraya que cualquier interferencia con el derecho a la protección de datos solo podrá autorizarse si es conforme a la ley y si es necesaria, en una sociedad democrática, para proteger un interés público importante"[14]. Las tensiones que pueden desencadenarse entre el derecho al respeto de la vida privada y familiar, la dignidad humana y, por ejemplo, el derecho a la protección de datos por la utilización de datos biométricos humanos para fines de identificación, entre otras posibles aplicaciones de la biomatría, deben resolverse, sin duda, a la luz de la legalidad vigente sustentada en el interés público necesitado de amparo en una sociedad democrática.

Volviendo al citado documento de trabajo del GPD 29 (año 2003), éste pone de manifiesto la funcionalidad de las aplicaciones biométricas pudiendo ser utilizadas tanto para fines de autenticación y comprobación como para fines de identificación plena de una persona. A ésta se la identifica realmente por lo que es; no se la identifica por lo que tiene o posee, por ejemplo, una tarjeta, o por lo que sabe, un código secreto o un número personal de identificación, un PIN (*Personal Identification Number*)[15]. Por este motivo,

---

[12] Dicho precepto relativo al respeto de la vida privada y familiar establece: "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber ingerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta ingerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás". Como se recordará, el Convenio Europeo de Derechos Humanos, también denominado Convenio de Roma, fue ratificado por España el 26 de septiembre de 1979.

[13] GPD 29 (WP193) Dictamen 3/2012 sobre la evolución de las tecnologías biométricas. 00720/12/ES, adoptado el 27 de abril de 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_es.pdf [Fecha de consulta: 09/02/2016].

[14] Ibíd. p. 9.

[15] En este sentido, Simón Zorita habla de la autenticación por posesión o por conocimiento frente al sistema biométrico que ofrece una nueva dimensión en la autenticación-identificación de personas; así afirma: "Un sistema tradicional de "identificación personal" efectúa la autenticación de una determinada entidad relacionada con la persona, a través de: "algo que la persona tiene*"* (una llave, una tarjeta de identificación, etc), "y/o algo que la persona sabe*"* (una palabra clave, un PIN, etc). Es la forma de

los componentes físicos y/o fisiológicos, incluso de comportamiento, de una persona, su mesura en el sentido de su medición y tratamiento posterior, adquieren un extraordinario valor en la identificación. Como bien nos detalla Simón Zorita[16] "los rasgos biométricos de un individuo proporcionan una mayor fiabilidad en la identificación personal, ya que no se pierden, no se olvidan, ni tampoco se pueden compartir". Está claro que lo que no se puede compartir es el rasgo; el dato, en cambio, se puede compartir.

De forma precisa lo expresa Rodotá con la siguiente afirmación: "la sola realidad desmaterializada corre el riesgo, en muchos casos, de no asegurar la certeza de la identificación de un sujeto que, por ejemplo, podría haber comunicado a otra persona la contraseña necesaria para el uso de un cajero automático"[17].

En este sentido, ya en el año 1994, y en relación con la necesidad de identificación y autenticación de usuarios de sistemas informáticos, se afirmó que "además de la identificación (qué usuario es) debe existir autenticación: demostración al sistema que valida que se trata del propio usuario titular y no de un suplantador […]"[18]. No obstante, en aquel entonces, se utilizó un concepto de autenticación distinto al esbozado por el GPD 29, en cuanto que se consideraba complementario al de identificación siendo, sin embargo, para el GPD 29 la autenticación previa o básica respecto de la identificación que, en este sentido, es superior y permite excluir, identificar-aislar, a una persona respecto del resto. Esta diferencia puede provenir del hecho de que los profesionales informáticos ya utilizaban el término autentificar cuando los computadores sólo pedían usuario y contraseña, y nada más.

---

proceder de los llamados sistemas de autenticación por posesión y por conocimiento, respectivamente. Un "sistema biométrico" es un sistema de reconocimiento en el que la identidad de un individuo es determinada a partir de alguna de sus características fisiológicas o de comportamiento [Miller 94, Shen 97, Jain 99a, Zhang 00a, Nanavati 02, Ortega 02b, Zhang 02]. Se añade así un nuevo paradigma a la identificación personal, ya que la autenticación se realiza por medio de "algo que la persona es" (un rasgo fisiológico personal, como, por ejemplo, la huella dactilar, el iris, etc), o "algo que la persona genera" (un patrón de comportamiento, como puede ser la voz, la firma escrita, etc)". SIMÓN ZORITA, D., *Reconocimiento automático de patrones biométricos de huella dactilar*, Universidad Politécnica de Madrid. Escuela Universitaria de Ingeniería Técnica de Telecomunicación, 2004, p. 11.

[16] Ibíd.

[17] RODOTÁ, S., *Tecnología y derechos fundamentales.* Conferencia pronunciada en los actos de inauguración de la sede de la Agencia Catalana de Protección de Datos, Barcelona, 2004. Disponible en http://www.apdcat.net/media/188.pdf. [Fecha de consulta: 10/04/2017].

[18] DEL PESO NAVARRO, E., RAMOS GONZÁLEZ, M.A., *Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socioeconómicas,* Madrid, Díaz de Santos, 1994, p. 43.

Es evidente que, al acercarnos al tratamiento del dato biométrico se plantean las dos utilidades o campos de aplicación social de la biometría: la autenticación/comprobación y la identificación de las personas. Como hemos dicho con anterioridad, la autenticación, la comprobación de que la persona es quien dice ser, determina que el sistema informático tome una decisión lógica donde solo caben dos valores u opciones, o sí o no. Sin embargo, en el concepto de identificación está implícito el reconocimiento de la persona y la distinción del resto, tarea evidentemente más compleja donde el sistema debe tomar una decisión, pero no entre dos posibilidades entre sí excluyentes, sino entre muchas alternativas que estarán almacenadas en una base de datos[19]. Las cuestiones tanto jurídicas -como puede ser el impacto en la privacidad del individuo-, como técnicas que plantea uno y otro sistema, el de autenticación y el de identificación, son diferentes y serán abordadas más adelante. Entre estas cuestiones baste ahora señalar el alto impacto en la privacidad de la persona que puede suponer un sistema de identificación. Utilizamos, a continuación, un cuadro explicativo de la guía Inteco[20]:

Impacto en la privacidad	Proceso	Tipo de tecnología	Muestra	Tipo de base de datos
Alto	Identificación	Fisiológico	Imagen biométrica	Bases de datos grandes/centralizadas
Bajo	Verificación	De comportamiento	Muestra cifrada	Bases de datos pequeñas/locales

[19] En este sentido la OCDE ha puesto de manifiesto cómo los distintos sistemas biométricos actualmente existentes operan esencialmente de la misma manera: el sistema captura una muestra biométrica del individuo, almacena el rasgo extraído o permite la creación de una base de datos y, posteriormente, permite la ejecución de un o dos tipos de búsquedas. Estos sistemas permiten realizar búsquedas de uno a uno (1:1) o bien de uno a varios (1:N). En la búsqueda de uno a uno se comprueba por el sistema si la muestra tomada es la misma que la almacenada. En el segundo tipo de búsqueda el sistema permite una comparación de una muestra tomada con muchas almacenadas en una base de datos, permitiendo comprobar la coincidencia con una de las muchas almacenadas y excluyendo al resto. Cfr. OCDE Organisation for Economic Co-operation and Development. Directorate for Science, Technology and Industry. Committee for Information, Computer and Communications Policy. Working Party on Information Security and Privacy. Biometric-based technologies. DSTI/ICCP/REG(2003)2/FINAL Unclassified. 30 de junio de 2004, p. 4. www.oecd.org/sti/security-privacy [Fecha de consulta: 20/01/2016].

[20] PÉREZ SAN JOSÉ, P, (*et al*), *Guía sobre las tecnologías biométricas aplicadas a la seguridad*, INTECO (Instituto Nacional de Tecnologías de la Comunicación), Observatorio de la seguridad de la Información. Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Ministerio de Industria y Comercio, octubre 2011, p. 35. https://www.incibe.es/CERT/guias_estudios/Estudios//estudio_biometria [Fecha de consulta: 25/01/2016].

Por último, pero no en grado de importancia sino muy al contrario como origen de buena parte de las cuestiones que abordaremos en nuestro estudio, debemos apuntar en esta breve introducción que el espectacular desarrollo de las telecomunicaciones en las dos últimas décadas ha permitido la conexión de todo con todo de una forma simple para el usuario final. La interconexión a nivel mundial de las redes de ordenadores digitales ha permitido la globalización de la información. Y la información personal, la generada por cada usuario, por cada uno de nosotros, es de un altísimo valor y criticidad[21]. Asimismo, hay que tener en cuenta que hoy, en el pasado inmediato y en un futuro, los sistemas informáticos de muchas empresas, organizaciones, profesionales o particulares ya no son propietarios y se ubican en la Red, en la nube global, en un entorno de *cloud computing*[22]. Gracias a una profusión en el desarrollo de servicios de valor añadido de los proveedores de redes, la virtualización de acceso y la intercomunicabilidad a nivel mundial de redes es hoy una realidad. El trabajo en la nube se facilita con el desarrollo de herramientas de la *Web 2.0* que permiten al usuario liberarse de la atadura de un equipo, un *hardware*, terminal concreto, ubicado en un lugar geográficamente fijo, para pasar a un modelo donde cualquier terminal es susceptible de servir de terminal de acceso. Las aplicaciones que se usan en la *Web 2.0* almacenan en la nube datos y *software* a los que se accede a través de sitios web que identifican al usuario por medio de un número o clave de usuario y una contraseña. La pregunta que aquí nos plantearemos es si esa identificación se realiza verdaderamente de forma única y si la tecnología biométrica ayuda a lograr esa identificación digital única. En este contexto, y siguiendo a Lage, podemos afirmar que hoy más que nunca se hace imprescindible "garantizar la confidencialidad de la información que se

[21] "La información principal, nuestra propia información personal, puede estar en algún lugar del ciberespacio, en lo que se viene dando en llamar la nube, donde se mantiene y se comparte; y no sólo la información, los propios recursos de cómputo y las mismas aplicaciones están en un servidor remoto, con el que interactuamos en tiempo real sin ser siempre conscientes expresamente…". CASAR CORREDERA, J. R., *Transformaciones audaces de las Tecnologías de la Información: los espacios, el conocimiento, los otros*, Real Academia de Doctores de España. Discurso de toma de posesión como académico de número, Madrid, 2016, p. 20.

[22] "*Cloud computing* representa una nueva forma de entrega y consumo de servicios flexibles, altamente escalables y globales, según un modelo de negocio de pago por uso". Todo tipo de servicios pueden estar en "la nube" desde potencia computacional, servicios de infraestructura hardware en general, capacidad de almacenamiento, uso de software, procesos de negocio en general, interacciones personales, etc…, DE NICOLÁS, E., "Cloud computing: qué es y para qué se usa*"* en *Cloud computing: la nueva frontera de servicios tecnológicos. GEOECONOMÍA*, invierno, 2010-2011, Instituto Choiseul España y Instituto de Postgrado CEU Cátedra de Geoeconomía y Estrategia Internacional, Madrid, 2010, p. 19.

intercambie y la identidad de los intervinientes"[23]. Internet se ha convertido en el "medio propicio"[24] para la circulación transfronteriza de datos

En definitiva, el nuevo espacio global donde desarrollamos nuestras vidas hace ineludible encontrar una solución fiable a la necesidad de identificación de todos los individuos intervinientes en ese mundo. Sin individualidad natural, física, no hay individualidad jurídica. ¿Puede ser la biometría la respuesta a esa necesidad de identificación? Si la respuesta es afirmativa, se abre ante nosotros un amplio abanico de cuestiones, entre ellas, jurídicas. Se plantean múltiples tensiones entre nuestros derechos individuales, los derechos de los otros y los intereses generales. Todo ello hace recomendable un detenido análisis.

II. Objeto de la investigación. La sociedad de la información y el tratamiento de los datos biométricos: implicaciones jurídicas.

Vivimos en la sociedad de la información, concepto que no por ser frecuentemente utilizado debe obviarse la aproximación al mismo. Ya en 1973 el sociólogo estadounidense Daniel Bell introdujo el concepto de "sociedad de la información"[25]. La base fundamental de esta sociedad, en opinión de Bell, será el conocimiento teórico y, a su vez, los servicios sobre el conocimiento serán la base de la nueva economía[26].

Al hilo de esta última cuestión, se ha afirmado que el sistema económico actual todavía se basa en el capitalismo, aunque ya no industrial sino "informacional"; hoy cabe hablar

[23] Cfr. LAGE, J., "El cloud computing no está en la nube*"* en *Cloud computing: la nueva frontera de servicios tecnológicos GEOECONOMÍA*, invierno, 2010-2011, Instituto Choiseul España e Instituto de Postgrado CEU Cátedra de Geoeconomía y Estrategia Internacional, Madrid, 2010, pp. 58-59.
[24] DE MIGUEL ASENSIO, P.A., *Derecho privado de Internet*, Madrid, Civitas, 2000, p. 473.
[25] BELL, D., *The coming of post-industrial society; a venture in social forecasting*, - New York, Basic Books [1973], - xiii, 507 p. illus. 25 cm. [traducción: Advenimiento de La Sociedad Post-Industrial. - Alianza (January, 1992). Ttraducción: *Vers la société post industrielle*. - Robert Laffont, 1976.
[26] Sobre el particular, Fernández Esteban hace sinónimos sociedad de la información, la sociedad del aprendizaje y sociedad del conocimiento, entendiendo que el proceso de aprendizaje en la sociedad de la información para alcanzar el conocimiento necesario para desenvolverse en ella es tarea de toda la vida, si se quiere ser miembro activo de dicha sociedad. FERNÁNDEZ ESTEBAN, M.L., *Nuevas tecnologías, Internet y Derechos Fundamentales*, Madrid, McGrawHill, Monografía Ciencias Jurídicas, 1998, p. XXIII. Además, "con la aparición de las nuevas tecnologías, la información ha pasado a ser el oro del siglo XXI, y por consecuencia el primer activo de toda empresa, sin información no hay negocio." LLEIXÀ ALSINA, À., *La economía colaborativa y el nuevo Reglamento. ¿Qué ocurre con mis datos?* http://www.abogacia.es/2017/11/06/la-economia-colaborativa-y-el-nuevo-reglamento-que-ocurre-con-mis-datos/?lang=es [Fecha de consulta: 5/12/2017].

de una nueva economía donde el conocimiento y la información son la base de la productividad y la competitividad[27]; desde una perspectiva económica, cabe establecer los tres pilares definitorios de la sociedad de la información extrapolables a otros ámbitos: información y conocimiento que se comparten en redes interconectadas. Esta conectividad de redes ha venido favorecida, sin duda, por el desarrollo de Internet que para el Libro Verde sobre la convergencia de los sectores de las telecomunicaciones "puede considerarse una red de redes interconectadas de forma abierta mediante IP, que normalmente se vale de enlaces de transmisión alquilados a los operadores de telecomunicaciones. […] El carácter abierto, sin pertenencia a un propietario, de las normas de Internet ha hecho posible que las empresas puedan aprovechar y dar continuidad a los avances realizados por otras empresas del sector"[28]. Internet ha propiciado la infraestructura tecnológica para que hoy los lugares y formas de captación de datos, sean éstos personales o no, se hayan multiplicado. Y lo que es aún más relevante, el dato una vez captado, en cualquier punto del planeta, puede ser procesado en cualquier otro punto. Así, esta forma global de procesar los datos en la Red, Internet, ha permitido la irrupción del denominado *ubiquitous computing*[29] que plantea arduas

[27] Vid. CASTELLS, M., *L´etá dell´informazione economica societá cultura*, Milano, Universitá Bocconi, 2004. Para el Profesor Castells, la nueva economía tiene tres características interrelacionadas: la primera, el conocimiento y la información como base de la productividad y la competitividad y el fortalecimiento de éstas últimas por las tecnologías; la segunda, la nueva economía es una economía en la que el conocimiento y la información se comparten en red y es tecnológicamente simple formar parte de la red, o quedar excluido de la misma, en función de la contribución a la cadena de valor estructurada de información y conocimiento que se genera en dichas redes; y la tercera, añadida a las dos anteriores características, las telecomunicaciones permiten que la economía funcione como una unidad en tiempo real y a escala planetaria. Todo ello está impulsado por una red mundial como Internet que permite la interconectividad de las redes.

[28] Junto al carácter abierto de Internet, el informe también señala como una de las características fundamentales que han favorecido la conectividad a través de Internet el hecho de la independencia tecnológica de Internet de la plataforma sobre la que se implanta, ya que el protocolo IP se ha convertido en "el protocolo de red de facto de Internet capaz de encaminar y transportar todos los elementos de un servicio multimedios (texto, imagen, vídeo de animación y sonido)". Cfr. Comisión Europea. COM(97) Versión 3. *Libro verde sobre la convergencia de los sectores de telecomunicaciones, medios de comunicación y tecnologías de la información y sobre sus consecuencias para la reglamentación, en la perspectiva de la sociedad de la información*. Bruselas, 3 de diciembre de 1997, p. 4. http://www.euskalnet.net/oig/archivo/lvmedia.pdf [Fecha de consulta: 03/12/2017].

[29] La computación ubicua se ha hecho posible porque existe una red mundial como Internet. Hoy cabe hablar de la ubicuidad de los servicios informáticos en la Red. Esta ubicuidad ha venido propiciada por la aparición del concepto de *cloud computing*, concepto que, poco a poco, ha ido desarrollándose al residenciarse la información personal y corporativa en la Red o en la "nube", en la *cloud* y no únicamente en local, en servidores o equipos ubicados en nuestra casa, empresa o corporación. Por ello, partiendo de este fenómeno imparable de residenciar fuera de nuestras infraestructuras la información que nos pertenece o manejamos, surge el otro concepto de computación ubicua en el sentido de virtual, ya que, con un dispositivo de acceso a la Red, terminal o un simple teléfono móvil, disponiendo de los adecuados servicios de acceso se puede consultar la información y manipularla desde cualquier área geográfica. La computación ubicua, que ha nacido a raíz de la ubicación de la información en la *cloud*, abre enormes interrogantes técnicos, empresariales y, cómo no, jurídicos entre otros los relacionados con los datos

cuestiones jurídicas, entre otras, respecto a la legislación aplicable a dichos procesos. Los Comisarios de Protección de Datos en la Declaración de Montreux en el año 2005 expresaron abiertamente su preocupación por "los crecientes riesgos de la omnipresente vigilancia de las personas en todo el mundo*"* y por las dispersiones, disparidades, o incluso ausencia de protección normativa de los datos de carácter personal en algunas partes del mundo, que redunda en una ineficaz protección de datos mundial[30].

Ya en 1987 Romeo Casabona[31] expuso que, si bien "la revolución industrial del siglo XIX permitió sustituir de forma sustancial el trabajo físico del hombre por máquinas, en la presente centuria estamos presenciando el diseño de otra gran transformación radical: reemplazar determinadas funciones intelectuales del hombre gracias a estas nuevas tecnologías. Esta situación nos está llevando a los inicios de una nueva era: la de la información y la comunicación, en el seno de lo que se ha venido a denominar la sociedad de la información."

En mayo de 1994, y en el seno de la UE, el ministro de Industria alemán, Martin Bangemann, dirigió un grupo de trabajo cuyo objetivo era sentar las bases para alcanzar la sociedad de la información real para todos los ciudadanos. Este grupo, denominado *grupo Bangemann* fue el que por primera vez utilizó el término sociedad de la información en el ámbito de la UE, en su informe denominado *informe Bangemann*[32].

---

personales, en este sentido cabe plantearse cuestiones como ¿dónde residirán los datos personales manejados por una empresa relativos, por ejemplo, a sus clientes una vez que han sido descargados por una persona desde un cibercafé? ¿Qué medidas de seguridad se adoptarán tras una descarga de datos personales en una computación ubicua? ¿Cómo asegurar que la descarga se ha realizado por personal autorizado en computación virtual? Quizá en este punto el reconocimiento de variables biométricas proporcione la respuesta ya que estas variables son totalmente personales, intransferibles, y siempre van con nosotros. Así, la seguridad va con la propia persona, esto es así siempre que se implemente un sistema de reconocimiento de sus características físicas o comportamentales para permitir el acceso. Cfr. LAGE, J., op. cit., p. 60.

[30] Declaración de Montreux "La protección de datos personales...", op. cit.

[31] Cfr. ROMEO CASABONA, C. M., *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información*, Madrid, FUNDESCO, Colección Impactos, 1987, p. 15.

[32] *Europa y la sociedad global de la información.* Recomendación del *Grupo Bangemann* al Consejo Europeo, 26 de mayo de 1994. Este informe recoge una serie de actuaciones imprescindibles para alcanzar la sociedad de la información que se pueden concretar resumidamente en cinco puntos: actuación conjunta de todos los Estados miembros con concienciación de la ciudadanía y de los poderes públicos y privados; evitar una fractura de la sociedad en dos niveles teniendo solo uno de ellos acceso real a los beneficios y posibilidades de la sociedad de la información; fomento de la competencia entre los operadores de telecomunicaciones y titulares de los medios de comunicación; imprescindible fomento de la estandarización de los sistemas, interconexión de las redes telemáticas y la interoperabilidad de los servicios y las aplicaciones y por último y fundamental protección de los derechos de propiedad intelectual y el derecho a la intimidad de los individuos a través de la regulación de la protección del dato

Más recientemente, un concepto amplio de sociedad de la información se recoge en la exposición de motivos de la Ley española de Servicios de la Sociedad de la Información (Ley 34/2002, de 11 de julio). Este concepto amplio viene determinado "(…) por la extraordinaria expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de transmisión e intercambio de todo tipo de información". Efectivamente, el concepto de sociedad de la información nace y está ineludiblemente unido al concepto de red de telecomunicación, red de telecomunicación que lleva de suyo la presencia de medios informáticos interconectados[33]. Así, la red ha contribuido a debilitar las antiguas barreras de tiempo y espacio que, sin que fueran absolutamente infranqueables, guardaban algunos de nuestros derechos individuales.

Aunque pueda resultar una obviedad, con todo lo que hasta aquí hemos dicho, podemos afirmar que la información es el valor fundamental de la nueva sociedad[34], y cabría añadir, la información de calidad. El tratamiento de una información no veraz (obsoleta, incompleta)[35] puede acarrear gravísimas consecuencias, entre otras, en la esfera privada, social, económica de individuos y Estados. De este modo, también llegamos a vislumbrar la estrecha relación que, entre sociedad de la información y datos, en general, y los personales, en particular, existe, ya que un elemento esencial de aquélla son éstos.

---

de carácter personal. Disponible en https://www.adrformacion.com/udsimg/bibliodigi/1/Informe%20Bangemann.pdf [Fecha de consulta: 27/07/2017].

[33] En este mismo sentido, CAMPUZANO TOMÉ, H., *Vida privada y datos personales. Su protección jurídica frente a la sociedad de la información*, Madrid, Tecnos, 2000, p. 19. Para esta autora, es el desarrollo y la universalización de las nuevas tecnologías de la información y las comunicaciones las que tendrán un impacto calificable de revolución en el ámbito cultural, económico, legal y social.

[34] "La revolución tecnológica ha redimensionado las relaciones entre los hombres. Estamos en una sociedad donde las tecnologías de la información han llegado a ser la figura representativa de nuestra cultura, hasta el punto de que para designar el marco de nuestra convivencia se alude reiteradamente a la expresión sociedad de la información". Así contempla la revolución tecnológica HERRERA BRAVO, R., "El Derecho en la sociedad de la información: Nociones generales sobre el Derecho de las tecnologías de la información y las comunicaciones*",* en *Observatorio Iberoamericano de Protección de Datos*. Disponible en: http://oiprodat.com/2014/08/11/el-derecho-frente-a-la-sociedad-de-la-informacion/ [Fecha de consulta: 26/01/2019].

[35] Romeo Casabona nos recordaba que los ordenadores son instrumentos de trabajo de especial magnitud y utilidad al reunir cuatro características esenciales: la ingente potencialidad para el almacenamiento de datos; la gran velocidad de sus operaciones; la adaptabilidad a las exigencias humanas y la exactitud y fiabilidad de éstas, pero puntualizaba el autor *"*siempre que sean correctos los datos de partida". Evidentemente si tratamos datos corrompidos obtenemos información corrompida. Por ello, el mismo autor llama la atención sobre la aparición de un nuevo valor en nuestra sociedad "el valor de la información sobre la información ", entendiendo por tal el valor de acceso a la información pertinente. ROMEO CASABONA, C.M, *Poder Informático…,* op. cit., p. 19.

Podríamos, al menos en una visión parcial del fenómeno, hacer sinónimos sociedad de la información y sociedad-red. Y, sin duda, esta sociedad-red es una sociedad global en la que se produce un efecto de "diluvio de datos" donde la masa de datos personales existente, objeto de tratamiento, aumenta constantemente. Los avances tecnológicos aplicados al crecimiento de los sistemas de información y comunicación y, así mismo, el crecimiento de las personas capaces de interactuar con estos sistemas, favorecen este "diluvio". El ciberespacio, generado por la extensión de Internet, cruza Estados, fronteras nacionales y ordenamientos jurídicos como el aire que nos envuelve. Con todo ello hemos puesto de manifiesto un aspecto de la sociedad de la información, como sociedad-red global, que incide en el tema central del estudio. Ello es así toda vez que la sociedad global exige identificación[36], de lo contrario hablaríamos de la sociedad del caos, "la Babel global", "la Babel electrónica". Y la identificación exige una unión o correlación segura entre el dato captado y una identidad que, en abstracto, preexiste a dicha captación. Así, adquiere una importancia renovada el derecho a la identificación de cada individuo. La vulneración de este derecho a la identificación puede acarrear consecuencias muy graves para derechos fundamentales de la persona, tales como el derecho a la libertad y a la seguridad o incluso el derecho a la vida. En este punto es trascendental la aportación de Rico Pérez, distinguiendo entre los conceptos de individualización e identificación de la persona humana al afirmar que "[…] la individualización aísla para distinguir, la identificación verifica para comprobar. La individualización actúa en el campo de las relaciones jurídicas privadas (Derecho civil, Derecho Mercantil, Registro del estado civil de las personas, Registros de la Propiedad y Mercantil, etc.), en cambio, la identificación es más propia del Derecho público (Penal. Procesal, policía, orden público, etc)[37]". Los dos procesos concatenados en orden secuencial transforman un grupo social informe en un grupo susceptible de ser organizado jurídicamente. En el proceso de individualización mediante la atribución de un nombre, el hombre pasa de ser un elemento indiferenciado de la especie humana a ser, como indica Pliner[38],"un individuo determinado"; se pasa de una masa social

[36] En este sentido se puede afirmar que "[…] vivimos en la sociedad de la identificación permanente, del tratamiento automático de la información personal y de la creación de perfiles" Cfr. LLÁCER MATACÁS, M. R., *Protección de datos personales en la sociedad de la información y la vigilancia*, La Ley, Madrid, 2011, p. 18.
[37] RICO PÉREZ, F., "La individualización…, op. cit., p. 13.
[38] PLINER, *El nombre de las personas.* Buenos Aires, 1966, p. 85, citado por RICO PÉREZ, F, "La individualización…", op. cit., p. 9.

amorfa al individuo, en el sentido de "*individum*", lo no partible, lo que no se puede dividir sin dejar de ser lo que es. Junto al concepto de la individualización, que es un procedimiento que viene "desde fuera", se puede avanzar un poco más al concepto de la "individuación", referido, éste último, más que a la persona a la personalidad siendo así más que individualizar; "individualizar es separar personas, individuar significa también calificar comportamientos". La individuación se alcanzaría con "[…] un nombre único para cada persona, sin homónimos[39]". Una vez que se ha dado el primer paso de individualizar a uno del resto, hay que plantear la identificación del individuo en todas las situaciones del devenir de su existencia; para ello, veremos que el método dactiloscópico, aún no siendo el único, sí ha marcado un hito en el reconocimiento de la individualidad previamente determinada. Una vez separada la persona de la masa, atribuyéndola un nombre, y una vez que hayamos arbitrado un método para identificarla, lo que se pretende es verificar que es ella; a lo que se ha de aspirar es a "individuarla", a determinar lo que la singulariza de forma única y la hace distinta del resto de la humanidad. Cada persona es única en el mundo, todos lo sabemos, pero hay que poder demostrarlo. Para conseguir la singularización, la técnica biométrica y, en concreto, la huella dactilar, puede resultar adecuada.

Y aquí es donde centraremos, con predominio de la perspectiva jurídica, el objeto de nuestro análisis: en las técnicas de captación de datos personales identificativos del individuo, que, habiendo multiplicado los lugares y métodos de captación, han llegado incluso, en algunos casos, a captar de manera inconsciente dichos datos de su titular. En este escenario de pluralidad de lugares donde los datos de un individuo pueden ser captados, en una sociedad de "riesgo ambiental", no es solo la legalidad del tratamiento del dato personal, como dato atribuible a una persona identificada o identificable lo que ha de analizarse, sino también el tratamiento del dato anónimo que genera un perfil no personal pero que puede provocar discriminación en el caso concreto. Es en este tratamiento del dato anónimo donde algunos autores han planteado un nuevo problema denominado "gap informativo"[40], problema que afecta de modo directo al ejercicio del derecho fundamental a la autodeterminación informativa.

---

[39] RICO PÉREZ, F., *Las homonimias, como problema. (En torno al artículo 109 del Código Civil),* Separata del Boletín del Ilustre Colegio de Abogados de Madrid, Nº 1/1983, p. 4.

[40] La personal y voluntaria participación en la sociedad de la información sitúa al individuo, o puede situarlo en algunos casos, en un entorno de riesgo informacional en un doble sentido: por una parte, al desconocer la captación de un dato personal de su titularidad desconoce su posterior tratamiento y, por

La captación del dato biométrico dactiloscópico proporciona un medio de identificación alternativo a otros medios tradicionales (por ejemplo, exhibición de un DNI) que tiene a su vez una virtualidad expansiva en el sentido de poder constituir el extremo del hilo conductor del que desencadenar incluso perfiles[41] personales almacenados en una base de datos. Con todo ello, a lo largo de este trabajo comprobaremos cómo las tecnologías de la información y la comunicación permiten ya un fácil, rápido y masivo acceso a información de todo género, pero en particular, información relativa a los individuos.

La telemática puede constituir "el cauce potencial para una intromisión no deseable en la intimidad individual"; y, a continuación, cabe hacerse una pregunta que adquiere hoy una relevancia innegable: *"¿*Estamos en camino de pasar a convertirnos en ciudadanos transparentes, a modo de escaparates de uno de los aspectos más preciados de nuestra personalidad? "[42]. Podría calificarse de premonitoria y de plena actualidad la pregunta y el término de "ciudadanos transparentes*"*. La tecnología biométrica (*software* y *hardware*) puede llegar a extraer, leer, del interior del cuerpo humano lo más oculto y

otra parte, desconociendo esta captación y tratamiento no utiliza los medios jurídicamente a su alcance para su control. Con ello, podemos encontramos en una situación en la que el titular de los datos está a merced del poder ajeno del responsable de dicho tratamiento produciéndose así el "gap informativo" citado que, en definitiva, alude a la fractura o desequilibrio en la base de la estructura de la sociedad de la información como organización social. La simetría entre dato y tratamiento debe ser perfecta para permitir al individuo el ejercicio de su derecho fundamental a la autodeterminación informativa. Si la vía de conexión, en el sentido de conocimiento, entre dato y tratamiento del dato está rota el ejercicio del derecho de autodeterminación se hace inviable y el efecto reequilibrador de poderes se rompe produciendo una asimetría de poder en favor del responsable de ese tratamiento. Es decir, esta asimetría informativa, entre titular del dato y responsable del tratamiento, produce una asimetría de poder en favor del responsable del tratamiento. Al ser un tratamiento desconocido para el titular del dato éste no puede neutralizar jurídicamente, con el ejercicio del derecho de autodeterminación, la asimetría de poder que dicho tratamiento produce. Cfr. LLÁCER MATACÁS, M. R., "La autodeterminación informativa en la sociedad de la vigilancia: Ubiquitous Computing*"* en *Protección de Datos Personales en la Sociedad de la Información y la Vigilancia*, Madrid, LA LEY, 2011, p. 69 y ss. Esta autora nos deleita con una exposición en torno a una sociedad de "riesgo ambiental".

[41] La Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (PRGPD), recogía en su artículo 20 el derecho del interesado, persona física, a no ser objeto de una medida basada en la elaboración de perfiles. Perfiles entendidos como tratamientos automatizados destinados a evaluar determinados aspectos personales propios de la persona en cuestión, o bien a analizar o predecir su rendimiento profesional, situación económica, su localización, su estado de salud, sus preferencias personales, su fiabilidad o su comportamiento. No obstante, este artículo 20 establece una serie de premisas bajo las cuales estos tratamientos son admisibles que pasan indefectiblemente por el conocimiento y consentimiento del interesado. Este derecho del individuo ha quedado definitivamente consagrado, en términos prácticamente coincidentes con la Propuesta, en el artículo 22 del Reglamento General de Protección de Datos (RGPD) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[42] Estos son los valiosos planteamientos de ROMEO CASABONA, C.M., *Poder informático*…, op. cit., p. 16.

profundo: desde la presión arterial, la frecuencia de latidos del corazón, el fondo de ojo, etc[43]. En esta misma línea argumental es muy ilustrativa la Sentencia del Tribunal Supremo de 11 de noviembre de 2014:[44] "[…], en concreto, del representado por la determinación y el examen del ADN a partir de los restos del material biológico eventualmente dejados por el autor o autores del delito en la víctima o en el escenario del mismo, ha supuesto un cambio de trascendencia ciertamente revolucionaria en los procedimientos de investigación, suscitando, a la vez, interrogantes jurídicos de no pequeño calado. De un lado, porque, en virtud de estas técnicas, el imputado se convierte en objeto pasivo de la averiguación probatoria, llevada a cabo ahora con medios extraordinariamente incisivo en su esfera más personal, en la medida en que están dotados de una capacidad de hacer hablar al cuerpo humano, en su materialidad, con una locuacidad inédita y en términos de una extraordinaria fertilidad informativa, que podría ser eficazmente de cargo". Sin duda, los avances tecnológicos actuales permiten que el cuerpo humano hable y con una profusión de datos y de tal importancia que su "locuacidad" puede afectar a diversos derechos fundamentales del individuo. Así, presentando o mostrando ordenadamente esos datos, haciendo visible y objeto de tratamiento lo que antes estaba en el claustro de nuestro ser, esta tecnología nos hace, en el sentido más amplio y literal del término, seres, ciudadanos, personas, transparentes para instituciones públicas o privadas. En este mismo sentido, nos viene a la memoria la afirmación que Salmerón Cabañas nos hizo en conversación distendida: "hoy en día las personas estamos en abierto", en paralelismo con la terminología utilizada para el software de fuente abierta.

En un ámbito distinto, aunque cercano como es el de la medicina, una reflexión paralela a la que realiza Pera[45], cabría hacer en relación con la tecnología biométrica: la mirada del médico sobre el cuerpo del paciente, con el avance experimentado en la tecnología médico-hospitalaria, ha traspasado los límites morfológicamente externos de ese cuerpo. Así este autor reflexiona diciendo que: "[…] la mirada médica puede aparecer, en estas circunstancias, como intimidante, hegemónica y motivo de preocupación de la persona (…), aunque en el fondo pretenda ser tranquilizadora o incluso compasiva".

[43] Hoy conocemos la tecnología aplicada al control de acceso a determinadas zonas de embarque en algunos aeropuertos donde se aplican escáneres corporales a los pasajeros en un ejercicio de auténtica transparencia corporal.
[44] Sala 2ª, nº 734/2014, rec. 289/2014, Fundamento de Derecho Segundo.
[45] PERA, C., *Pensar desde el cuerpo. Ensayo sobre la corporeidad humana,* Madrid, Triacastella, 2006, pp. 197-213.

Efectivamente la misma reflexión sobre la mirada del médico sobre el cuerpo enfermo o herido cabe hacer sobre la mirada de un sistema de reconocimiento biométrico sobre el cuerpo en general de cualquier individuo que entra en contacto con dicho sistema. Con la tecnología médica y con la tecnología biométrica el límite, hasta hace unos años, infranqueable de la propia corporeidad del individuo ha desaparecido y todo nuestro ser queda a la vista. De tal manera que podemos afirmar que esta exhibición tecnológica de nuestro cuerpo desencadena, por un lado, una expansión *ad intra*, de partes del mismo antes encerradas en el claustro de su propio límite morfológico y, por otro, una expansión en el sentido de dispersión *ad extra*, configurándose un concepto nuevo que Rodotá denomina el "cuerpo electrónico"[46]. Este cuerpo electrónico aparece disperso al existir multitud de lugares de captación y proceso de los datos a él referidos, y sólo se consigue que cada persona recomponga su propio yo y no pierda el control sobre cada uno de sus fragmentos si se garantiza el ejercicio del derecho a la autodeterminación informativa que desempeña así un papel reunificador, siempre que ese derecho tenga un reconocimiento tan amplio como amplia pueda ser la dispersión que pretende controlar[47].

[46] Rodotá define el cuerpo electrónico como conjunto de informaciones existentes sobre nosotros dispersas, y así afirma que "fragmentos de cualquiera de nosotros se conservan en innumerables bancos de datos en los que nuestra identidad es objeto de selección y descomposición, en los que aparecemos como consumidores, como electores, deudores, trabajadores, usuarios de autopistas, y así sucesivamente. Una vez más, nos dispersamos en el tiempo y en el espacio. … Se plantea, por consiguiente, el problema de cuál debe ser la relación ordinaria de cada persona con la realidad de un cuerpo que ha quedado institucionalmente dispersado". RODOTÁ, S., *La vida y las reglas. Entre el derecho y el no derecho*, Madrid, Editorial Trotta Fundación Alfonso Martín Escudero, 2010, p. 101.

[47] Si bien es cierto que el consentimiento de cada interesado en la recogida y tratamiento de los "fragmentos ", datos, sobre su persona y la posterior limitación de las interconexiones de esos fragmentos es garantía de protección del citado cuerpo electrónico no es menos cierto, como advierte el mismo Rodotá, que: "El consentimiento del interesado puede desplegar sus efectos sólo en un ámbito territorial limitado y así seguirá siendo mientras las convenciones internacionales no hagan coincidir la protección del cuerpo electrónico con las fronteras del mundo, evitando así la aparición de "paraísos informáticos" donde nuestras informaciones pueden ser recogidas y cruzadas sin control alguno". RODOTÁ, S., *La vida y las reglas…,* op. cit., p. 102. Ha de tenerse en cuenta que el principio del consentimiento, sin dejar ser piedra angular en el edificio de la protección de datos, admite excepciones y ha de ser interpretado a la luz de la doctrina establecida por el TJUE, en su sentencia del 24 de noviembre de 2011, según la cual, a pesar de que el tratamiento de datos de carácter personal requiere el consentimiento del afectado, éste no será preciso cuando el tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable "siempre que no prevalezcan los derechos y libertades fundamentales del interesado". Hay que tener en cuenta que el RGPD, transforma lo que se consideraban excepciones al consentimiento (recogido en lo que era el art. 6.2 LOPD), en requisitos equivalentes e independientes para que el tratamiento no resulte ilícito. No en vano, la nueva LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, incorpora un precepto (art. 59) relativo a los tratamientos contrarios al RGPD.

La Exposición de Motivos de la antigua LORTAD advertía ya que el tiempo y el espacio habían sido barreras que en el pasado preservaron nuestra intimidad y ahora, cabría añadir, que también en el pasado nuestro cuerpo encerraba dentro de sus límites la información que a él le concernía. Hoy la tecnología biométrica traspasa ese límite y hace posible la exposición y manifestación pública de la información de la identidad del individuo.

III. Metodología de la investigación.

El estudio parte del análisis de uno de los posibles sistemas de captación de datos biométricos; un sistema de captación de huella dactilar. Este análisis nos permitirá acercarnos a las múltiples cuestiones jurídicas derivadas del uso de medios tecnológicos que obtienen elementos propios del individuo aptos para su posterior identificación. Dentro del amplio abanico de sistemas de captación de datos biométricos, los destinados a la captación de la huella digital o palmar, son objeto de especial análisis para posteriormente, desde una perspectiva jurídica, estudiar las implicaciones del tratamiento de dichos datos en los derechos fundamentales del individuo[48].

La segunda parte del estudio abarca, dentro del denominado Capítulo II, las implicaciones jurídicas del dato biométrico dactiloscópico en sí, como bien de la personalidad, y las consecuencias de su tratamiento posterior en relación con los derechos de la persona concernidos por dicho tratamiento. En este sentido, deseamos poner de relieve la aprobación, hace unos meses, de la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales -ya referenciada en nota *ut supra*-, para su adaptación al nuevo Reglamento (UE) 2016/679 (en lo sucesivo, RGPD), lo cual ha obligado a revisar este capítulo en su totalidad, pues, tanto

[48] En el análisis *ius* fundamental que se realizará podremos comprobar cómo del principio de legalidad, en su formulación decimonónica original donde partiendo del planteamiento de Rousseau de que la ley es expresión de la voluntad general y la protección de la libertad individual se produce por la ley, se tiende a sustituir por un principio de constitucionalidad donde las libertades individuales deben ser protegidas frente a la ley; ley, entendida como ley ordinaria sometida a las contingencias y vaivenes políticos. Así adquiere la Constitución el papel de pilar y salvaguarda de los derechos y libertades fundamentales de un país o de un conjunto de países y en nuestro entorno cercano la Carta de los Derechos Fundamentales de la Unión Europea adquiere relevancia máxima. Cfr. PEDRAZ PENALVA, E., "La utilización en el proceso penal de datos personales recopilados sin indicios de comisión delictiva" en *Protección de datos y proceso penal*, Madrid, LA LEY, 2010, p. 24 y ss.

la LO 15/1999 (en adelante, LOPD) como su Reglamento de desarrollo (en lo sucesivo, RLOPD), han quedado derogados por la nueva LO 3/2018, si bien, haremos algunas matizaciones sobre el particular; lo mismo que la Directiva 95/46, de la cual también debemos afirmar que "la mayoría de los objetivos y principios generales reguladores del régimen jurídico de los tratamientos, recogidos en la misma, siguen siendo válidos, sin desconocer que el paso de los años ha dejado constancia de la existencia de divergencias en la ejecución y aplicación de aquella Directiva"[49], como puede ser el caso de la biometría.

Por último, el Capítulo III, dentro de esta segunda parte, incluye una breve referencia a alguno de los ámbitos de aplicación de los sistemas biométricos dactiloscópicos, sobre todo en el sector público, analizando parte de la regulación sectorial en la materia. Estos ámbitos de aplicación práctica están relacionados con el uso de sistemas biométricos dactiloscópicos en aeropuertos y en puestos fronterizos como medios de identificación de pasajeros y/o personas en frontera. Un sistema biométrico puede constituirse en un medio adecuado de autenticación en el sentido de verificación o control de acceso a lugares públicos y/o privados. Y, así mismo, puede ser, como más arriba ha quedado apuntado, un medio de identificación de personas. También hay que tener en cuenta que, desde una perspectiva criminológica, la utilización de sistemas biométricos puede aportar un medio valioso de lucha contra la delincuencia. Posiciones a favor y en contra de la implantación de sistemas de reconocimiento biométrico pueden manifestarse al respecto. Posiciones escépticas plantean los riesgos que para los derechos individuales y para la propia estructura democrática pueden llegar a representar los sistemas de reconocimiento biométrico.

Así pues, la investigación parte de un acercamiento a la biometría como fenómeno técnico (capítulo I) pasando de la tecnología, en abstracto, al estudio, en concreto, del tratamiento del dato biométrico dactiloscópico dentro del contenido constitucional de los derechos fundamentales que pueden resultar afectados (capítulo II) y de sus

[49] Cfr. GARCÍA-CUEVAS ROQUE, E., "La transparencia en el nuevo Reglamento Europeo de Protección de Datos", *Anales de la Real Academia de Doctores*, Vol 3, 2018, p. 67. No obstante, remitimos al lector al soberbio cuadro comparativo que nos ofrece PIÑAR MAÑAS, J. L., (*et al*), "Cuadro comparativo del articulado del Reglamento (UE) 2016/679 y la Directiva 95/46/CE" en Piñar Mañas, J.L. (Dir.), *Reglamento General de Protección de Datos*. *Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus, 2016, pp. 685 y ss.

aplicaciones prácticas dentro del ámbito de relaciones de coerción entre individuos (a través de un breve capítulo III).

A tal fin, se ha analizado la normativa nacional y de la UE, así como referenciado algunas leyes sobre protección de datos de países de la Unión. Del mismo modo, ha sido necesario acudir a la jurisprudencia y doctrina tanto de los tribunales nacionales (fundamentalmente del TC) como comunitarios (sobre todo, del TEDH).

IV. Cuestiones previas conexas con la lectura biométrica.

Como en otros ámbitos, tales como la utilización de la videovigilancia, la sombra amenazante de un Estado vigilante puede cernirse sobre la implantación generalizada de sistemas de reconocimiento biométrico. Sin embargo, la amenaza apuntada, y ya vislumbrada, en el tan reiteradamente citado libro de Orwell "1984" de un "gran hermano" vigilante se desarrollaba en un entorno autoritario, no democrático, donde la división de poderes y el control judicial independiente no se contemplaban[50]. En relación con esta idea, y siguiendo a Nehf, del gran hermano vigilante, del "*Big brother*", hoy cabe hablar que se ha pasado a una multitud de "*Little brothers*" de situaciones de la vida cotidiana donde la recogida de datos personales es continua y casi inconsciente y en la que los individuos participan voluntariamente[51]. Abundando en la cuestión, esta situación es más frecuente en el ámbito privado que en el público y puede denominarse "*Internet of things*" [52], es decir, un intercambio y una interrogación constante, rápida y *on line* en actos de la vida cotidiana como el consumo, uso de la sanidad, acceso a edificios que generan una multitud de puntos de suministro de datos personales. El elemento novedoso, diferencial, del Internet de las cosas, Internet de los Objetos (en adelante IO), es precisamente que escapa al control inmediato del ser

[50] En este mismo sentido, cfr. ARZOZ SANTISTEBAN, X., *Videovigilancia, seguridad ciudadana y derechos fundamentales*, Navarra, Civitas, Thomson Reuters, 2010, p. 28.
[51] Cfr. NEHF, J. P., *Recognizing the societal value in Information privacy,* 78 Wash. L. Rev. 1 2003, pp. 11-14.
[52]Cfr. LLÁCER MATACÁS, M. R., "La autodeterminación informativa…, op. cit., pp. 66-67. En el Internet de las cosas tu nevera se comunica con la mía, o con el contador de la luz y la televisión con el coche, por supuesto que en su comunicación se intercambian datos del dueño del electrodoméstico en cuestión. Es decir, hay "un internet" en el que dos individuos hablan a través de sus pertenencias, objetos asociados a ellos. También podría considerarse internet de las cosas aquél en el que por el móvil un humano enciende a distancia uno de sus electrodomésticos. Pero en el auténtico internet de las cosas, las cosas se comunican entre sí.

humano. El GPD 29 ha tratado este tema en su Opinión 8/2014[53], circunscribiendo su análisis a tres aspectos del IO: los ordenadores corporales, el "yo cuantificado" y la automatización de viviendas, la denominada domótica. En los dos primeros aspectos citados la captación y tratamiento de datos biométricos se puede producir[54]. Hay quien define internet de las cosas cuando hay más cosas conectadas que personas, por lo tanto, ya casi estamos en el Internet de las cosas[55]. El Intercambio de datos que conlleva el IO hace que, dentro de una red global como Internet, con las facilidades de conexión que le son inherentes, se pueda restar iniciativa, proactividad, en el tráfico de datos a las personas y trasladarla a las cosas. Así, se podría incluso hablar de una cosificación de los individuos, en el sentido de que se convierten en "cosas" sin libertad. Una pérdida de control en el tráfico de datos lleva a una pérdida de libertad de las personas a quienes pertenecen esos datos. Esta exposición tiene, a nuestro entender, paralelismos con la idea ya apuntada por Rodotá de fragmentación del cuerpo electrónico donde el individuo necesita del poder reunificador del derecho de autodeterminación informativa para, precisamente, evitar el riesgo de fragmentación y cosificación apuntado. El

[53] Es muy relevante la Opinión 8/2014 del GPD 29 que afirma que el concepto del Internet de las cosas se refiere a una infraestructura en la cual billones de sensores están engarzados en común, dispositivos del día a día están diseñados para recopilar, procesar, almacenar y transferir datos y al estar asociados con un identificador único interactúan con otros dispositivos o sistemas usando las capacidades de las redes de telecomunicaciones. El Grupo del 29 da un paso más y advierte del verdadero riesgo que puede conllevar para los individuos esta infraestructura ya que permite el tratamiento de datos de personas físicas identificadas o identificables, en definitiva, de datos de carácter personal. El Internet de las cosas, o Internet de los Objetos, al llevar de suyo el tratamiento de datos personales, en el sentido del artículo 2 y 4 del vigente Reglamento General de Protección de Datos, puede permitir analizar los hábitos de dichos individuos y afectar a su privacidad. Cfr. *Opinion 8/2014 on the on Recent Developments on the Internat of Things*. Adopted on 16 September 2014. Article 29 Data Protection Working Party 14/EN WP 223. 1471/14/ES WP 223, p. 4. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf [Fecha de consulta: 09/02/2017].

[54] Se denominan ordenadores corporales a objetos o prendas de uso cotidiano, como un reloj o unas gafas, con sensores añadidos que amplían sus funciones básicas tradicionales (mostrar la hora actual o facilitar la visión). Estos sensores pueden recoger datos del entorno o del propio usuario y transferirlos al fabricante o, incluso, compartirlos con terceros. Un ejemplo es el Android Wear http://developer.android.com/wear/index.html [Fecha de consulta:01/03/2017]. En el segundo aspecto del "yo cuantificado" los sensores están diseñados para registrar hábitos y estilos de vida sobre la base de la captación y registro de datos biométricos como el ritmo respiratorio, los movimientos del abdomen y mostrar información resultante como el nivel de estrés de la persona. La cuestión se agudiza respecto a la posible afección a la privacidad si los datos biométricos captados se relacionan con la salud puesto que son datos especialmente protegidos. Si la aplicación de IO trata datos que puedan referirse a la salud, el origen racial, la vida sexual, etc… del individuo se deberá contar con el consentimiento explícito del usuario de la aplicación a no ser que los datos los haya divulgado previamente de forma pública.

[55] Como ejemplo práctico del Internet de las cosas cabe citar el siguiente: en un foro de poesía que en el lateral se visualizaba el nombre de los usuarios conectados, había 2 humanos y 3 robots tipo *crawlers* de internet como *googlebot*, 6 minutos después en una nueva entrada, ya no aparecía ningún usuario humano, sólo 4 robots *crawlers*, por lo que cabría concluir que los robots les empezaba a gustar más la poesía que a los humanos, los datos concretos son http://www.foroshoshan.com, 17:03, 1 diciembre de 2010, Foro de poesía Usuarios registrados: ABELSAL, Google [Bot], Laura Gimenez, MSNbot Media, Yahoo [Bot] y a las 17:09 Usuarios registrados: Google [Bot], MSNbot Media, Speedy [spider], Yahoo [Bot].

control sobre el propio cuerpo físico y electrónico, con las salvedades que la ley prevea, debe residenciarse en la persona. Y si el riesgo de cosificación existe, como hemos visto al analizar las consecuencias de un cuerpo tecnológicamente observado, este riesgo se dispara si pasamos a un cuerpo modificado con la implantación de un *chip*[56]. En definitiva, Rodotá está poniendo en evidencia un riesgo de vigilancia constante. Parece que se esté cumpliendo la teoría del Benthan[57] del *Panopticon*, en la que imaginaba una cárcel cuya estructura, o diseño constructivo, permitía al carcelero vigilar a todos los presos sin que éstos se dieran cuenta, lo que permitía que desarrollaran una actitud sumisa al saberse constantemente observados.

Con este breve planteamiento inicial, se pretende llamar la atención sobre la posible afección a derechos del individuo proveniente de la utilización de sistemas biométricos. Hay que analizar, desde una perspectiva jurídica, si derechos individuales recogidos en la Constitución Española (en adelante, CE) de profundo arraigo como el derecho a la intimidad personal (art. 18.1 CE), integridad física (art. 10 CE), propia imagen (art. 18.1 CE), libertad de circulación (art. 19 CE) e indudablemente al derecho fundamental a la protección de datos de carácter personal (art. 18.4 CE) quedan comprometidos por la utilización de los sistemas biométricos. A priori entendemos que, sin duda, una persona puede ver afectados alguno o algunos, o todos, los derechos fundamentales citados en la recogida, almacenamiento, tratamiento o cesión posterior de sus datos biométricos dactiloscópicos.

Sin perjuicio del análisis posterior, procede ahora apuntar que en la captación del dato biométrico dactiloscópico pueden verse comprometidos derechos fundamentales como los apuntados, intimidad, integridad física, propia imagen, pero las principales cuestiones y debate jurídico se genera en torno al derecho fundamental a la protección de datos en la fase de tratamiento del dato biométrico dactiloscópico ya recopilado. El análisis de las características de los derechos fundamentales citados se llevará a cabo con el fin de aproximarnos a las posibles zonas de conflicto entre esos derechos y los

---

[56] Son transformaciones progresivas, de la persona "observada" mediante sistemas de videovigilancia y técnicas biométricas se pasa a la persona "modificada" con la implantación de *chips* y etiquetas "inteligentes", en un contexto que se nos identifica cada vez más como *networked persons*, personas perennemente conectadas a la red…". Frente a esta situación el Profesor reivindica "el derecho a hacer silencioso el chip". RODOTÁ, S., *La vida y las reglas…*, op. cit., pp. 109-110.

[57] BENTHAM, J., *El Panoptico.* https://iedimagen.files.wordpress.com/2012/02/bentham-jeremy-el-panoptico-1791.pdf [Fecha de consulta:21/03/2018].

procesos de recogida y de tratamiento de datos biométricos dactiloscópicos. Así, por ejemplo, el derecho fundamental a la protección de datos de carácter personal está enunciado en el artículo 18.4 CE, pero ha sido la jurisprudencia del Tribunal Constitucional quien ha formulado, o incluso podríamos decir "descubierto", el derecho fundamental a la autodeterminación informativa.

El citado artículo 18.4 CE contiene un mandato al legislador para que regulara, como así hizo, el uso de la informática para que ésta no dañara los derechos al honor, a la intimidad personal y familiar y a la propia imagen y, en general, para que no menoscabara el ejercicio de los demás derechos[58]. Pues bien, ese mandato que fructificó en la antigua LORTAD, en la (LOPD) y en la Ley Orgánica 3/2018[59] cobra, si cabe, plena vigencia y relevancia al tener las nuevas tecnologías de la información y las comunicaciones la virtualidad práctica, real, de recoger, tratar, almacenar y reproducir elementos intrínsecos al propio cuerpo humano. Estos elementos ya no son solo datos o informaciones sobre un individuo, sino que son el individuo en sí mismo, pudiendo quedar comprometidos o afectados los derechos a que hace referencia el citado artículo 18.4 del texto constitucional.

La información sobre aspectos físicos de los individuos puede afectar a ámbitos tan críticos como su intimidad y tener un alto potencial discriminatorio, afectando así al principio de igualdad. Aunque también es cierto que, para la doctrina más especializada,

[58] Conviene recordar la gestación jurisprudencial que el Derecho Fundamental a la protección de datos personales ha tenido en nuestra jurisprudencia Constitucional. La STC 292/2000, de 30 de noviembre, reconoce un nuevo derecho fundamental que no es el derecho a la intimidad personal, aunque en parte coincida con ella. Con anterioridad a esta Sentencia 292/2000, se habían dado pasos significativos como la aprobación de la LORTAD, que en su Exposición de Motivos distinguía claramente entre los conceptos de intimidad y privacidad considerando aquélla más amplia respecto de ésta. Así mismo, la Sentencia 254/1993 habló de un nuevo derecho. Y en el mismo camino de "descubrimiento" de este nuevo derecho la STC 11/1998 puso de manifiesto con claridad que no solo es el consentimiento informado o la autorización de la Ley en origen, el presupuesto de un tratamiento lícito de los datos de carácter personal sino también el respeto posterior a la finalidad para la que fueron obtenidos que, a modo de renovación constante y en cada caso de la licitud inicial del tratamiento, hace lícito el tratamiento posterior. Así un tratamiento posterior que no respete la finalidad inicial para la que fueron recabados los datos que ahora se tratan es ilícito. En definitiva, el respeto a la finalidad se convierte en la vía que el titular de los datos personales tiene para el ejercicio de su derecho a la protección de datos o autodeterminación informativa. Cfr. LUCAS MURILLO DE LA CUEVA, P., "El derecho fundamental a la protección de los datos relativos a la salud*"* en *Estudios de Protección de datos de carácter personal en el ámbito de la salud*. Madrid Barcelona, Marcial Pons-Agencia Catalana de Protección de datos, 2006, pp. 22 y ss.

[59] Hay que tener en cuenta que el 6 de septiembre de 2018 se aprobó el Real Decreto-Ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, el cual ha quedado derogado por la Ley Orgánica 3/2018.

el hecho de que el dato de perfil de ADN y el dato biométrico puedan considerarse identificativos, y no datos de salud, facilita más su tratamiento[60].

Dentro de una clasificación de los datos y la información, que de ellos se desprenda, tanto aquéllos como ésta pueden clasificarse como atinentes bien a la intimidad, o bien, a la privacidad. Esta diferente tipología de datos, íntimos o privados, implica distintos niveles de protección. La incardinación de los datos biométricos dactiloscópicos dentro de la categoría de datos que afectan a la intimidad, o bien, a la vida privada del individuo será objeto de análisis, puesto que las consecuencias en cuanto al régimen jurídico de su recogida, almacenamiento y tratamiento varía de una a otra categoría. No es, por ello, baladí la distinción de considerar al dato biométrico como conformador de la esfera de la intimidad o de la privacidad. Analizaremos, así mismo, la distinción entre categorías de datos que tienen puntos de confluencia, pero que son esencialmente distintas. Así, como ya hemos expuesto, el dato biométrico puede considerarse dato identificativo y ésta es una característica que lo distingue, por ejemplo, del dato de salud. No obstante, hay puntos de confluencia entre dato biométrico y de salud, sobre todo en aquellos casos en que aquél revele una enfermedad. Todas ellas serán cuestiones a discernir.

[60] Cfr. TRONCOSO REIGADA, A., *La protección de datos personales en busca del equilibrio*, Valencia, Tirant lo blanch, 2010, p. 783.

PRIMERA PARTE: Base científica del estudio.

Capítulo I. Los datos biométricos.

1. Concepto de dato biométrico.

A los efectos de este estudio, y siguiendo al GPD 29 en su Dictámen 4/2007 (WP136), los datos biométricos pueden definirse como: "propiedades biológicas, características fsiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad"[61]. El WP193[62] nos indica que el dato biométrico puede tratarse y almacenarse de dos formas diferentes: en bruto, permitiendo reconocer la fuente de la que procede, o bien, la plantilla biométrica, es decir, solo ciertos rasgos o características. Más adelante nos detendremos en ello.

1.1. Antecedentes históricos de la biometría dactiloscópica.

La biometría es un concepto amplio que nosotros abordaremos en una de sus facetas: la relativa a la medición de las características físicas o fisiológicas de una persona, de un individuo de la especie humana. Además, dentro de los posibles usos o aplicaciones de la biometría será la finalidad de la identificación, y en su caso la autenticación, de los individuos la que merezca nuestra atención. Y, a su vez, dentro de las múltiples características físicas de una persona, que puedan utilizarse para su identificación, nos centraremos en las huellas dactilares. Lo cierto es que, en la base de este aparente "nuevo" interés por la biometría y el tratamiento de datos obtenidos del individuo, existe una aspiración o necesidad tan antigua como el propio hecho de la vida del hombre sobre la tierra: la necesidad de identificar al semejante y de ser identificado. Ya en las primeras y primitivas formas de vida en común se planteó la necesidad de identificar al miembro del grupo. Esta identificación se resolvía, en ocasiones, con fórmulas tan crueles como a la vez infalibles: la mutilación de determinadas partes del cuerpo (la nariz o las orejas), la marca con hierro candente, el tatuaje, etc[63]. Como

[61] GPD 29 (WP193). Dictamen 3/2012 sobre la evolución de las tecnologías biométricas…, op.cit., p. 4.
[62] Ibíd.
[63] La marcación de un ser humano por otro con fines de identificación ha generado innumerables ejemplos: periódico "Ya" (28-1-1971) noticia gráfica donde se ve que un policía de Tucson –Arizona-

señala Rico Pérez, también en el mundo de la ficción literaria, teatral o dramática, el reconocimiento o "agnición" de una persona por otra, u otras, por medio de sus características físicas tiene escritas páginas imborrables. Así el citado reconocimiento puede producirse por signos o medios físicos congénitos (manchas de nacimiento)[64] o bien adquiridos en el decurso de la vida (cicatrices)[65].

Pero, en una evolución de la técnica identificativa, pasando de la modificación del propio cuerpo, que se quiere identificar, a la lectura o reconocimiento de un elemento propiamente identificador de dicho cuerpo, nos encontramos con el amplio y complejo campo de la lofoscopia[66]. Veremos a continuación cómo los antecedentes reseñados, relativos a las huellas dejadas por la epidermis humana, se refieren a uno de los posibles sistemas de obtención de datos biométricos, la huella dactilar. Con ello queremos poner de manifiesto que la mayoría del resto de sistemas biométricos (de reconocimiento y tratamiento) se han desarrollado al albur de las nuevas tecnologías[67]. No debemos

---

marca con una W la frente de un estudiante, unos ciento cuarenta universitarios fueron arrestados y marcados. RICO PÉREZ, F., "La individualización*… ",* op. cit., p. 28.

[64] Este tipo de reconocimiento es magistralmente descrito por Miguel de CERVANTES en *La Gitanilla*. *Novelas ejemplares.* Ahí se recoge el relato de cómo la madre de Preciosa reconoce a su hija, "[…] arremetió a ella, y sin decirle nada, con gran priesa le desabrochó el pecho y miró si tenía debajo de la teta izquierda una señal pequeña, a modo de lunar blanco, con que había nacido, y hallóle ya grande, que con el tiempo se había dilatado. Luego, con la misma celeridad, la descalzó, y descubrió un pie de nieve y de marfil, hecho a torno, y vio en él lo que buscaba, que era que los dos dedos últimos del pie derecho se trababan el uno con el otro por medio con un poquito de carne, la cual, cuando niña, nunca se la había querido cortar, por no darle pesadumbre". Citado por RICO PÉREZ, F., "La individualización…", op. cit. p.11.

[65] Este reconocimiento por marcas indelebles en el cuerpo se recoge en la *Odisea*. En uno de sus pasajes se hace referencia a la cicatriz de la herida que sufrió Ulises, cuando anduvo de caza en el monte Parnaso, que permite el espontáneo reconocimiento de su vieja ama; y el mismo Ulises utiliza su cicatriz para ser reconocido, entre otros, por Laertes. Ibíd.

[66] "Lofoscopia: deriva de las palabras griegas *lofos* (cresta) y *skopia* (examen u observación), designa el capítulo de la policía científica encargado del examen de las huellas dejadas por una parte cualquiera de la epidermis y más concretamente de aquellas caracterizadas por la presencia de crestas. Se subdivide en dactiloscopia, quiroscopia y pelmatoscopia". La dactiloscopia estudia las crestas papilares de las yemas de los dedos, la quiroscopia las de las palmas de las manos y la pelmatoscopia las de las plantas de los pies. Cfr. DE ANTÓN y BARBERÁ, F., *Iniciación a la Dactiloscopia y otras Técnicas Policiales*, Valencia, Tirant Lo Blanch, Colección Ciencia policial, 2004, p. 293.

[67] Sin duda, en el desarrollo tecnológico han jugado un papel determinante los programas espaciales con vehículos tripulados de la Administración Nacional de Aeronáutica y del Espacio (NASA) en los años sesenta y setenta. Estos programas supusieron un impulso claro de actividades de investigación y desarrollo de la Telemetría. La telemetría biomédica podría citarse como antecedente de algunos de los actuales sistemas de reconocimiento y tratamiento de datos biométricos (lectura del ritmo cardiaco, presión arterial, etc…). En este sentido, Avanzini Blanco señala que "… las actividades de investigación y desarrollo sobre Telemetría, emprendidas por la misma NASA, la cual, aplicada a parámetros médicos, permitía la monitorización de las funciones fisiológicas de los astronautas por médicos de especialidades diversas, desde estaciones terrestres a millones de kilómetros de distancia.

Inicialmente los científicos de la NASA estaban preocupados por los efectos psicológicos que, por la continua exposición a una gravedad cero, se podrían presentar en los tripulantes, con los consiguientes efectos perjudiciales para su salud y, por qué no decirlo, para el éxito de la misión. Habiéndose

olvidar que el espectro de características fisiológicas, en las que se puede basar un sistema de reconocimiento biométrico, conforma un amplio campo que abarca desde la huella dactilar, en la que nos detendremos, a la huella palmar (palma de la mano), la geometría de la mano/dedos, la cara, el iris o la retina. También merece especial mención la técnica de reconocimiento facial a la que el GPD 29 ha dedicado su atención en el Dictamen 02/2012 dentro del contexto de servicios en línea y móviles, definiéndola como "[…] el tratamiento automático de imágenes digitales que contienen las caras de personas a fines de identificación, autenticación/verificación o categorización de dichas personas" [68]. En relación con esta técnica se ha pronunciado la Agencia Española de Protección de Datos (AEPD) en su Informe jurídico 0392/2011[69].

Pero también existen otras características, como indica Simón Zorita menos utilizadas, pero también mensurables, como la forma de la oreja, el termograma del cuerpo (o de partes de él), la estructura de las venas, la estructura de poros (en alguna zona del cuerpo como por ejemplo en la cara o en la yema del dedo) o el olor corporal. Junto a estas características fisiológicas las de comportamiento como la voz, la escritura, la firma escrita, la forma de pulsar un teclado o el modo de andar son características reconocibles en un sistema biométrico[70].

---

comprobado que cada astronauta podía ser monitorizado por médicos desde la Tierra, una pléyade de científicos e ingenieros desarrollaron sofisticados sistemas de telemetría biomédica y telecomunicaciones para ser utilizados al efecto. Y así, de una forma continuada se podía analizar la información transmitida sobre el ritmo cardíaco, la presión sanguínea sistólica y diastólica y la temperatura de cada uno de los tripulantes". Cfr. AVANZINI BLANCO, E., "Tecnologías para una asistencia sanitaria global: la telemedicina" en *Tecnologías del espacio aplicadas a la industria y servicios de la defensa*. Documentos de Seguridad y Defensa nº 41, Centro Superior de Estudios de la Defensa Nacional, Ministerio de Defensa, mayo de 2011.

[68] Dictamen 02/2012 sobre reconocimiento facial en los servicios en línea y móviles. 00727/12/ES WP 192. Adoptado el 22 de marzo de 2012, p. 2. Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_es.pdf [Fecha de consulta: 09/02/2017].

[69] Disponible en: https://www.aepd.es/informes/historicos/2011-0392.pdf [Fecha de consulta: 02/11/2018].

[70] Lo que para este autor no cabe considerar como una técnica de reconocimiento biométrico es la autenticación de personas basada en el ADN por los tiempos de respuesta que deben satisfacer estos sistemas que los hacen no realistas o inviables. SIMÓN ZORITA, D., op. cit., pp. 11 y 12. No obstante, hay que tener en cuenta los avances en este punto de los que ya se hace eco el GPD 29 en su Dictamen 3/2012 al decir que: "Uno de los principales cambios en las tecnologías de la elaboración de perfiles de ADN es la reducción del tiempo necesario para las operaciones de correspondencia y secuenciación del ADN. Los continuos avances realizados a lo largo de los años por los investigadores académicos y los desarrolladores de biotecnología han reducido el tiempo necesario para la generación de un perfil de ADN de días a horas e incluso a fracciones de hora. […] Es muy probable que en un futuro próximo sea posible elaborar perfiles de ADN y realizar correspondencias de muestras en tiempo real (o casi), utilizando dispositivos portátiles, lo que será el punto de partida para el desarrollo de sistemas de autentificación o identificación biométrica del ADN con mayores niveles de precisión en relación a la autenticación mediante impresiones dactilares, voz y reconocimiento facial*"*. GPD 29 (WP 193), op. cit., p. 27.

Dentro de este amplio espectro de características fisiológicas y comportamentales, que pueden ser objeto de reconocimiento biométrico, está adquiriendo creciente auge la denominada firma biométrica, la cual, en definitiva, no es sino la captación del comportamiento del individuo en la realización de su firma manuscrita. Para la captación electrónica de la firma manual de una persona existen dos tipos de dispositivos de contacto sensible capaces de almacenar los datos de esta firma manuscrita. Uno de ellos, que podríamos denominar de firma estática, se limita a grabar la imagen de la firma, que se puede efectuar o no directamente sobre el aparato, para comparar la imagen de la firma digitalizada con otra del mismo firmante, y así comprobar las posibles coincidencias. Y el otro tipo de dispositivo o sistema es la firma dinámica, mucho más sofisticado, que además realiza un análisis de la forma, la velocidad, la presión del bolígrafo y la duración del proceso de firma. Estos segundos sistemas son capaces de captar los cambios de velocidad y la presión en el proceso de firma. De esta forma, se recogen datos biométricos comportamentales del firmante ya que cada individuo desarrolla en el proceso de firma unas características diferentes. Entendemos que, aunque ambos tipos de dispositivos pueden servir para identificar a las personas y, de hecho, así están funcionando en numerosas entidades financieras, el segundo sistema al añadir características de comportamiento aumenta las características manejadas en la identificación y puede suponer un aumento en la seguridad. Con todo ello puede revelarse como un proceso adecuado para la identificación de las personas. En el sentido expuesto el GPD 29 define la firma biométrica como:

> "[…] es una técnica biométrica basada en el comportamiento, que mide la conducta de una persona según lo expresado por la dinámica de su firma manuscrita. Mientras que el reconocimiento de firma tradicional se basa en el análisis de características fijas o geométricas de la imagen visual de la firma (aspecto de la firma), la firma biométrica, en cambio, hace referencia al análisis de las características dinámicas de la firma (cómo se hizo la firma) y esto hace que estas técnicas se denominen «firma dinámica».
>
> Las características dinámicas típicas medidas por un sistema de firma biométrica (como un tablero digitalizado) son la presión, el ángulo de escritura, la velocidad y aceleración del bolígrafo, la formación de las

> letras, la dirección de los rasgos de la firma y otras características dinámicas únicas. […]
>
> Algunos dispositivos de reconocimiento de firma pueden realizar verificaciones mediante la combinación del análisis tanto estático (imagen) como dinámico (presión, ángulo, velocidad, etc.) de las características de la firma[71].”

El GPD 29 plantea, en su Dictamen 3/2012, lo que denomina “riesgos de protección de datos asociados a la utilización de firmas biométricas” identificándolos en tres categorías: la “precisión”, el “impacto” y la “anti-suplantación”. Consideramos que los riesgos englobados bajo el término de “impacto” son los más relevantes en relación con la protección de datos ya que los sistemas de firma biométrica al tratar datos basados en el comportamiento pueden captar cambios en el comportamiento de firma que, a su vez, pueden responder a cambios fisiológicos producidos por una enfermedad en ciernes o ya avanzada. Indudablemente estos cambios junto al planteamiento de problemas funcionales al sistema, en el sentido de dificultar la verificación de la identidad de los individuos, pueden constituir la captación de datos sensibles merecedores de una especial protección.

Más adelante analizaremos si los datos así captados son datos personales; y si lo son, veremos los principios que en su recogida y tratamiento deben respetarse. Podría incluso llegarse a considerar que los datos de firma biométrica, como sostiene Martínez Ferre[72], son un tipo de firma electrónica conforme a la definición de la Ley 59/2003, de 19 de diciembre, de firma electrónica. Si esto fuera así habría que tenerlo en cuenta no ya en el proceso de declaración e inscripción del fichero que lo contenga en la AEPD, ya que ha desaparecido la obligación formal de inscripción, si no en la política de privacidad establecida por el responsable. Otras cuestiones relevantes en relación con el almacenamiento de firmas biométricas son los niveles de seguridad aplicables a los ficheros que las contengan. En la determinación de estos niveles de seguridad influye la finalidad del tratamiento. Si la finalidad es la identificación de las personas podría plantearse unas medidas de seguridad de nivel básico, tal y como las definía el Real

[71] GPD 29 (WP193) Dictamen 3/2012. “Sobre la evolución de las tecnologías …”, op. cit., p. 30.
[72] MARTÍNEZ FERRE, A., https://psnsercon.com/blog/index.php/la-firma-biometrica-y-la-ley-de-proteccion-de-datos. [Fecha de consulta: 8/09/2016].

RLOPD. Pero otra cuestión es si los datos de la firma biométrica se utilizan con finalidades más ambiciosas, en el sentido de más amplias. Si, como hemos expuesto, se almacenan datos de velocidad y nivel de presión en la ejecución del trazo se podrían realizar estudios grafológicos del individuo que exceden, con mucho, de la simple identificación y abarcarían a la obtención de un perfil de individuo evaluando características de su personalidad. Y, desde luego, los síntomas de algunas enfermedades o dolencias graves podrían revelarse con estos sistemas ya que el trazo inseguro se produce en enfermedades como el párkinson o en enfermedades cardiovasculares graves. En este caso, entraríamos de lleno en un ámbito distinto; el formado por los datos de salud que constituye por su criticidad datos merecedores de especial protección y con exigencias legales de adopción de medidas de seguridad de nivel alto.

Centrándonos en los sistemas de huella dactilar, y siguiendo en esta aproximación histórica a De Antón[73], cabría remontar tanto en Europa como en América los antecedentes históricos de los dibujos papilares al paleolítico. Los hombres en aquel momento grabaron toscamente sobre roca petroglifos, es decir, las líneas y filigranas que apreciaban a simple vista en sus manos y pies. Otros autores como Jain[74] y Maltoni[75] se remontan a los hallazgos arqueológicos de poblaciones asirias y chinas del año 6000 a.C., donde la huella dactilar aparece impresa en restos de objetos de cerámica utilizándose como medio de identificación del alfarero autor de la obra. También documentos chinos de la época tienen estampada la huella dactilar como firma del documento. Estos mismos autores refieren cómo los ladrillos de la antigua ciudad de Jericó presentan huellas dactilares. En todo caso, de estos ejemplos no cabe deducir la existencia de un sistema universal basado en la huella dactilar que se utilizase para la identificación de individuos en aquellos tiempos.

De Antón refiere cómo del período de la antigüedad y de la Edad Media hay pocos datos. No obstante. cabría citar el Antiguo Testamento que, en el libro de Job capítulo 37 versículo 7, dice*: "*Sobre la mano de todos pone un sello, para que todos conozcan

[73] DE ANTÓN Y BARBERÁ, F., op. cit., p. 23.
[74] Vid., JAIN, A.K., BOLLE, R.M., PANKANTI, S. (editors), *Biometrics: Personal Identification in a Networked Society*, Kluwer Academic Piblishers, 1999.
[75] Vid., MALTONI, D., Maio, D., JAIN, A.K., PRABHAKAR, S., *Handbook of Fingerprint Recognition*, Springer -Verlag. 2003.

Su obra". Hace referencia, aunque sea en sentido figurado, a que conozcan la obra de Dios, de ahí el "Su" en mayúsculas. La huella de Dios, o su grandeza, queda patente en la huella que cada hombre lleva en su mano, en el sello específico, en las huellas dactilares diferentes para cada uno. Esa diferencia que Dios ha puesto en cada uno de nosotros nos hace ser únicos, irrepetibles y es la base de la dignidad humana. Indudablemente también sirve para que se conozca la obra de cada hombre, en inglés "*He sealeth up the hand of every man; that all men may know his work.*". Así, cabe también citar las leyes de Taiho (año 702), tomadas de las leyes de Yung-Hwui (año 650 a 655). En Oriente se utilizó la estampación, en documentos antiguos, de la mano o los dedos. Parece ser que en China se utilizó la estampación desde al menos el siglo XIV. Joao de Barros, escritor y explorador, escribió que los comerciantes chinos estampaban las impresiones de las palmas de las manos de los niños sobre papel con tinta. Podría considerarse este un antecedente del uso de huella dactilar para identificación de personas[76].

Pero no solo la identificación de los dibujos papilares sino su ordenación es lo que representó el avance fundamental en el reconocimiento de las huellas de personas para su identificación. Así, según De Antón, la primera descripción de la ordenación de las papilas del tacto y la situación de los poros en la cumbre de las crestas la realizó el italiano Marcelo Malpighi en la segunda mitad del siglo XVII[77]. En esa misma segunda mitad del siglo XVII y principios del XVIII, el botánico y médico inglés Nehemías Grew[78] establece por primera vez la separación de las áreas táctiles que componen la cara palmar, de la palma de la mano. Así mismo, este científico inglés descubrió cómo estas áreas táctiles se delimitan por las divergencias y prolongaciones délticas, de los dedos. En Alemania Cristian Jacobo Hintze en 1747 estudia y determina la disposición

[76] En este mismo sentido, y siguiendo con los antecedentes de identificación de personas a través de huella dactilar, cabe hacer referencia al método que los alfareros hace más de mil años utilizaban en China donde dejaban impresas sus huellas dactilares en los objetos que fabricaban como medio de distinción del resto. Más reciente (Siglos XVIII y XIX) la industria de fabricación de tinajas para almacenar vino en Colmenar de Oreja (Madrid) se sellaba la autoría de cada tinaja con la huella del dedo del tinajero. Cfr. Instituto Nacional de Tecnologías de la Comunicación (INTECO). *Guía sobre las tecnologías biométricas aplicadas a la seguridad.* Instituto Nacional de Tecnologías de la Comunicación (INTECO), Observatorio de la Seguridad de la Información, Ministerio de Industria, Turismo y Comercio, Gobierno de España, octubre 2011, p. 5.

[77] DE ANTÓN Y BARBERÁ, F., op. cit., p. 24.

[78] Este morfologista inglés publicó en 1684 el primer estudio científico sobre la estructura de crestas, valles y poros de las huellas dactilares. Posteriormente muchos investigadores han trabajado en este campo. Así, en 1823 Purkinje estableció un sistema de clasificación de huellas en nueve clases en función de la configuración de la estructura de las crestas. SIMÓN ZORITA, D., op. cit., p. 47.

de los surcos de las plantas de los pies. Y el prusiano Juan Cristóbal Andrés Mayer sienta, a finales de ese siglo XVIII, el siguiente principio: "la disposición de las crestas cutáneas nunca se duplica en dos personas". Es ya en el siglo XIX, y gracias al profesor Juan E. Purkinje, cuando se establece la primera clasificación de nueve tipos de dactilograma[79]. Los estudios científicos de principios del S XIX llegaron a dos conclusiones fundamentales para el desarrollo posterior de sistemas de identificación a través de huella dactilar: primera, no existen dos individuos cuyas huellas tengan un patrón[80] de crestas igual o coincidente, y segunda, el patrón de crestas de un individuo permanece invariable toda su vida.

Si es cierto que estos pueden considerarse antecedentes de un sistema de identificación segura de personas como es la huella dactilar, palmar o plantar, no es menos cierto que no es hasta finales del siglo XIX y principios del XX cuando se desarrolla un verdadero método técnico de identificación segura. Ya en este periodo de método técnico, tiene un puesto destacado el francés Alfonso Bertillon que, avanzando un poco más en la identificación de individuos, desarrolló a finales del siglo XIX un sistema antropométrico. Bertillon diseñó un sistema de descripción antropométrica del delincuente. Los actuales sistemas de reconocimiento facial utilizan en su funcionamiento el principio de medición enunciado por Bertillon. Así Bertillon, jefe del departamento fotográfico de la policía de París, desarrolló el sistema antropométrico (*Bertillonage*) en 1883. Es el primer sistema preciso, utilizado ampliamente para identificar a criminales. Este sistema funcionaba midiendo de forma muy precisa las longitudes y anchura de ciertas partes del cuerpo[81] y también registraba marcas, tatuajes o cicatrices. Por tanto, el sistema antropométrico se basaba en un sistema de medidas realizadas a los detenidos, por ejemplo, la medición de la longitud de la oreja derecha. Bertillon fue el primero en utilizar la oreja como medio para identificar a las personas. A través de este sistema antropométrico cabía identificar a los individuos ya que, en su

[79] Dactilograma: "conjunto de crestas papilares correspondientes a cada dedo". Cfr. DE ANTÓN Y BARBERÁ, F., op. cit., p. 291.

[80] En una primera aproximación al concepto de patrón seguimos a Simón Zorita que define el *área patrón* de una huella como aquella "… formada por todas aquellas crestas y valles circunscritas entre dos crestas llamadas crestas de referencia. Estas crestas se definen como las dos crestas divergentes más internas de la estructura de la imagen que circunscriben la zona central de la huella". Veremos como los sistemas de lectura de huella dactilar consideran estas áreas patrón de las huellas en las que se encuentran dos puntos singulares de referencia los denominados *deltas* y *núcleo*s. Cfr. SIMÓN ZORITA, D., op.cit., p. 54.

[81] "Longitud del brazo izquierdo, longitud, anchura y el diámetro del cráneo, la braza, altura sentado y de pie, longitud dedo medio y pequeños, longitud pie izquierdo, longitud oreja derecha, etc." DE ANTÓN Y BARBERÁ, F., op. cit., p. 25.

opinión, se podía enunciar un principio por el cual "la oreja gracias a los múltiples valles y colinas es el factor más importante desde el punto de vista de la identificación"[82]. También se registraban, como hemos dicho, otras características físicas como color de los ojos, tatuajes o cicatrices y la fotografía del individuo de frente y de perfil derecho. En definitiva, Bertillon desarrolló una teoría en virtud de la cual cabía establecer, en su opinión, de forma invariable en el tiempo una cierta combinación de medidas del cuerpo de un individuo, siendo así factible identificar a esa persona en concreto a través de las medidas de ciertas partes de su cuerpo[83].

Aunque es indiscutible la importancia de las aportaciones de Bertillon a la identificación de personas, su procedimiento de medidas corporales fue abandonado, al no aportar medidas totalmente fiables y únicas en algunos casos, como por ejemplo, en el supuesto de personas extremadamente similares como los gemelos. No cabía establecer, por la medida de una parte del cuerpo, la identidad de un individuo, sino que era necesario acudir a múltiples datos de medida para establecer esa identidad y nunca con absoluta o, al menos, alta probabilidad de seguridad en la identificación.

De este modo, cabe afirmar, que con la aparición de la dactiloscopia la antropometría cayó en desuso. Ya a principios del S XX se admitían de forma generalizada en la identificación de individuos a través de huella dactilar tres principios básicos: primero, la estructura de crestas y valles de cada individuo es única y se asocia de forma unívoca a su identidad; segundo, es posible que la estructura de crestas y valles de un individuo varíe a lo largo de su vida pero se trataría de una variación mínima que sigue permitiendo la clasificación sistemática de la huella y, por ende, la identificación del individuo; y tercero, junto a la estructura de crestas y valles, las minucias son únicas en cada persona e invariables en el tiempo. El primer y tercer principio siguen siendo hoy el pilar para la identificación de los individuos y el segundo permite la clasificación de las huellas dactilares. No obstante, cabría preguntarse si las nuevas tecnologías han traído de nuevo a la antropometría[84] al escenario de la identificación de individuos retomando relevancia sistemas antropométricos casi olvidados[85].

---

[82]. Ibíd., p. 263.

[83] Cfr. Instituto Nacional de Tecnologías de la Comunicación (INTECO), *Guía sobre las tecnologías biométricas*…, op. cit., p. 5.

[84] Reproducimos, por su interés, la definición del Diccionario de la Real Academia de la Lengua Española de antropometría y biometría. "Antropometría: Tratado de las proporciones y medidas del

En este camino de la identificación de las personas a través de su huella dactilar son relevantes las aportaciones de Galton. A principios del siglo XX, Galton lleva a cabo una ordenación de los dibujos digitales e implanta la reseña decadactilar con impresiones rodadas de un costado a otro, que aun hoy en día sigue vigente en la práctica policial. Por último, Edward Richard Henry[86], apoyándose en los estudios de Galton, consigue una clasificación y método dactilar práctico conocido como sistema de Galton-Henry, que se ha extendido por todo el mundo y que perfeccionado es utilizado en el F.B.I. (EE.UU.)[87]. A partir del S XIX, se instauraron en las agencias policiales de todo el mundo sistemas de identificación a través de huella digital y se crearon bases de datos criminales. En nuestro país representa un hito relevante en la identificación de individuos la creación en 1911 del Servicio de Identificación dactilar dentro de la Jefatura Superior de Policía de Madrid. Y en lo que a la historia de la dactiloscopia en España se refiere, ocupa un lugar destacado Olóriz que, entre otros avances, elaboró el número de registro personal, antecedente del actual DNI. Así la incorporación de la huella dactilar al documento nacional de identidad de todos los españoles se puede considerar fue una "destilación" del contenido o "campos" de la ficha policial[88].

---

cuerpo humano." "Biometría: Estudio mensurativo o estadístico de los fenómenos o procesos biológicos". http://lema.rae.es/drae/?val=antropom%C3%A9trico. [Fecha de consulta: 7/04/2017].

[85] En el ámbito de las técnicas policiales de identificación, tras el antecedente citado establecido por Bertillón, ya en el siglo XX en el año 1979 un oficial de la policía holandesa Van Der Lugt retomó la individualización de la oreja como método de identificación de personas. Con anterioridad W. J. Herschel a finales del siglo XIX y principios del siglo XX como responsable del gobierno civil de Bengala utilizó las impresiones dactilares sobre documentos y recibos como medio de identificación de personas y método para evitar suplantaciones de personalidad entre los hindúes. Es la primera autoridad que aplica de modo oficial las impresiones digitales (dactilares) para identificar a las personas. Realmente son estas impresiones dactilares (más ampliamente lofoscópicas) las que podemos considerar antecedentes de los sistemas de lectura biométrica actuales ya que debe distinguirse claramente entre impresión y huella. Las huellas se dejan involuntariamente por una persona (puede ser el autor de un hecho delictivo o no) y necesitan de reactivos apropiados para ponerlas de manifiesto. Sin embargo, las impresiones se obtienen conscientemente de la persona a que pertenecen. Así las huellas representan una pequeña parte del total del dibujo papilar que sí que consta completo en la impresión lofoscópica. Henry Faulds, contemporáneo de Herschel, y en el ámbito de la investigación policial concluye que por medio de las huellas dactilares puede identificarse al autor de un hecho delictivo. DE ANTÓN Y BARBERÁ, F., op. cit., p. 263.

[86] Sir Edward R. Henry ante las deficiencias apreciadas en el sistema de Bertillon buscó otras técnicas de identificación de personas tomando en consideración las investigaciones de Sir Francis Galton que utilizaba la huella dactilar como método de identificación. Sir Edward Henry inicialmente en Bengala y después en Londres, año 1901, implantó una oficina de huella dactilar. Cfr. Instituto Nacional de Tecnologías de la Comunicación (INTECO), *Guía sobre las tecnologías biométricas…*, op. cit., p. 6.

[87] DE ANTÓN Y BARBERÁ, F., op. cit., p. 26.

[88] Esta reminiscencia policial ya la puso de manifiesto RICO PÉREZ en la Revista YA, domingo 14 de mayo de 1989, p. 8, afirmando que el documento nacional de identidad ni era documento, ni nacional, ni de identidad y el hecho de mantener la huella dactilar en el mismo "es infamante y tercermundista, como si todos los españoles fuéramos criminales en potencia". Lo cierto es que fruto de esta y otras adverencias y reflexiones el legislador suprime la huella del documento personal externo que se entrega al titular. Así

Entre las muchas aportaciones a la dactiloscopia, el profesor Olóriz definió el dactilograma como "el conjunto de líneas que existen en las yemas de los dedos y el dibujo de cada uno de éstos, impreso, como si fuera un sello, en circunstancias adecuadas*"* [89].

Dando un salto en el tiempo, es a partir de los años 60 del pasado siglo cuando comienzan a desarrollarse sistemas de reconocimiento automático de huellas digitales. Podemos citar como uno de los primeros sistemas de identificación automática a través de huella dactilar de uso comercial el *Identimat* desarrollado por la empresa *Shearson Hamil* en los años 70 del siglo pasado[90]. Ya en la década de los años 90, se produce la informatización decadactilar desarrollándose el sistema S.A.I.D. (Sistema Automático de Identificación Dactilar). Actualmente, dependiente del Ministerio del Interior la Comisaría General de Policía Científica, del cuerpo nacional de policía, tiene distribuidas sus funciones por áreas de actividad siendo dos de esas áreas la antropología forense y el sistema S.A.I.D. Este sistema, basado en un *software* muy especializado, es capaz de leer e interpretar un dactilograma y comparar sus puntos característicos. La función de comparación se lleva a cabo con los dactilogramas existentes en unas bases de datos, si el resultado de la comparación es negativo el nuevo dactilograma se archiva en la base de datos. El sistema realiza tres procesos básicos: el primero, la lectura e interpretación de dactilogramas donde se detectan, en número y posición, los puntos característicos del dactilograma; el segundo, la comparación automática de los puntos característicos detectados con los existentes almacenados en las bases de datos. Como resultado de esta segunda fase, el sistema presenta una relación de candidatos o coincidencias ordenada de mayor a menor en el grado de semejanza. Por último, la tercera fase muestra en pantalla las imágenes del dactilograma de los candidatos y es el cotejo realizado por el usuario del sistema el que determina finalmente la coincidencia y, en definitiva, realiza la identificación.

---

la Orden de 12 de julio de 1990, sobre contenido y formato del documento nacional de identidad, dice textualmente en su primer párrafo: "El avance de las nuevas tecnologías aconseja la modificación del formato y de los datos a consignar en el nuevo documento nacional de identidad, haciéndolo más fiable, seguro y manejable, para lo cual se estima conveniente cambiar su diseño y suprimir del mismo la impresión dactilar, que únicamente será recogida en el documento-base, por necesidades de identificación civil" . BOE martes 17 de julio de 1990, número 170, pp. 20563-20564.

[89] DE ANTÓN Y BARBERÁ, F., op. cit., p.43.

[90] Cfr. Instituto Nacional de Tecnologías de la Comunicación (INTECO), *Guía sobre las tecnologías biométricas*…, op. cit., p. 6.

Vemos cómo la historia de la identificación de las personas a través de sistemas antropométricos, en un primer momento, y a través de sistemas dactiloscópicos, después, ha estado y está unida a la técnica y ciencia policial de investigación del delito y persecución del delincuente. Hoy la identificación a través de perfiles genéticos de ADN se revela como poderosa arma de identificación de autorías criminales. En concreto, el ADN no codificante es equiparable a la huella dactilar. Así el preámbulo de la Ley Orgánica de Base de Datos Policial de Identificadores Obtenidos a partir del ADN[91] establece: "Desde que en 1988, en el Reino Unido y por primera vez, la información obtenida del ADN fuese utilizada para identificar y condenar al culpable de un delito, tanto en España como en el resto de los países de nuestro entorno se ha tomado conciencia de la trascendencia de los marcadores genéticos en las investigaciones criminales […]".

En esta aproximación histórica merece hacer una especial mención al concepto de dactilograma como posible antecedente, a su vez, del concepto de "plantilla biométrica", que más adelante en este estudio se abordará. A simple vista podemos apreciar en las yemas de los dedos de cualquier persona surcos y crestas que describen diferentes formas. Pues bien, el dactilograma como ya hemos apuntado, es "el dibujo formado por las crestas papilares y surcos existentes entre ellas, que aparecen en las yemas de los dedos de las manos o su impresión o reproducción gráfica"[92]. En relación con las crestas papilares, a continuación, haremos referencia a tres conceptos fundamentales en dactiloscopia: la clasificación de las crestas, los puntos característicos y los sistemas papilares.

En lo referente a la clasificación de las crestas, las formas que describen las líneas en la superficie de la yema han sido clasificadas en tres grupos: arcos, asas y círculos. Cualquier dactilograma presenta líneas o crestas papilares describiendo formas asimilables a uno de estos tres grupos mencionados. Estas crestas papilares o líneas en relieve adoptan, como ya se ha indicado, diversas formas, pero todas ellas asimilables a uno de estos tres grupos: crestas arciformes, ansiformes, o bien, verticilares. Las crestas

[91] Ley Orgánica 10/2007, de 8 de octubre. Ley Orgánica reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN. BOE 9 octubre 2007, núm. 242, [pág. 40969].
[92] Cfr. DE ANTÓN Y BARBERÁ F., op. cit., p. 43.

arciformes presentan forma de arco, las ansiformes tienen forma de asa u horquilla y las verticilares son crestas curvas que aparecen en el centro de los dactilogramas con forma de remolinos, círculos, elipses, espirales, etc. Pero, no son éstas las únicas formas de las crestas que cabe apreciar en un dactilograma; hay algunos que presentan otras formas particulares que se han venido en denominar "puntos característicos", siendo diez los más importantes: línea abrupta, bifurcación, convergencia, desviación, fragmento, punto, empalme, ojal, interrupción y rama. Como veremos a continuación, estos puntos característicos o características particulares son un elemento relevante en la identificación de las personas. Y, por último, llegamos al tercer concepto mencionado: los sistemas papilares. Las crestas papilares se distribuyen sobre toda la yema del dedo, agrupándose en tres zonas o sistemas; el sistema basilar, en la base del dactilograma; el sistema nuclear, situado encima del basilar en el centro y rodeado por el tercer sistema, el marginal, formado por las crestas del entorno del dactilograma. La cresta superior del sistema basilar se denomina limitante basilar y la más externa del sistema nuclear, limitante nuclear.

Por su parte, los dactilogramas pueden ser clasificados en tres categorías atendiendo al soporte sobre el que se encuentran: naturales, artificiales o latentes. El dactilograma natural, siguiendo a De Antón, es el directamente observable en la yema o pulpa de cualquier dedo, es decir, el dactilograma de la piel. El artificial es el dactilograma que aparece grabado en un soporte externo, en la "tarjeta decadactilar", después de haber entintado el dedo y haberlo estampado como un sello sobre dicha tarjeta o soporte. Por último, el dactilograma latente es lo que también se conoce como huella digital. La huella se deja involuntariamente por una persona, en el ámbito de una investigación criminal por el autor de un hecho delictivo, sobre una superficie y son necesarios reactivos adecuados para ponerla de manifiesto. Nuestro interés recae sobre los dactilogramas artificiales como antecedentes de los sistemas biométricos de lectura de huella dactilar. Podríamos afirmar que los sistemas de lectura biométrica de huella son un nuevo soporte del dactilograma artificial de un individuo.

Por todo lo expuesto hasta ahora, en la función o tarea de identificación de las personas a través de su dactilograma es imprescindible distinguir dos tipos de características que aparecen en dicho dactilograma, y que ya han quedado apuntadas más arriba, que son

las denominadas características generales[93], ubicadas en los tres sistemas papilares, y las características particulares o individuales que antes hemos denominado "puntos característicos". Son, en muchos casos, las características específicas y las individuales las que llevan a la identificación del individuo. No obstante, hay que matizar esta afirmación ya que, actualmente, existen tecnologías biométricas fisiológicas de huella dactilar donde la identificación basada en huella dactilar se puede fundamentar en dos tipos de técnicas: una de búsqueda de coincidencias entre muestras de huella dactilar basada en minucias, las características particulares o individuales, y otra la basada en el patrón global de la huella. A esta segunda técnica se la denomina técnica basada en la correlación[94].

Ahora bien, llegados a este punto se debe hacer referencia a un concepto fundamental en dactiloscopia que es el concepto de "delta". El profesor Olóriz define delta como "la figura triangular formada en la confluencia de los tres sistemas" (basilar, marginal y nuclear que conforman las características generales del dactilograma de un individuo), que se unen en la convexidad. Para el profesor Mora, delta es "la figura triangular que determina la aproximación de tres sistemas distintos de crestas papilares" y también puede definirse como la figura "en forma de trípode que resulta de la fusión de las crestas limítrofes correspondientes a dichos sistemas[95]". En definitiva, se llama delta en un dactilograma al dibujo formado por la confluencia o aproximación de las líneas límite de los tres sistemas. La delta tiene una función fundamental al servir para clasificar los dactilogramas. Esta función clasificadora se puede desarrollar porque se han podido determinar cuatro tipos de dactilogramas dependiendo de si aparece o no la

[93] Estas características generales de la huella se ubican en alguno de los tres sistemas o zonas donde se agrupan las crestas o líneas papilares, que ya se ha indicado se denominan sistema o zona basilar, zona marginal y zona o sistema nuclear. El sistema basilar lo forman las crestas de la base del dedo que se elevan hasta llegar a una cresta límite que se denomina el limitante basilar. El sistema marginal lo constituyen las crestas de la parte alta y laterales del dactilograma. Estas crestas, como determinó el profesor Olóriz, comienzan por un lado del dedo en paralelo a las crestas basilares, suben hacia el extremo de la pulpa describiendo unas curvas muy acentuadas cóncavas y descienden por el lado opuesto al de su inicio. Por último, el sistema nuclear se encuentra en la parte central de la pulpa delimitado por los otros dos sistemas, basilar abajo y marginal arriba y al lateral. Cfr. DE ANTÓN Y BARBERÁ, F., op. cit., p. 48.

[94] Por tanto, la búsqueda de coincidencias entre muestras de huella dactilar se puede basar en minucias o en la correlación del patrón global seguido por la huella dactilar. En la técnica basada en minucias se registran por el sistema las características particulares o minucias que aparezcan en la huella, la posición de las mismas y las distancias entre unas minucias y otras. Por el contrario, en las técnicas basadas en correlación lo que se analiza es el patrón global de la huella, es decir, las crestas papilares de la zona basilar, marginal y nuclear. Cfr. Instituto Nacional de Tecnologías de la Comunicación (INTECO). *Guía sobre las tecnologías biométricas…*, op. cit., pp. 9-10.

[95] DE ANTÓN Y BARBERÁ, F., op. cit., p. 51.

delta y dónde aparece. Así hay dactilogramas adeltos, que carecen de deltas; dactilogramas monodeltos, que a su vez pueden ser dextrodeltos si la delta aparece a la derecha o sinistrodeltos si la delta aparece a la izquierda; dactilogramas bideltos con dos deltas y dactilogramas trideltos con tres deltas. Junto a esta clasificación de los dactilogramas por el número de deltas el profesor Olóriz estableció otra clasificación atendiendo a la forma y relieve que presentan las deltas. Cabe distinguir, entonces, entre deltas hundidos o blancos y deltas salientes o negros. Los primeros son el resultado de la aproximación de las crestas limitantes de los tres sistemas (basilar, marginal y nuclear) sin llegar a fusionarse dichas crestas. Los salientes o negros resultan de la fusión, convergencia, de las crestas limitantes que toman la forma de un trípode con tres ramas.

Hasta aquí hemos reseñado las que se han denominado características generales de las crestas papilares, pero, si como hemos dicho, son las características específicas las que permiten, en la mayoría de las ocasiones, identificar a una persona, habrá de ser a ellas a las que nos refiramos a continuación. Estas características o también denominadas "minucias", o "puntos característicos", particularizan cada dedo y tienen tres señas de identidad: se encuentran en número de treinta o más en cada dedo; son congénitas y no sufren alteraciones, a no ser que la piel sea destruida. Es de la combinación de estos tres elementos cantidad, carácter congénito e inalterabilidad de la que se puede derivar la identificación de un individuo. La cuestión es cuántos de estos puntos característicos[96], o minucias, son los mínimos imprescindibles para establecer la identidad de una persona. Parece ser que no está establecido con carácter universal y único el número mínimo de estas minucias y, en opinión de De Antón, esta falta de unidad de criterio puede llevar a una desconfianza en el sistema como medio de identificación y *"*(…) al menos los países miembros de la Unión Europea, deberían

[96] De Antón y Barberá recoge los siguientes puntos característicos como aquellos que son actualmente utilizados por los distintos servicios de identificación españoles: abrupta, bifurcación, convergencia, desviación, empalme, fragmento, interrupción, ojal, punto, transversal, cuña o ensamble, secante y los puntos Y o M. La presencia o ausencia de estas minucias o puntos característicos en un dactilograma permitirá la identificación de la persona a la que pertenece. No sólo son estos puntos los utilizados en la identificación sino también los producidos por la combinación de dos de ellos por ejemplo la convergencia de ojal o el ojal con cresta abrupta, etc. En definitiva, en el Sistema Dactiloscópico Español se utilizan, para el establecimiento de identidad entre huella e impresión digital sea de la palma de las manos o de la planta de los pies, de 10 a 12 de los puntos característicos mínimos que hemos citado anteriormente. Si esos puntos coinciden se puede realizar una afirmación de identidad. Pero también puede realizarse esta afirmación con menos puntos, en concreto, y como ya estableció el profesor Olóriz se pueden fijar en cinco el número de estas minucias. Cfr. DE ANTÓN Y BARBERÁ, F., op. cit., pp. 59-62 y p. 251.

llegar a un único criterio, en cuanto al señalamiento de un número de puntos característicos mínimos para todos"[97]. En resumen, hemos pretendido con este análisis acercarnos a los elementos que forman la base material física de identificación de uno de los sistemas biométricos por excelencia hoy en uso: la huella dactilar.

Hasta este punto de la exposición hemos estado considerando deca-dactilogramas en la hipótesis más habitual de personas con diez dedos. Pero existen malformaciones congénitas que pueden ponerse de manifiesto en un sistema de lectura biométrica de huellas dactilares o de palma de la mano. Por tanto, hay que tomar en consideración el riesgo de discriminación[98] y/o atentados a la dignidad humana que puede derivarse del tratamiento de datos biométricos que patenticen malformaciones congénitas u otras anomalías patológicas. Con total claridad, el T-PD, en su informe de situación relativo a la aplicación de los principios de la Convención 108 a la recogida y al proceso de los datos biométricos elaborado en su 21ª reunión del 2-4 febrero de 2005, al que ya se ha hecho referencia, planteó la necesidad de garantizar el respeto a la dignidad humana en todo proceso de recogida y utilización de las características del cuerpo humano. En particular el Comité se refiere, en el citado informe, a la necesidad de que los sistemas de reconocimiento de características físicas de los individuos, si revelan inevitablemente información sobre enfermedades o una discapacidad, tengan un sistema de protección de esos datos. Entre las malformaciones congénitas,[99] que pueden revelarse en un

[97] Ibíd., p. 59.

[98] El GPD 29, en su Dictamen 3/2005 sobre la aplicación del Reglamento (CE) nº 2252/2004 del Consejo advierte sobre los riesgos éticos del uso de elementos biométricos en pasaportes u otros documentos de viaje y carnés de identidad y explícitamente menciona a varios colectivos que pueden verse afectados o discriminados como inmigrantes, minusválidos, personas con alguna enfermedad; expresamente dice el Grupo del 29: "También se plantean otras cuestiones de naturaleza diversa: las personas a quienes resulte más difícil probar su identidad, como los inmigrantes, podrán sufrir un trato injusto en virtud de tal sistema; los minusválidos que no puedan pasar las pruebas biométricas podrán ser estigmatizados; y podrá obtenerse información médica sensible". En lo referente al almacenamiento de huellas dactilares el Dictamen menciona "(…) un debate en curso sobre la correlación entre ciertos dibujos papilares y determinadas enfermedades. Al parecer, algunos dibujos papilares dependen de la nutrición de la madre (y por tanto del feto) durante el tercer mes del embarazo. La leucemia y el cáncer de mama parecen estar estadísticamente relacionados con determinados dibujos papilares". Cfr. Dictamen 3/2005 sobre la aplicación del Reglamento (CE) nº 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros. Adoptado el 30 de septiembre de 2005. WP 112. 1710-01/05/ES-rev. Diario Oficial L 385 de 29 de diciembre 2004 p. 8. Disponible en http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm [Fecha de consulta: 03/04/2016].

[99] Se pueden enumerar las siguientes deformidades congénitas: "polidactilia (mayor número de dedos de lo normal); Sindactilia (adherencia o fusión , por medio de membrana, de dos o más dígitos); Ectrodactilia (Número de dedos inferior al normas); Anisodactilia (Uno o varios dedos es de menor altura); Isodactilia (Todos de igual tamaño); Queratodermia (engrosamiento de la capa córnea de la epidermis, enfermedad de Meleda); Sinfalangia (cerece de pliegue de flexión); Braquidactilia (dedos muy

tratamiento de datos biométricos de reconocimiento de la palma de la mano cabe citar la polidactilia o presencia de dos dedos pulgares. Así, la tecnología biométrica de reconocimiento de la palma de la mano incorpora al sistema de tratamiento automatizado información sobre una malformación congénita. Estas malformaciones obviamente no dificultan la identificación de una persona, sino que al contrario la facilitan, al ser de muy rara presencia, pero pueden plantear cuestiones colaterales tan delicadas como, la afección a derechos individuales, tales como el derecho a la no discriminación o el derecho a la intimidad, el derecho al respeto al cuerpo humano o a la dignidad humana. Estas cuestiones no se plantean, o al menos no con tanta intensidad, en el tratamiento de un dactilograma sin dichas anomalías. De hecho, el tratamiento de un dactilograma sin anomalías no se considera atentatorio al derecho a la intimidad ni al derecho a la autodeterminación informativa. Así se ha entendido por buena parte de la doctrina de nuestros Tribunales y así, entre otras, cabe citar la STJ de Murcia Sala de lo Social, sec. 1ª, S 25-1-2010, nº 47/2010, rec. 1071/2009[100]. La Sentencia del TSJ, en su Fundamento Tercero, estima al igual que el Juzgado *a quo* (Juzgado de lo Social número 3 de Murcia Sentencia de 25 de septiembre del 2009) que la implantación del nuevo sistema de control de acceso a las instalaciones no constituye modificación sustancial de las condiciones de trabajo (artículo 41.1); que la implantación de tal sistema no requiere acuerdo del Comité de Empresa (artículo 41.2 y 4 y artículo 64) y que para la implantación de tal sistema la empresa está amparada por las competencias que le atribuye el artículo 20 del ET. Ahora bien, si la medida adoptada por la empresa afectara a la dignidad humana o a los derechos fundamentales, en ese caso, sí habría lugar a apreciar una sustancial modificación de las condiciones de trabajo. Por ello, la Sentencia, en su Fundamento Tercero, comienza analizando la posible vulneración de la integridad física de los trabajadores, la posible vulneración de su intimidad o de su derecho a la autodeterminación informativa. Concluye afirmando que "ninguno de dichos derechos resulta afectados". En cuanto a la integridad: "en un principio, de los hechos declarados probados y de las alegaciones de las partes, no existe constancia que, tanto la obtención de determinados parámetros biométricos de las huellas digitales a los trabajadores de la empresa, como la ulterior lectura electrónica de las mismas, con ocasión del acceso a las dependencias de la empresa, comporte riesgo alguno para la

cortos); Macrodactilia (dedos muy grandes) y Displasia (carece de dibujo)". Es la enumeración que realiza DE ANTÓN Y BARBERÁ, F., op. cit., pp. 99-100.

[100] EDJ 2010/18129. Fuente de suministro: Centro de Documentación Judicial. IdCendoj: 30030340012010100047.

integridad física de los trabajadores. La demanda se limita a afirmar la vulneración de su derecho a la intimidad informática". En lo que respecta a la intimidad, indica lo siguiente: "la sala estima que la captación por un sistema electrónico de determinados parámetros biométricos de la huella digital para, mediante tratamiento informático que lo relaciona con otros datos personales existentes en la empresa, identificar a los empleados de la empleadora HEFAME, con el fin de controlar su acceso a las instalaciones de la misma, no reviste caracteres de intromisión ilegítima en la esfera de la intimidad". Y ello es así, razona el TSJ, por dos órdenes de razones: primero "por la parte del cuerpo utilizada" y segundo "por las condiciones en que se usa". Es fácil convenir con el Tribunal que la captación de la huella dactilar no afecta a la intimidad puesto que se trata de una parte del cuerpo expuesta al público y porque el proceso del tratamiento en sí (poner un dedo en una superficie de lectura o, incluso si se tratara de la huella palmar, toda la palma de la mano) en modo alguno atenta a la intimidad. Otra cuestión es si en esa captación por el sistema los parámetros biométricos captados son reveladores de una enfermedad o malformación, cuestiones estas que en absoluto aborda la Sentencia. Lo que sí analiza la Sentencia es la legitimidad de las condiciones en las que se usa por la empresa la información obtenida. Así, el Tribunal atiende al principio de calidad en cuanto a la finalidad, siendo ésta tan legítima como controlar el cumplimiento por los trabajadores de su jornada laboral. El artículo 20.3 ET atribuye al empleador facultades suficientes para la implantación del nuevo sistema de control de acceso, ya que éste no atenta a su dignidad. Además, no hay prueba de la utilización de tales datos para fines diversos. Añade el TSJ que el hecho de la lectura de la huella no hace visible su imagen por terceros ni puede ser captada por éstos, quedando todos los datos del sistema guardados en los ordenadores de la empresa a efectos de su custodia. Por tanto, el TSJ analiza la captación a la luz de las normas garantes del derecho a la autodeterminación informativa, ya que se admite por el Tribunal, sin ningún género de dudas, que la huella digital se puede considerar un dato personal y no está prohibida su recogida y tratamiento, sino que, ha de hacerse conforme a lo dispuesto en el artículo 4 de la LOPD. Así, estima la Sala "que el control de acceso a las instalaciones de la empresa constituye una finalidad legitima, concreta y que fue suficientemente puesta de manifiesto a los trabajadores y que tal medida de control, que vincula la lectura de las huellas digitales a los datos de identidad de los trabajadores existentes en la empresa, es adecuada, pertinente y no excesiva". ¿Pero seguiría siendo adecuada, pertinente y no excesiva la medida de control si revelara una malformación física del trabajador?

Nos planteamos estas cuestiones porque cabe la posibilidad de que una persona pueda ser tratada de una forma diferente, discriminada, por otras personas como consecuencia del tratamiento de sus datos personales que revelen una deformación congénita de polidactilia o sufrir discriminación por la presencia en un dactilograma de alteraciones patológicas provocadas por una enfermedad venérea como la sífilis[101]. En resumen, estamos planteando que los sistemas biométricos de reconocimiento de huella dactilar o reconocimiento de la palma de la mano, entre otros, pueden revelar información personal sensible[102], cualitativa, que, almacenada en una base de datos, puede crear perfiles[103] de individuos y, posteriormente, tomar decisiones que afectan a ese individuo

[101] Estas cuestiones ya han sido puestas de manifiesto por el GPD 29, entre otros, en el documento de trabajo sobre biometría 12168/02/ES WP 80, en el que se afirma que determinados datos biométricos pueden revelar información sensible relativa a la salud o a la vida sexual de sus titulares, o bien revelar el origen racial o étnico de los mismos y como consecuencia de ello ser una posible fuente de discriminación. Pensemos por ejemplo en las anomalías o cambios del dibujo papilar, ya aludidos, producidos por una lesión, cicatriz o enfermedad como la sífilis o la lepra. O bien otras alteraciones producidas en un dactilograma como consecuencia de la actividad profesional del individuo, por ejemplo, la manipulación constante de materiales de gran aspereza, cementos, materiales cáusticos o corrosivos. Estas alteraciones provocadas por el ejercicio de una profesión tales como desgastes, hipertrofias epidérmicas, que incluso pueden hacer desaparecer el dibujo papilar, revelan datos del individuo más allá del propio dato biométrico recopilado.

[102] El GPD 29 no duda en calificar de sensible la información que instituciones y poderes públicos podrán recoger sobre sus nacionales con la aplicación del Reglamento (CE) 2252/2004, el cual prevé la obligatoriedad de incluir una imagen facial digitalizada e impresiones dactilares en los pasaportes de los ciudadanos de la UE. La recogida de elementos biométricos significa recoger datos del cuerpo de una persona y hay que garantizar que solo las autoridades competentes puedan acceder a esos datos para lo que será necesario que cada Estado miembro mantenga un registro de las autoridades competentes y de los órganos autorizados al acceso y, en todo caso, se aplique un Control de Acceso Ampliado. Cfr. *Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (Official Journal L 385, 29/12/2004 p. 1 - 6)* Adopted on 30 September 2005. (Dictamen 3/2005 sobre la aplicación del Reglamento (CE) nº 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros. Adoptado el 30 de septiembre de 2005). p. 1-6. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp112_en.pdf [Fecha de consulta: 02/02/2016].

[103] Sin ánimo de plantear una visión opresiva, sino más bien lo más cercana posible a la realidad de la sociedad actual, podemos afirmar que vivimos en una sociedad de la identificación y de la incardinación de las personas en perfiles pre-establecidos. En este sentido el GPD 29 en el *Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE,* hace referencia al suministro de datos, sea de forma consciente o inconsciente, por el usuario de Internet que permite crear perfiles de usuarios. En este caso nos estamos refiriendo a perfiles no personales pero que pueden provocar *ad hoc* una situación de discriminación. Aunque no nos encontremos en un entorno de tratamiento de información personal *stricto sensu* el tratamiento tiene fines decisionales sobre el individuo, aunque en principio se esté trabajando sobre información anónima. Así expone la práctica muy extendida de recogida de datos personales por medio de un fichero de texto, las conocidas *cookies*, que permite crear dichos perfiles no personales o adscribir al individuo a uno de estos perfiles ya creado. El citado documento define las *cookies* como "datos creados por un servidor web que pueden almacenarse en ficheros de texto que pueden colocarse en el disco duro del usuario de Internet, mientras una copia puede conservarse en el sitio web. Son una parte normal del tráfico HTTP, y pueden, por tanto,

en función de su adscripción a uno u otro perfil[104]. En definitiva, y sin carácter exhaustivo, hemos mencionado algunos datos de un individuo que pueden quedar al descubierto al analizar una reseña dactilar, es decir, el dactilograma de un individuo: la anquilosis o imposibilidad de movimiento en la articulación del dedo; amputaciones parciales de los dedos; polidactilia o mayor número de dedos; ectrodactilia o menor número de dedos; la sindactilia o dedos unidos por una membrana y las alteraciones profesionales o patológicas que pueden llegar incluso a impedir obtener el dactilograma. Entendemos que estas situaciones deben tener una adecuada respuesta y protección jurídica que, si no es en el ámbito de los derechos fundamentales a la intimidad, el honor o la propia imagen, habrá de serlo en el del derecho a la autodeterminación informativa a través de la categoría de los datos especialmente protegidos, como analizaremos más adelante.

---

transportarse sin obstáculos con el tráfico IP. Una *cookie* puede contener un número único (GUI, identificador global único), que permite una mejor personalización que las direcciones IP dinámicas. Permite al sitio web guardar un rastro de las prácticas y preferencias del usuario. Las *cookies* contienen una serie de URL (direcciones) para las cuales son válidos. Cuando el navegador vuelve a encontrar estos URL, envía las *cookies* específicas al servidor web. Las *cookies* pueden ser de naturaleza diferente: pueden ser permanentes o tener una duración limitada (los denominados *cookies* de sesión)". Es decir, cuando el usuario con el mismo navegador vuelve a visitar alguna de estas URL, direcciones, el o los servidores web de estas direcciones intentan leer las *cookies* que en su día alguno de ellos guardó y, si así se hizo y si el usuario no las ha borrado, recuerdan al usuario, qué visita hizo, qué visitas a sitios controlados por ellos ha realizado posteriormente, etc. Lo importante es que no parezca que el navegador las envía aleatoriamente, sino que es el servidor el que pide leerlas y entonces, es el navegador el que las envía, los datos de las cookies viajan del navegador al servidor, pero es importante que la orden primera la da el servidor. Cfr. Grupo de trabajo del artículo 29 sobre Protección de Datos. *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE),* Aprobado el 30 de mayo de 2002, (5035/01/ES/Final WP 56), pp. 10-11. Disponible en http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf [Fecha de consulta: 02/02/2016].
En relación con estas *cookies*, el mismo GPD 29, en su Recomendación 1/1999 sobre el tratamiento invisible y automático de los datos personales en Internet, entiende que los productos de software y hardware en Internet deben permitir al usuario saber qué datos se van a recoger, con qué fin se recogen y cómo acceder posteriormente a ellos. Para dar cumplimiento a estas medidas, y en relación con las *cookies*, la Recomendación entiende que el usuario debe ser informado en el momento en que un *cookie* está intentando ser recibido en el equipo local, o almacenado o bien enviado por el navegador y se le debe dar al usuario la opción de aceptar o no su recepción. En todo caso hay que tener en cuenta que la *cookie* identifica el ordenador del usuario no al usuario mismo pero esta información anónima se trata con el fin de futuras identificaciones de ese ordenador en futuras visitas a la misma página web desde la que se envió la *cookie* pasando ya a un tratamiento decisional que sí afecta a un individuo. Cfr. *Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware*. 5093/98/EN/final WP 17, p. 3. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp17_en.pdf [Fecha de consulta: 09/02/2016].

[104] En este mismo sentido, Llácer afirma que: "La creación de perfiles es el paso intermedio entre la monitorización y la adopción de una conducta o decisión ya que la definición de las personas a través de categorías es el nexo para aplicarles las consecuencias apropiadas, según el criterio e interés del gestor de la información". LLÁCER MATACÁS, M. R., "La autodeterminación informativa…", op. cit., p. 68.

1.2. Distinción entre biometría, sistemas biométricos y datos biométricos.

Para finalizar este epígrafe inicial de antecedentes históricos de la biometría haremos referencia, brevemente, a la diferencia entre los conceptos de biometría, sistemas biométricos de datos de personas y los propios datos biométricos de los individuos.

La palabra biometría, definida por el Diccionario de la Real Academia de la Lengua española, es "el estudio mensurativo o estadístico de los fenómenos o procesos biológicos".

Abad Amorós considera que "los datos biométricos pueden identificarse con rasgos fisiológicos o del comportamiento de una persona viva, principalmente aquellos que van a identificarla o van a verificar una identidad que ha sido demandada"[105]. El término biometría aplicado a las personas, en la definición ofrecida por INTECO, "es un método de reconocimiento de personas basado en sus características fisiológicas o de comportamiento"[106]. Para el Instituto de Biometría dependiente de la oficina del Comisionado de privacidad del gobierno de Australia la biometría "significa las características biológicas y de comportamiento únicas de un individuo que son capturadas con la finalidad de identificación y/o verificación de ese individuo"[107].

Los sistemas biométricos o tecnologías biométricas, también para INTECO, son "métodos automáticos utilizados para reconocer a personas sobre la base del análisis de sus características físicas o de comportamiento"[108]. Ahora bien, un sistema de identificación biométrico, como sistema de identificación electrónico-digital, implica el desarrollo de varios procesos y en este sentido siguiendo a la OCDE[109] podemos

[105] ABAD AMORÓS, M. R., *El carácter sensible de los datos biométricos.* Datos Personales – Núm. 4, septiembre 2003. vLex. http://vlex.com/vid/caracter-sensible-datos-biometricos-204792. [Fecha de consulta: 06/07/2016].
[106] Instituto Nacional de Tecnologías de la Comunicación (INTECO). *Guía sobre las tecnologías biométricas…*, op. cit., p. 5.
[107] Biometrics Institute. *Biometrics Institute Privacy Code, section 18BB(2) of the Privacy Act 1988 (Cth).* 19 July 2006. http://www.biometricsinstitute.org, p. 3. [Fecha de consulta:06/07/2016].
[108] Instituto Nacional de Tecnologías de la Comunicación (INTECO). *Guía sobre las tecnologías biométricas…*, op. cit., p. 8.
[109] En este sentido, la OCDE haciendo referencia a los procesos que engloba, en general, un sistema de identificación digital de personas enumera los anteriormente enunciados. Cfr. OECD, "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for

enumerar los siguientes: proceso de registro; proceso de autorización; proceso de autenticación; control de acceso y proceso de revocación

Más adelante, analizaremos el *iter* de cada uno de estos procesos; ahora solo cabe apuntar que el objeto de nuestro estudio abarcará el análisis de las implicaciones jurídicas de los procesos incluidos en estos sistemas biométricos, al tratar datos personales de individuos, huellas dactilares, de alta criticidad. Así habrá de analizarse algo muy relevante: cómo proporcionar una protección práctica real a los tratamientos de datos personales biométricos y en particular a los de datos dactiloscópicos. Para ello, será necesario diseñar arquitecturas jurídicas de sistemas basados en la responsabilidad[110]. El principio de responsabilidad, desde un punto de vista práctico, pretende garantizar de hecho un cumplimiento efectivo de los principios de la protección de datos. Los responsables del tratamiento deberán determinar las medidas de seguridad aplicables atendiendo a los riesgos del tratamiento y a la naturaleza de los datos. Así, si los datos biométricos se consideran como datos de nivel básico se deberá, en su tratamiento, adoptar medidas de seguridad acomodadas a este nivel, pero si los datos biométricos revelan datos de salud, vg, una discapacidad, entrarán dentro de la categoría de datos especialmente protegidos y sería necesario implantar medidas de seguridad de nivel medio y/o alto. Aquí debemos recordar que el RGPD y la LO 3/2018 ya no contemplan estos niveles, a lo que nos referiremos en su momento.

En lo que respecta a los riesgos que representa el tratamiento, éstos pueden variar en función del tamaño de las operaciones, los objetivos de dicho tratamiento (identificación o simple validación de identidad) o el número de transferencias previstas. Todos ellos son factores que influyen en el nivel de riesgo del tratamiento y habrán de tenerse en cuenta por el responsable a la hora de determinar las medidas de seguridad aplicables a dicho tratamiento.

Government Policy Makers", OECD Digital Economy Papers, No. 186, OECD Publishing, 2011. Disponible en http://dx.doi.org/10.1787/5kg1zqsm3pns-en, p. 4. [Fecha de consulta: 09/07/2016].

[110] Esta arquitectura jurídica de responsabilidad se desarrolla en dos niveles: el primer nivel que exigiría a todo responsable de tratamiento la aplicación de medidas y procedimientos que permitan poner en práctica los principios de protección de datos garantizando su eficacia, y manteniendo pruebas de ello. Y un segundo nivel con medidas discrecionales de responsabilidad. Cfr. Dictamen 3/2010 sobre el principio de responsabilidad. 00062/10/ES GT 173, Adoptado el 13 de julio de 2010. Disponible en http://ec.europa.eu/justice/policies/privacy/index_en.htm, p. 6. [Fecha de consulta: 09/07/2016].

2. Delimitación del estudio. Los datos biométricos dactiloscópicos.

Si atendemos a la definición que recogía la PRGPD, en su artículo 4 apartado 11) consideraremos "«datos biométricos»: cualesquiera datos relativos a las características físicas, fisiológicas o conductuales de una persona que permitan su identificación única, como imágenes faciales o datos dactiloscópicos; […]". El RGPD, en su redacción definitiva en el mismo artículo 4, "Definiciones", en el apartado 14) dice: "«datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;". La definición del nuevo Reglamento es más completa, pues hace expresa mención a la existencia de un tratamiento técnico específico al que se someten determinadas características de una persona física.

Por tanto, la función de identificación única de personas es lo que nos hace detener nuestro estudio en los datos dactiloscópicos que, como la imagen facial, permiten la identificación de individuos.

2.1. Aproximación al concepto de sistema dactiloscópico español y dato biométrico dactiloscópico.

Como ya hemos expuesto en la introducción, los datos a los que nos referiremos en el estudio son el dactilograma de un individuo que, en concreto, y con referencia al sistema dactiloscópico español, viene conformado por veinte puntos característicos. En el sistema español se usan veinte características, dos de cada dedo, esto es, las dos manos completas, por lo que no es el caso de una sola huella dactilar. Como resumen del sistema dactiloscópico español, recogemos los siguientes conceptos fundamentales:

Crestas papilares: cara palmar de la mano, infinidad de líneas en relieve de lomo redondeado, con puntillos glandulares que ocupan su superficie en diversas direcciones, son las crestas papilares, los espacios que las separan son los surcos interpapilares. Las crestas papilares componen los dactilogramas. El dactilograma, recordamos, es el dibujo de crestas y surcos de las yemas de los dedos de las manos. Las crestas papilares tienen las siguientes formas más frecuentes: Arciformes: arco, generalmente transversales.

Ansiformes: forma de asa u horquill y Verticilares: círculos, elipses, espirales. A su vez las crestas papilares se agrupan en los dactilogramas formando 3 sistemas: “Basilar”, situado en la parte inferior del dactilograma, entre el despliegue de flexión del dedo y la parte baja del delta. Con crestas generalmente transversales y arqueadas. Su cresta superior se denomina limitante basilar; “Marginal”, que se describe como crestas del entorno del dactilograma. Su cresta inferior se denoina limitante marginal. Y “Nuclear”, situado por encima del basilar y rodeado por el marginal. Su cresta más externa se denomina limitante nuclear. Conviene aquí ahora recordar que Delta en un dactilograma es el dibujo formado por la confluencia de las líneas limitantes de los tres sistemas anteriores. Es el elemento esencial en que se basó Olóriz para establecer la clasificación de los dactilogramas. Olóriz los divide dependiendo de su forma en: hundidos o blancos: en los que hay una aproximación de las limitantes de los 3 sistemas de crestas papilares. Salientes o negros: en los que hay una fusión de las 3 limitantes en forma de trípode o estrella de tres puntas. A su vez, el Punto déltico en el hundido es el centro del espacio triangular y en el saliente es la intersección de las líneas que forman el delta.

El Núcleo es el centro aproximado de la impresión digital o centro del dactilograma. Para Olóriz: "núcleo es el grupo de crestas que ocupa la parte central de la impresión de la yema del dedo, hallándose circunscrita por las líneas limitantes de los otros sistemas".

En el Sistema dactiloscópico español, existen cuatro tipos fundamentales:

- A - 1 - Adeltos: que carecen de delta y de núcleo.

- D - 2 - Dextrodeltos: un solo delta a la derecha del observador.

- S - 3 - Sinistrodeltos: un solo delta a la izquierda del observador.

- V - 4 - Vorticilos o Bideltos: dos deltas o más deltas.

La Fórmula es la siguiente: Pulgares se representan con su letra A D S V según sean Adeltos, Detro, Sini o Vorti. Índice, medio, anular y meñique se representan por 1, 2, 3

ó 4 1-Adeltos, 2-Dextro, 3-Sinis y 4-Vorticilos. Longitud 10: 2 letras (pulgares) y 8 números (índices, medios, anulares y meñiques).

Por ejemplo: S 1 3 3 1 - D 1 2 2 1

Si un dedo no se observa por lesión, cicatriz, callosidad se pone una X. Puede haber persona con los mismos 10 caracteres por eso se aplica una subfórmula. Subfórmula: basada en característas secundarias de los dactilogramas. Se escriben bajo el caracter de cada dedo (como si fuera un quebrado).

Dextrodeltos y sinistrodeltos: Se les aplica el sistema de Galton, nº de crestas entre el punto déltico y el punto central. Se cuentan todas, incluyendo fragmentos y puntos, excepto el punto déltico y el central (este es el nº que va al denominador)

Bideltos: Se parte del delta izquierdo y se sigue la trayectoria de su limitante basilar:
- si se interna en el núcleo antes de llegar al delta derecho -> bidelto interno (i),
- si contribuye a formar el delta derecho -> mesodelto (m) y
- si la limitante pasa por debajo del delta derecho se clasifica de externo (e).

Son las letras minúsculas i, m y e las que van al denominador

Luego son 2 manos, 10 dedos, 2 caracteres-características por dedo, son 20 caracteres, esto es, 20 observaciones y NO de un sólo dedo.

Por tanto, una anomalía accidental que provoca un cambio en el dibujo papilar de origen profesional o patológico puede revelar datos sobre actividades del individuo, o incluso datos sensibles, de salud o relativos a la vida sexual de su titular. Indudablemente el tratamiento de estos datos sensibles debe respetar las normas de protección de la privacidad del individuo.

2.2. Diferencias entre el dato genético, el dato de salud y el dato biométrico.

Las tres categorías de datos están muy relacionadas siendo, sin embargo, muy distintas. La imbricación entre ellas parte del hecho de que los progresos tecnológicos actuales,

tanto en el ámbito de la investigación genética como en el ámbito de la salud o en los sistemas de identificación biométrica, plantean nuevas cuestiones en materia de protección de datos, ya que las tres categorías de datos pueden utilizarse de forma abusiva en perjuicio del individuo llegando a provocar su discriminación. De la adecuada protección de los datos genéticos, de los datos de salud y de los datos biométricos depende la posibilidad misma de garantía del principio de igualdad e, incluso, de la existencia real del derecho a la salud. La posibilidad de discriminación basada en datos genéticos, biométricos existe. Por ello la protección, entre otros derechos, del derecho a la salud depende de la seguridad de que ningún dato que la afecte se revele a terceros que puedan utilizarlo para discriminar o estigmatizar a las personas. Partiendo de este común denominador –potencialidad discriminatoria-, las tres categorías de datos presentan características diferentes, que abordaremos brevemente a continuación, para concluir que será únicamente sobre los datos biométricos sobre los que centraremos el análisis posterior.

En primer lugar, era habitual en los trabajos doctrinales sobre la materia hacer constar, previamente, que no existe una definición en nuestro ordenamiento jurídico de dato de salud, pero esta situación ha cambiado con la aprobación del RGPD. El Reglamento, dentro del artículo 4. "Definiciones", recoge en su apartado 15) lo que denomina "«datos relativos a la salud»" y los define como: "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;" Además, podemos acercarnos a los textos internacionales. El considerando 45 del Convenio 108 define los datos sobre la salud como "las informaciones concernientes a la salud pasada, presente y futura, física o mental de un individuo". Y, como indica Rebollo Delgado[111], también se incluía dentro de estos datos "las informaciones relativas al abuso de alcohol o al consumo de drogas".

Por su parte, el artículo 7 de la LOPD dentro de la categoría de datos especialmente protegidos mencionaba en su apartado 3 a los datos que hagan referencia a la salud a los únicos efectos de establecer que sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta

[111] REBOLLO DELGADO, L., SERRANO PÉREZ, M., M., *Manual de Protección de Datos*, Madrid, Dykinson, 2019, pp. 233-234.

expresamente; añadiendo en el párrafo 6, de este mismo artículo, que, entre otros, los datos que hagan referencia a la salud podrán ser objeto de tratamiento cuando éste resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que este tratamiento se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto, concretando, por último, el segundo párrafo de este artículo 7.6, que también pueden ser objeto de tratamiento los datos de salud en el caso de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento y dicho tratamiento sea necesario para salvaguardar el interés vital de éste o de otra persona. Y no debemos olvidar que el RLOPD incluía en su artículo 5 g) la definición de "Datos de carácter personal relacionados con la salud" [112].

Como sabemos, la nueva LO 3/2018, hace referencia al tratamiento de datos en el ámbito de la salud en su art. 9.2, dentro de las "categorías especiales de datos".

Teniendo en cuenta el derecho positivo citado, es una cuestión fundamental abordar el concepto de dato de salud. Inicialmente la expresión "datos de salud" aludía a los datos obtenidos a consecuencia de un tratamiento médico o una asistencia sanitaria a la que había sido sometida la persona titular de los mismos. Pero, como siempre, los avances tecnológicos han provocado una extensión del concepto inicial de dato de salud ya que pueden obtenerse datos relativos a la misma sin que medie un fin terapéutico concreto, es decir, sin que exista una patología a tratar en la persona titular del dato. De hecho, esto es lo que ocurre al captarse y tratarse un dato dactiloscópico de una persona con una patología cutánea. La captación y tratamiento de ese dato revela un dato de salud en un entorno totalmente ajeno al entorno sanitario.

Por tanto, llegamos a la conclusión que los datos de salud no son solo los que se obtienen o generan en el desarrollo de una relación concreta entre médico y paciente. En

[112] A este respecto, es conveniente tener en cuenta la Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal. El nivel de protección de los datos de salud, al tratarse de datos especialmente protegidos, se extiende excepcionalmente a los ficheros mauales o no automatizados. BOE núm. 110, de 9 de mayo de 1995.

este sentido, es muy acertada la afirmación de Gómez Sánchez,[113] al entender que la definición del dato de salud ha de basarse en el tipo de dato en sí mismo y no en el fin para el que se obtiene.

Este enfoque lo asumía la normativa interna española, LOPD y Reglamento de desarrollo, introduciendo un concepto amplio de dato de salud y permitiendo, así mismo, dar paso al enunciado de diferentes categorías de datos como por ejemplo los "datos de salud" y los "datos sanitarios" que, como veremos más adelante, no tienen el mismo régimen jurídico.

El artículo 5.1 g) del RLOPD, sin distinguir las dos categorías apuntadas, datos de salud y sanitarios, lo que sí definía son los datos relacionados con la salud y establece:

> *"*(…)
> g) Datos de carácter personal relacionados con la salud: Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética*".*

Este artículo recogía, como hemos apuntado, una definición amplia de lo que denomina "datos relacionados con la salud", que podríamos considerar coincidente con la categoría de datos de salud, y lo hace en el mismo sentido amplio en que la Organización Mundial de la Salud define ésta como "un estado de completo bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades". En definitiva, el RLOPD, al definir los datos relacionados con la salud, lo hacía atendiendo al tipo de dato en sí mismo, sin aludir a un supuesto fin terapéutico para el que se obtiene. Llama la atención en este artículo 5.1.g) la mención explícita de dos categorías de datos, no excluyentes de otras, relacionadas con la salud: los referidos al porcentaje de discapacidad y la información genética. Y decimos que llama la atención porque son

[113] GÓMEZ SÁNCHEZ, Y., "Datos de salud como datos especialmente protegidos" en TRONCOSO REIGADA, A. (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de carácter personal*, Cizur Menor, Civitas, 2010, p. 648.

dos categorías muy diversas entre sí y porque no se mencionan otros datos, como por ejemplo, los datos biométricos, que pueden revelar información relacionada con la salud.

Continuando con el análisis de la categoría del dato de salud, y siguiendo al profesor Lucas Murillo de la Cueva[114], se pueden predicar cinco características fundamentales del mismo: primera, es dato personal, en el sentido ya apuntado conforme definición de la LOPD y su Reglamento de desarrollo. Segunda, puede constar en un tratamiento automatizado o no. Tercera, está mantenido por una institución sanitaria relacionada con la salud[115]. Cuarta, el tratamiento y mantenimiento del dato se efectúa dentro del marco de la prestación de una asistencia médica o sanitaria a una persona y quinta el legislador tanto nacional como europeo ha creado una categoría específica para el dato de salud calificándolo de dato especialmente protegido. En estas cinco notas se delimita el concepto de dato de salud, que ampliaremos a continuación, siendo definitorio del mismo su carácter de especialmente protegido al afectar a derechos fundamentales del individuo como intimidad, autodeterminación informativa, dignidad e incluso libertad religiosa.

Las normas que tutelan el derecho a la autodeterminación informativa incluyen los datos relativos a la salud dentro de una categoría denominada datos especialmente protegidos.

Resulta de interés incluir la distinción entre los conceptos de dato de salud, dato relativo a la salud, dato sanitario y dato médico. Siguiendo en esta distinción terminológica a Nicolás Jiménez[116], dato de salud y dato relativo a la salud se pueden considerar sinónimos pudiendo establecerse ya sí diferencias con los otros dos términos: dato sanitario y dato médico. Así, Nicolás Jiménez define el dato sanitario como "el dato de salud que se obtiene y utiliza en instituciones sanitarias con el fin de preservar la salud de los ciudadanos." Por tanto, el dato sanitario es un dato de salud que referido a una persona física identificada o identificable tiene un régimen jurídico particular dentro de la regulación general de protección de datos. Y este régimen jurídico particular se

[114] LUCAS MURILLO DE LA CUEVA, P., "El derecho fundamental a la protección…", op. cit., p. 29.
[115] En esta tercera característica divergemos de la fundada doctrina de Murillo de la Cueva puesto que, como hemos visto, es frecuente que datos de salud estén en poder de instituciones financieras o instituciones de la Administraciòn relacionadas con el control migratorio y de fronteras.
[116] NICOLÁS JIMÉNEZ, P., *La protección jurídica de los datos genéticos de carácter personal*, Granada, Cátedra de Derecho y Genoma Humano-Editorial Comares, 2006, p. 78.

derivaba, no solo de lo dispuesto en el artículo 7.3 de la LOPD respecto datos especialmente protegidos, sino también de lo establecido en el artículo 8. El citado artículo 7.3, en relación con los datos de salud, establecía que solo pueden ser recabados, tratados y cedidos, cuando por razones de interés general así lo disponga una ley o el afectado consienta expresamente y, cabría añadir, de forma inequívoca[117]. Pero este régimen particular del dato de salud sanitario, a su vez, tiene una particularidad si se trata de forma preventiva o terapéutica en centros sanitarios públicos y privados por profesionales sanitarios. Así el artículo 8 LOPD establecía:

> *"*Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad[118]".

Por tanto, el dato de salud tratado en un determinado ámbito, el sanitario, lo convierte en dato sanitario que tiene un régimen diferente al dato de salud propiamente dicho. Por ello, no se pueden utilizar como sinónimos los términos dato de salud y dato sanitario. Ahora bien, todos los datos sanitarios son datos de salud, pero no todos los datos de

[117] El artículo 6.1 LOPD disponía: "Consentimiento del afectado.- 1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa". Por su parte los artículos 10.1 y 12.1 y 12.3 del RLOPD establecían:
"Artículo 10. Supuestos que legitiman el tratamiento o cesión de los datos.- 1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello."
"Artículo 12. Principios generales.- 1. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.
La solicitud de consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos".
(…)
"3. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho".

[118] Ley 14/1986, de 25 de abril, General de Sanidad, artículo 10.3 y 5, y Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. PIÑAR MAÑAS, J.L., "El derecho fundamental a la protección de datos personales. Contenido esencial y retos actuales. En torno al nuevo Reglamento de Protección de Datos*"* en *Legislación de Protección de Datos*, Madrid, Iustel, 2011, p. 123.

salud son datos sanitarios, debido a que, por ejemplo, no se hayan obtenido o se utilicen en instituciones sanitarias.

En esta tarea de delimitación del concepto de dato biométrico por exclusión, es decir, estableciendo sus diferencias con otras categorías de datos, llegamos a su delimitación respecto del "dato genético". El acercamiento al concepto de dato genético plantea una primera dificultad de carácter técnico: ¿qué entendemos por dato genético? Si citamos la más reciente definición nos referiremos al RGPD que en su artículo 4 apartado 13) entiende por "«datos genéticos»" a los: "datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;". EL RGPD hace referencia a características "adquiridas" que, como veremos a continuación, no recogen otras definiciones.

Si atendemos a la definición recogida en la Recomendación R (97) 5 del Comité de Ministros del Consejo de Europa datos genéticos son *"*todos los datos, con independencia de su tipo, que se refieren a las características hereditarias de una persona o al modelo de herencia de estas características de un grupo de personas de la misma familia"[119]. Pero, además, como así señala Troncoso Reigada, también son datos genéticos los referentes a "intercambios de información genética de un individuo o línea genética, con relación a cualquier aspecto de la salud o de la enfermedad"[120]. Los datos genéticos se califican por la Recomendación como datos de salud y, por tanto, están sometidos al régimen jurídico específico de éstos.

Así mismo, la Declaración Universal sobre los Datos Genéticos Humanos de la UNESCO de 16 de octubre de 2003 define estos datos como toda "información sobre

[119] Cfr. Documento de trabajo sobre datos genéticos. Adoptado el 17 de marzo de 2004 por el Grupo del artículo 29 sobre protección de datos. WP 91 12178/03/ES. www.europa.eu.int/comm/privacy, p. 4. [Fecha de consulta: 20/09/2016]. Este mismo documento de trabajo cita la definición de dato genético recogida en la Ley luxemburguesa como "cualquier dato relativo a las características hereditarias de una persona o de varias personas de la misma familia [letra g) del artículo 2 de la Ley luxemburguesa de 2 de agosto de 2002 relativa a la protección de las personas con respecto al tratamiento de datos de carácter personal]".

[120] TRONCOSO REIGADA, A., *La Protección de Datos Personales…,* op. cit., p. 1617.

las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos u otros análisis científicos"[121].

En las tres definiciones citadas, el dato genético es una información, o un conjunto de datos, sobre las características hereditarias de las personas físicas. Parece que lo que denominamos dato genético es la representación de una información que está soportada en cada individuo. Por tanto, cabría preguntarse ¿dónde está almacenada esa información? La respuesta es aparentemente sencilla: esa información está soportada en el ADN[122]. Y llegados a este punto es muy ilustrativa la exposición de Aparicio Salom que distingue con claridad entre datos genéticos y muestras biológicas, estando constituidos los primeros por *"*la información que puede obtenerse del análisis del mapa genético de una persona"[123] y siendo las muestras "la materia orgánica" susceptible de ser analizada genéticamente. De esta distinción, este autor, a su vez, deriva tres conceptos necesitados de análisis independiente: la muestra biológica (propiamente dicha), el resultado del análisis genético, es decir, el mapa genético y las conclusiones obtenidas del estudio de dicho mapa. Es evidente que la muestra no es un dato; sólo cuando la muestra se somete a un análisis genético se puede obtener de ella un dato, o unos datos de carácter personal. Y atendiendo al estado actual de la ciencia, ese análisis genético, sigue diciendo Aparicio Salom, puede realizarse a nivel superior sobre la región del ADN denominada codificante, o bien, a nivel inferior sobre regiones del ADN denominadas no codificantes. La información que cabe obtener del ADN codificante está relacionada directamente con la salud de la persona ya que puede revelar su predisposición a sufrir determinadas enfermedades o descubrir una enfermedad latente, en cambio el análisis del ADN no codificante es totalmente apto para la identificación de una persona, ya que "la variabilidad de sus secuencias hacen que el análisis del ADN no codificante sea extremadamente apto desde la perspectiva de

[121] Cfr. Documento de trabajo sobre datos genéticos. Adoptado el 17 de marzo de 2004 por el Grupo del artículo 29 sobre protección de datos, op. cit., p. 4.

[122] La dificultad de aproximación a un concepto científico nos hace apoyarnos en una autora que desde una perspectiva jurídica ha abordado este tema. Así, siguiendo a Nicolás Jiménez podemos afirmar que el ADN es el ácido desoxirribonucleico que se encuentra en el núcleo de todas las células de los organismos vivos en forma de una molécula constituida por dos cadenas paralelas que se trenzan. Por tanto, el ADN se presenta como una secuencia, un encadenamiento, de nucleótidos que constituyen un gen. Este gen (elemento biológico) es el elemento material o soporte de la información. Pero la información genética propiamente dicha es un elemento inmaterial. Una característica de la información genética es que se hereda y se comparte con la familia biológica. NICOLÁS JIMÉNEZ, P., *La protección jurídica…*, op. cit., pp. 3 y ss.

[123] APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de datos de carácter personal,* Navarra, Aranzadi, 2009, p. 79.

la medicina legal al efecto de identificación de las personas, puesto que, salvo el caso de gemelos univitelinos, no existen dos personas que tengan la misma secuencia de bases en el ADN"[124].

Habiendo visto dónde se encuentra almacenada la información genética, el genoma, de cada individuo cabría preguntarse ¿cómo se accede a ella? Cabría distinguir hasta tres técnicas: el examen de los modos de herencia de los caracteres, estudios citogenéticos y la tercera vía el análisis molecular o bioquímico que requiere la obtención de ADN (células de la sangre)[125]. Así mismo, se podría hablar hasta de tres tipos de análisis de ADN en función de la finalidad que se persiga: el análisis clínico, el de investigación y el de identificación. La información que se puede obtener de los análisis genéticos sobre muestras biológicas es amplísima y puede no sólo afectar a la persona física de quien proceden las muestras sino también a toda su familia. El mal uso de esta información lleva aparejados unos riesgos que han llevado a que la jurisprudencia se pronuncie afirmando que fuera de la investigación sanitaria los análisis deben limitarse a las regiones del ADN no codificante.

Siguiendo a Nicolás Jiménez[126] y, en el mismo sentido, a Troncoso Reigada, cabe afirmar que en las investigaciones genéticas de los años 90 se determinó que cada persona es portadora de un código genético exclusivo y se puede plantear un nuevo modelo de identificación. Del análisis genético cabe distinguir dos resultados distintos: el ADN-codificante o expresivo[127] y el ADN no codificante o perfiles de ADN. El ADN-codificante proporciona información relativa a la salud de la persona y sus familiares y el ADN no codificante no facilita información sobre la salud de la persona, sino que únicamente la identifica, por eso se habla de perfil genético o huella genética. Las bases de datos de perfiles genéticos no almacenan información genética sino únicamente datos de identificación genética o esencial frente a la identificación clásica o periférica[128]. Esta distinción entre ADN codificante y no codificante es fundamental y

[124] LORENTE ACOSTA, J. A., *El ADN y la Identificación en la Investigación Criminal y en la Paternidad Biológica*, Granada, Comares, 1995, p. 48, Citado por APARICIO SALOM, J., op. cit., p. 81.
[125] Ibíd., p. 16.
[126] NICOLÁS, P., "El concepto de dato médico y genético" en RIPOL CARULLA, S. (ed.), BACARIA MARTRUS, J. (coord.). *Estudios de protección de datos de carácter personal en el ámbito de la salud*, Barcelona-Madrid, Agencia Catalana de Protección de Datos y Marcial Pons, 2006, p. 88.
[127] TRONCOSO REIGADA, A., *La protección de datos personales…,* op. cit., p. 1618.
[128] Cfr. GARCÍA, O. y ALONSO A., "Las bases de datos de perfiles de ADN como instrumento en la investigación policial"; CUESTA PASTOR, P. J, "Los mecanismos de identificación y su uso en el

de hecho el Tribunal Constitucional Federal alemán, en su Auto de 18 de septiembre de 1995, afirmó que las muestras biológicas obtenidas pueden ser investigadas siempre que se limite la investigación al ámbito no codificante del ADN[129]. Por su parte el Tribunal Supremo español reconoce que cada persona dispone de una huella genética, igual que dispone de una huella dactilar exclusiva y excluyente.

En relación con la diferencia entre ADN codificante y ADN no codificante es muy ilustrativo el voto particular que formula el magistrado Juan Ramón Berdugo Gómez de la Torre, a la sentencia número 734/2014, dictada en el recurso de casación 289/2014 por la Sala 2ª del Tribunal Supremo de fecha 11 de noviembre de 2014. Dice así el magistrado Berdugo Gómez de la Torre:

> "[…] Coincidiendo con la mayoría en el pronunciamiento recaído en la sentencia en cuanto supone estimación parcial del recurso interpuesto, discrepo respetuosamente en relación a la exigencia de que el consentimiento del acusado detenido para la práctica de prueba de ADN y su inclusión en la base de datos policial, precise de asistencia letrada conforme el acuerdo del Pleno de esta Sala de 24.9.2014.
>
> Como premisa de partida desde el punto de vista funcional es necesario precisar que el ADN puede clasificarse como codificante en referencia a los genes con información para la síntesis de proteínas, y no codificante en referencia a las regiones de ADN cuya secuencia no aporta información directa para la síntesis de proteínas y por lo tanto de su estudio no se obtiene información alguna de las características físicas o fenotípicas del sujeto (predisposición individual de padecer enfermedades de base genética). [la diferencia entre ADN codificante y no codificante radica en la información que cabe derivar de uno y otro, en concreto, del primero mucho más amplia que del segundo].

proceso penal: interrogantes a propósito de la huella de ADN", en ROMEO CASABONA, C., citado por TRONCOSO REIGADA, A., *La protección de datos* personales…, op.cit., p. 1619.
[129] Ibíd.

> Los marcadores del ADN codificante son distintos en cuanto aportan una información excesiva e íntima del sujeto: su huella o herencia genética; rasgos físicos, enfermedades congénitas o predisposición a contraer determinadas enfermedades. El conocimiento de esta información afecta sin discusión a la intimidad de la persona.
>
> El perfil del ADN no codificante consiste en cambio en una serie de números que confirman un código anónimo diferenciador de los que no se puede descubrir ningún dato relativo al contenido genético de la persona.
>
> De hecho, la información que aportan carece de valor hasta ser contrastada con otro perfil procedente de muestra debitada.
>
> Por ello, a efectos de identificación los análisis de la cadena de ADN se ciñen al estudio de los marcadores del ADN polimórfico o no codificante, que solo contienen información sobre identidad y sexo*"*[130].

De lo expuesto derivan dos conclusiones: primera el ADN codificante contiene información genética que, sin duda, afecta a la intimidad de la persona, y segunda: el ADN no codificante no contiene información genética sino simplemente información sobre identidad y sexo. Cabría establecer paralelismos entre este ADN no codificante y la huella dactilar. Así lo recoge la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN, tanto en su exposición de motivos como en su articulado. En concreto, establece que para preservar la intimidad de los individuos sólo se permite la inscripción en la base de datos de ADN del ADN no codificante a los solos efectos identificativos sin que quepa revelar otros datos genéticos[131]. En su exposición de motivos, la LO 10/2007 afirma taxativamente que: «Esta regulación contiene una salvaguarda muy especial, que resulta fundamental para eliminar toda vulneración al derecho a la intimidad, puesto que sólo podrán ser inscritos aquellos perfiles de ADN que sean reveladores, exclusivamente, de la identidad del sujeto -la misma que ofrece una huella dactilar- y del sexo, pero, en

[130] Fuente de suministro: Centro de Documentación Judicial. IdCendoj: 28079120012014100738.
[131] En España existen dos tipos de ficheros de perfiles de ADN: los de perfiles de ADN de delincuentes y los de perfiles de ADN para la identificación de personas desaparecidas.

ningún caso, los de naturaleza codificante que permitan revelar cualquier otro dato o característica genética». En el mismo sentido, el artículo 4 de la Ley bajo el epígrafe de "Tipos de datos" establece que: "Sólo podrán inscribirse en la base de datos policial regulada en esta Ley los identificadores obtenidos a partir del ADN, en el marco de una investigación criminal, que proporcionen, exclusivamente, información genética reveladora de la identidad de la persona y de su sexo". Esta preocupación por mantener a salvo el derecho a la intimidad de las personas conservando únicamente su ADN no codificante está en consonancia con el criterio mantenido por el TEDH en su Sentencia de 4 de diciembre de 2008, caso S. y *Marper vs.* Reino Unido en la que afirma que "la cantidad de información personal contenida (en las muestras celulares) conduce a considerar que su conservación constituye en sí misma una lesión del derecho a la vida privada, de suerte que poco importa que las autoridades extraigan o utilicen solo una pequeña parte de tal información para la creación de perfiles de ADN"[132]; porque "el mero hecho de que las autoridades públicas conserven o memoricen datos de carácter personal, cualquiera que sea la manera en la que hayan sido obtenidos, tiene unas consecuencias directas en la vida privada de la persona afectada".

Por último, y en lo que a Derecho interno se refiere, hay que tener en cuenta que, aunque no lo precisara el artículo 5.1.g) del RLOPD, la información genética tiene un doble tratamiento por el derecho positivo: por una parte los datos genéticos que se obtengan y traten para aplicaciones policiales, de seguridad del Estado o de seguridad pública, es decir, datos que puedan utilizarse para la represión de infracciones penales y, por otra, los utilizados para establecer el parentesco biológico que tienen una regulación específica. Además, el artículo 2.3 LOPD establecía que "se regirán por sus disposiciones específicas los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas, los datos derivados del Registro Civil y del Registro Central de penados y rebeldes y los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras

[132] TEDH, sentencia de 4 de diciembre de 2008, nº 30562/04 y 30566/04 (S. y Marper contra Reino Unido). Disponible en https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%22CASE%20OF%20S.%20AND%20MARPER%20v.%20THE%20UNITED%20KINGDOM%20-%20[Albanian%20Translation]%20summary%20by%20the%20European%20Centre%20with%20the%20assistance%20of%20the%20Regional%20Balkans%20Rule%20of%20Law%20Unit%20of%20the%20Dutch%20Ministry%20of%20Foreign%20Affairs%20and%20the%20Dutch%20Ministry%20of%20Justice%20and%20Security\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-183664%22]} [Fecha de consulta:15/08/2018].

por las Fuerzas y Cuerpos de Seguridad". En cualquiera de estos ámbitos los datos tratados pueden ser genéticos y estar sometidos a dichas disposiciones específicas. En definitiva, este artículo 2.3 establecía la exclusión de determinados datos genéticos de la regulación de la LOPD en atención a las aplicaciones o fines a que se destinen dichos datos. Y, por otra parte, el dato genético, al considerarse dato relacionado con la salud, como así lo establece el citado artículo 5.1.g) del RLOPD, gozaba de una protección jurídica reforzada conforme a lo dispuesto en los artículos 7.3 y 8 LOPD. Lo que ni la ley española (ni la Directiva 95/46/CE anteriormente), ni el RGPD hacen es definir el dato genético como sinónimo de dato biométrico. Pero, tanto nuestro ordenamiento jurídico, como anteriormente la Directiva y, actualmente, el RGPD, establecen un "régimen jurídico particular o particularidades en el régimen general"[133] de la protección de los datos de carácter personal. Igualmente, la LO 3/2018, en su Disposición adicional decimoséptima ("Tratamientos de datos de salud"), hace una remisión al artículo 9.2 del RGPD.

En resumen, la vigente normativa española sobre protección de datos de carácter personal identifica, como uno de los datos relacionados con la salud, los datos genéticos haciendo aplicable a ellos la restricción establecida para los datos de salud en general respecto a su recopilación, tratamiento y cesión[134], que quedan reservadas a que por razones de interés general así lo disponga una ley o medie el consentimiento expreso, inequívoco, del afectado. A su vez, el dato biométrico puede, en algunos casos, revelar datos de salud, pero no siempre es así. Siendo indudable que hay casos de confluencia del dato de salud y el dato biométrico, en absoluto, son categorías de datos equivalentes. Y, por último, el hecho de que algunos datos de ADN se orienten a la identificación de personas físicas, como así lo hacen los datos biométricos, tampoco los convierte a

[133] Cfr. NICOLÁS, P., "El concepto de dato médico...", op. cit., p. 78.

[134] En concreto, en relación con la cesión de los datos de salud la propia LOPD establecía una excepción al consentimiento, al establecer su artículo 11.2. f) que "no será necesario el consentimiento del afectado cuando la cesión de los datos relativos a la salud sea necesaria para solucionar una urgencia, entendemos que médica, o para realizar estudios epidemiológicos". Esta excepción al consentimiento al recogerse en la propia LOPD cumplía con el requisito de la habilitación legal del artículo 7.3 y ha de interpretarse junto a lo dispuesto en el artículo 8 que habilita a las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes a tratar a los datos de salud, de las personas que a ellos acudan o deban ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad. Es decir, la LOPD remitía a la Ley 14/1986, de 25 de abril, General de Sanidad, artículo 10.3 y 5 y a la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

ambos en categorías equivalentes de datos, manteniendo así cada uno sus características compartiendo, eso sí, algunas soluciones de su régimen legal.

2.3. Zonas de confluencia de la biometría y la videovigilancia.

Hablamos de zonas de confluencia de biometría y videovigilancia porque, en la base de ambas, se encuentra la imagen gráfica de un individuo que analizaremos si es o no dato de carácter personal y, en caso de serlo, si es dato personal biométrico y el tratamiento jurídico dado por la normativa sobre videovigilancia. En esta tarea de delimitación del objeto de estudio puede resultar de ayuda analizar un dato que cabe calificar *a priori* como dato biométrico: la imagen gráfica de un individuo. La imagen gráfica de una persona es objeto de regulación jurídica por parte de la normativa sobre protección de datos, en cuanto que puede afectar a la intimidad de las personas, y, a su vez, dispone de una regulación específica en lo atinente a la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. Del estudio del tratamiento jurídico de la imagen y de sus características buscaremos extraer las señas de identidad de los datos biométricos en general.

La imagen de un individuo, reflejada por ejemplo en una fotografía, fue calificada por la STC 14/2003, de 30 de enero, como dato de carácter personal; en este mismo sentido se ha pronunciado el GPD 29 en su Opinión 4/2007. Si un criterio delimitador del carácter personal de un dato es su potencial identificador de una persona es indudable que la imagen es un dato de carácter personal pues de su simple visualización cabe establecer su atribución o conexión con una persona. Este criterio era acorde con lo dispuesto en el artículo 5.1.f) del RLOPD que calificaba de datos de carácter personal, entre otros, cualquier información gráfica o fotográfica concerniente a personas físicas identificadas o identificables.

La cuestión es ahora determinar el concepto de la imagen como dato de carácter personal que la hace merecedora del amparo de las leyes de protección de datos. O lo que es lo mismo, cuándo a un tratamiento de imágenes se le ha de aplicar la normativa de protección de datos. Para ello, atenderemos al Considerando 14 de la Directiva 95/46/CE que determinaba que no toda captación, transmisión, manejo, registro,

conservación o comunicación de imagen quedaba bajo la regulación de la Directiva sino que esos procesos deben estar automatizados o incluidos en archivo estructurado que permita el acceso posterior. Así, partiendo de que la imagen ha de haber sido sometida a tratamiento hay dos exclusiones básicas: una, el tratamiento cuya finalidad sea la seguridad pública y otra, el tratamiento que se realiza con fines periodísticos en el sector audiovisual, el resto de tratamientos, en principio, caerían dentro del ámbito de aplicación de la normativa sobre protección de datos. No obstante, para precisar adecuadamente esta delimitación hay que comprobar, para que la imagen quede bajo la normativa de protección de datos, que, como se ha indicado, no solo se realice con ella un tratamiento, cualquier tipo de operación, sino que esa operación la haga accesible, se incorpore a un fichero, siendo la imagen relativa a una persona identificada o identificable. En definitiva, lo que hace que la imagen sea dato de carácter personal es el hecho de haber sido sometida a un tratamiento e incluida en un fichero que como conjunto organizado de datos facilite el acceso y su recuperación posterior.

Partiendo de que "la imagen de una persona" es un dato de carácter personal, la segunda cuestión es si puede constituir un dato personal biométrico. Para ello nos detendremos en recoger una vista panorámica de su regulación. La captación y tratamiento de la imagen de una persona puede conllevar la violación de sus derechos fundamentales y ya hemos visto que la imagen de una persona identificada o identificable sometida a un tratamiento e incorporada a un fichero entra dentro del ámbito de aplicación de la normativa sobre protección de datos. El artículo 2.3 e) de la LOPD establecía que "se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos… e) los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia". En desarrollo de esta exclusión se publicó la Ley Orgánica 4/1997 que regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. Esta Ley Orgánica regula por primera vez en España la videovigilancia y desarrolla el artículo 104.1 de la CE, que contiene el mandato a las Fuerzas y Cuerpos de Seguridad, bajo dependencia del Gobierno, de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana. La utilización de videocámaras en lugares públicos exige proporcionalidad tanto desde el punto de vista de la idoneidad como de la intervención mínima. Así, el artículo 6.2 de la LO 4/97 establece que "la idoneidad determinará que

sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, de conformidad con lo dispuesto en esta ley". Y en el apartado 3, el mismo artículo 6 en relación con la intervención mínima establece que ésta "exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara del derecho al honor, a la propia imagen y a la intimidad de las personas". Lo cierto es que, en el ámbito de la videovigilancia (que se contempla ahora en el art. 22 LO 3/2018), como indica Rebollo Delgado, hay que poner "en equilibrio, de forma genérica, derechos individuales en contraposición a derechos colectivos. De forma concreta lo que está en juego es la prevalencia del derecho a la intimidad, honor y propia imagen, y protección de datos de carácter personal frente al derecho a la seguridad. La norma no se decanta a priori por ninguno de ellos, y son los hechos o el caso singular, donde habrá de determinarse la prevalencia[135]". Esta disyuntiva, o conflicto entre derechos, también se plantea en el uso de datos biométricos en el ámbito de la seguridad, como más adelante se verá.

Pero también, junto a la videovigilancia en el ámbito público hay que tener en cuenta la videovigilancia en el ámbito privado[136]. Tanto en lugares cerrados públicos como privados es habitual la presencia de cámaras que graban[137] la imagen con fines de seguridad. La videovigilancia en lugares privados con grabación y tratamiento quedaba, sin duda, dentro del ámbito de la Directiva 95/46/CE y ahora bajo el amparo del RGPD[138] y la LO 3/2018. Además, la seguridad privada está regulada en España por la

[135] REBOLLO DELGADO, L., SERRANO PÉREZ, M. M., *Manual de Protección…*op. cit., pp. 253 y 272.

[136] Merece una especial mención la reciente Sentencia del TEDH de 9 de enero de 2018 (Caso López Ribalda y Otros - Asuntos 1874/13 y 8567/13) mencionada en el cuadragesimoséptimo fundamento de derecho de la sentencia del TSJ Canarias (Santa Cruz de Tenerife) Sala de lo Social, sec. 1ª, S 17-1-2018, nº 25/2018, rec. 584/2017. El TEDH rechaza la licitud de una videovigilancia secreta de trabajadores en sus puestos de trabajo de forma indiscriminada. Es necesario informar a los trabajadores sobre la instalación de un sistema de videovigilancia. El Tribunal Europeo afirma taxativamente que: "[…] en el momento en que se produjeron los hechos enjuiciados la normativa española era clara con respecto a la necesidad de informar a los afectados de la instalación del sistema de videovigilancia, cosa que no se verificó por la empresa, y la grabación de imágenes se realizó de forma indiscriminada a la totalidad de la plantilla, durante varias semanas y durante toda la jornada". EDJ 2018/526873 STSJ Canarias (sede Santa Cruz) Sala de lo Social de 17 de enero de 2018.

[137] Es conveniente diferenciar la videovigilancia de la monitorización, ya que ésta es simplemente la reproducción de imágenes en tiempo real sin guardar copia de las mismas y, por ello, no cabe tratamiento. Sin embargo, la videovigilancia en lugares privados de la que se obtiene grabación de imágenes haciendo posible el tratamiento entra claramente en el ámbito de la Ley de protección de datos.

[138] La definición de "datos personales" recogida por el artículo 4 1) abarca la videovigilancia, sin mencionarla expresamente, ya que en el concepto se engloba "toda información sobre una persona física indentificada o identificable […] o uno o varios elementos propios de la identidad física […]".

Ley 5/2014, de 4 de abril, que considera en su artículo 5.1.f) actividades de seguridad privada "la instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas o a centros de control o de videovigilancia". Sin ánimo de agotar el tema, y en este primer momento de delimitación del concepto de dato personal biométrico, conviene hacer un breve repaso por la regulación del tratamiento de la imagen humana como dato personal recogida en las siguientes Instrucciones de la AEPD: Instrucción 1/1996, de 1 de marzo, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios; Instrucción 2/1996, de 1 de marzo, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo, que se refieren expresamente a los datos relativos al sonido y la imagen; Instrucción 1/2006, de 8 de noviembre, sobre tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. Esta Instrucción 1/2006 se une a la tendencia de la normativa europea de no excluir de la regulación sobre protección de datos a la videovigilancia. Ya la Conferencia Internacional de Autoridades de Protección de Datos, celebrada en Londres en noviembre de 2006, había puesto de manifiesto la necesidad de acomodar la videovigilancia a las exigencias del derecho fundamental a la protección de datos. La actividad de la videovigilancia queda sometida a la normativa de protección de datos al decir expresamente el artículo 1.1 de la Instrucción que: "La presente Instrucción se aplicará al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables con fines de vigilancia a través de sistemas de cámaras y videocámaras". Excluyéndose por el artículo 7.2 de la Instrucción la monitorización de imágenes al establecer que: "no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real". A su vez, se establecen dos exclusiones más: la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado y el tratamiento de imágenes en el ámbito personal y doméstico. Junto a estas disposiciones de ámbito nacional, las Agencias autonómicas también han aprobado disposiciones dentro de su ámbito territorial sobre la materia. Así, la Agencia de Protección de Datos de la Comunidad de Madrid regula a través de la Instrucción 1/2007, de 16 de mayo, el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los órganos y Administraciones Públicas de la Comunidad de Madrid. Por su parte, la Agencia Catalana de Protección de Datos regula, a través de la Instrucción

1/2009, de 10 de febrero, el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia.

La Agencia estatal a través de la primera de las Instrucciones citadas, la 1/1996 de 1 de marzo, aborda el tema de la regulación de los datos constituidos por sonido e imagen de personas físicas captados en el acceso de éstas a centros de trabajo o dependencias públicas. Expresamente la Instrucción en su norma primera considera dato personal la información concerniente a una persona física consistente en el sonido y/o la imagen de dicha persona. Aunque no se especifique debe entenderse que el sonido que identifica a una persona debe hacer referencia a su voz. No olvidemos que, de acuerdo con lo que disponía el artículo 5 o) RLOPD el dato debe identificar a una persona, directa o indirectamente, pudiendo consistir en cualquier información referida a su identidad física o fisiológica. Es indudable que la voz identifica a las personas con márgenes de error aceptables. Nos encontramos así con que la voz es un dato biométrico de identificación captado por un sistema de videovigilancia.

La segunda Instrucción citada, la 2/1996, de 1 de marzo, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo, en el mismo sentido que la anterior, define en su norma primera apartado 2. lo que se considera dato personal entendiendo por tal: *"*cualquier información concerniente a personas físicas identificadas o identificables, debiendo entenderse comprendidos dentro de la misma el sonido y la imagen"[139]. La norma tercera apartado 2. limita estos datos a los que aparecen en el documento identificador exigido para la entrada al casino o sala de bingo. Si como parece se está refiriendo al DNI sería la imagen del individuo, su nombre, apellidos, número de DNI, fecha y lugar de nacimiento, nombre de los padres, sexo y domicilio los datos que cabe recoger en el acceso a casinos y salas de bingo. Sin embargo, con la incorporación al DNI electrónico, almacenados en un chip, de otros datos cabría entender ampliado el ámbito de datos susceptibles de ser recogidos y tratados. Incluso cabría plantearse la licitud del almacenamiento y posterior tratamiento del dactilograma[140] de cada individuo.

[139] BOE núm. 62, de 12 de marzo de 1996.

[140] Como ya hemos apuntado anteriormente entendemos, de la mano de De Antón y Barberá, por dactilograma el conjunto de crestas papilares correspondientes a cada dedo. Pero los dibujos papilares se forman por el conjunto no solo de las líneas o crestas papilares sino también por los espacios entre esas crestas denominados surcos papilares. Así con más precisión podemos definir el dactilograma como "el

Y ya pasando a la Instrucción 1/2006[141], de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, y de acuerdo con lo dispuesto por la LOPD, las imágenes captadas o grabadas por cámaras o videocámaras deben ser consideradas datos de carácter personal, incluidas en la definición del artículo 3.a) ya citado.

Indudablemente, de todo lo expuesto, cabe deducir que la imagen es considerada dato de carácter personal en cuanto se trata de una información gráfica o fotográfica de un individuo. La imagen es dato personal si se refiere a una persona identificada o identificable. Para la Instrucción 1/2006 la legitimación del tratamiento de imágenes pasa necesariamente por el respeto y aplicación íntegra del artículo 6.1 y 2 y del artículo 11.1 y 2 de la LOPD[142]. Hoy, la LO 3/2018, también en su art. 6 ("Tratamiento basado

---

dibujo formado por las crestas papilares y surcos existentes entre ellos, que aparecen en las yemas de los dedos de las manos o su impresión o reproducción gráfica". Teniendo en cuenta que el dactilograma suele dividirse en natural (el apreciable a simple vista en la pulpa de cualquier dedo humano), artificial (el estampado o grabado en una tarjeta decadactilar después de entintar el dedo) y latente (el que no se manifiesta si no es con un agente reactivo) entendemos que no es tecnológicamente ardua la tarea de almacenar en un DNI electrónico el dactilograma artificial de cada individuo para su posterior comprobación. DE ANTÓN Y BARBERÁ, F., op. cit., pp. 43 y ss.

[141] A nivel autonómico, ya se ha apuntado, que tanto la Agencia de Protección de Datos de la Comunidad de Madrid como la Autoridad Catalana de protección de datos han dictado sendas instrucciones sobre la materia. La primera ha dictado la Instrucción 1/2007, de 16 de mayo, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los órganos y Administraciones Públicas de la Comunidad de Madrid (BO. Comunidad de Madrid de 18 de julio de 2007, núm. 169, [p. 12]. Por su parte la Autoridad Catalana de Protección de Datos ha dictado la instrucción 1/2009, de 10 de febrero, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia, DOGC núm. 5322, de 19 de febrero de 2009.

[142]Artículo 6. Consentimiento del afectado- 1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, aparatado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertados fundamentales del interesado." "Artículo 11. Comunicación de datos- 1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. 2. El consentimiento exigido en el apartado anterior no será preciso: a) Cuando la cesión está autorizada en una ley. b) Cuando se trate de datos recogidos de fuentes accesibles al público. c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. d) Cuando la comunicación que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con

en el consentimiento del afectado") regula esta cuestión, haciendo una remisión al art. 4.11 RGPD.

El artículo 1 de la Instrucción, al determinar el ámbito de aplicación expresamente establece: "La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras*".* Si, como hemos visto, la imagen es dato de carácter personal, este primer párrafo del artículo 1 delimita la vertiente a la que exclusivamente atenderá la Instrucción: el tratamiento de la imagen con fines de vigilancia. ¿Cabría plantearse el tratamiento de la imagen con otros fines? Entendemos que sí, que el control de accesos a zonas restringidas o el tratamiento de la imagen de una persona física con la única finalidad de identificación de un delincuente son otros fines que cabría plantearse, pero, a priori, excluidos de esta Instrucción.

Esta Instrucción 1/2006, que venimos comentando, en este mismo artículo 1.1. considera identificable una persona "cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente Instrucción, sin que ello requiera plazos o actividades desproporcionados". Siendo un concepto indeterminado el de "plazos o actividades desproporcionados[143]", entendemos hace aplicable el principio de proporcionalidad que, aunque desarrollado en el ámbito de la limitación a derechos fundamentales, tiene plena vigencia en nuestra jurisprudencia constitucional y en la jurisprudencia europea. Se limitan así las actividades a realizar para mostrar la imagen de una persona a las que mantengan una proporción entre los medios empleados y el fin que se pretende. Los nuevos medios tecnológicos pueden esclarecer la imagen de una

funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas. e) Cuando la cesión se produzca entre administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos y científicos. f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica."

[143] La tecnología de video analógico o digital en la captación de imágenes influye decisivamente en lo que haya de considerarse proporcionado o no. En un principio la captación de imágenes se realizó por métodos analógicos. En un sistema analógico la degradación de salida es la suma de las degradaciones que se producen en cada etapa por la que la señal haya pasado. Sin embargo, la tecnología digital se basa en una información codificada en forma binaria y, por tanto, a diferencia de la grabación analógica en la digital al ser una serie de dígitos éstos se pueden reproducir en infinitas copias sin experimentar degradación. Además, la información digital permite un uso y corrección de errores donde la relación señal/ruido en las pistas grabadas es mas simple de identificar que en una grabación analógica. También cabe señalar que en una grabación digital se pueden construir filtros y ecualizadores digitales estables que pueden manipular la imagen. En definitiva, entendemos que hay que tener en cuenta qué tecnología de tratamiento de la imagen se ha utilizado para calificar sobre la proporcionalidad de los plazos o actividades. Cfr. ARZOZ SANTISTEBAN, X., op. cit., p. 39.

persona, pero si el tiempo y el propio coste es desproporcionado no cabría considerar imagen, ni dato personal, a una imagen-representación desfigurada de un individuo. En cuanto a lo que ha de considerarse tratamiento y el medio para llevarlo a cabo, la Instrucción en este mismo artículo 1.1. claramente amplía los medios de tratamiento no solo a los sistemas de cámaras y videocámaras sino también a "cualquier medio técnico análogo". Y en cuanto al tratamiento, éste comprende: "la grabación, captación, transmisión, conservación y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas*".*

El RGPD en su artículo 4. 2) definie «tratamiento» como: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;". Indudablemente queda incluida la grabación y/o captación de imágenes de personas físicas y sus usos posteriores.

Hemos completado una somera aproximación al concepto de dato personal y, en concreto, a un tipo de datos personales, la imagen, que por excelencia constituye una dimensión del dato biométrico. En esta tarea inicial de delimitación del ámbito de nuestro estudio, resulta de interés enumerar algunas aplicaciones de captación de datos biométricos de individuos que en unión de la tecnología de la videovigilancia se encuentran actualmente en uso.

Así lo pone de manifiesto Arzoz Santisteban[144] al decir que los sistemas de videovigilancia hoy en día ya no se limitan en muchas ocasiones a la simple captación de imágenes y sonido y a su transmisión hasta un receptor, sino que esa captación de imágenes se combina con programas informáticos de captación y tratamiento de datos biométricos.

[144] Ibíd., p. 46.

De este modo, la tecnología de la videovigilancia puede combinarse o completarse con programas de identificación de personas. Estos programas identifican personas, por ejemplo, a través de los rasgos físicos de la cara. De este modo, un sistema de videovigilancia con reconocimiento facial puede ser un instrumento eficaz para el control de acceso a un edificio. De forma simplificada, el sistema funciona captando los rasgos morfológicos de una cara y procediendo a una comparación de uno a uno, los datos captados con los almacenados correspondientes a un determinado individuo. Si no hay coincidencia, es decir, si se produce una incapacidad de reconocimiento por el sistema, éste automáticamente transmite una solicitud de autorización junto a la imagen captada a una base central o a un centro de acceso donde se autorizará o no dicho acceso. También estos sistemas que combinan la tecnología de la videovigilancia con la identificación son utilizados como sistemas de detección de sospechosos. En esta segunda función de detección, el sistema emitirá una señal de alarma cuando se reconozca una cara coincidente con los rasgos de una persona buscada por la policía[145]. Otras posibles combinaciones de la tecnología de la videovigilancia son: con programas de reconocimiento de la voz, con signos acústicos o con programas de reconocimiento térmico por infrarrojo[146].

En los ejemplos que hemos reproducido es indudable que existe una estrecha relación entre la tecnología de la videovigilancia y la captación de datos biométricos, pero a la vez una clara diferencia puesto que la captación de imágenes por sistemas de videovigilancia sirve de base a la captación de datos biométricos, pero no necesariamente y en todos los casos. Además, la captación de imágenes tiene, habitualmente en la videovigilancia, un fin no identificador de individuos concretos sino simplemente de control de seguridad pública o privada siendo ese el campo exclusivo de la regulación específica en la materia sobre videovigilancia. En conclusión, la vigilancia en lugares públicos está sometida a la previa obtención de autorización gubernativa y el tratamiento de los ficheros grabados quedan igualmente sometidos a un régimen estricto de limitaciones (según Ley Orgánica 4/1997) y la videovigilancia

[145] En el municipio de Tampa (Florida, EE.UU.) se instaló en una zona de ocio de afluencia nocturna el sistema *FaceIt* que permitía captar primero la imagen, la procesaba analizando 80 puntos del rostro entre los ojos, la nariz y los pómulos y se comparaba con una base central de delincuentes. Si a los 10 segundos no se había establecido una coincidencia las imágenes se desechaban. ARZOZ SANTISTEBAN, X., op. cit., p. 49.

[146] La instalación de un software que analice signos acústicos en la vía pública que expresen agresividad o miedo puede provocar el encendido de las cámaras y ordenar la intervención policial. Con ello se pasaría de una vigilancia visual a una vigilancia acústica.

privada queda sometida a la normativa de protección de datos y a la Ley de seguridad privada. En definitiva, la captación de la imagen humana tiene una regulación específica desde el ámbito de la seguridad, la prevención del delito y los fines de vigilancia y no así desde otros fines como, por ejemplo, los de identificación propiamente dichos.

Es muy claro, en este punto, el Considerando (51) del RGPD que reza así: "[…] El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. […]".

La fotografía de un individuo es dato de carácter personal biométrico y especialmente protegido si, y solo si, permite la identificación de ese individuo, de esa persona física concreta.

2.3.1. **Exclusión del dato de salud, del dato genético y de la videovigilancia**

En definitiva, ninguno de los tres ámbitos normativos, ni la protección de los datos de salud, ni los datos genéticos ni la imagen grabada en un entorno de videovigilancia, abarcan o se acomodan a las exigencias de protección del dato biométrico dactiloscópico. Este dato puede revelar, pero no necesariamente, un dato de salud. Por otra parte, la información genética puede atender a un fin identificador del individuo, pero no en todos los casos. Y la imagen grabada dista mucho de coincidir en características y por tanto necesidades de protección con respecto a un dato dactiloscópico que solo indirectamente y tras un proceso de comparación puede llegar a identificar a una persona. Indudablemente ya hemos delimitado a la imagen como dato de carácter personal y hemos reseñado su protección en la normativa específica sobre videovigilancia, pero no cabe confundir los ámbitos de protección de la imagen y los datos biométricos dactiloscópicos, puesto que éstos no permiten la identificación directa de un individuo cosa que sí permite la imagen. La normativa sobre videovigilancia no es aplicable a la protección de dato biométrico.

2.4. La recopilación de datos biométricos dactiloscópicos en la investigación criminal. El peligro de reutilización.

Ya en 2003 el GPD 29 en su "Documento de trabajo sobre biometría" ya citado, alertó de dos potenciales peligros en relación con la recopilación de datos biométricos dactiloscópicos: por una parte, la tendencia a la creación de grandes bases de datos sobre huellas digitales propiciadas por fines absolutamente legítimos como son los derivados de una investigación criminal pero que abren la posibilidad de reutilización de estos datos con otros fines; y por otra parte, el peligro de recopilación sin que el interesado sea consciente de ello. El GPD 29, en este documento de trabajo, expresamente califica de datos de naturaleza especial a los datos biométricos porque pueden permitir la identificación inequívoca de una persona. Los datos dactiloscópicos pueden llevar a la identificación única dependiendo, como bien apunta este documento, de las dimensiones de la base de datos donde se encuentren almacenados. No es la única función del dato dactiloscópico, pero efectivamente permite la identificación de individuos uniendo el dato con una identidad concreta, con un nombre y unos apellidos llevándose a cabo un proceso en el que se distingue a un individuo del resto. La identificación sólo puede realizarse almacenando los datos dactiloscópicos en una base de datos centralizada donde se encuentren todos los datos del resto de individuos que han de ser cotejados para lograr finalizar con la identificación final de un individuo. La identificación de detenidos es una diligencia inicial y fundamental en la investigación de un hecho delictivo. Para llevar a cabo esa identificación las fuerzas y cuerpos de seguridad del estado utilizan, entre otros elementos, la reseña dactilar. Esta reseña de una persona detenida como indica De Antón[147] es una diligencia policial de naturaleza administrativa que se encuentra sometida a lo dispuesto en la normativa sobre protección de datos[148]. Este peligro de reutilización se abordó por el TEDH en el caso S.

[147] DE ANTÓN Y BARBERÁ, F., op. cit., p. 118.

[148] Conforme a lo dispuesto en el artículo 2.2.c) el régimen de protección de los datos de carácter personal establecido en la LOPD no será de aplicación: "c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos". Y, por otra parte, se regirán por sus disposiciones específicas según el artículo 2.3. e) los tratamientos de datos personales: "e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia". Por tanto, dejando a salvo estas dos excepciones el resto de tratamientos de datos personales, y entre ellos los dactiloscópicos, llevados a cabo por las Fuerzas y Cuerpos de Seguridad se encontraban dentro del ámbito de aplicación de la LOPD. Ahora, el art. 2 LO 3/2018 contempla el ámbito de aplicación, con constantes remisiones al RGPD.

y *Marper v.* El Reino Unido, que más adelante comentaremos. Así mismo, la OCDE habla de la que denomina "*Function creep*"[149] es un término que explica la expansión o extensión de un proceso a otras finalidades distintas a aquellas para las que fueron recogidos inicialmente los datos o aplicado el sistema.

3. Descripción de los sistemas biométricos.

El dato biométrico es un dato de naturaleza especial que tiene que ver con las características comportamentales y fisiológicas de una persona. El dato biométrico, en general, y el dactiloscópico particularmente puede permitir la identificación inequívoca de personas. Sobre la huella dactilar ya se ha pronunciado el Tribunal Supremo en numerosas sentencias estableciendo respecto a su valor probatorio que cosntituye una prueba plena en lo referente a la acreditación de la presencia de una persona determinada en un lugar concreto, aquél donde la huella se ha encontrado, esto si atendemos a un objeto fijo. Pero también la huella permite esclarecer, con seguridad prácticamente absoluta, que las manos de un individuo han estado en contacto con la superficie en la que aparecen impresas las huellas en objetos muebles móviles[150]. Como veremos, las aplicaciones biométricas tienen fines de autenticación y de identificación. La autenticación en definitiva es una comprobación de que la persona es quien dice ser. Los sistemas de autenticación toman decisiones lógicas Si/No. Por el contrario, en un

[149] "*(also known as "purpose creep)" is the term used to describe the expansion of a process or system, where data collected for one specific purpose is subsequently used for another unintended or unauthorised purpose. In privacy principle terms, we may think of function creep as a violation of the "finality" principles; the subsequent use, retention or disclosure of data without the consent of the individual and inconsistent with the purpose specification given at the time of data collection."* Organisation for Economic Co-operation and Development. Directorate for Science, Technology and Industry. Committee for Information, Computer and Communications Policy. Working Party on Information Security and Privacy. Biometric-based technologies. DSTI/ICCP/REG(2003)2/FINAL Unclassified. 30 de junio de 2004. Disponible en https://doi.org/10.1787/232075642747 [Fecha de consulta: 08/08/2016], p. 12.

[150] (STS 4345/2014 ó 4113/2013). En el mismo sentido la STS, Sala 2ª, S 2-2-2013, nº 60/2013, rec. 10729/2012 (EDJ 2013/11812) que en su Fundamento de Derecho Primero dice: "[…] En efecto es cierto que la doctrina de esta Sala ha estimado desde siempre, como suficiente los dictámenes dactiloscópicos para enervar la presunción de inocencia (SSTS. 1.2.95, 435/98 de 20.3 EDJ 1998/1298)". Y añade en su Fundamento de Derecho tercero: "[…] Pues bien, con respecto al valor probatorio de las huellas dactilares, esta Sala STS. 468/2992 de 15.3 EDJ 2002/4282 , 169/2011 de 18.3 EDJ 2011/19668 - considera que constituye un indicio especialmente significativo, es decir, de una "singular potencia acreditativa", y reiteradamente se ha admitido por esta Sala, la efectividad de esta prueba para desvirtuar la presunción constitucional de inocencia (SS. de 17 de marzo EDJ 1999/5863 o 30 de junio de 1999 EDJ 1999/14371 y las de 22 de marzo EDJ 2000/3599 , 27 de abril EDJ 2000/10370 o 19 de junio de 2000 EDJ 2000/14673), en cuanto constituye una prueba plena en lo que respecta a la acreditación de la presencia de una persona determinada en el lugar en el que la huella se encuentra -si éste es un objeto fijo- o permite esclarecer, con seguridad prácticamente absoluta, que sus manos han estado en contacto con la superficie en la que aparecen impresas -en el caso de objetos muebles móviles-"

sistema de identificación se produce un reconocimiento de la persona y distinción del resto de personas. Para ello, al tratarse de una tarea más compleja puesto que el sistema debe tomar una decisión entre muchas, es necesario el acceso a bases de datos centrales. Indudablemente la existencia y el acceso a estas bases de datos centrales plantea no pocas cuestiones con una dimensión jurídica relevante entre otras la seguridad en el acceso, tratamiento y almacenamiento de la información a la que aludiremos en la tercera parte de este estudio al comentar algunos de los sistemas de estas características en uso.

3.1. La tecnología biométrica en su doble funcionalidad.

La tecnología biométrica en su doble funcionalidad se presenta como un medio de autenticación/comprobación de personas, o bien, como un medio de identificación de individuos. La biometría y la tecnología biométrica, en particular, permite reconocer seres humanos en entornos digitales de forma similar a como habitualmente nos reconocemos unos a otros en la vida cotidiana, por la apariencia física, la voz, la forma de andar o de comportarnos. Como veremos a continuación, la tecnología biométrica ofrece un medio de reconocimiento de individuos en un entorno digital a partir de la base física de cada uno que difiere de la de los demás.

3.2. Recogida del dato biométrico. Fase de inscripción o registro.

Como ya hemos apuntado anteriormente los sistemas biométricos permiten tanto la autenticación como la identificación de las personas. Estos sistemas servirán a un fin de comprobación (autenticación) o a un fin de reconocimiento (identificación), dependiendo del proceso que se lleve a cabo con el elemento biométrico que, en concreto, se utilice. Las tecnologías biométricas consideran parámetros físicos del individuo que son diferentes en cada uno de nosotros. Por ejemplo, la geometría de la mano, la voz, la imagen de la cara o en concreto los surcos de la huella dactilar objeto de nuestro análisis. Estos parámetros o características únicas permiten conformar un patrón único, una plantilla, para cada individuo que se utilizará posteriormente en operaciones bien de comprobación, o bien, de reconocimiento. Llegados a este punto, resulta muy ilustrativa, para esta exposición, la aclaración de las fases, momentos o

procesos, propiamente dichos que cabe distinguir en un sistema de recopilación de las muestras biométricas para su posterior almacenamiento y tratamiento.

Tanto el documento de trabajo sobre biometría del GPD 29 (Dictamen 4/2007) como el informe de situación del T-PD (2005) distinguen dos momentos en el tratamiento de la información por estos sistemas: uno primero que es el momento de "registro" durante el cual se introduce el dato biométrico, el parámetro considerado, de una persona en el sistema que se denominaría "fase de inscripción" o momento de registro y otro segundo, posterior, que es cualquier recogida subsiguiente a efectos de "comparación". Por su parte, INTECO en su "Guía sobre las tecnologías biométricas aplicadas a la seguridad*"* distingue, en el mismo sentido, entre lo que denomina "proceso de registro" y "proceso de autenticación". El registro o proceso de incorporación al sistema es imprescindible, ya que con las características de identidad de cada individuo el sistema proporciona a éste unas credenciales para posteriores accesos, de ahí la denominación que la OCDE da a esta fase de *enrolment process*[151].

Haciendo especial referencia a la adquisición de huellas dactilares, este proceso es muy diferente dependiendo del tipo de aplicación biométrica en que se van a procesar las imágenes obtenidas. Ya se ha mencionado en los antecedentes históricos que el método tradicional de obtención, en el ámbito judicial y forense, es la impresión tintada de la huella dactilar o adquisición de huellas *off line*[152]. Pero actualmente los sistemas de reconocimiento automático, ampliamente utilizados, ofrecen una gran diversidad dependiendo del entorno y finalidad a la que se destina la recogida. Así, por ejemplo, en

[151] OCDE *Working Party on Information Security and Privacy. Biometric-based technologies*, op. cit.

[152] La adquisición de huellas *off line "…*se efectúa imprimiendo directamente la huella del dedo sobre papel. Para ello, se extienden unas gotas de tinta sobre una tableta plana. La piel queda impregnada al hacer rodar la yema del dedo sobre la superficie, de izquierda a derecha. A continuación, se hace rodar de nuevo el dedo sobre un papel blanco para que el patrón de crestas quede definitivamente impreso". Este procedimiento presenta algunos inconvenientes al quedar impresas deformaciones en la estructura de las crestas motivadas por el propio sistema de impresión. Este autor también indica que pueden recogerse las huellas sin hacer rodar el dedo con una sola impresión, en este caso la imagen obtenida es más pequeña, pero con menor grado de distorsión. Posteriormente, hay que digitalizar esta huella obtenida a través de un dispositivo de entrada de datos al sistema informático, por ejemplo, un escáner óptico o una cámara de video. En todo caso, este procedimiento de adquisición de huellas es poco eficiente por su lentitud, habilidad que requiere, en un sistema de reconocimiento automático de huella digital. Cfr. SIMÓN ZORITA, D., op. cit., p. 50.

sistemas de acceso a entornos de seguridad impera el uso de técnicas *on-line* a través de dispositivos de adquisición electrónicos[153].

3.2.1. Datos de características físicas -estáticos- y datos de comportamiento -dinámicos-.

Añade el GPD 29 que se pueden distinguir dos técnicas biométricas en función de si se utilizan datos estables o datos dinámicos sobre el comportamiento. Así, existen técnicas biométricas fisiológicas que se basan en datos estables, por ejemplo, las huellas dactilares[154], que son las que consideraremos en este estudio, y técnicas biométricas comportamentales que se basan en datos dinámicos, por ejemplo, las pulsaciones[155].

Por tanto, las técnicas biométricas fisiológicas miden características fisiológicas de una persona y las técnicas biométricas del comportamiento miden su comportamiento.

3.2.2. Datos brutos y plantillas. El *template*.

Debemos analizar si la plantilla biométrica reune las características para poder ser considerada como dato de carácter personal. En la primera fase, que hemos denominado de inscripción (registro), un sensor que será distinto, específico, para cada tipo de biometría, extrae los rasgos biométricos concretos de la persona para elaborar una

[153] Ibíd., p. 48. Este autor distingue en estos dispositivos de adquisición electrónicos tres partes: el sensor de lectura, que captura la imagen de la huella; el conversor analógico/digital que transforma la imagen analógica captada por el sensor en digital y la interfaz de comunicaciones con un equipo informático. Distingue este autor dependiendo del principio físico de funcionamiento del sensor entre ópticos, de estado sólido y ultrasónicos.

[154] La dactiloscopia entendida como estudio de las crestas papilares de las yemas de los dedos es una de las ramas en las que se subdivide la lofoscopia que designa el capítulo de la policía científica encargado del análisis de las huellas dejadas por una parte cualquiera de la epidermis y, en concreto, de las huellas caracterizadas por la presencia de crestas. Partiendo de estas precisiones previas las crestas papilares existentes en las caras de las extremidades de las personas tienen tres características fundamentales: son perennes, inmutables y diversiformes. DE ANTÓN Y BARBERÁ, F., op. cit., pp. 37 y ss.

[155] DEL PESO NAVARRO, E., RAMOS GONZÁLEZ, M.A., *Confidencialidad y seguridad…,* op. cit., p. 43. En 1994, al tratar el control de acceso a un sistema utilizando tarjetas inteligentes, donde se almacena información sobre el usuario incluso datos biométricos, plantean la posibilidad del análisis de estos que hemos denominado datos dinámicos como medio de neutralización de un riesgo de acceso forzado al sistema, así dicen: "En un plano meramente teórico, sólo quedaría por resolver la detección del caso del verdadero usuario que está actuando bajo amenaza, para que facilite un acceso o porque le están apuntando con un arma para que obtenga dinero de un cajero. Quizá podrían haberse registrado algunas de sus constantes vitales para detectar que las pulsaciones u otras características (nerviosismo, sudoración no justificada por la temperatura) responden a una situación anómala y denegar el acceso". Ya, en ese momento, los autores planteaban la posibilidad, hoy técnicamente posible, de combinar características biométricas estáticas y dinámicas del usuario en aras de una mayor seguridad.

plantilla biométrica (*template*)[156]; esta plantilla biométrica es una "reducción estructurada" de una imagen biométrica. En definitiva, la plantilla es resultado de un tratamiento. Se almacena esta plantilla en forma digitalizada y no el propio elemento o rasgo biométrico, el dato bruto[157], lo que también antes se ha denominado la imagen biométrica. Centrándonos en huellas dactilares se obtiene y almacena el patrón o plantilla de la huella dactilar de cada individuo. Llegados a este punto conviene hacer referencia brevemente a las características de la imagen biométrica. Al colocar la yema del dedo sobre una superficie sensible, como es un escáner, se obtiene la imagen de la huella dactilar que reproduce el patrón o estructura de las crestas y valles de la epidermis, afirma Simón Zorita; las imágenes digitales proporcionadas por el escáner, añade el autor, presentan cuatro características, de cuya combinación se deriva una imagen de mayor o menor calidad y fiabilidad, que son: la resolución, el área de captura, el número de *píxeles* y el rango dinámico[158]. Alonso-Fernández (*et al*),[159] amplían los factores que determinan la calidad de la imagen de la huella y, por ende, el rendimiento y función de un sistema de reconocimiento de huella dactilar. Para estos autores hay varios factores determinantes de la calidad de la imagen de la huella: las condiciones en las que se encuentre la piel (húmeda, seca, sucia, con cortes o

[156] La guía de INTECO habla de "patrón único". Dependiendo de los parámetros que en cada caso se traten, bien sea la imagen de la cara, la huella dactilar o la voz, etc. se extrae un patrón único para cada individuo que se utilizará en las fases posteriores para establecer comparaciones. INTECO, Instituto Nacional de Tecnologías de la Comunicación, op. cit., p. 8.

[157] En relación con el concepto de dato bruto e información resulta muy esclarecedora la exposición del Del Peso Navarro y Ramos González. Estos autores distinguen entre el concepto de información y el de dato. La información es el resultado de haber sometido los datos a algún proceso, automatizado o no, que les proporciona una utilidad, una plusvalía, que puede ayudar a conocer una situación o ayudar a la toma de decisiones. El dato como tal es un dato en bruto, sin elaborar, que solo sería aprovechable por quien sea experto. DEL PESO NAVARRO, E., RAMOS GONZÁLEZ, M.A., *La Seguridad de los Datos de Carácter Personal*, Madrid, Díaz de Santos, 2002, p. 3.

[158] La primea característica, la resolución, varía dependiendo del tipo de dispositivo de captura que se emplee. Una resolución media de dispositivos que se encuentran en el mercado es de 500 dpi que permite la extracción de los puntos característicos (minucias) de la estructura de crestas de la huella dactilar. La segunda característica del área de captura se refiere al tamaño de la superficie del escáner. Cuanto mayor es el área de captura mayor es el número de características de la huella que pueden obtenerse. El área de captura más pequeña que permite obtener un número de características suficiente es de 0,5 pulgadas ó 1,6 cm^2. Por su parte, la característica del número de *píxeles* teniendo en cuenta la resolución *R* en dpi y el área de captura *A* x *B* (alto x ancho) en pulgadas el número de *píxeles* sería *R.A* x *R.B píxeles*. Por último, el rango dinámico se refiere al número de *bits* utilizados para codificar la luminancia de cada *píxel*. SIMÓN ZORITA, D., op. cit., p. 49.

[159] Para estos autores los métodos para la obtención computerizada de una imagen de calidad de la huella dactilar son tres: los basados en características locales, los basados en características globales y los basados en clasificadores. ALONSO-FERNÁNDEZ, F., (*et al*), "*A review of schemes for fingerprint image quality computation"* en *Biometrics on the Internet.* Proceedings of Third COST 275 Workshop. University of Hertfordshire, United Kingdom 27 and 28 October 2005. Luxembourg: Office for Official Publications of the European Communities, 2006, p. 3.

quemaduras), las condiciones del sensor (suciedad, ruido, tamaño) y la cooperación o actuación del propio usuario del sistema.

Por tanto, y en materia de protección de datos, hay que distinguir entre plantilla y datos brutos porque el régimen jurídico aplicable a uno y otros es distinto; no en vano, el documento de trabajo sobre biometría del GPD 29 (Dictamen 4/2007) pone claramente de manifiesto esta diferencia y se centra en el análisis jurídico de sistemas biométricos basados en plantillas, es decir, en datos estructurados.

Como ya hemos expuesto anteriormente, la plantilla es, pues, información y conforme con lo que establecía el artículo 2 de la Directiva 95/46/CE, cabe considerarla dato de carácter personal. El citado artículo 2 establecía:

> «Artículo 2. Definiciones. A efectos de la presente Directiva, se entenderá por: a) "datos personales": toda información sobre una persona física identificada o identificable ("el interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;»

En el mismo sentido, el RGPD de forma expresa menciona, en la definicición de "datos personales": "un identificador", "un número de identificación" o "uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona". Esta definición puede encajar con el concepto de plantilla que en definitiva no es sino la medida biométrica registrada de una persona[160] que habrá que analizar si cabe considerar dato personal.

Es evidente que el rasgo biométrico permanece en la persona y solo cuando el sistema lo extrae para elaborar la plantilla hay tratamiento[161], porque hay estructura y registro y

[160] Documento del Grupo de Trabajo del artículo 29, WP 80, 12168/02/ES, op. cit., p. 4.
[161] No olvidemos que el tratamiento es el elemento determinante en la aplicabilidad del régimen jurídico de la protección de datos. Así, y en el ámbito de aplicación de la Directiva 95/46/CE, se establecía en su

posibilidad de almacenamiento. Pero, no obstante, la aplicabilidad del régimen de protección de datos a la plantilla biométrica será posible si se puede predicar de ésta el carácter de dato personal.

De la distinción entre imagen biométrica (datos brutos) y plantilla se deriva un distinto régimen jurídico aplicable y de la distinción entre fase de registro y fase de comparación también se derivan diversas cuestiones a analizar, como, por ejemplo, la fiabilidad de los sistemas biométricos como sistemas de identificación ya que un sistema biométrico se basa en probabilidades de orden estadístico, de concordancia o coincidencia de las plantillas almacenadas o registradas en el sistema con la recogida subsiguiente de datos biométricos.

3.2.3. Sistemas de identificación y de verificación.

Las dos funciones que puede desarrollar la recogida y tratamiento de datos biométricos dactiloscópicos y la biometría en general son la verificación y la identificación. La verificación sustancialmente consiste en comparar una muestra biométrica concreta, una huella dactilar concreta, con los datos biométricos registrados previamente y que pertenecen a una única persona. Como resultado del proceso de comparación entre la muestra captada, la huella captada, y la almacenada se puede producir, o bien, una aceptación, o bien, un rechazo de aquélla. En el caso de la identificación, el proceso no se limita a comparar unos datos con otros almacenados pertenecientes a una misma persona, sino que el proceso se amplía a la comparación con los datos biométricos dactiloscópicos de otras personas contenidos en una base de datos. Es decir, se produce un proceso de búsqueda para lograr una concordancia entre la muestra, la huella, presentada y los datos registrados previamente de un conjunto de personas. Por tanto, la función de verificación y la de identificación tienen diferencias esenciales y la elección de una u otra dependerá en gran medida de la finalidad para la que se recogen los datos, ya que, si con un sistema de autenticación es suficiente, adecuado y proporcional para alcanzar la finalidad legítima del tratamiento, entonces no debe utilizarse un sistema de

---

artículo 3: "Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

identificación. Así, por ejemplo, para atender a la finalidad de expedición de un pasaporte a una persona es necesario implantar un sistema de identificación[162], sin embargo, para el control de acceso a un puesto de trabajo es suficiente un sistema de autenticación (verificación). Podemos encontrarnos, entonces, con dos posibles objetivos: la identificación o la comprobación. Para Cavoukian y Stoianov "la identificación hace referencia a la capacidad de un sistema informático de distinguir de forma única a un individuo entre un grupo más amplio de expedientes biométricos individuales en archivo (usando solo los datos biométricos)"[163]. Esta función de identificación permitiría sostener un sistema nacional de identificación biométrica, que en parte actualmente existe con la identificación dactiloscópica en el DNI. Un sistema de identificación biométrica más amplio, con la incorporación al mismo de más datos biométricos, "[…] permitiría a un ciudadano probar quién es sin recurrir a documento alguno, dando por hecho que dicho ciudadano ya estuviese inscrito en el sistema"[164]. El funcionamiento del sistema sería aparentemente sencillo. Se debería producir una lectura del dato biométrico a través del sistema de recogida adecuado o de la combinación de más de un sistema (lectura de huella dactilar y fondo de ojo). Los datos recogidos "se compararían con el resto de entradas en la base de datos nacional para un cotejo, y tras una coincidencia correcta, los datos de identidad asociados a dicho ciudadano serían entregados por la base de datos"[165]. Esta correspondencia se denomina por la doctrina de "uno a varios" ("*one to many")*. Este es el sistema que sigue la policía en la identificación de delincuentes, y también es el sistema de identificación público, en otros ámbitos, como el acceso a ayudas públicas, permisos de circulación, etc… El otro sistema que hemos denominado de verificación se conoce como búsqueda "uno a uno" ("*one-to-one*"). "La correspondencia de la biometría viva con la muestra es lo único necesario para autenticar al individuo como un usuario apto"[166]. La verificación o autenticación parten de la lectura "en vivo" de la huella dactilar del individuo y su

[162] En la expedición de un pasaporte es necesario comprobar que el solicitante no ha presentado previamente otra solicitud bajo otro nombre o coincide con la identidad de otro documento ya expedido. Sin embargo, una vez expedido el pasaporte basta con un sistema de verificación para comprobar que la persona que porta el documento coincide con aquella a cuyo favor se expidió. Cfr. *Informe de situación relativo a la aplicación de los principios de la Convención 108 a la recogida y al proceso de los datos biométricos,* op. cit.

[163] CAVOUKIAN, A., STOIANOV, A., "Guía de cifrado biométrico. Comisionado de Protección de Datos de Notario (Canadá)", *Revista Española de Protección de Datos. 2,* enero-junio, 2007, Madrid, Civitas, 2007, p. 313.

[164] Ibíd.

[165] Ibíd.

[166] Ibíd., p. 314.

correspondencia, coincidencia, con la huella de ese individuo almacenada en la memoria del sistema.

3.3. **Fase de almacenamiento**.

El uso del dato biométrico dactiloscópico en el sistema presenta, en la fase de almacenamiento, varias alternativas. Por una parte, se puede almacenar la imagen completa de una característica biométrica, de la huella, o bien un extracto en forma de patrón. Por otra parte, en lo que al soporte se refiere, los datos registrados, ya sean imágenes o patrones, se pueden conservar en un soporte de almacenamiento individual una tarjeta, o bien, otra estructura del sistema puede consistir en almacenar los datos registrados en una base de datos local o regional. La elección de una u otra estructura tiene efectos jurídicos diversos.

3.3.1. Soporte de almacenamiento individual. Tarjeta *chip*.

La elección de un almacenamiento individual o un almacenamiento masivo tiene consecuencias en dos ámbitos fundamentales: la accesibilidad a los datos y la diseminación de éstos. La estructura de un sistema biométrico dactiloscópico puede ser diseñada de forma que el dato se almacene únicamente en una tarjeta dotada de algún sistema de seguridad, es decir, una tarjeta con *chip*. Si únicamente se utiliza el sistema biométrico con fines de verificación el almacenamiento de los datos de huella en una tarjeta resulta adecuado. Sin embargo, si el sistema debe cubrir necesidades de identificación, la tarjeta individual no se muestra como el sistema más pertinente. Dentro de este soporte de almacenamiento cabe establecer una distinción entre la tarjeta tradicional de lectura con contacto en la que el titular de la tarjeta mantiene un control total sobre la misma, ya que la tarjeta a modo de una llave es utilizada cuando la persona que la tiene la necesita. Pero también hay que contemplar sistemas de tarjeta de lectura sin contacto, tarjetas RFID (*Radio Frequency Identification).* Con este sistema la persona afectada pierde el control exclusivo de la lectura de sus datos dactiloscópicos. Si atendemos a la legislación sobre protección de datos, estos sistemas deberían incluir un medio de aviso al titular de que sus datos se han leído evitando una lectura secreta de

datos. Y, en todo caso, esta lectura ciega o secreta, si se produjera, debería estar habilitada por unos supuestos legalmente previstos.

3.3.2. Almacenamiento en base de datos local o regional.

La otra estructura del sistema de almacenamiento de datos biométricos dactiloscópicos es el registro de éstos en bases de datos locales o regionales. En estos casos, podemos considerar sistemas de tratamiento públicos en los que estas bases se encuentren bajo el control de autoridades policiales, como así ocurre en el sistema para la expedición de pasaporte, donde es necesario identificar a los individuos para evitar conflictos de doble identidad atribuida a una misma persona. Pero también en el ámbito privado cabría plantear la existencia de estas bases de datos, siempre que sea necesario proceder a la identificación de personas y no a la simple verificación, ya que si es esta última la finalidad que debe cubrir el sistema en atención al principio de proporcionalidad, no cabría implantar un sistema más amplio y complejo como el de identificación de personas. En relación con la creación de una base de datos de huellas de clientes con fines específicos comerciales, hacemos mención aquí al Informe 0082/2010[167] de la AEPD que resuelve la cuestión planteada en relación con la citada creación atendiendo al principio de proporcionalidad. La Agencia comienza estudiando la aplicabilidad de la LOPD a la base de datos que se pretende crear, concluyendo que es de aplicación ya que dicha base de datos es un fichero sometido a la Ley "[…] dado que el código alfanumérico obtenido a través de la huella dactilar identifica sin ningún tipo de esfuerzos a los clientes"[168]. Ahora bien, teniendo en cuenta que estamos dentro del ámbito del derecho de protección de datos personales ha de evaluarse la proporcionalidad de la creación de la citada base de datos. Así el tratamiento del dato de huella dactilar debe ser proporcionado a la finalidad que lo motiva. Para el Tribunal Constitucional el juicio de proporcionalidad, respecto de medidas restrictivas de derechos fundamentales, encierra en sí a su vez tres requisitos o condiciones: juicio de idoneidad, juicio de necesidad y juicio de proporcionalidad, en sentido estricto. Es decir, que si la finalidad que se persigue con la creación de la base de datos "[…] pudiera ser conseguida por la realización de una actividad distinta al citado tratamiento,

[167] Agencia Española de Protección de Datos. Gabinete Jurídico. *Informe0082/2010*. https://www.aepd.es/informes/historicos/2010-0082.pdf [Fecha de consulta: 20/11/2018].
[168] Ibíd., p. 1.

sin que dicha finalidad sea alterada o perjudicada, debería optarse por esa última actividad, dado que el tratamiento de los datos de carácter personal supone, tal y como consagra nuestro Tribunal Constitucional, en Sentencia 292/2000, de 30 de noviembre, una limitación del derecho de la persona a disponer de la información referida a la misma"[169]. La Agencia acaba concluyendo que la misma finalidad, prestar un servicio comercial al cliente, puede alcanzarse con otro tipo de medidas menos intrusitas en su privacidad, como por ejemplo simples tarjetas de fidelización. Por ende, la creación de la base de datos de huellas dactilares con fines comerciales es desproporcionada y no acomodada a la Ley.

3.4. Tratamiento del dato biométrico. Fase de comparación.

Dependiendo si la finalidad del tratamiento del dato biométrico es la identificación de una persona o, simplemente, la autenticación el método de comparación varía. Así, como ya hemos expuesto, para identificar a una persona por biometría es necesario acceder a una base de datos central. Para reconocer al individuo hay que distinguirlo del resto cuyos datos están almacenados en dicha base de datos. Sin embargo, una autenticación en el sentido de comprobación puede hacerse a través de un sistema descentralizado.

Por tanto, en esta fase, que se viene en denominar de comparación, la problemática jurídica varía sustancialmente dependiendo de si es necesario el acceso a una base de datos o si este acceso no es necesario porque, por ejemplo, la comprobación de la identidad es una simple autenticación de una persona y se resuelve a través de un sistema descentralizado.

3.5. El dato dactiloscópico como dato de carácter personal.

No podemos perder de vista que el derecho fundamental de la protección de datos, distinto del derecho a la intimidad, ha sido reconocido como tal derecho independiente en La Carta Europea del año 2000 en su artículo 8. En este artículo este derecho

[169] Ibíd., p. 3.

fundamental se configura como el poder de las personas físicas de disposición sobre los propios datos, sean éstos íntimos o no, que hayan sido sometidos a tratamiento.

Por tanto, es fundamental para determinar la aplicación del derecho fundamental a la protección de datos determinar si la plantilla biométrica dactiloscópica se refiere a una persona, y si ha sido sometida a tratamiento. Ya sabemos que la plantilla biométrica dactiloscópica es una reducción estructurada de una imagen biométrica de una característica física de una persona. En definitiva, la plantilla es la medida biométrica registrada de un individuo. Por tanto, el rasgo biométrico permanece en la persona y solo cuando el sistema lo extrae, para elaborar la plantilla, hay tratamiento porque hay estructura y registro y posibilidad de almacenamiento. De acuerdo con lo expuesto el dato biométrico dactiloscópico será dato personal si, una vez extraído de la persona en su versión digital, en forma de plantilla, utilizando un conjunto de medios razonables, es posible atribuirlo a una persona identificada o identificable.

4. Referencia a sistemas de reconocimiento biométrico dactiloscópico.

En este punto se plantean, con independencia de que el sistema se base en la obtención y tratamiento de datos estáticos o dinámicos, una serie de cuestiones comunes a cualquiera de ambos sistemas: primero, determinar el conjunto de características que definirán el patrón biométrico de cada individuo; segundo, la obtención o extracción de dichas características y tercero, el reconocimiento de los patrones cuando, o bien, hay que identificar o, simplemente, autenticar a un individuo.

A continuación, sin carácter exhaustivo, se recogen algunas de las técnicas más comunes de reconocimiento de patrones biométricos.

4.1. Sistemas basados en datos estáticos de características físicas: la huella dactilar y la geometría de la oreja.

Abordamos, en este punto, algunas de las más comunes tecnologías biométrico-fisiológicas que presentan como rasgo diferenciador común la medición directa de alguna característica física del cuerpo de un individuo.

En lo que respecta a la huella dactilar, **y**a hemos destacado en la Introducción, en el punto referente a los antecedentes históricos de la biometría, cómo las huellas dactilares han sido un rasgo físico mensurable, único e inalterable utilizado desde antiguo por la humanidad para identificar a las personas. Este sistema precisa de una cierta cooperación por parte del individuo en el momento inicial de recogida de la huella. En este momento de la captura bien pueden utilizarse unos algoritmos de reconocimiento sencillos, si la huella presenta la suficiente calidad, o bien algoritmos complejos si las condiciones de captura y la calidad de la huella son menores.

Como ya se ha expuesto en el punto referente a la recogida del dato biométrico, la adquisición de huellas *on line* se realiza directamente al situar el dedo sobre el correspondiente sensor electrónico. Estos sensores, ya apuntábamos, se pueden clasificar en tres categorías: ópticos, de estado sólido y ultrasónicos. Esta triple clasificación atiende al principio físico que utiliza cada uno para transformar la huella capturada en imagen digital. Los sensores ópticos se basan, la mayoría, en la reflexión de la luz sobre la yema del dedo (FTIR *Frustrated Total Internal Reflexion*[170]). Estos sensores pueden estar basados en fibra óptica, combinar sistemas electro-ópticos, o bien, tratarse de sensores sin contacto.

Por su parte, los sensores de estado sólido conforman un grupo integrado por los sensores capacitivos, térmicos, de campo eléctrico y piezoeléctricos[171]. Por último, los sensores ultrasónicos analizan la superficie de contacto proyectando pulsos ultrasónicos

[170] El sistema de captura *FTIR* es uno de los más antiguos y a la vez más utilizados. El sistema se pone en funcionamiento al apoyar la yema del dedo sobre una superficie de cristal del sensor y se proyecta un haz de luz por debajo del cristal. La luz que incide sobre las crestas de la huella se dispersa reflejándose en múltiples direcciones y la que incide sobre los valles se refleja en una única dirección. A través de esta situación de reflexión múltiple (crestas) y reflexión única (valles) se obtiene la imagen de la huella dactilar. Cfr. SIMÓN ZORITA, D., op. cit., p. 52.

[171] Estos sensores de estado sólido no presentan ningún componente óptico y en función de la forma en que se convierte la información física en señal eléctrica se distinguen cuatro tipos de sensores: capacitivos, térmicos, de campo eléctrico y piezoeléctricos. En los capacitivos el sensor va integrado en un único *chip* donde los componentes del sensor detectan mayor tensión eléctrica en las crestas que en los valles representando así los dos valores que conforman la estructura del dactilograma. En los sensores térmicos se crean diferentes corrientes eléctricas a partir de diferencias de temperatura ya que el sensor mantiene mayor temperatura que la del dedo. El contacto de crestas y valles sobre el sensor origina diferencias de temperatura, las diferencias originadas por las crestas son menores que las originadas por los valles formando así la imagen térmica de la huella. Los sensores de campo eléctrico son capaces de detectar cambios de amplitud de señal eléctrica en el contacto con las dermis. Finalmente, los sensores piezoeléctricos presentan una superficie sensible a la presión ejercida por el dedo convirtiendo las diferencias de presión en diferencias de tensión eléctrica. SIMÓN ZORITA, D., op. cit., pp. 52-53.

sobre la yema del dedo. La ventaja de estos sensores es su menor sensibilidad a la presencia de algunas alteraciones en la yema del dedo como suciedad, sudor, grasa, etc.

En cuanto a la geometría de la oreja, deseamos recordar la afirmación vertida en 1882 por Bertillón en el sentido de que "la oreja gracias a los múltiples valles y colinas es el factor más importante desde el punto de vista de la identificación"[172]. Aunque como dijimos el sistema antropométrico de identificación a través de medidas corporales fue abandonado al no ser totalmente fiable ha recobrado hoy interés con proyectos como FEARID (*Forensic Ear Identification*) dentro de la propia Unión Europea.

Por otra parte, los otogramas o huellas latentes de orejas dejadas en el lugar de comisión de un hecho delictivo, tienen una importancia destacada en la investigación forense y se han admitido como prueba de cargo en el proceso penal (véase Sentencia 19 de noviembre de 2001, ciudadano colombiano 31 años, Jaime Millán Ruiz, Juzgado de lo Penal nº 1 de Palencia por robo en vivienda).

4.2. Sistemas basados en datos dinámicos de comportamiento.

Aunque no constituyen el objeto central de este estudio, haremos una breve referencia a los datos dinámicos de comportamiento. Las tecnologías biométricas de comportamiento se caracterizan por considerar en el proceso de identificación características o rasgos derivados de una acción realizada por una persona. Al hablar de acción o comportamiento de un individuo estamos introduciendo la variable tiempo en el sistema ya que toda acción se desarrolla en un tiempo determinado. Todo comportamiento o acción, tiene un comienzo, un desarrollo y un final.

Dentro de los datos dinámicos de comportamiento, podemos destacar los siguientes:

- Reconocimiento de firma. Este sistema analiza la firma manuscrita para identificar al usuario firmante. Para identificar a las personas según su firma hay dos variantes: la comparación simple y la verificación dinámica; la simple es una comparación estática del grado de similitud entre dos firmas, la original y la que está siendo verificada. Sin embargo, en la verificación dinámica el análisis es de

[172] DE ANTÓN Y BARBERÁ, F., op. cit., p. 263.

la acción de firmar propiamente dicha. Así se hace un análisis de la forma, la velocidad, la presión del instrumento de escritura (pluma/bolígrafo) y la duración del proceso de firma. En la verificación dinámica no es significativa la forma o el aspecto final de la firma, sino que lo que se analiza es el proceso hasta llegar a ese aspecto final, se analiza cómo se firma no el resultado, la firma final.

- Reconocimiento de voz. Los sistemas de reconocimiento de voz usan redes neuronales para aprender a identificar voces. Los algoritmos deben medir y estimar la similitud para devolver un resultado o una lista de posibles identificaciones. Algunos autores consideran que la voz es un claro ejemplo de un tipo de datos biométricos que combinan características físicas, estáticas, y características de comportamiento[173].

- Reconocimiento de escritura de teclado**.** Estos sistemas se basan en la existencia de un patrón de escritura en teclado que es propio de cada persona. Se miden aspectos como la intensidad/fuerza en las pulsaciones, tiempo de pulsación sobre cada tecla, velocidad entre una pulsación y otra.

- Reconocimiento de la forma de andar. Estos sistemas toman como referencia la forma de caminar de una persona. Este proceso se graba y se somete a un análisis que genera una plantilla biométrica.

[173] Cfr. *Guía para gestionar los datos personales*. Alianza Formación Gestión. Edición en formato digital: julio 2015, Madrid, Álvaro López-Amo Editor, 2015. Disponible en www.alianzaformacion.com [Fecha de consulta: 28/03/2016.

SEGUNDA PARTE: La tecnología biométrica desde la perspectiva jurídica.

Capítulo II. El tratamiento del dato biométrico dactiloscópico y los Derechos Fundamentales.

1. Naturaleza jurídica del dato biométrico y la identidad fisiológica del individuo.

Seguidamente, analizaremos tanto el elemento material como inmaterial para aproximarnos a la naturaleza jurídica del dato biométrico.

1.1. El elemento material.

Ya hemos visto que los datos biométricos son, o bien, los rasgos biológicos o los rasgos del comportamiento de una persona. Así pues, existen dos categorías de datos biométricos: los datos biométricos biológicos con base en la anatomía del individuo, y los datos biométricos del comportamiento basados en acciones de la persona. Hemos restringido nuestro ámbito de estudio a la primera categoría y, dentro de ella, a su vez, a los datos biométricos biológicos obtenidos de la huella dactilar. En el anterior capítulo hemos expuesto brevemente la tecnología biométrica actualmente en uso, y es importante recordar, que independientemente de los parámetros o rasgos, biológicos o comportamentales, que se consideren (huellas, geometría de la mano, voz, imagen…) de ellos se extrae un patrón único, una plantilla susceptible de tratamiento digital, con las características del parámetro, pero que ya no son el parámetro mismo. Se produce una transformación del dato biométrico biológico en un código numérico que hace identificable a la persona. Por tanto, aunque en una primera aproximación y en paralelismo con el dato genético[174] cupiera distinguir dos vertientes o facetas en el dato

[174] Siguiendo con la hipótesis de un paralelismo entre propiedades biológicas de un individuo (dato biométrico) y el genoma humano de una persona (dato genético), en opinión de Nicolás Jiménez, el genoma de un individuo abarca dos elementos: el material (la molécula de ADN) y el inmaterial, que es la información que portan los genes. Sobre el elemento material se plantean las cuestiones relacionadas con la disponibilidad sobre el propio cuerpo y en relación con el elemento inmaterial, que ya sí cabe calificar de datos, se derivan los derechos de la personalidad. Aquí radica la distinción que en la naturaleza jurídica cabe establecer entre elemento material y dato. Entre material genético o biológico y dato genético o dato biométrico. La base material, sea el genoma o las propiedades biológicas de una persona, tienen una naturaleza jurídica distinta a la información que ese material contiene. En todo caso hay que salvar las distancias entre el dato genético y el dato biométrico dactiloscópico, ya que, en éste, no hay separación de la base fisiológica del individuo, el dactilograma, como sí ocurre en aquél. Cfr. NICOLÁS JIMÉNEZ, P., *La protección jurídica…*, op. cit., pp. 53 y ss.

biométrico, por una parte un elemento material, las propiedades o parámetros biológicos del individuo que son atribuibles a una sola persona y medibles, mensurables, y por otra parte el elemento inmaterial que es la información que sobre la persona contiene el elemento material, información a la que cabría llamar propiamente dato biométrico, entendemos que no es así, ya que en el dato biométrico es únicamente esta segunda vertiente inmaterial la que es objeto de tratamiento.

Para analizar esta cuestión, resulta de gran utilidad la aportación de Christian Byk[175] que entiende que, mientras el gen está dentro de la persona, es parte de la persona. Así cabría hablar en el mismo sentido de las propiedades biológicas, las características fisiológicas, los rasgos de la personalidad o incluso tics de un individuo que mientras permanecen en él son parte de su persona, son él mismo. Pero si se extrae el gen, si se extrae la propiedad biológica, de la persona se convierte en una *res* con una doble vertiente (el elemento material e inmaterial antes mencionado) con distintas naturalezas jurídicas. Del elemento material cabría predicar su indisponibilidad, *res communis*, y sobre el elemento inmaterial, como bien de la personalidad, cabría predicar derechos de la personalidad. Pero, ciertamente, en el ámbito de las tecnologías biométricas las propiedades biológicas, las características fisiológicas o de comportamiento de los individuos no se extraen, siguen en el individuo y lo único que se extrae es un patrón único creándose una plantilla, un código numérico, que no reúne las características de elemento material como *res communis* ya aludidas. No cabe, por tanto, plantear un régimen jurídico específico para las propiedades biológicas de las que se obtiene el dato biométrico dactiloscópico, sino que es la información obtenida la que sí tiene ese régimen jurídico independiente, como se verá en el siguiente epígrafe.

El GPD 29 también repara en esta cuestión al afirmar que: "las muestras de tejido humano (al igual que las muestras de sangre) son fuentes a partir de las cuales se extraen datos biométricos, pero no son en sí mismas datos biométricos (como, por ejemplo, un modelo de huellas dactilares es un dato biométrico, pero no así un dedo)"[176]. De todas formas, la obtención de datos biométricos dactiloscópicos no se hace separando el tejido del cuerpo sino leyéndolo y creando el código numérico ya

[175] Cfr. BYK, C., *La patente de genes humanos. El Derecho ante el Proyecto Genoma Humano*, vol. II, Bilbao, Fundación BBV, 1994, pp. 141 y ss.
[176] Cfr. Dictamen 4/2007 sobre el concepto de datos personales Adoptado el 20 de junio 01248/07/ES WP 136 por el Grupo de Trabajo del artículo 29, p. 9.

aludido. Por tanto, el rasgo biológico del que se lee la huella no se separa de la persona no hay un elemento material propiamente dicho "separado" del individuo por ello no se plantean derechos como *res* o cosa perteneciente al cuerpo, pero separada de él, sino únicamente derechos sobre la lectura del propio cuerpo. En efecto, como veremos en este capítulo, la dignidad, la integridad, la intimidad, la propia imagen son derechos que despliegan su ámbito de protección sobre el cuerpo en su unicidad y que han de ser analizados en los procesos de lecturas biométricas dactiloscópicas. De lo expuesto deriva que es el elemento inmaterial, la información, lo verdaderamente relevante ya que el dato biométrico dactiloscópico tiene una naturaleza dual: por una parte, es "contenido" de la información sobre un individuo y, por otra, sirve para "vincular" esa información a una única persona, es decir, cumple función de identificador.

En definitiva, el GPD 29, en este dictamen, distingue entre el elemento material e inmaterial aludido. Y es solo respecto del elemento inmaterial respecto del que cabe predicar un derecho de la personalidad como es el derecho a la autodeterminación informativa. En este sentido, acaba afirmando el dictamen, la aplicabilidad de la Directiva 95/46/CE a la extracción de información de las muestras, es decir, al dato biométrico.

En función de la vía por la que se conocen los rasgos biológicos de un individuo, Pilar Nicolás[177] distingue tres tipos de rasgos: los morfológicos externos, los morfológicos internos y los rasgos celulares. En el caso de los datos dactiloscópicos obtenidos de la huella dactilar, los rasgos morfológicos de los que se extraen, son externos están a la vista. La estructura de surcos y valles de la yema del dedo está a la vista, el dactilograma de una persona se ve a simple vista y serviría por sí solo para identificar a dicha persona si retuviéramos en nuestra memoria esa estructura como retenemos su imagen facial, pero eso es imposible. Esta autora, con apoyo en la jurisprudencia, sostiene que los rasgos morfológicos internos no son íntimos y los externos, que la persona voluntariamente deja a la vista de todos, son objeto de protección del derecho fundamental a la propia imagen. En el caso de las huellas dactilares, expuestas siempre a la vista en todas las culturas y que no identifican a la persona directamente sino tras obtener su estructura y compararla, no pueden equiparase con la imagen facial y cabe

[177] NICOLÁS JIMÉNEZ, P., *La protección jurídica…,* op. cit., p. 58.

considerarlas fuera de la intimidad corporal e incluso personal del individuo. Otra cosa muy distinta es la información ya convertida en código numérico que al servir de identidad fisiológica es susceptible de protección no solo por los derechos subjetivos sino también por la vía de los derechos fundamentales.

1.2. El elemento inmaterial.

Al referirnos al elemento inmaterial nos adentramos en la información contenida en los rasgos biológicos del individuo, en su identidad fisiológica. Sobre los datos biométricos dactiloscópicos no se ejercen derechos de propiedad porque, como ya hemos apuntado, no hay un elemento, una *res*, una cosa separada del cuerpo. Lo que cabe apreciar es la existencia de derechos subjetivos sobre un bien de la persona, no sobre la persona misma, sino sobre sus atributos. Esta referencia a los derechos subjetivos lo hacemos en el sentido dado a los mismos por Kelsen que, a su vez, cita la tesis de Dernburg: "Derechos en sentido subjetivo existían históricamente desde mucho antes de que se formase un ordenamiento estatal consciente. Se fundaban en la personalidad del individuo y en el respeto que hacia su persona y sus bienes sabía conquistar y obtener. Sólo mediante la abstracción se debió obtener, lentamente, a partir de la contemplación de los derechos subjetivos existentes, el concepto de ordenamiento jurídico"[178]. Para Kelsen el reconocimiento de derechos subjetivos constituye "[…] una técnica especial, consistente en que el derecho atribuye a un determinado individuo la facultad de demandar cuando se incumple una obligación jurídica"[179]. Así el atributo de la identidad fisiológica, derivada de la huella dactilar, se perfila como un nuevo derecho de la personalidad. La información biométrica de la que cabe derivar la identidad fisiológica es un atributo de la personalidad sobre el que la persona debe ostentar un poder jurídico de control correlativo a un deber jurídico de respeto por los demás.

Hemos de detenernos en diferenciar los conceptos de bien / derecho de la personalidad, derechos humanos y derechos fundamentales. En esta tarea nos ayuda Escobar, al afirmar: "los derechos humanos son demandas de abstención o actuación, derivadas de

[178] KELSEN, *Reine Rechtslebre,* 2ª ed., 1960, p. 135, recogido en KELSEN, H., *Esencia y valor de la Democracia*, Barcelona, ediciones Guadarrama, Punto Omega. Sección: Historia social y política, Número 233, 1977, pp. 169 y 170.
[179] KELSEN, H. *Esencia y valor…,* op. cit, p. 170.

la dignidad de la persona y reconocidas como legítimas por la comunidad internacional, siendo por ello merecedoras de protección jurídica del Estado"[180].

2. La fase de recogida-captación del dato biométrico dactiloscópico y los Derechos Fundamentales.

Esta fase suscita notable interés por la indudable influencia que, sobre los derechos fundamentales, ejerce.

2.1. El registro o introducción del dato dactiloscópico en el sistema.

A lo largo de los distintos epígrafes de este capítulo nos plantearemos cómo la recogida-captación de muestras y datos biométricos dactiloscópicos de los individuos puede afectar a algunos, de lo que la doctrina civilista ha denominado, bienes o derechos de la personalidad o, en terminología constitucional, a sus derechos fundamentales. Identificar qué bienes o derechos fundamentales pueden verse afectados, y con qué alcance, será el objeto de este capítulo. La obtención de una huella dactilar, la extracción de un perfil de ADN o unas muestras celulares de un individuo pueden afectar a derechos de la personalidad como la dignidad o la integridad física. Ahora bien, por ejemplo, una vez obtenido e introducido el dato dactiloscópico del individuo en el sistema (automatizado obviamente), aunque no se haya visto comprometida su dignidad ni su integridad física ¿la persona pierde ya el poder de disposición sobre el dato obtenido de su cuerpo? O, por el contrario, cabe plantear un poder de control de la aquélla sobre ese dato. Pero no acaba aquí la utilización del dato obtenido del cuerpo del individuo. ¿Qué ocurre en momentos posteriores de recogida subsiguiente de datos? ¿Tiene la persona algún derecho de control sobre ese proceso ulterior? Veremos cómo en el análisis *iusfundamental*, desde el que abordaremos este estudio, el principio de proporcionalidad desempeña un papel equilibrador en el juicio sobre la licitud o ilicitud de la recogida y uso de datos biométricos, en general y dactiloscópicos, en particular.

[180] ESCOBAR, G., *Introducción a la teoría jurídica de los derechos humanos*, Madrid, Cicode-Trama, 2005, p. 17.

Como ya sabemos, y atendiendo al concepto jurídico positivo que ofrecía el artículo 3 c) de la LOPD, el tratamiento de datos abarca todas las "… operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias". Sin perjuicio de que el tratamiento siga abarcando dichas operaciones, la vigente LO 3/2018, en su artículo 8 nos recuerda. en relación con el tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos. que: "1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679". Con respecto al tratamiento fundado en el interés público el mismo artículo 8.2. establece: "2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma de rango de ley". Por ello, en un mismo capítulo, este capítulo II, se abordan dos fases: captación y recogidas subsiguientes (ambas consideradas tratamiento para la normativa sobre protección de datos, como hemos visto). En la primera, de "captación", junto al derecho a la protección de datos hay, o puede haber, otros derechos concernidos; pero es ya en la segunda fase, ante "recogidas subsiguientes de datos" y "comparación" con los previamente almacenados, donde la normativa de protección de datos se erige en único baluarte de defensa de la libertad y libre desarrollo de la personalidad y voluntad del individuo. No obstante, veremos cómo en la captación de datos la proporcionalidad entre la finalidad de la recogida y la amplitud de los datos recogidos ofrece un principio básico para poder juzgar la licitud o ilicitud de todo el tratamiento desde la captación en sí, hasta el tratamiento subsiguiente, y este principio básico de proporcionalidad nos lo proporciona la normativa sobre protección de datos. Por ello, es el derecho fundamental a la protección de datos, o el derecho a la

autodeterminación informativa, el que ilumina o esclarece los límites dentro de los cuales el tratamiento del dato dactiloscópico es admisible en Derecho. Dejamos para la segunda parte del capítulo el estudio más detallado del ámbito jurídico competente en el tratamiento de la información obtenida de la lectura del propio cuerpo humano, entendiendo *a priori* que este ámbito es el del aludido derecho fundamental a la protección de datos. No debemos olvidar, como ya expusimos en el capítulo I, que el supuesto de hecho que estamos contemplando es la recopilación de muestras biométricas llevada a cabo durante una fase llamada de "inscripción" utilizando un lector-sensor específico para cada tipo de biometría. Y es, a continuación, cuando el sistema biométrico extrae rasgos específicos del individuo, usuario del sistema, para elaborar así la "plantilla" biométrica que es la que se almacena, en forma digitalizada. El sistema biométrico, en definitiva, permite o bien la identificación automática o la autenticación/comprobación de una persona. Esta realidad es la que contemplamos ahora desde la perspectiva de los posibles derechos del individuo que puedan verse concernidos.

A la vista de lo expuesto, nos parece relevante referirnos brevemente al concepto de proporcionalidad que la STC 207/1996 recogió con claridad al afirmar que se trata de:

> "una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad[181]".

[181] Cfr. PIÑAR MAÑAS, J. L., "El derecho fundamental…", op. cit., p. 355. Introducción a la Instrucción 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. BOE núm. 296, de 12 de diciembre de 2006; corr. Err., BOE núm. 3, de 3 de enero de 2007. La introducción a esta Instrucción 1/2006, continúa afirmando que, en relación con el juicio de proporcionalidad, al que se ha hecho referencia, para determinar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad citado ha de analizarse la concurrencia o no de tres requisitos o condiciones: juicio de idoneidad, juicio de necesidad y juicio de proporcionalidad en sentido estricto. El juicio de idoneidad analiza si la medida restrictiva del derecho fundamental es susceptible de conseguir el objetivo propuesto. El juicio de necesidad, por su parte, estudia si además la medida es necesaria en el sentido de que no existe otra medida más moderada que permita alcanzar el mismo propósito con igual eficacia. Por último, el juicio de proporcionalidad en sentido estricto sopesa los beneficios o ventajas para el interés general y los perjuicios a otros bienes o valores en conflicto.

A lo largo de esta primera fase del capítulo será necesario delimitar los posibles derechos fundamentales implicados en la captación de datos biométricos dactiloscópicos. En principio planteamos el derecho al honor, a la intimidad personal, a la propia imagen y a la integridad física**,** como derechos a evaluar en la fase de captación de referencia**.**

La delimitación de la naturaleza y contenido de estos derechos permitirá conocer el alcance o, lo que es lo mismo, si se ven o no comprometidos en la recogida de la huella dactilar. Recogida, por otra parte, imprescindible para generar el dato dactiloscópico. No obstante, partimos de una dificultad previa que es la estrecha relación entre los derechos de libertad, dignidad e integridad física. Como acertadamente afirma Canosa Usera, no resulta especialmente difícil "inferir del principio general de libertad y de la dignidad de la persona un principio de protección de la integridad personal"[182]. Pueden plantearse problemas de delimitación entre libertad, dignidad e integridad, pero ésta es necesaria para el adecuado estudio de las implicaciones jurídicas del fenómeno tecnológico relacionado con la recogida automatizada del dato dactiloscópico. Es, en todo cas,o en esta fase en la que puede verse comprometido alguno de los derechos aludidos puesto que una vez pasada esta fase de lectura directa del cuerpo humano lo que se haga con lo leído, con la información obtenida, tiene otro ámbito regulatorio. Entendemos que esta fase de recogida, sin que sea ajena a la regulación sobre protección de datos personales -pues ya es tratamiento-, tiene, o puede tener, otros derechos concernidos que nos proponemos estudiar.

Analizaremos, entre otras cuestiones, si la identidad física y fisiológica, enunciada en el capítulo anterior, cabe considerarla como bien de la personalidad y si el derecho subjetivo al trasladarse al ámbito público, como ha ocurrido con la mayoría de los derechos de la personalidad, adquiere la condición de derecho fundamental[183].

[182] CANOSA USERA, R., *El Derecho a la Integridad personal,* Valladolid, Lex Nova, 2006, p. 21.

[183] Es muy probable que con esta afirmación caigamos en el error de pretender crear, sin tasa, multitud de derechos con la categoría de fundamentales cuando en el fondo pueden no ser mas que un deseo o una pretensión, o como dice el profesor Sánchez González "(…) necesidades que, por el ferviente deseo de que sean satisfechas, calificamos erróneamente de derechos fundamentales o de derechos humanos". SÁNCHEZ GONZÁLEZ, S., "Los derechos fundamentales en la Constitución Española de 1978*"* en *Dogmática y Práctica de los Derechos Fundamentales,* Valencia, Tirant lo blanch, 2006, p. 18.

Por otra parte, el análisis de los distintos derechos que pueden verse comprometidos o implicados en la captación, en general, de los datos biométricos puede servir como punto de partida para el análisis de la conveniencia, o no, de la inclusión de los datos biométricos dactiloscópicos como una categoría más de los denominados datos sensibles, o especialmente protegidos, que recoge la legislación sobre protección de datos. En este sentido, Murillo de la Cueva, aunque en relación con otro tipo de datos sensibles, los relativos a la salud, da una explicación al hecho de que el legislador los haya incluido en la categoría de datos especialmente protegidos, entendiendo que ello "se debe a que se sitúan en un plano en el que confluyen dos derechos fundamentales al menos: el derecho a la intimidad y el derecho a la autodeterminación informativa"[184]. No debemos olvidar que los datos sensibles se han utilizado a lo largo del tiempo en muchas ocasiones para la jerarquización de los individuos y, cómo no, para su discriminación posterior. No es un *iter* desconocido en la historia aquél que primero jerarquiza a las personas en función de su salud, su raza, su religión, su orientación sexual, etc…; y luego las discrimina. Entendemos que el dato biométrico dactiloscópico puede jerarquizar para luego discriminar. Por tanto, del estudio de los derechos individuales afectados puede derivarse una conclusión que aconseje, tanto de *lege ferenda* como *lege data,* la necesidad de un régimen específico de protección del dato biométrico.

2.2. Los derechos a la intimidad, a la propia imagen y a la integridad física en la recogida del dato biométrico dactiloscópico.

Partimos del análisis de los derechos reconocidos en el artículo 18.1 CE[185]: derecho al honor, a la intimidad y a la propia imagen.

Tal y como expone Fernández Esteban[186], estos derechos, reconocidos en el apartado 1 del artículo 18, vuelven a ser mencionados en el artículo 20.4 como límites a la

[184] LUCAS MURILLO DE LA CUEVA, P., "El derecho fundamental a la protección…, op. cit., p. 29.
[185] "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen". Este artículo 18 fue objeto en el Senado de una única enmienda presentada por Camilo José Cela que proponía el siguiente texto: "Se garantiza el derecho al honor y a la intimidad" para el firmante de esta enmienda no era preciso aclarar que la intimidad es personal y familiar porque intimidad significa "zona espiritual íntima de una persona o de un grupo, especialmente de una familia" y, además, la referencia a la propia imagen sobra ya que es un concepto impreciso englobado en el concepto de intimidad. Cfr. LÓPEZ DÍAZ, E., *El Derecho al honor y El Derecho a la Intimidad: Jurisprudencia y Doctrina*, Madrid, Dykinson, 1996, p. 26.

comunicación libre. De aquí deriva que la práctica totalidad de la doctrina y la jurisprudencia procedan al estudio del derecho al honor dentro del marco de la libertad de expresión cuando, como en el caso de la recogida y tratamiento de datos biométricos dactiloscópicos, el derecho al honor tiene virtualidad y debe desplegar su contenido en un ámbito independiente, e indudablemente más amplio, al exclusivo de la libertad de expresión.

Como ya hemos concluido en el capítulo I, los datos biométricos y, en particular, los dactiloscópicos son datos de carácter personal. Debemos poner de relieve que la base física de un dato dactiloscópico (los surcos y valles de la huella dactilar) no revelan, sin el concurso de un medio tecnológico, ningún dato relevante de un individuo y lo mismo ocurre con el iris o el fondo de ojo. Por tanto, la base física citada por sí sola en nada puede afectar a la dignidad de la persona o a sus derechos al honor, intimidad o propia imagen. Sin embargo, la imagen del rostro, dato biométrico indiscutible, por sí sola sí puede ser identificativa y, por ello, afectar a tales derechos.

Las bases físicas de los datos, aunque pueden tener un carácter público, en el sentido de que están a la vista de todos, porque no se puede ocultar la manera de andar, la voz, nuestro rostro (al menos en la cultura occidental), los dedos o la palma de nuestras manos, no por ello carecen de protección jurídica, ni quedan fuera del poder de disposición y de control de la persona. Si esto cabe predicar de la base física del dato biométrico, con más razón cabe afirmarlo de la información o del dato extraído. Así, y por lo expuesto, los datos biométricos y, en concreto, los dactiloscópicos desde el mismo momento de su captación quedan dentro del poder de disposición del individuo y están amparados por el derecho fundamental a la protección de datos personales; pero además en la fase inicial de captación hay algún otro derecho que ampara al individuo ¿Este posible que este amparo pueda provenir de derechos como el derecho al honor, a la intimidad y a la propia imagen? ¿Y la integridad física puede verse afectada? O si queremos plantear la cuestión a la inversa ¿Están concernidos estos derechos, es decir, cabe apreciar una limitación de los mismos en la recogida o lectura del dato biométrico del cuerpo humano?

[186] FERNÁNDEZ ESTEBAN, M. L., op. cit., pp. 115 y ss.

Si el amparo del artículo 18.1 CE puede ser sostenible respecto de elementos (partes del cuerpo) que, como hemos dicho, están a la vista, son públicos, aun es más evidente respecto partes íntimas o más reservadas del cuerpo. No obstante, en todo caso la base física del dato dactiloscópico entra dentro del grupo de elementos públicos puesto que no es tanto la parte del cuerpo de la que se capta el dato la que puede afectar al honor o la intimidad de una persona, que está claro que no, sino la información que se revela. Si la información revelada con el tratamiento de la muestra biométrica, es el padecimiento de una enfermedad, común o no, o una malformación física, esto sí puede afectar a los citados derechos. Con este planteamiento ¿podría verse comprometida la intimidad, o incluso el honor, de un individuo si al captarse la muestra de sus huellas digitales se revela el padecimiento de una enfermedad venérea?[187] Y, así mismo, cabría preguntarse si cualquier dato biométrico entraría dentro del carácter de dato público amparado por el artículo 18.4 CE o si alguno de esos datos afectarían, ya propiamente, a la intimidad y al honor protegidos por el artículo 18.1 CE. Para responder a ello, entendemos es necesario abordar la naturaleza y contenido de los derechos al honor, a la intimidad, a la propia imagen y a la integridad física.

En primer lugar, y como expone Sempere Rodríguez[188], cabe adoptar dos puntos de vista el constitucional y el civilista; es decir, una misma materia tiene un doble tratamiento público y privado. En concreto, en nuestro ordenamiento jurídico hasta la aprobación de la Constitución de 1978 el honor, la intimidad y la propia imagen eran básicamente derechos de la personalidad amparados por la vertiente privada del derecho y, como indica Herrero-Tejedor[189], por una progresiva interpretación y aplicación jurisprudencial de la responsabilidad extracontractual o aquiliana del artículo 1902 del Código Civil. Tras la promulgación del texto constitucional han pasado a tener simultáneamente una vertiente pública al gozar del carácter de derechos

[187] En este sentido, el GPD 29, en su documento sobre biometría, advierte de la correlación que cabe establecer entre ciertos dibujos papilares y determinadas enfermedades, es más, algunos de estos dibujos dependen de la alimentación de la madre que se transmite al feto, durante el tercer mes del embarazo. Hay estudios estadísticos que relacionan la leucemia y el cáncer de mama con determinados dibujos papilares. Este planteamiento de la cuestión afectaría igualmente a los datos obtenidos de la lectura de los dibujos papilares convirtiéndolos en datos especialmente protegidos. En contra de esta opinión, TRONCOSO REIGADA, A., *Comentario a la Ley Orgánica…,* op.cit. p. 221.

[188] SEMPERE RODRÍGUEZ, C., "Artículo 18 Derecho al honor, a la intimidad y a la propia imagen" en ALZAGA VILLAAMIL, O. (Dir.), *Comentarios a las leyes políticas. Constitución española de 1978.* Tomo II, Madrid, EDERSA, 1984, pp. 430 y ss.

[189] HERRERO-TEJEDOR, F., *Honor, intimidad y propia imagen*, Madrid, COLEX, 1994, p. 21.

fundamentales[190]. Este carácter de *ius* fundamental aporta seis características a estos derechos[191]: Primera, su exigibilidad frente a los poderes públicos y no sólo entre particulares. Segunda, su reconocimiento positivo con eficacia también entre particulares completando la única referencia que existía a estos bienes de la personalidad en el artículo 1902 del Código civil. Tercera, otorgamiento de mayor rango normativo puesto que un derecho declarado como fundamental, al considerarse fundamento del orden político y de la paz social, tiene normas específicas en relación a su modificación y goza de garantías privilegiadas en todos los órdenes. Cuarta, otorgamiento de mayor protección en una triple vertiente: ante los Tribunales ordinarios, frente al legislador y ante el Tribunal Constitucional. El artículo 53.2 CE establece un procedimiento sumario y preferente para la protección de estos derechos ante los Tribunales ordinarios. Frente al legislador el recurso y la cuestión de inconstitucionalidad protegen estos derechos. Y, por último, el recurso de amparo proporciona la vía de acceso ante el Tribunal Constitucional por violación de estos derechos. En el caso de vulneración de los derechos del artículo 18.1 CE, honor, intimidad y propia imagen, en la mayoría de los casos ésta va a provenir del ámbito

[190] Como antecedentes constitucionales de la protección de la intimidad recogida en el texto de la Constitución de 1978, las diferentes Constituciones de la historia reciente de España, aunque sea de un modo indirecto protegiendo la dignidad de la persona y el derecho al libre desarrollo de su personalidad, también han protegido el derecho a la intimidad. Así a través de la inviolabilidad de la propia persona, de su domicilio, de la correspondencia se han protegido diferentes aspectos de la intimidad. En concreto, protegiendo el domicilio, entendiendo éste como el lugar físico donde se desarrolla gran parte de la intimidad, se ha protegido indirectamente ésta. López Díaz, en un rápido repaso por la tradición constitucional española, nos hace ver que la inviolabilidad del domicilio está expresamente regulada en el artículo 306 de la Constitución de Cádiz de 1812, en las Constituciones de 1837 y 1845 en sus artículos 7 y la de 1856 en su artículo 8. Posteriormente en la Constitución Española de 1869 se regula de nuevo la inviolabilidad del domicilio y la correspondencia estableciendo que es competencia de la autoridad judicial, y no de la gubernativa, interceptar la correspondencia y, en todo caso, la apertura se llevará a cabo en presencia del procesado. La Constitución Federal de la República Española de 1873 recoge la protección de la correspondencia unida a la inviolabilidad del domicilio. La Constitución de 1876 en la misma línea de los textos anteriores establece en su artículo 6: Nadie podrá entrar en el domicilio de ningún español o extranjero residente en España sin su consentimiento excepto en los casos y en la forma expresamente previstos en las leyes. El registro de papeles se verificará siempre en presencia del interesado o de un individuo de su familia y en su defecto de dos testigos vecinos del mismo pueblo". El artículo 7: "No podrá detenerse ni abrirse por la autoridad gubernativa la correspondencia confiada al correo*"*. El posterior Anteproyecto de Constitución de la Monarquía Española de 1929 y la Constitución de la República Española de 1931 no introducen variaciones significativas. Por su parte el Fuero de los Españoles de 17 de julio de 1945 reconoce la inviolabilidad del domicilio, aunque limitada al domicilio "de un español", y los registros en aquél solo podrán llevarse a cabo con mandato de la autoridad competente. Y el Fuero reconoce expresamente por primera vez a lo largo de la tradición constitucional española el derecho al honor del siguiente modo: "Los españoles tienen derecho al respeto de su honor personal y familiar. Quien lo ultraje, cualquiera que fuese su condición incurrirá en responsabilidad*"*. Cfr. LÓPEZ DÍAZ, E., op.cit., pp. 21 y ss.

[191] Características reflejadas por HERRERO TEJEDOR, F., op. cit., pp. 22 y ss.

privado[192] no de los poderes públicos y, en el caso de violaciones entre privados, el recurso de amparo ante el Tribunal Constitucional requiere agotar la vía de los tribunales ordinarios. Quinta, destacado carácter público de estos derechos que se manifiesta en una triple vertiente: primero, en todos los derechos fundamentales concurre un manifiesto interés público; segundo, por ello es preceptiva la intervención del Ministerio Fiscal tanto en el recurso de amparo ante el Tribunal Constitucional como en el proceso previsto en el artículo 12.3 de la Ley 62/78 y, tercero y último, la vinculación que despliegan respecto a los poderes públicos que no solo han de respetarlos sino que de forma positiva deben "promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivos; remover los obstáculos que impidan o dificulten su plenitud …" (artículo 9.2 CE). Y como sexta, y última, característica, en materia de derechos fundamentales la formulación positiva de estos derechos, tanto en la legalidad ordinaria como en la constitucional, ha de ser interpretada en la forma más favorable a su efectividad[193]. Es conveniente puntualizar, como nos advierte Sánchez González[194], que los constituyentes españoles en el texto de 1978 siguieron la corriente imperante en esos momentos, y posteriormente, de enunciación extensa de derechos fundamentales. Así en el Título I, "los derechos fundamentales", se recogen tanto bienes de la personalidad, como manifestaciones de la libertad autonomía – *status negativus libertatis* -, de la libertad participación – *status positivus libertatis* - y de necesidades sociales – *status debitoris* - en general. Partamos, por tanto, del origen civil de estos derechos fundamentales, los derechos de la personalidad.

2.2.1. Aproximación a su naturaleza jurídica.

El derecho fundamental a la protección de datos, los bienes de la personalidad y la dignidad personal tienen una conexión que merece su estudio. En este sentido, la STC 170/1987, de 30 de octubre, en su FJ 4[195], concluyó que:

[192] Esta situación se denomina por la doctrina alemana *Drittwirkung* o lesión de derechos fundamentales por actos de particulares. HERRERO-TEJEDOR, F., op.cit., p. 331.
[193] STC 34/83, de 6 de mayo, y posteriores. En este mismo sentido la STC 159/86, de 12 de diciembre, refiriéndose a la interpretación de las limitaciones a un derecho fundamental establece que las que quepa imponer a las personas en el ejercicio de sus derechos fundamentales han de ser nada mas que las que exija el bien común y el respeto a los derechos de los demás, tal y como así lo recoge el artículo 10.1 CE.
[194] SÁNCHEZ GONZÁLEZ, S., op. cit., p. 20.
[195] Tribunal Constitucional, Sala 2ª, S 30-10-1987, nº 170/1987, BOE 279/1987, de 21 de noviembre de 1987, rec. 383/1986. EDJ 1987/170 Sala 2ª de 30 de octubre de 1987. Lefebvre El Derecho.

"Los derechos a la intimidad personal y a la propia imagen, garantizados por el art. 18.1 CE, forman parte de los bienes de la personalidad que pertenecen al ámbito de la vida privada. Salvaguardan estos derechos un espacio de intimidad personal y familiar que queda sustraído a intromisiones extrañas. Y en este ámbito de la intimidad, reviste singular importancia la necesaria protección del derecho a la propia imagen frente al creciente desarrollo de los medios y procedimientos de captación, divulgación y difusión de la misma y de datos y circunstancias pertenecientes a la intimidad que garantiza este precepto".

2.2.1.1. El papel de la dignidad personal.

Consideramos imprescindible, en el arranque del análisis de los derechos de la personalidad y de los derechos fundamentales, tomar en consideración la dignidad humana como elemento vertebrador de todo el sistema. Es innegable, desde una perspectiva histórica, el papel de la dignidad humana en la aparición de los Derechos Humanos en el escenario mundial. Como bien pone de relieve Vidal, para analizar desde un punto de vista ético-jurídico el significado y el contenido de los derechos fundamentales del hombre, es necesario recordar su trayectoria histórica. Así, sigue diciendo este autor, "la toma de conciencia de los derechos fundamentales del hombre puede ser constatada de dos modos: anotando el reconocimiento progresivo de las exigencias o <<libertades sociales>> de la dignidad humana, y recordando las declaraciones, más o menos vinculantes, de los <<derechos>> del hombre"[196]. Por tanto, el acercamiento a los que cabe considerar derechos inherentes a la persona exige tomar en consideración la dignidad del hombre como piedra clave de esos derechos.

En este análisis histórico, y siguiendo a Vidal, cabe afirmar que en la toma de conciencia por la humanidad de la existencia de "libertades sociales" dimanantes de la dignidad humana, radica el origen de lo que posteriormente hemos denominado derechos humanos. Es innegable que, en el mundo antiguo, Grecia y Roma, se conoció

[196] VIDAL, M., *Moral de Actitudes. Moral Social*, Tomo III, Madrid, Perpetuo Socorro, 1981, p. 155.

el concepto de libertad y que el cristianismo[197] influyó de forma determinante en el desarrollo de ese concepto. El concepto del hombre y su libertad se recoge en la "Magna Charta" de 1215 y posteriormente la filosofía nominalista, el espíritu individualista del Renacimiento y la Reforma (calvinismo y luteranismo) también influyeron en el desarrollo de aquellos conceptos. Todas estas etapas de la historia han dejado su impronta en la aparición de las "libertades sociales" en sentido moderno. Ahora bien, estas libertades sociales se desarrollan como tal en el último tercio del siglo XVIII y a lo largo del siglo XIX[198] y, de la toma de conciencia de ellas, surgen las "declaraciones de los derechos" de la persona en los tiempos modernos. La declaración de independencia de los Estados Unidos de América, en el año 1776, tiene en cuenta ciertos derechos inalienables del hombre. En ese mismo año, la Declaración de derechos de Virginia recoge, por vez primera, un catálogo específico de derechos del hombre y del ciudadano[199]. En 1789 la Declaración francesa proclamó con fuerza un concepto de hombre y de sociedad que, posteriormente en 1793, asumió la Declaración de los derechos del hombre y del ciudadano adoptada por la Asamblea Constituyente francesa y que sirvió de base en el siglo XIX a muchas constituciones de países occidentales que desarrollaron una sociedad con fundamento liberal. Cassese[200], en un análisis global de estas Declaraciones, plantea tres notas características de las mismas: primera, la sociedad solo puede estar compuesta por individuos libres; segunda, no se admiten fórmulas distintas, alternativas, a la organización en sociedad (carácter perentorio o totalizante); y tercero, contienen un gran número de mitos políticos. En relación con la primera característica, los hombres libres e iguales, que conforman la sociedad, lo son en la medida que puedan gozar sin molestias de sus bienes (derecho de propiedad), no estén oprimidos por un gobierno tiránico y puedan realizarse o desarrollarse libremente, no admitiéndose más distinciones sociales que las fundadas en la utilidad común y

[197] Para Luño Peña "el cristianismo representa y constituye la más solemne proclamación de los derechos de la personalidad humana, mediante la idea de una verdadera fraternidad universal que implica la igualdad de derechos y la inviolabilidad de la persona con todas sus prerrogativas, individuales y sociales", cit. CASTÁN TOBEÑAS, J., *Derecho Civil Español, común y foral. (*Tomo Primero, Introducción y Parte General. Vol. II Teoría de la relación jurídica. La persona y los derechos de la personalidad. Las cosas. Los hechos jurídicos), Madrid, REUS, 1984, p. 356.

[198] Tras la caída del Antiguo Régimen aparecen la burguesía y el Estado Liberal y el liberalismo como sistema social y forma general de cultura. Pero en la interpretación liberal, aunque el estado de Derecho garantiza las libertades de los individuos, las libertades garantizadas son las de los individuos burgueses. La libertad es para todos, pero meramente formal, y privilegio realmente para unos pocos (los burgueses) y donde el Estado del *laissez-faire* es ineficaz y clasista. Cfr. VIDAL, M., op. cit., pp. 156 y ss.

[199] En este mismo sentido, la Constitución de la Comunidad de Massachussets (1780), en la que se proclama que el "hombre" es digno de este nombre si "puede gozar, con seguridad y tranquilidad, de sus derechos naturales y de las bendiciones de la vida" (*the blessings of life*).

[200] CASSESE, A., *Los derechos humanos en el mundo contemporáneo,* Barcelona, Ariel, 1993, p. 31.

justificadas por la diversidad de virtudes y talentos y estando tan sólo sometidos a la Ley. La segunda característica hace referencia al papel que desempeñan estas Declaraciones como auténticas constituciones, que estructuran todo el ordenamiento jurídico y no admiten situaciones intermedias. O los gobiernos respetan los derechos del hombre o, si no es así, son una "bárbara yuxtaposición de individuos dedicados a sobrepujarse recíprocamente"[201]. Respecto a la tercera nota característica, los mitos contenidos en el texto de estas Declaraciones, se puede decir, siguiendo a este mismo autor, que son: la existencia de derechos naturales e imprescriptibles del hombre, la soberanía de la nación o la Ley como expresión de la voluntad general. De todo lo expuesto, merece ser destacado que, en relación con el concepto de hombre, todas estas declaraciones, lo consideran como tal si puede realizarse libremente. En la base de estos grandes textos políticos del pasado se encuentra el mismo germen que en la actualidad constituye la base de los que hoy conocemos como derechos fundamentales y, cómo no, entre ellos del derecho a la autodeterminación informativa: el libre desarrollo de la personalidad del individuo.

Ya en el siglo XX, la Declaración Universal de Derechos Humanos[202], aprobada en 1948 por la Asamblea General de las Naciones Unidas, estableció un equilibrio entre las libertades individuales y los derechos sociales. Es en esta Declaración en la que por primera vez se establece, en un instrumento jurídico internacional, un derecho a la protección de la esfera privada de las personas frente a posibles intrusiones de terceros o del propio Estado. En palabras de Glendon, transformó "significativamente el terreno moral de las relaciones internacionales"[203]. Ahora bien, hay que tener en cuenta que la Declaración Universal lo que encierra es una obligatoriedad moral en cuanto expresión de la conciencia jurídica de la humanidad. Por ello, y para reforzar la Declaración, se adoptaron por la Asamblea General dos pactos en el año 1966: el Pacto internacional de derechos económicos, sociales y culturales y el Pacto internacional de derechos civiles y

[201] Ibíd. En este sentido el preámbulo de la Declaración francesa dice así: "la ignorancia, el olvido o el desprecio de los derechos del hombre son las únicas causas de las desventuras públicas y de la corrupción de los gobiernos". Y el artículo 16 establece: "toda sociedad en que la garantía de los derechos no está asegurada, ni determinada la separación de los poderes, carece de constitución".

[202] En relación a los derechos objeto de nuestro análisis es destacable el artículo 12 de la Declaración que dispone: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene Derecho a la protección de la ley contra tales injerencias o ataques".

[203] GLENDON, M.A., "70 años de la Declaración Universal de Derechos Humanos", *Revista Nuestro tiempo,* año LXV, número 701, invierno 2019, Universidad de Navarra, p.104.

políticos[204]. En un análisis del contexto histórico en el que surge la Declaración Universal, podemos afirmar, siguiendo a Cassese[205], que la idea de que la causa de la segunda guerra mundial residía en el desprecio de las libertades y los derechos humanos fue calando en la opinión mundial. En este mismo sentido, señala Glendon que "a lo largo del gran periodo de procesos constituyentes que siguió a la guerra, sirvió como modelo para las cartas adoptadas por las nuevas naciones y para los catálogos de derechos que se iban añadiendo a las construcciones antiguas"[206]. Pero ahora, en la actualidad, hay que señalar que nos encontramos ante un momento de cierta crisis en lo que a los derechos humanos se refiere por varias razones; por una parte, lo que Glendon denomina "la proliferación de derechos y reivindicaciones de derechos" que conduce a un aumento de conflictos de derechos; y, junto a ello, "las concepciones altamente individualistas de los derechos promovidas por tantos activistas que han dado nuevo vigor a viejos desafíos a la universalidad de los derechos humanos"[207].

En lo referente a Europa, se ha recorrido un largo camino hasta llegar a la proclamación, en la Cumbre de Niza del 7 de diciembre de 2000, de la Carta de los Derechos Fundamentales de la Unión Europea[208]. La protección de datos se encuentra incardinada

[204] También cabe destacar en la actividad de la O.N.U. con respecto a los derechos humanos la Declaración de la Asamblea General en relación con los derechos del niño en 1959 y la Declaración sobre la eliminación de la discriminación de la mujer en 1967. Cfr. VIDAL, M., op. cit., pp. 160 y ss.

[205] Una perspectiva internacional en relación con la irrupción de los derechos humanos en el escenario mundial es la ofrecida por este mismo autor que complementa lo hasta aquí expuesto. Se analiza el periodo histórico delimitado por la paz de Westfalia (1648) y finales del siglo XIX y se afirma con rotundidad que en esos dos siglos y medio no hay reconocimiento en el ámbito internacional de los individuos, como tal, y los pueblos. Indudablemente sí se estudió en este periodo el papel del hombre en el interior de la sociedad, pero en el ámbito de las relaciones internacionales sólo contaban los Estados. Es evidente que las dos posguerras mundiales, 1917 y 1945, sirvieron de revulsivo para replantear "las estructuras sociales y los modelos de vida, para decidirse a renovar el entramado del consorcio humano en un esfuerzo de adaptación a los nuevos desarrollos de la realidad". La segunda posguerra, sigue diciendo este autor, lanza una doctrina iusnaturalista de los derechos humanos aplicable en las relaciones entre cada Estado y sus ciudadanos. La Carta de la ONU consagró tres grandes ideales: el derecho de los pueblos a su autodeterminación, los derechos humanos y el pacifismo. Es posteriormente en 1948 con la proclamación de la Declaración Universal de los Derechos Humanos y los dos Pactos de la ONU en esta materia de 1966 cuando se llena de contenido la ideología de los derechos humanos. Cfr. CASSESE, A., op. cit., pp. 17 y ss.

[206] GLENDON, M.A., op. cit., p. 104.

[207] Ibíd., p. 107.

[208] En su Preámbulo la Carta de los Derechos Fundamentales de la Unión Europea proclama como fundamento del acervo moral y espiritual de Europa a la dignidad humana. Reza así: "Consciente de su patrimonio espiritual y moral, la Unión está fundada sobre los valores indivisibles y universales de la dignidad humana, la libertad, la igualdad y la solidaridad, y se basa en los principios de la democracia y del Estado de Derecho. Al instituir la ciudadanía de la Unión y crear un espacio de libertad, seguridad y justicia, sitúa a la persona en el centro de su actuación". Además, dedica su primer artículo a la Dignidad humana diciendo: "La dignidad humana es inviolable. Será respetada y protegida". DOCE serie C 364/1 de 18 de diciembre de 2000. http://www.europarl.europa.eu/charter/pdf/text_es.pdf [9 de abril de 2015]. La Carta de Derechos Fundamentales de la UE fue proclamada por el Parlamento Europeo, el Consejo de

en la consagración de los derechos a la intimidad y a la vida privada de los artículos 7 y 8 de la Carta. Y es precisamente a propósito de la protección de datos, así configurada en la Carta, donde la jurisprudencia del TJUE ha sido más determinante de la línea jurisprudencial de los Tribunales Constitucionales nacionales de los Estados miembros[209]. Cabe destacar, siguiendo el recorrido de este camino, el importante papel desempeñado por el Consejo de Europa[210] que, tras la firma el 5 de mayo de 1949 de su Carta fundacional -el Tratado de Londres- por parte de Bélgica, Francia, Luxemburgo, Países Bajos y Reino Unido (poco después, se adhirieron Irlanda, Italia, Dinamarca, Noruega y Suecia) desarrolló, como una de sus primeras medidas, la redacción de la Convención Europea para la salvaguardia de los derechos humanos y las libertades fundamentales aprobada en Roma en el año 1950, y que entró en vigor en 1953, también conocido como Convenio Europeo de Derechos Humanos, instrumento destinado a la protección de los derechos civiles y políticos. Por su parte, los derechos de carácter socioeconómico tuvieron que esperar hasta 1961, año en el que se adoptó la Carta Social Europea[211]. Así mismo, en 1967 se constituyó en el seno del Consejo de Europa una Comisión Consultiva para analizar la injerencia en la vida privada de los individuos de las tecnologías de la información. De esta Comisión Consultiva surgió la Resolución 509 de la Asamblea del Consejo de Europa, adoptada en 1968, sobre "los Derechos humanos y los nuevos logros científicos y técnicos". La actividad del Consejo de Europa en pro de la salvaguarda de los datos de carácter personal continuó, en los años

---

la Unión Europea y la Comisión Europea el 7 de diciembre de 2000 en Niza. Posteriormente una versión revisada de esta Carta fue proclamada y firmada el 12 de diciembre de 2007 en Estrasburgo por el Parlamento, la Comisión y el Consejo.

[209] Cfr. LÓPEZ AGUILAR, J. F., "La protección de datos personales en la más reciente jurisprudencia del TJUE: los Derechos de la CDFUE como parámetro de validez del Derecho europeo, y su impacto en la relación transatlántica EU-EEUU*"* en *Teoría y Realidad Constitucional* núm. 39, 1º semestre 2017, p. 561.

[210] El Consejo de Europa se constituyó terminada la Segunda Guerra Mundial por algunos Estados de Europa, inicialmente Estados vencedores, con la finalidad fundamental de servir de soporte y promoción del Estado de Derecho, la democracia, los derechos humanos, entre otros fines. Cfr. Agencia de los Derechos Fundamentales de la Unión Europea (FRA), *Manual de legislación europea en materia de la protección de datos*, Secretaría del Tribunal Europeo de Derechos Humanos, Consejo de Europa, Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2014, p. 14.

[211] La Carta Social Europea recoge los principales derechos de carácter económico y social y, a diferencia de lo que ocurre en el Convenio Europeo de Derechos Humanos, no establece un sistema judicial de control del cumplimiento por parte de los Estados de sus principales disposiciones. Entre los derechos de la segunda generación más importantes contenidos en la Carta Social Europea figuran, entre otros, el derecho a: el trabajo (art. 1), organizarse para la defensa de intereses económicos y sociales (art. 5), la negociación colectiva (art. 6), la seguridad social (art. 12), la asistencia social y médica (art. 13), la protección social, jurídica y económica de la familia (art. 16), y la protección y asistencia por parte de los trabajadores migrantes y sus familias (art. 19). De estos siete artículos, los Estados Partes tienen que aceptar al menos cinco de ellos y no menos de 10 de los derechos recogidos en toda la Parte II de la Carta. Se trata así de un sistema flexible, que no obliga al Estado a aceptar todos los derechos de la Carta. Disponible en http://www.dicc.hegoa.ehu.es/listar/mostrar/64 [Fecha de consulta: 19/08/2017].

70 del pasado siglo, adoptando el Comité de Ministros del Consejo varias resoluciones en esta materia[212]. En el año 1976 se creó una comisión de expertos en el seno del Consejo de Europa que se encargó de desarrollar los trabajos previos del documento de transcendental importancia, conocido como el Convenio 108[213]. También merece mención el Acta final de Helsinki de 1975 que considera a los derechos humanos "un factor esencial de la paz, la justicia y el bienestar necesarios para asegurar el desarrollo de relaciones amistosas y de cooperación" entre todos los Estados.

Con este breve recorrido histórico, hemos constatado el progresivo e imparable reconocimiento de libertades y derechos del hombre que no son sino emanación de la, a su vez, progresiva conciencia común de la dignidad del individuo.

Nuestra Constitución recoge estos antecedentes y explícitamente proclama en su artículo 10.1 la dignidad de la persona como fundamento del orden político y de la paz social: "La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social"[214]; sin olvidar el apartado 2 de este mismo precepto: "Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España". Así pues, los constituyentes españoles asumieron en el Título I, De los Derechos y Deberes Fundamentales, el acervo

[212] Consejo de Europa, Comité de Ministros (1973), Resolución (73) 22 relativa a la protección de la vida privada de las personas físicas en relación con los bancos de datos electrónicos en el sector privado, de 26 de septiembre de 1973. Así mismo es destacable la Resolución (74) 29 del mismo Comité de Ministros del Consejo de Europa relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector público, de 20 de septiembre de 1974.

[213] CETS nº 108, 1981. El 28 de enero de 1981 el Consejo de Europa aprobó el Convenio europeo sobre protección de datos personales que contiene todos los pilares fundamentales de lo que hoy conocemos como los principios de la protección de datos. Destacamos su artículo 6 referido a lo que denomina "categorías particulares de datos" que son aquellos que revelen el origen racial, las opiniones políticas, las convicciones religiosas, u otras convicciones, la salud, la vida sexual y condenas penales, prohibiendo en todos estos casos su tratamiento automatizado a no ser que el derecho interno prevea garantías apropiadas. El Convenio fue modificado el 15 de junio de 1999 para permitir la adhesión de las Comunidades Europeas y en 2001 se adoptó un Protocolo Adicional relativo a transferencia transfronteriza de datos y al establecimiento obligatorio de autoridades nacionales de supervisión.

[214] Coincidiendo con Sánchez González, esta afirmación de principio sigue a la recogida en la Declaración Universal de los Derechos Humanos de 10 de diciembre de 1948 y también a la recogida en el Pacto Internacional de Derechos Civiles y Políticos de 19 de diciembre de 1966. Ambos documentos en sus respectivos Preámbulos fundamentan la libertad, la justicia y la paz en el reconocimiento de la dignidad intrínseca a todos los miembros de la familia humana. SÁNCHEZ GONZÁLEZ, S., op. cit., pp. 23 y 24.

internacional en relación con los derechos del hombre y erigieron a la dignidad de la persona en el fundamento o razón de ser[215] de los derechos y libertades recogidos en su texto.

Llegados a este punto, conviene recordar brevemente qué se entiende por dignidad apoyándonos para ello en la jurisprudencia de nuestro Tribunal Constitucional. La STC 53/85, en su Fundamento Jurídico octavo, reconoce que "la dignidad es un valor espiritual y moral inherente a la persona que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión al respeto por parte de los demás". Es esencial la conexión entre dignidad y autodeterminación, siendo manifestación ésta de aquélla. El concepto de dignidad se ofrece en esta Sentencia a través de su manifestación, la autodeterminación. Es decir, el acercamiento ontológico a la dignidad se hace por medio, o a través, de su manifestación que es la autonomía del individuo o la autodeterminación para tomar sus propias decisiones en el desarrollo de su vida. De ello se deriva que, en la base de la mayoría de los derechos fundamentales, expresión de distintos aspectos de la autodeterminación del individuo, se encuentre la dignidad del mismo. En opinión de reconocida doctrina, este concepto de la dignidad bien podría considerarse una muestra de un hipotético "iusnaturalismo subyacente" en la parte dogmática de nuestra Constitución, ya que, si la dignidad es inherente, consustancial, al ser humano eso quiere decir que es previa a su formulación constitucional o a su reconocimiento por el Derecho. Pero el mismo Tribunal Constitucional se ha encargado de desbaratar esta interpretación al afirmar, en el Fundamento Jurídico cuarto de su Sentencia 150/91, que "[…] las normas constitucionales relativas a la dignidad de la persona y al libre desarrollo de la personalidad […] si bien integran mandatos objetivos […] no pretenden la consagración constitucional de ninguna construcción dogmática […]"[216].

Es muy esclarecedora a este respecto, y concretando ya la relación entre el derecho fundamental a la protección de datos y los bienes de la personalidad, la STC 292/2000, de 30 de noviembre, que en su Fundamento Jurídico Sexto afirma: "[…] De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más

[215] Lo que la doctrina alemana denomina *Auffangsgrundprinzip* o principio fundamental de referencia. SÁNCHEZ GONZÁLEZ, S., op. cit., p. 24.
[216] Ibíd.

amplio que el del derecho a la intimidad, ya que "el derecho fundamental a la protección de datos extiende su garantía", no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino "a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal" (STC 170/1987, de 30 de octubre, FJ 4), como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para, o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado".

No obstante, el hecho de que se haya recogido expresamente en este artículo 10 CE la referencia a la dignidad tiene mucha trascendencia puesto que, junto a ser fundamento de los derechos constitucionales, esta positivación constitucional de la dignidad desempeña otras funciones. Así para Ruiz-Giménez cabe hablar de una triple función, por una parte, legitimadora del orden político, por otra, promocional de los derechos del individuo y, por último, una función interpretativa para todos los poderes públicos de todas las normas del ordenamiento jurídico[217]. Sin embargo, para Sánchez González constitucionalizar la dignidad no ha sido una decisión acertada, primero por innecesaria, si ya es inherente al hombre no añade nada a los derechos que ya se le reconocen, y segundo por falta de dotación de un contenido jurídico preciso[218].

[217] Cfr. RUIZ-GIMÉNEZ, J., RUIZ-GIMÉNEZ, I., "Artículo 10 Derechos Fundamentales de la Persona" en *Comentarios a la Constitución Española de 1978*, Madrid, Cortes Generales-EDERSA, 1997, pp. 58-59. En su función legitimadora la dignidad proporciona legitimidad al régimen político en la medida que respete y tutele la dignidad de la persona y sus derechos. De aquí se deriva una función promocional de soporte y enriquecimiento de la personalidad. Y en tercer lugar la dignidad sirve de pauta interpretativa para Estado, Comunidades Autónomas e instituciones subordinadas de todas las normas del ordenamiento jurídico. Cit. SÁNCHEZ GONZÁLEZ, S., op. cit., p. 25. En torno a las cuestiones de legitimación, de valores y principios, véase JIMÉNEZ CAMPO, J., "Artículo 10.1" en Rodríguez-Piñero, M. y Casas Baamonde, M. E. (Dir.), *Comentarios a la Constitución española*, Tomo I, Conmemoración del XL Aniversario de la Constitución, Madrid, Wolters Kluwer, BOE, TC y Ministeriode Justicia, 2018, pp. 213-215.

[218] SÁNCHEZ GONZÁLEZ, S., op. cit., p. 26.

En todo caso, y sobre la base de este concepto de dignidad hasta aquí apuntado, ¿es compatible con él la recogida o lectura de datos del cuerpo humano? ¿Se puede decir que se atenta a la dignidad de un individuo convirtiéndolo en un soporte de lectura como si tratara de un objeto? Tiene una gran relevancia en el estudio de esta cuestión la STS, de 2 de julio de 2007[219]; vemos cómo ha sido en el orden contencioso-administrativo donde se ha planteado y dado una respuesta a la cuestión jurídica de si los sistemas de control de horario mediante captación por infrarrojos de una imagen tridimensional de la mano del funcionario-trabajador atentan, o no, a su dignidad y conculcan algunos de sus derechos fundamentales como el derecho a la integridad o a la intimidad personal, consagrado en el artículo 18 CE. Es por ello por lo que ha sido la sala 3ª, de lo contencioso-administrativo[220], del Tribunal Supremo la que ha enjuiciado esta cuestión resolviéndola de manera completa y exhaustiva en la ya citada Sentencia de 2 de julio de 2007 en la que, en esencia, viene a rechazar que se produzca con estos sistemas de control la vulneración de ningún derecho fundamental. Esta Sentencia reviste gran importancia porque recoge a su vez la doctrina del Tribunal Constitucional al respecto y es seguida por Tribunales de otros órdenes jurisdiccionales como por ejemplo el social. Por su parte, el Tribunal Supremo establece que "reducir a la persona a un mero número y tratarla solamente en cuanto magnitud" sí atentaría a su dignidad porque, en consonancia con la interpretación del Tribnal Constitucional en la más arriba citada Sentencia 53/85, cercenaría su autodeterminación. Pero, finalmente, el Tribunal Supremo no estima que exista ninguna afrenta a la dignidad humana por la conversión a

[219] Sala 3ª (sala de lo contencioso-administrativo), sec. 7ª -ponente Lucas Murillo-. Recurso de casación 5017/2003, sobre derechos fundamentales, interpuesto por la Confederación General del Trabajo de Cantabria y por el Sindicato de Trabajadores de la Enseñanza de Cantabria, contra la Sentencia dictada el 21 de febrero de 2003 por la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Cantabria, recaída en el recurso 763/2002, sobre la implantación del nuevo sistema de control horario del personal a través de huellas biométricas.

[220] Es en el ámbito de la función pública donde se plantea por primera vez ante un tribunal la legalidad de un sistema de control horario y es por ello por lo que la primera Sentencia dictada por un Tribunal español que aborda directamente el tratamiento de datos biométricos de huella dactilar es la Sentencia del Tribunal Superior de Justicia de Cantabria, Sala de lo Contencioso-Administrativo, S 23-1-2003, rec. 166/2002. Pte: Tolosa Tribiño, César. EDJ 2003/76961. Aunque esta Sentencia no estudia todas las posibles implicaciones que del tratamiento de estos datos pueden derivarse para los derechos fundamentales de la persona, sí analiza los tres derechos fundamentales que en hipótesis pueden verse afectados: intimidad, integridad corporal y libertad informática. Esta Sentencia estima el recurso de apelación promovido por el Gobierno de Cantabria y revoca la Sentencia dictada en instancia por el Juzgado de lo Contencioso-Administrativo nº 1 de Santander, desestimando por ello la demanda planteada por el particular. No obstante, el promotor del recurso contencioso-administrativo recurre en amparo ante el Tribunal Constitucional dando lugar al Auto del Tribunal Constitucional, sección 3ª, Auto de 26 de febrero de 2007, nº 57/2007, rec. 4243/2003 (EDJ 2007/16816) por el que se inadmite el recurso de amparo planteado al no haber quedado acreditada la vulneración de ningún derecho fundamental.

un código binario de la imagen de una parte del cuerpo[221]. Con ello, no se reduce a la persona a un algoritmo, sin perjuicio de que la captación de la imagen tridimensional de la mano deba realizarse con arreglo a unos fines legítimos en cumplimiento de la normativa de protección de datos. Creemos que es aquí donde el Tribunal Supremo apunta certeramente el núcleo del verdadero debate jurídico en relación con el tratamiento del dato biométrico, los fines legítimos del mismo, ya que es la finalidad de ese tratamiento y, por tanto, su acomodación al derecho fundamental a la protección de datos la que debe regir el caso.

En definiva, que en relación con un sistema de captación por infrarrojos de una imagen tridimensional de la mano que acaba convertida en un registro de nueve bytes, válido para identificar a los empleados públicos mediante tratamiento informático que lo relaciona con otros datos, y así controlar el cumplimiento del horario de trabajo de los mismos, no vulnera sus derechos fundamentales. El Tribunal Supremo, en el Fundamento de Derecho séptimo de la referida Sentencia, hace referencia a ello:

> "[…] Parece como si los sindicatos que han promovido el proceso vieran en la conversión en un código binario de la imagen tridimensional de la mano una afrenta a la dignidad humana. Pero el alcance del sistema no llega a tanto. Lo que podría considerarse contrario a esa dignidad sería reducir la persona a un mero número y tratarla solamente en cuanto magnitud y no es eso lo que sucede aquí. En realidad, la captación de imágenes o registros de distintas partes del cuerpo humano a efectos de identificación no es desconocida. Así, no se considera lesiva la fotografía del rostro o del cuerpo entero, se admite la toma de huellas digitales o del pie, el registro del iris o de la voz y hasta del mismo ADN en determinados supuestos. Por otra parte, se usan de forma creciente los códigos de identificación, los cuales por ajustarse a la definición del artículo 3 a) de la Ley Orgánica, tienen la consideración de dato de

[221] En el mismo sentido TSJ de Canarias, Sala de lo Contencioso-Administrativo, sec. 1ª, S 18-9-2009, nº 190/2009, rec. 443/2007. De una manera tangencial la Sentencia aborda la posible agresión a la dignidad humana derivada de la conversión a un código binario de la imagen tridimensional de la mano. El Tribunal no considera este hecho atentatorio a la dignidad de la persona. Lo que podría considerarse atentatorio a la dignidad de la persona es reducirla a un mero número y tratarla en cuanto magnitud binaria.

> carácter personal: así los números de identificación personal, la dirección de correo electrónico o la dirección IP para la transmisión de datos en Internet.
>
> Todos ellos, del mismo modo que aquellos aspectos del cuerpo humano que se han mencionado, se recogen y archivan para su utilización con fines legítimos y con arreglo a las leyes en un creciente número de supuestos. Puede, pues, decirse que, por sí sola, la plasmación numérica de datos o aspectos personales, no es contraria al derecho fundamental invocado, ni, desde luego, la reducción a algoritmo digitalizado de la imagen de la mano tiene entidad para devaluar la persona de la manera que temen los recurrentes.
>
> Por lo demás, hay que resaltar el sentido fundamentalmente hipotético que informa el planteamiento que han hecho en esta cuestión".

En términos absolutamente coincidentes se expresa la Sentencia 18-9-2009 del TSJ de Canarias[222]: "[…] En realidad, la captación de imágenes o registros de distintas partes del cuerpo humano a efectos de identificación no es desconocida. Así, no se considera lesiva la fotografía del rostro o del cuerpo entero, se admite la toma de huellas digitales o del pie, el registro del iris o de la voz y hasta del mismo ADN en determinados supuestos"[223].

Efectivamente, nuestro cuerpo se está revelando como una fuente inagotable de información y casi podría afirmarse, conicidiendo con la opinión de Rodotá, que el cuerpo de la persona corre el riesgo de considerarse como un lugar público y esto determina una redefinición del estatuto político e institucional de los ciudadanos frente al Estado. Si volvemos los ojos al origen del constitucionalismo, "No te pondremos la mano encima" es la promesa de la Carta Magna. El hombre libre consiguió el respeto de su cuerpo en su integridad y esa conquista no tiene marcha atrás. La lectura y

[222] Sala de lo Contencioso-Administrativo, sec. 1ª, nº 190/2009, rec. 443/2007.
[223] Así lo prevé la LO 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

tratamiento de cualquier dato biométrico de una persona debe respetar su integridad física y psíquica[224].

Ahora bien, la idea que acabamos de exponer en el párrafo anterior no es expresada con tal rotundidad por el TSJ de Canarias. De hecho, la Sentencia afirma que puede decirse que, por sí sola, la plasmación numérica de datos o aspectos personales, no es contraria a la dignidad de la persona, ni, desde luego, la reducción a algoritmo digitalizado de la imagen de la mano tiene entidad para devaluar la persona. Sin estar en desacuerdo con esta afirmación, sin embargo, nos planteamos ¿dónde está el límite que ya no se puede traspasar y que sí podría considerarse atentatorio a la dignidad de la persona y capaz de devaluarla? Probablemente para contestar a esta pregunta hay que atender a las normas sobre protección de datos de carácter personal.

El TSJ de Canarias analizó la posible infracción del derecho fundamental[225] del artículo 18.4 CE. De nuevo, el TSJ de Canarias analiza con rigor la posible vulneración de este derecho fundamental en la Sentencia de instancia; recordemos que estamos ante un recurso ante Tribunal Superior en segunda instancia.

Para este análisis, es necesario determinar si nos encontramos ante un dato de carácter personal, es decir, si el registro de nueve bytes es dato de carácter personal. Para ello el Tribunal analiza la cuestión partiendo de la definición del artículo 3 a)[226] LOPD, y expresando, sin margen de dudas, que la lectura biométrica es dato al incorporarse al fichero, al ser objeto de tratamiento. Aquí radica el elemento diferenciador de la aplicación o no del derecho fundamental a la protección de datos, si el dato se incorpora o no a un fichero (automatizado o no), si es objeto de tratamiento, porque si esto no se produce el dato personal quedaría dentro del ámbito de protección de otros derechos fundamentales sea la intimidad personal y familiar o el honor. Al integrarse el registro

[224] RODOTÁ, S., *La vida y las reglas…*, op. cit., pp. 109 y ss.

[225] Se trata del derecho fundamental a la protección de datos de carácter personal consagrado con carácter independiente por el Tribunal Constitucional español en su Sentencia número 290, de 30 de noviembre de 2000, que se extrae de la interpretación del apartado 4 del artículo 18 CE.
Así mismo, este derecho fundamental a la protección de datos de carácter personal se recoge en textos internacionales, baste citar aquí el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, que no es sino la culminación de una evolución que tiene su origen en las leyes de protección de datos de los años setenta, pasando por el Convenio 108 del Consejo de Europa y la Directiva 95/46/CE.

[226] Por dato de carácter personal ha de entenderse "cualquier información concerniente a personas físicas identificadas o identificables".

de nueve bytes en un fichero que incluye nombre y apellidos y Documento Nacional de Identidad cae bajo el ámbito de aplicación de la LOPD. Al entrar en aplicación la Ley Orgánica de protección de datos ha de estudiarse si el tratamiento de ese registro de nueve bytes se realiza conforme a los principios de la protección de datos.

No obstante, la Sentencia no entra a conocer sobre la acomodación del registro, de la imagen tridimensional de la mano, a todos y cada uno de los principios de la protección de datos porque los propios recurrentes no lo han planteado en su recurso.

Así se analizan tres principios básicamente: el principio de la finalidad[227], el consentimiento y la calidad de los datos como adecuación al fin.

El Tribunal considera que la finalidad perseguida es plenamente legítima: el control del cumplimiento del horario de trabajo por los funcionarios públicos y desde el momento que la obligación de cumplimiento del horario es inherente a la relación que une al funcionario con la Administración no es necesario que ésta recabe su consentimiento. Continúa diciendo la Sentencia, la toma a través de escaner de una imagen de la mano no incumple lo que establecía en el artículo 4.1 de la LOPD, puesto que cabe calificarla de adecuada, pertinente y no excesiva con arreglo a la finalidad legítima perseguida. (Como sabemos, hoy, la LO 3/2018, habla de la exactitud de los datos -art. 4-).

Por este motivo, entendemos que, posteriormente, la Sentencia del TSJ de Canarias en su último fundamento, y resolviendo el último argumento impugnatorio de los recurrentes, considera justificado el sistema elegido de control horario y dice textualmente:

> "[…] no hay norma que prohíba el recurso a la tecnología escogida para realizar el control del cumplimiento del horario de trabajo. Su novedad o complejidad no la convierten en lesiva de los derechos fundamentales

[227] "1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido" (art. 4 LOPD). Y el art. 4 LO 3/2018, reza así: 1. Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados. 2. A los efectos previstos en el artículo 5.1.d) del Reglamento (UE) 2016/679, no será imputable al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos: (…)".

> invocados. Y el posible desequilibrio que pudiera existir entre uso de la biometría y ese control no es cuestión a dirimir jurisdiccionalmente en este proceso".

Deja así el Tribunal abierto al análisis de un posible desequilibrio del uso de la biometría con el fin de control para otro proceso. No parece que el Tribunal esté lejos de asumir una nueva concepción de la persona que tenga garantías para mantener siempre el pleno control sobre su cuerpo tanto en el plano físico como electrónico. La transformación del material físico, biométrico, en material digitalizado, en ceros y unos, puede afectar al equilibrio de fuerzas siempre frágil entre las de un individuo, siempre limitadas, y las del exterior. Entre el poder de control del individuo sobre sus datos y el uso de esos datos incontroladamente por terceros, sea por el Estado o por otros particulares. Siempre la persona deberá conservar el control sobre su propio cuerpo digital[228].

2.2.1.2. Derechos de la personalidad.

Enlazando con la precisión antes planteada por Sánchez González, relativa a la falta de dotación de contenido constitucional preciso de la dignidad, observamos que si bien ésta queda recogida en el artículo 10.1 CE, como expresamente dice el Fundamento jurídico 1, de la STC 64/86, "[…] no puede servir de base a una pretensión autónoma de amparo", pero sí cabe esta pretensión respecto de los derechos que dimanan de ella y, como ella, son inherentes a la condición humana, los derechos de la personalidad. Iniciamos así con ello el estudio de los mismos. Los derechos de la personalidad están inseparablemente unidos a la persona siendo inherentes a ella por el mero hecho de su existencia. No se trata de derechos concedidos por el Estado, por otros hombres, por la Comunidad Internacional o por las relaciones que establezca el individuo con otros individuos. Son derechos innatos, que se adquieren por el mero hecho del nacimiento.

[228] Rodotá manifiesta de nuevo esta necesidad de equilibrio que apunta la Sentencia comentada al afirmar que "no podemos poner la mano sobre los datos personales, sobre el cuerpo electrónico, si esta no es una medida compatible con los principios de una sociedad democrática, si no se respetan el conjunto de garantías indicadas en las directivas europeas, que han construido un verdadero nuevo modelo de protección de los derechos de la persona. RODOTÁ, S., *La vida y las reglas*…, op. cit., pp. 109 y ss.

Hay varias definiciones clásicas de los derechos de la personalidad que inciden sobre uno u otro aspecto de la esfera personal del individuo. Castán parte de la existencia de bienes de la persona que pueden ser de diversa naturaleza, así distingue entre bienes personales, como la vida, el nombre y el honor; bienes patrimoniales y bienes familiares y sociales. Y es precisamente el conjunto de derechos que ofrecen protección a los bienes personales los que cabe calificar de derechos de la personalidad[229].

Es importante destacar que los derechos de la personalidad cronológicamente, en lo que a su formulación doctrinal se refiere, aparecen antes que los derechos fundamentales. Por eso no es de extrañar que muchos de los logros jurídicos alcanzados en la configuración de la doctrina de los derechos de la personalidad sean aplicables a la doctrina de los derechos fundamentales. También es verdad que la constitucionalización de estos derechos, como a continuación veremos, aporta un límite y/o garantía a su desarrollo ya que, como determina el artículo 53.1 CE, solo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse su ejercicio[230]; bien entendido que la garantía viene dada por la reserva de ley en su desarrollo y el límite lo constituye el impuesto al legislador que en ese desarrollo ha de respetar su contenido esencial.

2.2.2. Formulación actual como Derechos Fundamentales: contenido esencial y garantías de su ejercicio.

Como acertádamente expone Alexy[231], la fundamentalidad o la importancia de las normas iusfundamentales para el sistema jurídico se deriva de su fundamentalidad formal y de su fundamentalidad material, la primera referida a la posición jerárquica de estas normas en la cúspide del ordenamiento jurídico, y la segunda, referida a su

[229] Otras definiciones clásicas de los derechos de la personalidad, recogidas por el mismo profesor Castán, son por ejemplo la de Gierke que los define como los derechos que "garantizan al sujeto el señorío sobre una parte esencial de la propia personalidad"; De Cupis como "aquellos que tienen por objeto los modos de ser, físicos o morales, de la persona"; De Castro como los derechos "que conceden un poder a las personas para proteger la esencia de su personalidad y sus más importantes cualidades" o la definición de Díez Díaz como "aquellos derechos cuyo contenido especial consiste en regular las diversas proyecciones, psíquicas o físicas, de la persona misma". Cfr CASTÁN TOBEÑAS, J., op. cit., p. 355.
[230] HERRERO-TEJEDOR, F., op.cit., p. 27.
[231] ALEXY, R., *Teoría de los Derechos Fundamentales,* (Título original *Theorie der grundrechte.* Suhrkamp-Verlag 1986), Versión castellana Ernesto Garzón Valdés, Madrid, Centro de Estudios Políticos y Constitucionales, 2002, p. 503.

influencia material en la toma de decisiones "sobre la estructura normativa básica del Estado y de la sociedad"[232].

Los derechos fundamentales, respecto de los derechos de la personalidad, presentan un mayor grado de formalismo en su desarrollo y modificación, por ende, acusan menos intervención jurisprudencial y, por último, presentan un juego más limitado de los principios generales del derecho[233]. Efectivamente, el artículo 53.1 CE, como ya hemos indicado, establece que solo por ley podrá regularse el ejercicio de los derechos fundamentales y las libertades públicas. Y, en todo caso, esta ley habrá de tener el rango de ley orgánica (art. 81.1 CE), lo que supone una mayoría cualificada para su aprobación y modificación. Esta reserva de ley limita el papel de la jurisprudencia en el desarrollo y modificación de los derechos fundamentales, a diferencia de lo que ocurre en relación con los derechos de la personalidad en los que la jurisprudencia puede llegar a ser generadora de los mismos. Por ejemplo, la doctrina del daño moral, como indica De Castro[234], puede calificarse de "descubrimiento" jurisprudencial, aunque no es menos cierto que ha de tenerse en cuenta una tradición antigua germana de *Schmerzensgeld* denominada la *pecunia doloris* que resarcía o compensaba un daño sufrido en la persona, pero no propiamente en su conformación física o en su patrimonio, es decir, se trataba de compensaciones a dolores, discriminaciones o padecimientos del alma. Estas situaciones pueden plantearse sin duda en el tratamiento del dato biométrico dactiloscópico, por ello también en nuestro estudio debemos hacer referencia al dolor jurídicamente relevante. Como muy gráficamente expresa Rodotá, "la tortura puede realizarse sin hierros, sin carnes sufrientes: basta violar una sensibilidad, humillar culturalmente"[235]. En definitiva, estas violaciones o humillaciones discriminan; y la discriminación es indudable que es posible en la lectura biométrica dactilar. Con la lectura y el tratamiento biométrico dactilar identificamos al individuo. Dicho de otro modo, lo extraemos del conjunto difuso y confuso de la masa poblacional y lo aislamos. Identificándole, conseguimos la extracción del individuo del resto, conseguimos su individuación. Pero, si ello lleva aparejado evidenciar, o bien, una malformación o una alteración física que esa persona tiene derecho a que permanezca

[232] Ibíd, p. 505.
[233] HERRERO-TEJEDOR, F., op. cit., p. 27.
[234] DE CASTRO y BRAVO, F., "Los llamados derechos de la personalidad*", Anuario de Derecho Civil* X-XII, 1959, p. 8.
[235] RODOTÁ, S., *La vida y las reglas…*, op. cit. p. 251.

oculta provocando un dolor y/o daño moral relevante ¿no debería el Derecho dar una respuesta eficaz a esta situación?

Por último, y consecuencia de la reserva de ley indicada, el juego de los principios generales del derecho es más limitado en la configuración de los derechos fundamentales. Es el formalismo legal el que se impone cuando ya se han constitucionalizado los bienes y/o intereses de la personalidad. Si estos bienes no han tenido acceso a la Constitución tienen un mayor apoyo, para su reconocimiento y ejercicio, en los principios generales del derecho.

Ahora bien, conviene también tener en cuenta que esta reserva de ley puede presentar problemas para la protección y desarrollo, en definitiva, para la eficacia de los derechos fundamentales. Esta situación de riesgo puede plantearse en una doble vertiente, como apunta el Ull Pont[236], bien por ausencia de ley de desarrollo o bien por existencia de una ley restrictiva. Es decir, cabe la posibilidad que la remisión a una ley lleve a un vacío legislativo, que no haya ley reguladora del concreto derecho fundamental, o bien, que, aun existiendo la ley, ésta tenga un carácter restrictivo que, en definitiva, lejos de garantizar la eficacia del derecho lo que haga es limitar su ejercicio. En relación con el primer problema hay que tener en cuenta que, aunque no haya una ley reguladora, el artículo 53.1 CE establece que los derechos y libertades reconocidos en el Capítulo II del Título I (artículos 14 al 38) "vinculan a todos los poderes públicos". Podría considerarse a estos derechos, como así apunta el profesor Ull, derechos de aplicación directa. En este mismo sentido, las SSTC 75/1982 y 39/1983 expresan con claridad que el hecho de que el legislador incumpla su obligación legislativa, impuesta por la Constitución, no puede ser causa de lesión de esos derechos que la misma reconoce. En cuanto al segundo riesgo apuntado, el mismo artículo 53.1 advierte que la ley que regule el derecho "en todo caso deberá respetar su contenido esencial". El respeto del contenido esencial del derecho es una garantía material frente a la reserva de ley que podemos calificar de garantía formal. Esta garantía material tiene su origen en el artículo 19 de la Ley Fundamental de Bon. Ante la desconfianza por los excesos en que puede incurrir el legislador ordinario surge esta garantía material. En todo caso el "contenido esencial de los derechos" es un concepto jurídico indeterminado que ha de

[236] ULL PONT, E., *Derecho público de la informática (Protección de datos de carácter personal)*, Madrid, UNED, 2000, p. 47.

ser llenado por la doctrina y la jurisprudencia. En la Constitución no se estimó suficiente ni el detalle con que se proclaman y garantizan los distintos derechos, ni su carácter vinculante, ni la garantía formal de la reserva de ley y, por ello, se estableció esta garantía material. No obstante, al ser un concepto jurídico indeterminado, como hemos dicho, ha sido el Tribunal Constitucional alemán el encargado de desarrollar este concepto a través de una doble vía: la de la naturaleza jurídica[237] y la de los intereses jurídicamente protegidos en el derecho que en cada caso se considere.

Además, hay que tener en cuenta la protección por inconstitucionalidad que prevé el artículo 161.1.a) CE. Según este artículo el Tribunal Constitucional es competente para conocer "a) Del recurso de inconstitucionalidad contra leyes y disposiciones normativas con fuerza de ley. La declaración de inconstitucionalidad de una norma jurídica con rango de ley, interpretada por la jurisprudencia, afectará a ésta, si bien la sentencia o sentencias recaídas no perderán el valor de cosa juzgada". En definitiva, la ley debe respetar el contenido esencial del derecho para ser constitucionalmente válida. Ese contenido esencial exige que el derecho no quede en mera retórica semántica y la propia Constitución de nuevo, en el artículo 10.2, indica que la interpretación de las normas relativas a los derechos fundamentales y a las libertades reconocidas por ella ha de hacerse "de conformidad con la Declaración Universal de los Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España". Con todo ello, la garantía de estos derechos queda establecida en la propia Constitución siendo, no solo el TC, si no también el TEDH, las instancias ante las que cabe recurrir en caso de extralimitaciones de cualquiera de los Estados. Por último, el artículo 53 CE reconoce el derecho del ciudadano a pedir la tutela judicial de los derechos y libertades reconocidos en el artículo 14 y en la Sección primera, del Capítulo II Título I (artículos. 15 al 29), por un procedimiento basado en los principios de preferencia y sumariedad. Una vez agotada la vía de recurso ante los Tribunales Ordinarios cabe recurrir en amparo ante el Tribunal Constitucional.

[237] "Constituyen el contenido esencial de un derecho subjetivo aquellas facultades o posibilidades de actuación necesarias para que el derecho sea recognoscible como pertinente al tipo descrito y sin las cuales deja de pertenecer a ese tipo y tiene que pasar a quedar comprendido en otro, desnaturalizándose". Sentencia del Tribunal Constitucional federal alemán de 11/1981, de 8 de abril.

2.2.3. Derechos al honor y otros derechos.

Todo lo hasta aquí expuesto es aplicable a los derechos al honor, a la intimidad, a la propia imagen y a la integridad física**,** como derechos fundamentales que son. Y todo lo descrito nos permite evaluar la recogida de datos biométricos dactiloscópicos, desde la perspectiva del respeto a estos derechos fundamentales enunciados. Hemos visto que se han planteado casos en sede judicial en los que la conversión de las características físicas de las personas en un código de identificación digital y su almacenamiento en una base de datos puede plantear dudas respecto a una posible vulneración del derecho a la integridad física y moral y a la intimidad corporal.

Brevemente, podemos confirmar, en relación con estos derechos fundamentales, que es el artículo 18 CE el que, con su contenido múltiple, los reconoce en nuestro ordenamiento. Este precepto protege varios derechos que, si bien parecen inspirados todos en la protección de la intimidad, no obstante, ofrecen matices importantes.

El artículo 18.1 cuenta ya con un contenido complejo, pues en él se protegen, en primer lugar, el derecho al honor, en segundo lugar, el derecho a la intimidad, tanto personal como familiar, y en tercer lugar el derecho a la propia imagen, derechos con rasgos comunes pero diferentes entre sí. Así lo ha señalado la STC 14/2003, al afirmar que son tres derechos autónomos y sustantivos, aunque estrechamente vinculados entre sí, en tanto que derechos de la personalidad, derivados de la dignidad humana y dirigidos a la protección del patrimonio moral de las personas. Estos tres derechos podrán verse afectados, por tanto, de manera independiente, pero también, con frecuencia, de forma conjunta, dada su evidente proximidad. Se ha tratado extensamente en la doctrina y en la jurisprudencia la amenaza a estos derechos que representa el ejercicio de las libertades de expresión e información. Ello lleva a que será necesario un ejercicio de ponderación entre los derechos del artículo 18 y del artículo 20 para resolver los conflictos entre ellos. El desarrollo de la protección de estos derechos lo efectúa, principalmente, la L.O. 1/1982, de 5 de mayo, de protección civil del derecho al honor, la intimidad y la propia imagen, en la que se intentan deslindar los supuestos de intromisión ilegítima (art. 7), de aquellos que no puedan reputarse como tales, por mediar consentimiento o por recoger imágenes públicas (art. 8).

En lo que respecta al derecho al honor, éste goza en nuestro Derecho de una larga tradición como derecho indiscutible de la personalidad. Así mismo, y como destaca Elvira Perales, cabe afirmar que es por excelencia un derecho de las personas individualmente consideradas y en él se puede distinguir un aspecto inmanente y otro trascendente del honor. En el primer ámbito se enmarca la estima que cada persona tiene de sí misma y, en el segundo, el honor consiste en el reconocimiento por los demás de nuestra dignidad conectándose el honor con la fama y la opinión social (STS de 23 de marzo de 1987). Pero junto a estos dos aspectos del honor hay que tener en cuenta que el honor está estrechamente conectado con: 1º las circunstancias del tiempo y del lugar variando de una época a otra (STC 185/1989, de 13 de noviembre); 2º con la propia visión personal puesto que la vulneración del honor de un individuo debe valorarse atendiendo a la relevancia pública que tenga; 3º hay que valorar las circunstancias concretas en las que se produce el atentado al honor (en un momento de acaloramiento o con frialdad...) así como su repercusión exterior (SSTC 46/2002, de 25 de febrero; 20/2002, de 28 de enero; 204/2001, de 15 de octubre; 148/2001, de 27 de junio...)[238].

En ninguno de los dos aspectos del derecho al honor que hemos comentado (inmanente y trascendente) cabe entender que un sistema biométrico de lectura de huella dactilar o de la palma de la mano puede verse afectado.

2.2.3.1. El Derecho a la Integridad.

Nos acercaremos a la cuestión de la integridad física y la integridad moral en el uso de sistemas de reconocimiento dactiloscópico de individuos. Entramos así en el análisis de si la utilización de una parte del cuerpo como elemento de identificación puede conllevar lesión corporal o menoscabo físico. En este punto es ilustrativa la STC de 16 de diciembre de 1996[239], que estima el recurso otorgando el amparo solicitado por el recurrente declarando los derechos de éste a la integridad física (art. 15 CE) y a la intimidad personal (art. 18.1 CE). Merece la pena detener la atención en esta Sentencia,

[238] Cfr. ELVIRA PERALES, A., "Sipnosis artículo 18", disponible en http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2 [Fecha de consulta: 10 de abril de 2018].
[239] Sala 1ª, nº 207/1996, BOE 19/1997, de 22 de enero de 1997, rec. 1789/1996.

ya que incorpora la doctrina del Tribunal en relación con el derecho fundamental a la integridad física y moral y las inspecciones y registros corporales. El mismo TC en otras sentencias -como la de 5 de diciembre de 2013- entiende que un examen dactiloscópico no afecta a este derecho a la integridad. No obstante, el TC en esta sentencia de 1996 concreta que el objeto del presente recurso de amparo consiste en determinar si el requerimiento para soportar una intervención corporal ha podido suponer una vulneración de los derechos fundamentales del recurrente a la intimidad personal (art. 18.1 CE) y a la integridad física (art. 15 CE). La diligencia acordada por el Juzgado de Instrucción contra la que recurre el imputado consiste en proceder a cortar mechones de cabello de distintas partes de la cabeza y la totalidad del vello de las axilas. Este supuesto de hecho nos permite conocer la doctrina del TC sobre la legitimidad de intervenciones en el cuerpo que, a su vez, nos servirá posteriormente para evaluar la legitimidad de la captación de la huella dactilar.

Así la Sentencia, en su Fundamento de Derecho, segundo establece:

> "Una vez delimitado el objeto del recurso procede examinar, en primer lugar (y como paso previo para apreciar una posible vulneración), si la diligencia acordada incide o no en el ámbito constitucionalmente protegido de los derechos a la integridad física y a la intimidad.
>
> Comenzando por el primero de los enunciados derechos, cabe señalar que, según doctrina reiterada de este Tribunal, mediante el reconocimiento del derecho fundamental a la integridad física y moral (art. 15 CE) «se protege la inviolabilidad de la persona, no sólo contra ataques dirigidos a lesionar su cuerpo o espíritu, sino también contra toda clase de intervención en esos bienes que carezca del consentimiento de su titular» (SSTC 120/1990 [RTC 1990\120], fundamento jurídico 8.º, 137/1990 [RTC 1990\137], 215/1994 [RTC 1994\215] y 35/1996 [RTC 1996\35]).
>
> Así pues, y aunque el derecho a la integridad física se encuentra evidentemente conectado con el derecho a la salud (tal y como señalamos en la STC 35/1996, fundamento jurídico 3.º), su ámbito constitucionalmente protegido no se reduce exclusivamente a aquellos

> casos en que exista un riesgo o daño para la salud, pues dicho derecho resulta afectado por «toda clase de intervención (en el cuerpo) que carezca del consentimiento de su titular».
>
> Resulta de ello, por tanto, que mediante el derecho a la integridad física lo que se protege es el derecho de la persona a la incolumidad corporal, esto es, su derecho a no sufrir lesión o menoscabo en su cuerpo o en su apariencia externa sin su consentimiento. El hecho de que la intervención coactiva en el cuerpo pueda suponer un malestar (esto es, producir sensaciones de dolor o sufrimiento) o un riesgo o daño para la salud supone un plus de afectación, mas no es una condición sine qua non para entender que existe una intromisión en el derecho fundamental a la integridad física. […]"

Deducimos así una nota característica del derecho a la integridad física que podemos enunciar como integridad equivalente a incolumidad corporal, o derecho a no sufrir lesión o menoscabo en el cuerpo sin consentimiento. Esto desliga el derecho a la integridad de la salud del individuo, ya que, aunque el derecho a la integridad física está conectado o relacionado con la salud no se reduce su ámbito a supuestos en que haya un riesgo para aquélla, sino que alcanza a toda clase de intervención sobre la persona sin su consentimiento. Con ello cabría deducir que una captación de huellas dactilares, o de la imagen tridimensional de la mano, salvo que se llevara a cabo de forma forzada, sin consentimiento del individuo, no afecta a la incolumidad corporal del individuo. Ahora bien, la captación forzada, aunque no afectara a su salud, vulneraría abiertamente su derecho a la integridad física.

Otra cuestión a plantear en este análisis es la "integridad moral", en la recogida de la huella dactilar. Es difícil considerar que se pueda producir una intromisión en la integridad moral en la recogida ya que en la captación no hay finalidad de humillar al individuo o envilecerle de ninguna manera[240], a no ser que se haga sin su

[240] Un caso especial lo representarían todos aquellos individuos que, por una malformación congénita, accidente, edad etc. presenten una alteración de sus dedos o de sus huellas o carezcan de ellas. El mero hecho de no poder someterse al sistema de captación o presentar dificultades o imposibilidad mecánica para la captación podría representar una intromisión en su integridad moral. No en balde, el GPD 29 ha llamado la atención, en relación con la obtención de los identificadores biométricos de los solicitantes de visado, sobre la existencia de grupos de riesgo como los niños y las personas mayores. Los niños de hasta

consentimiento. Respecto a si el tratamiento de la huella biométrica/dactilar provoca la humillación o el envilecimiento de la persona, el TEDH, en el caso *Campbell y Cosans v.* el Reino Unido (Sentencia de 25 de febrero de 1982[241]), en sus fundamentos de derecho y respecto a la presunta violación del artículo 3 de la Convención y a su vez refiriéndose a otra Sentencia de 25 de abril de 1978 del TEDH en el casos Tyrer[242], dice que "tratamiento" en sí no será "degradante" a menos que la persona en cuestión haya sido objeto -ya sea en su propia consideración o en la de los demás- de una humillación o envilecimiento que alcance un nivel mínimo de gravedad. Ese nivel tiene que ser evaluado en relación con las circunstancias del caso. El Tribunal dice *expresis verbis*: "*Nevertheless, it follows from that judgment that "treatment" itself will not be "degrading" unless the person concerned has undergone - either in the eyes of others or in his own eyes (ibid., p. 16, par. 32) - humiliation or debasement attaining a minimum level of severity. That level has to be assessed with regard to the circumstances of the case*". Otra Sentencia en el mismo sentido es la del Caso *Soering* de 7 de Julio de 1989[243]. En todo caso la captación y el tratamiento de la huella dactilar, en una generalidad de casos, no provoca la humillación o una sensación de envilecimiento de

---

6 años deberían estar exentos de la obligación de dar las impresiones dactilares. Hay que evaluar el respeto de la dignidad del niño. "El grupo de protección opina que, en razón a la dignidad de la persona […], la recogida y el tratamiento de impresiones dactilares debería limitarse en el caso de los niños y las personas mayores, […] Hay que tener en cuenta que la literatura científica no aporta pruebas concluyentes de que la tecnología de las impresiones digitales sea suficientemente fiable en el caso de los niños y las personas mayores. También deberá establecerse el margen de error que los fabricantes puedan garantizar con respecto a las impresiones dactilares conservadas en el sistema (durante 5 años) y los controles (*hit/no hit*) que se realizarán en los cinco años (ó 48 meses) en los que se conservarán las impresiones dactilares. Esto se aplica especialmente a los niños menores de cierta edad y a las personas con enfermedades específicas o en condiciones de deterioro progresivo, ya que en estos casos la posibilidad de desajustes aumenta con el tiempo. También en estos casos habrá que prever procedimientos que garanticen el respeto de la dignidad humana y las libertades fundamentales". Cfr. Grupo de protección de datos creado por el artículo 29. Dictamen nº 3/2007 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica la Instrucción consular común dirigida a las misiones diplomáticas y oficinas consulares de darrera en relación con la introducción de datos biométricos, y se incluyen disposiciones sobre la organización de la recepción y la tramitación de las solicitudes de visado (COM (2006) 269 final), adoptado el 1 de marzo de 2007, pp. 7 y ss. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp134_en.pdf [Fecha de consulta: 12/09/2018].

[241] *European Court of Human Rights*. Tribunal de Justicia (Sala) Caso de Campbell y Cosans v. el Reino Unido. (Aplicación no. 7511/76; 7743/76 (/sites/eng/Pages/search.aspx#{"appno":["7743/76"]}) http://hudoc.echr.coe.int/sites/eng/Pages/search.aspx#{"docname":["campbell"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-57455"]} [Fecha de consulta: 26/03/2016].

[242] *European Court of Human Rights*. Tribunal de Justicia (Sala) Caso de Tyrer v. el Reino Unido. (Aplicación no. 5856/72 (/sites/eng/Pages/search.aspx#{"appno":["5856/72"]}). Estrasburgo. 25 de abril de 1978. http://hudoc.echr.coe.int/sites/eng/Pages/search.aspx [Fecha de consulta: 27/03/2016].

[243] *European Court of Human Rights*. Tribunal de Justicia (Pleno) Caso de Soering v. el Reino Unido. (Aplicación no. 14038/88 (/sites/eng/Pages/search.aspx#{"appno":["14038/88"]}).Estrasburgo. 07 de julio de 1989. http://hudoc.echr.coe.int/sites/eng/Pages/search.aspx [Fecha de consulta:27/03/2017].

las personas, salvo casos excepcionales en que una alteración anatómica o la edad del individuo lo favorezcan.

En definitiva, y considerando este concepto amplio de integridad física y moral, la captación de una huella dactilar, aunque es evidente que no lesiona el cuerpo o el espíritu, ni afecta a la salud de una persona, puede, sin embargo, representar una limitación del derecho fundamental consagrado en el artículo 15 CE a la integridad física y moral del individuo si se lleva a cabo sin su consentimiento o en casos concretos de alteraciones físicas de dedos o palma de la mano del individuo concernido. Llamamos así la atención sobre una posible afección a la integridad moral de la persona en determinados casos de captación del dato, por ejemplo, sin su consentimiento. Hay que tener en cuenta la nueva regulación del consentimiento introducida por el RGPD, en su artículo 4.11. Para la nueva regulación, el consentimiento debe consistir en una manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. Se puede afirmar que la nueva regulación europea excluye el consentimiento tácito viniendo en apoyo de esta afirmación el considerando (32) de la referida norma, que dice: "Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento"[244]. Lo cierto es que el RGPD se distancia enormemente de la consideración del consentimiento como la piedra angular para la construcción de la legitimidad del tratamiento de los datos. La tradición de la legislación española del consentimiento ha experimentado un cambio sustancial; ya no lo podemos considerar clave única de legitimidad, relegando el resto de supuestos de tratamiento a excepciones o derogaciones de la necesidad de consentimiento.

Para completar el análisis de la STC de 16 de diciembre de 1996, nº 207/1996, y siguiendo con su Fundamento de Derecho Segundo, dentro del contexto de la instrucción penal de referencia, dice:

"[…]

[244] SEGURA RODRÍGUEZ, A., *Reglamento Europeo de Protección de Datos. Licitud de tratamiento sin consentimiento explícito.* Disponible en https://elderecho.com/reglamento-europeo-de-proteccion-de-datos-licitud-de-tratamiento-sin-consentimiento-explicito [Fecha de consulta: 23/04/2019].

Con el fin de precisar aún más esta doctrina dentro del ámbito en el que aquí nos movemos, habrá que señalar que, dentro de las diligencias practicables en el curso de un proceso penal como actos de investigación o medios de prueba (en su caso, anticipada) recayentes sobre el cuerpo del imputado o de terceros, resulta posible distinguir dos clases, según el derecho fundamental predominantemente afectado al acordar su práctica y en su realización:

a) En una primera clase de actuaciones, las denominadas "inspecciones y registros corporales", esto es, en aquellas que consisten en cualquier género de reconocimiento del cuerpo humano, bien sea para la determinación del imputado (diligencias de reconocimiento en rueda, exámenes dactiloscópicos o antropomórficos, etc.) o de circunstancias relativas a la comisión del hecho punible (electrocardiogramas, exámenes ginecológicos, etc.) o para el descubrimiento del objeto del delito (inspecciones anales o vaginales, etc.), en principio no resulta afectado el derecho a la integridad física, al no producirse, por lo general, lesión o menoscabo del cuerpo, pero sí puede verse afectado el derecho fundamental a la intimidad corporal (art. 18.1 CE) si recaen sobre partes íntimas del cuerpo, como fue el caso examinado en la STC 37/1989 (examen ginecológico), o inciden en la privacidad.

b) Por contra, en la segunda clase de actuaciones, las calificadas por la doctrina como "intervenciones corporales", esto es, en las consistentes en la extracción del cuerpo de determinados elementos externos o internos para ser sometidos a informe pericial (análisis de sangre, orina, pelos, uñas, biopsias, etc.) o en su exposición a radiaciones (rayos X, TAC, resonancias magnéticas, etc.), con objeto también de averiguar determinadas circunstancias relativas a la comisión del hecho punible o a la participación en él del imputado, el derecho que se verá por regla general afectado es el derecho a la integridad física (art. 15 CE), en tanto implican una lesión o menoscabo del cuerpo, siquiera sea de su apariencia externa. Y atendiendo al grado de sacrificio que impongan de este derecho, las intervenciones corporales podrán ser calificadas como leves o

> graves: leves, cuando, a la vista de todas las circunstancias concurrentes, no sean, objetivamente consideradas, susceptibles de poner en peligro el derecho a la salud ni de ocasionar sufrimientos a la persona afectada, como por lo general ocurrirá en el caso de la extracción de elementos externos del cuerpo (como el pelo o uñas) o incluso de algunos internos (como los análisis de sangre), y graves, en caso contrario (por ejemplo, las punciones lumbares, extracción de líquido cefalorraquídeo, etc.).
>
> De conformidad con lo anteriormente expuesto, resulta claro que la intervención y diligencia pericial acordada en el caso presente por el Juzgado de Instrucción, teniendo en cuenta, primero, su carácter imperativo y contrario a la voluntad del interesado (que, aunque inicialmente se ofreció a una pericia de este tipo, luego, una vez acordada, mostró de manera reiterada su negativa a someterse a ella), y, segundo, que implica una intervención consistente en la extracción de cabellos de diversas partes de la cabeza y de la totalidad del pelo de las axilas, ha incidido en el ámbito constitucionalmente protegido de su derecho fundamental a la integridad física, siquiera sea de una manera leve, pues, de acuerdo con la doctrina expuesta, la afectación de este derecho no presupone necesariamente la existencia de un riesgo o lesión para la salud de la persona. […]"

Se observa que el TC distingue dos supuestos: las inspecciones y registros corporales y las intervenciones corporales. En las primeras no resulta afectado el derecho a la integridad al no producirse lesión o menoscabo del cuerpo, pero puede verse afectado el derecho a la intimidad corporal si se trata de una inspección o registro sobre partes íntimas. Sin embargo, en las intervenciones o extracciones del cuerpo sí puede verse afectado el derecho a la integridad física. Así, al tratar las inspecciones y registros corporales introducimos un nuevo ámbito que es el de la intimidad corporal. En lo referente a la "intimidad corporal" ya el TC en su Sentencia 37/1989, fundamento jurídico 7º, reiterado en las SSTC 120/1990, 137/1990 y 57/1994 ha dejado claro que, sin perjuicio de que la intimidad corporal forme parte del derecho a la intimidad personal, el ámbito de aquélla no es coextenso con el de la realidad física del cuerpo humano. En definitiva, la intimidad corporal para el TC es un concepto afectado por lo

que en nuestra cultura se considera recato corporal. Por eso el TC tiene reiteradamente declarado en las Sentencias citadas que no puede entenderse "como intromisiones forzadas en la intimidad aquellas actuaciones que, por las partes del cuerpo sobre las que se operan […] no constituyen según un sano criterio, violación del pudor o del recato de la persona". Con estos planteamientos expuestos la lectura/captación de huellas dactilares o imagen de la mano, por una parte, entraría en la primera categoría de inspección o registro que en absoluto supone una lesión corporal o menoscabo de la integridad física y, por otra, no afectaría al recato o pudor de la persona, no afectando así a su intimidad corporal. Ahora bien, igual que hemos llamado la atención sobre una posible afección a la integridad moral, si en la recogida de la huella se produce una humillación o envilecimiento de la persona, también puede verse afectada la intimidad corporal de la persona que, sufriendo una alteración física de una parte de su cuerpo, se ve obligada por el sistema de captación a su exposición pública. Puede plantearse una situación en la que la captación de la huella de un dedo o dedos o palma de una mano alteradas físicamente afecte al pudor de la persona. Estamos planteando la posibilidad de que, en determinados casos, personas con alteraciones físicas o edad avanzada se vean humilladas o envilecidas o afectado su pudor al tener que exponer en un dispositivo de captación del dato biométrico su mano o dedo distinto del resto.

No obstante, la doctrina del TC sobre la intimidad corporal que ha quedado expuesta, hay que incardinarla dentro de las diligencias practicables en el curso de un proceso penal y es en ese ámbito donde el TC considera los exámenes dactiloscópicos como inspecciones corporales que no afectan a la integridad corporal y tampoco afectan a la intimidad corporal al recaer sobre una parte del cuerpo, la mano, que en modo alguno puede considerarse íntima. Cosa distinta son las intervenciones corporales, como la considerada en la STC 207/1996, que implican la extracción del cuerpo de determinados elementos en las que sí cabe apreciar, aunque sea de manera leve, una afección al ámbito constitucionalmente protegido por el derecho a la integridad física. Pero la captación de una huella nunca podrá suponer una intervención corporal porque no se extrae nada del cuerpo. Posteriormente, esta Sentencia 207/1996 examinó si tal afectación del derecho a la integridad física se justificaba o no desde la razonabilidad y proporcionalidad. En resumen, el TC considera que es necesario que exista una medida de intervención corporal bien leve o grave sin consentimiento del individuo para que quede afectado el derecho fundamental a la integridad física; así, una lectura de huella

dactilar con consentimiento es inocua jurídicamente. Cosa distinta es una intervención consistente en una actividad de investigación sobre el cuerpo de la persona, lo que la Sentencia califica de registros corporales, o la extracción de elementos internos, sangre, o externos, uñas, pelo, o la obtención de una muestra de ADN. Estas actuaciones sí plantearían un conflicto con el derecho a la integridad. En todo caso, esto no ocurre en la recogida de la huella dactilar.

El Tribunal Supremo, en su Sentencia de 2 de julio de 2007, anteriormente citada, se expresa en términos coincidentes con la doctrina expuesta del Tribunal Constitucional, al resaltar, en su Fundamento de Derecho quinto, lo siguiente:

> "[…] Un mecanismo de lectura biométrica de la mano mediante un escáner que utiliza rayos infrarrojos y que es inocuo para la salud no puede considerarse lesivo para el derecho a la integridad física y moral que alegan los recurrentes. […] conviene resaltar cuáles son los contornos de ese derecho reconocido en el artículo 15 de la Constitución. Ha sido definido por el Tribunal Constitucional como "la protección de la inviolabilidad de la persona frente a ataques tendentes a lesionar su cuerpo o espíritu y frente a toda clase de intervenciones en uno de esos bienes que carezca de consentimiento del titular" (STC 120/1990, reiterada por STC 119/2001). En términos sustancialmente coincidentes, en sede académica, ha sido conceptuado como "el derecho a disponer de la propia integridad personal y a no sufrir intervención alguna en ella sin consentimiento del titular, así como a su protección frente a cualquier ataque o riesgo en una sociedad tecnológicamente avanzada".
>
> En cualquiera de estas dos aproximaciones a esa categoría se subraya el elemento de la agresión o injerencia no consentida y el resultado perjudicial, físico o moral, para quien la sufre. Pero no hay traza de nada de ello en la lectura biométrica de la mano mediante un escáner".

Así podemos sostener que la lectura biométrica de la mano mediante un escáner no representa agresión ni injerencia alguna ni física ni moral en la integridad del individuo ya que ni la tecnología utilizada, un escáner, ni la parte del cuerpo comprometida, la

mano, afectan a la integridad individual. Es en esta línea en la que se ha pronunciado el TSJ de Canarias Sala de la Contencioso-Administrativo, sección 1ª, en Sentencia de 18-9-2009, nº 190/2009, rec. 443/2007 y en Sentencia de 21 de julio de 2009, nº 171/2009, rec. 93/2007 desestima los recursos planteados. El TSJ sigue la argumentación recogida en la STS de 2 de julio de 2007. Ahora bien, cuestiones que no se abordan en estas Sentencias son las apuntadas respecto a casos concretos de personas con alteraciones anatómicas en las que sí consideramos que cabría plantear que una persona con dificultades o imposibilidad mecánica para la captación podría ver lesionado su derecho a la no "intromisión en su integridad moral".

Para terminar, y sin perjuicio de otras líneas argumentales incluidas en la Sentencia del TS, que serán objeto de comentario más adelante, y respecto a la supuesta vulneración del artículo 15 CE por el mecanismo de lectura biométrica de la mano mediante un escáner que utiliza rayos infrarrojos, el Tribunal declara que es inocuo para la salud y no puede considerarse lesivo para el derecho a la integridad física y moral. Sigue diciendo la Sentencia que respecto a los contornos de este derecho a la integridad del artículo 15 CE ha de tenerse en cuenta cómo ha sido definido por el Tribunal Constitucional entendiéndolo como "la protección de la inviolabilidad de la persona frente a ataques tendentes a lesionar su cuerpo o espíritu y frente a toda clase de intervenciones en uno de esos bienes que carezca de consentimiento del titular" (STC 120/1990 EDJ1990/6901, reiterada por STC 119/2001 EDJ2001/6004). La doctrina lo conceptúa como "el derecho a disponer de la propia integridad personal y a no sufrir intervención alguna en ella sin consentimiento del titular, así como a su protección frente a cualquier ataque o riesgo en una sociedad tecnológicamente avanzada[245]".

En todo caso -continúa exponiendo la Sentencia- el derecho a la integridad, cuya vulneración se alega, lleva incorporado un elemento de agresión o injerencia no

[245] Resulta en este punto muy ilustrativa la opinión de Rodotá, donde afirma con rotundidad la revalorización del cuerpo humano como instrumento indispensable para la definición y el reconocimiento de la identidad en el entorno electrónico, que siendo algo cotidiano en el entorno físico de relación de unas personas con otras, nos reconocemos unos a otros por nuestras características física, se ha trasladado al entorno electrónico gracias al avance de las nuevas tecnologías. De tal modo, dice Rodotá, que nuestro cuerpo "pasa a ser fuente de nueva información, una mina de la cual se extraen datos ininterrumpidamente…. Cada vez con más frecuencia se recurre a estos datos biométricos no solo con fines de identificación o como llave para el acceso a los distintos servicios, sino también como elementos para clasificaciones permanentes, para nuevas formas de control". En definitiva, el autor pone sobre la mesa la nueva amenaza a la integridad de nuestro cuerpo ya que para las nuevas tecnologías éste es una mina de información constante. RODOTÁ, S., *La vida y las reglas*… op. cit. pp. 110 y ss.

consentida y con un resultado perjudicial físico o moral, para quien lo sufre; pero lo cierto es que nada de esto puede considerarse que ocurra en la lectura biométrica de la mano mediante un escáner. Ahora bien, debemos recordar, como ha quedado expuesto en este punto, que, si evaluadas las circunstancias de cada caso la captación/tratamiento de la huella resulta ser degradante para la persona, en su propia consideración o en la de los demás, al producirse su humillación o envilecimiento, con un nivel mínimo de gravedad, entonces cabría apreciar vulneración de su integración moral.

2.2.3.2. El derecho a la intimidad

Por lo que respecta al derecho a la intimidad, este derecho se refiere al ámbito más reservado de las personas; así lo expresa STC 151/1997, de 29 de septiembre. El derecho a la intimidad está vinculado con la dignidad y el libre desarrollo de la personalidad del artículo 10.1 CE. Aunque si bien es cierto que en un gran número de ocasiones los Tribunales han tenido que amparar este derecho ante vulneraciones provenientes de excesos en el ejercicio de las libertades de expresión e información, no es este el único ámbito en el que el derecho a la intimidad despliega sus efectos. En concreto, en el ámbito laboral hemos visto cómo pueden plantearse conflictos entre el poder de dirección y control del empleador y el derecho a la intimidad del empleado. Así, la STC 186/2000, de 10 de julio, considera que es necesario deslindar lo que cabe calificar de control idóneo, necesario y equilibrado de la actividad laboral de lo que es un exceso. Asimismo, la STC 98/2000, de 10 de abril, habla claramente de injerencia en la intimidad de los trabajadores injustificada o desproporcionada. Aquí es donde entra en juego la utilización de nuevas tecnologías como la videovigilancia o sistemas de reconocimiento biométrico del trabajador y el posible conflicto con su intimidad.

Siguiendo con el análisis de los tratamientos de datos biométricos de huella dactilar desde la perspectiva del respeto a los derechos fundamentales en relación con la intimidad personal merece ser destacada la STC 37/89, de 15 de febrero. Para el TC, si bien es cierto que la intimidad corporal forma parte del derecho a la intimidad personal, el ámbito de protección de aquélla no coincide con la configuración física del cuerpo humano; es decir, el derecho a la intimidad se ve o se puede ver afectado: primero, en función de la parte del cuerpo que se vea concernida y segundo, por los instrumentos

que se emplean que puedan constituir una violación del pudor o recato de la persona; en todo caso, ello está en función de criterios culturales. De aquí se desprende que no cabe apreciar vulneración del derecho a la intimidad corporal si el tratamiento es de datos de huella dactilar obtenidos de un dedo pues no existe tal posible violación. Esta doctrina constitucional es seguida por el TSJ de Canarias que pasamos a comentar.

Como ya hemos apuntado, ha sido el orden contencioso-administrativo el que ha dictado Sentencias sobre la materia y pasamos a comentar por su exhaustividad en el análisis del supuesto de hecho la ya citada del TSJ de Canarias[246]. En dicha sentencia, el TSJ desestima el recurso contencioso-administrativo ordinario interpuesto por los sindicatos contra la orden dictada por la Consejería de Presidencia y Justicia del Gobierno de la Comunidad Autónoma de Canarias de 8 de febrero de 2007, por la que se acordó la creación y regulación del fichero de datos de control horario del personal al servicio de la Administración de Justicia. La Sala de lo contencioso-administrativo del TSJ resuelve el recurso después de que las actuaciones pasaran por varios Juzgados.

Esta Sentencia es objeto de nuestro interés al incorporar el fichero de datos de control horario del personal datos biométricos de los empleados y/o funcionarios provenientes de un mecanismo de lectura biométrica de la mano mediante escáner que utiliza rayos infrarrojos. La captación por infrarrojos de una imagen tridimensional de la mano acaba convertida en un registro de nueve bytes o nueve octetos que se incorpora al citado fichero de datos de control. Los recurrentes consideran que puede resultar atentatorio a los derechos de las personas, al constituir una intromisión ilegítima en la esfera de su intimidad, e incluso lesivo de su derecho a la integridad física y moral, la lectura biométrica de la mano mediante un escáner que utiliza rayos infrarrojos. Esta Sentencia, recogiendo los planteamientos de la Sentencia previa del TSJ de Cantabria[247], no considera atentatorio a ningún derecho fundamental de la persona la captación y el uso de estos registros o plantillas.

En cuanto a la argumentación de los recurrentes, parte actora, solicitan la nulidad de la Orden de 8 de febrero de 2007 por la que se acuerda la creación y regulación del fichero

[246] Recordemos la referencia de la misma: (sede Santa Cruz de Tenerife), Sala de lo Contencioso-Administrativo, sec. 1ª, S 18-9-2009, nº 190/2009, rec. 443/2007. Pte: Alonso Dorronsoro, Rafael, EDJ 2009/290461.
[247] Sentencia del TSJ de Cantabria, Sala de lo Contencioso-Administrativo, S 23-1-2003, rec. 166/2002.

de datos de control horario del personal al servicio de la Administración de Justicia al entender: 1º que la captación de la imagen de la huella dactilar vulnera el derecho a la intimidad personal y supone una intromisión en la esfera personal del individuo. 2º Con base en la jurisprudencia del Tribunal Constitucional, cabe hablar de una conexión entre intimidad, libertad y dignidad de la persona que implica que la esfera de la inviolabilidad de la persona frente a injerencias externas ha de entenderse en el ámbito personal y familiar con proyecciones al exterior, es decir, que comprendería hechos referidos a las relaciones sociales y profesionales. Así pues, la Administración no está apoderada, aun con el pretexto del ejercicio de facultades de vigilancia y control, para realizar intromisiones ilegítimas en la intimidad de los funcionarios en los centros de trabajo. 3º En todo caso, la actora argumenta que la medida no cumple con el principio de proporcionalidad, en su triple faceta: juicio de idoneidad, juicio de necesidad y juicio de proporcionalidad en sentido estricto. Por tanto, y en definitiva, se produce una vulneración del artículo 18, apartados 1 a 4 CE.

La administración demandada contesta a la demanda solicitando su desestimación entendiendo, entre otros argumentos expuestos, que el derecho a la intimidad no es un derecho absoluto. Muy al contrario, debe existir un equilibrio derivado del principio de proporcionalidad entre dicho derecho y las facultades del empresario que sí se respetan en el presente caso.

Entrando ya en la resolución del recurso, y en cuanto a la segunda línea argumental (la primera referida al derecho a la integridad ya ha quedado comentada más arriba) de los recurrentes, referente a la infracción de la intimidad corporal (artículo 18.1 CE), el Tribunal también desestima esta línea atendiendo a los términos en que el Tribunal Constitucional ha conformado este derecho que tiene un indudable componente cultural. Derivado de ese componente cultural no cabe considerar que la captación por infrarrojos de una imagen tridimensional de la mano, dada la parte del cuerpo y el sistema de captación utilizado, sea una intromisión ilegítima en la esfera de la intimidad. La lectura de las dimensiones, largo, ancho y grosor de la mano acaba convertida en un registro de nueve bytes que, posteriormente, mediante tratamiento informático se relaciona con otros datos para identificar a los empleados públicos y así controlar el cumplimiento del horario de trabajo. Nada en este proceso atenta a la intimidad corporal del individuo.

Por otra parte, los recurrentes también adujeron en su recurso infracción del derecho a no sufrir menoscabo en la integridad física y psíquica pero ahora con base en el artículo 14[248] de la Ley 31/1995 en relación con derecho a la salud.

También se descartó infracción alguna en este sentido, ya que los recurrentes no aportaron elemento alguno que permitiera sostener que es nocivo para la salud el sistema de lectura tridimensional de la mano de una persona por rayos infrarrojos. Por el contrario, la administración recurrida presentó informes técnicos que excluían la posibilidad de que el sistema fuera dañino para la salud.

Para concluir, debemos tener en cuenta que en la jurisprudencia de nuestros tribunales se establece una estrecha relación entre la intimidad corporal y el concepto de pudor, concepto esencialmente cultural. Además, se establece una neta diferencia entre esta intimidad corporal y la intimidad personal que es un concepto mucho más amplio. De

[248] Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales. Con arreglo al art. 14 (Derecho a la protección frente a los riesgos laborales): "1. Los trabajadores tienen derecho a una protección eficaz en materia de seguridad y salud en el trabajo. El citado derecho supone la existencia de un correlativo deber del empresario de protección de los trabajadores frente a los riesgos laborales.
Este deber de protección constituye, igualmente, un deber de las Administraciones públicas respecto del personal a su servicio.
Los derechos de información, consulta y participación, formación en materia preventiva, paralización de la actividad en caso de riesgo grave e inminente y vigilancia de su estado de salud, en los términos previstos en la presente Ley, forman parte del derecho de los trabajadores a una protección eficaz en materia de seguridad y salud en el trabajo.
2. En cumplimiento del deber de protección, el empresario deberá garantizar la seguridad y la salud de los trabajadores a su servicio en todos los aspectos relacionados con el trabajo. A estos efectos, en el marco de sus responsabilidades, el empresario realizará la prevención de los riesgos laborales mediante la integración de la actividad preventiva en la empresa y la adopción de cuantas medidas sean necesarias para la protección de la seguridad y la salud de los trabajadores, con las especialidades que se recogen en los artículos siguientes en materia de plan de prevención de riesgos laborales, evaluación de riesgos, información, consulta y participación y formación de los trabajadores, actuación en casos de emergencia y de riesgo grave e inminente, vigilancia de la salud, y mediante la constitución de una organización y de los medios necesarios en los términos establecidos en el capítulo IV de esta ley.
El empresario desarrollará una acción permanente de seguimiento de la actividad preventiva con el fin de perfeccionar de manera continua las actividades de identificación, evaluación y control de los riesgos que no se hayan podido evitar y los niveles de protección existentes y dispondrá lo necesario para la adaptación de las medidas de prevención señaladas en el párrafo anterior a las modificaciones que puedan experimentar las circunstancias que incidan en la realización del trabajo.
3. El empresario deberá cumplir las obligaciones establecidas en la normativa sobre prevención de riesgos laborales.
4. Las obligaciones de los trabajadores establecidas en esta Ley, la atribución de funciones en materia de protección y prevención a trabajadores o servicios de la empresa y el recurso al concierto con entidades especializadas para el desarrollo de actividades de prevención complementarán las acciones del empresario, sin que por ello le eximan del cumplimiento de su deber en esta materia, sin perjuicio de las acciones que pueda ejercitar, en su caso, contra cualquier otra persona.
5. El coste de las medidas relativas a la seguridad y la salud en el trabajo no deberá recaer en modo alguno sobre los trabajadores."

ahí que el TC, en su Sentencia 37/89 de 15 de febrero, afirme que: "La Constitución garantiza la intimidad personal (artículo 18.1), de la que forma parte la intimidad corporal". Con ello vemos que los rasgos morfológicos externos de una persona, su aspecto físico exterior, no son íntimos y se protegen por el derecho fundamental a la propia imagen. Y respecto a los rasgos internos, el TS, en Sentencia de 18 de enero de 1993, siguiendo la doctrina del TC en la citada Sentencia 37/1989, afirma que "no pueden entenderse como intromisiones forzadas en la intimidad aquellas actuaciones que, por las partes del cuerpo humano sobre las que operan o por los instrumentos mediante los que se realizan, no constituyen, según un sano criterio, violación del pudor o recato de la persona". Podemos afirmar, entonces, que no son intromisiones en la intimidad una actuación en el cuerpo como es la lectura de huella dactilar porque no cabe hablar de violación del pudor o recato de la persona, cuestión distinta el acceso a los datos que se han obtenido que sí puede ser una intromisión en la intimidad. Por eso el TC en su sentencia 207/1996, de 16 de diciembre, ha determinado que la finalidad de un análisis o lo que se pretende averiguar puede vulnerar el derecho a la intimidad personal, aunque sea inocuo respecto de la intimidad corporal. Pero, además, debemos tener en cuenta que el pudor, que como hemos visto la jurisprudencia directamente vincula con la intimidad corporal, no es un concepto monolítico y único para todos los individuos, muy al contrario, es distinto en personas con alguna discapacidad, alteración física, o simplemente con corta edad o edad avanzada. Algunos colectivos de personas con alteraciones físicas en sus manos, por el mero hecho de que el sistema obligue a su exposición pública ya ven afectado su ámbito de intimidad corporal.

2.2.3.3. El Derecho a la Propia imagen.

Abordaremos la cuestión de deslindar la imagen como dato dentro de los datos biométricos. Es indudable que la imagen es un medio directo y en muchos casos inequívoco de identificación de una persona. Podemos afirmar que la propia imagen tiene dos proyecciones una interna o introspectiva que atañe al propio individuo y otra externa[249]. Tanto la proyección interna del concepto que cada uno tenemos de nosotros

[249] REBOLLO DELGADO, L., "El derecho a la propia imagen y la imagen como dato", *Revista española de Protección de Datos*, 5 Julio-Diciembre, 2008, Thomson, Civitas, p. 158.

mismos como la externa han de ser acordes, han de permanecer unidas no han de quedar disociadas. En Europa el primer reconocimiento en derecho positivo del derecho a la propia imagen se sitúa en Alemania en 1907. La evolución normativa en esta materia ha experimentado tres fases: una inicial en la que no existía reconocimiento autónomo sino más bien confusión con el derecho al honor o con el derecho a la intimidad; una segunda fase imbuida por la responsabilidad extracontractual nacida de la culpa o negligencia que con un marcado carácter patrimonial pretendía la indemnización del daño causado y, por último, la fase de reconocimiento constitucional del derecho a la propia imagen de forma autónoma teniendo su fundamento en la dignidad del ser humano y en su libertad.

El derecho a la propia imagen protege la proyección exterior de la imagen de la persona actuando a modo de escudo para evitar injerencias no deseadas (STC 139/2001, de 18 de junio). Además, este derecho vela por la protección de la concreta imagen externa que cada uno tenemos (STC 156/2001, de 2 de julio) y, por ende, preserva nuestra imagen pública (STC 81/2001, de 26 de marzo). El TC está afirmando que este derecho está íntimamente condicionado por la actividad de cada sujeto. En este sentido la STC 99/1994, de 11 de abril, afirma que no sólo las personas con una actividad pública, al estar más expuesta su imagen, deben verse protegidas, sino que cualquier persona tiene derecho a ver protegida su imagen si ésta aparece desvinculada de su ámbito laboral propio.

El carácter autónomo de este derecho se ha desprendido del hecho de que es posible lesionar el derecho a la propia imagen sin vulnerar el honor o la intimidad de la persona. Si aceptamos la definición de imagen ofrecida por el Diccionario de la Real Academia Española de la Lengua como “la reproducción de los rasgos físicos de una persona sobre un soporte material cualquiera” el derecho a la propia imagen no es sino la facultad de toda persona para permitir o no la captación y reproducción de su imagen física. Este derecho preserva un ámbito propio de cada sujeto frente a la acción, captación y reproducción, por los demás. Gitrama define el derecho a la propia imagen como “un derecho innato de la persona, que se concreta en la reproducción o representación de la figura de ésta, en forma visible y reconocible. Es un derecho subjetivo de carácter privado y absoluto. Es un derecho personalísimo, pero dotado de un contenido potencialmente patrimonial. Es un derecho inalienable e irrenunciable y en general

inexpropiable… en fin, es un derecho imprescriptible"[250]. El derecho a la propia imagen lo que protege es la captación y reproducción de la imagen física de un sujeto, a través de cualquier medio. Se protege un ámbito propio y reservado del sujeto que sin ser íntimo sí está amparado frente a la acción y reconocimiento de los demás. Entendido así el ámbito de protección del derecho a la propia imagen no se puede considerar el ámbito propio de protección del dato biométrico dactiloscópico puesto que la imagen facial-corporal del individuo no es equiparable a su huella dactilar. Tampoco la protección a la imagen como dato de carácter personal es el ámbito adecuado por la misma razón y, en este sentido, recordamos que la normativa de videovigilancia no es aplicable al dato dactiloscópico.

El TEDH, en su Sentencia de 4 de diciembre de 2008[251], cita el asunto *Friedl* tratado por la Comisión en relación a la conservación de fotografías anónimas. En este asunto la Comisión consideró que la conservación de fotografías anónimas tomadas durante una manifestación pública no se consideraba una injerencia en la vida privada. Llegó a esta conclusión al conceder un peso particular al hecho de que las fotografías en cuestión no hubiesen sido registradas en ningún sistema de tratamiento de datos y a que las autoridades no hubiesen adoptado medidas para identificar a las personas fotografiadas recurriendo al tratamiento de datos [Sentencia *Friedl*, opinión de la Comisión[252]]. A la luz de esta Sentencia entendemos que el Tribunal considera una fotografía anónima no como dato de carácter personal no en un sentido ontológico sino instrumental ya que el Tribunal así lo consideró porque no habían sido incorporadas a ningún sistema de tratamiento de datos que hubiera permitido identificar a las personas. Por ello, *a sensu contrario*, la fotografía tratada con medios técnicos que permita la identificación del individuo sí es dato personal y, en concreto, dato biométrico.

[250] GITRAMA: Voz "imagen, derecho a". *Nueva Enciclopedia Jurídica.* Tomo XI. Barcelona 1962, p. 326. Citado por REBOLLO DELGADO, L, SERRANO PÉREZ, M. M., *Manual de protección…,* op. cit., p. 263.

[251] S. *and Marper v. The United Kingdom* [GC], n.º 30562/04 y 30566/04, 04.12.2008.

[252] *Friedl v.* Austria, 31 de enero de 1995, serie A núm. 305-B, opinión de la Comisión, §§ 49-51. La Comisión estudió la toma y conservación de fotografías de un residente austriaco durante una manifestación pública en la que participó. La Comisión europea de Derechos Humanos al referirse las fotografías a un acontecimiento público, al haber sido capatadas sin interferir en el esfera privada del individuo, ser la la finalidad de las fotografías dejar constancia de la naturaleza del acontecimiento para facilitar la investigación sobre posible infracción de normativa de tráfico, al no haber sido incorporadas a bases de datos automatizadas no habiéndose tomado medidas para identificar a las personas, consideró por todo ello que no se había producido injerencia en el derecho protegido por el artículo 8.1 del CEDH.

El RGPD, en su Considerando (51), hace expresa referencia a esta cuestión al decir: "El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física". Parece que el RGPD equipara la fotografía que permita la identificación o autenticación de una persona con la categoría de dato biométrico especialmente protegido.

2.3 La dignidad humana y el tratamiento de datos biométricos: puntos de conflicto.

La recogida y tratamiento de datos biométricos supone recoger datos del cuerpo de una persona y esto puede conllevar, "graves riesgos éticos"[253]. Aunque si bien es cierto que el dato biométrico en general y, en concreto, el dactiloscópico no tiene por qué revelar un dato de salud de una persona, hay ocasiones en que esto sí ocurre. Y es en aquellos casos en los que el tratamiento del dato biométrico dactiloscópico puede tener puntos de conexión con la dignidad humana. Y de ahí igualmente que deba tener la consideración de dato sensible, o en terminología del RGPD, ser "una categoría especial de dato personal". Dato biométrico dactiloscópico revelador de dato de salud implica afectación de la dignidad humana y necesidad de ser sometido a normas de especial protección en su tratamiento. Y esta conexión del dato dactiloscópico con la dignidad puede derivarse, no solo de la revelación de datos de salud sino también, por las técnicas encubiertas por las que algunos sistemas pueden recabar secretamente información sobre características del propio organismo humano.

[253] PÉREZ GÓMEZ, J. M., "La protección de los datos de salud", en Rallo Lombarte, A. y García Mahamut, R., (editores), *Hacia un nuevo derecho europeo de protección de datos,* Valencia, Tirant lo blanch, 2015, p. 630.

2.3.1. Discapacitados o personas cuyas características físicas no se corresponden con las normas técnicas.

Hemos hecho referencia en el capítulo anterior, y en este mismo capítulo, a la idea de que los sistemas de captación de la huella dactilar pueden revelar inevitablemente información sobre enfermedades o una discapacidad y esa situación requiere arbitrar, por una parte, medidas que garanticen la dignidad humana en la captación y, por otra, medidas de protección de los datos obtenidos. En este sentido, ya se expresó el Comité Consultivo de la Convención para la protección de las personas respecto al proceso automatizado de los datos de carácter personal, en su informe de situación relativo a la aplicación de los principios de la Convención 108 a la recogida y al proceso de los datos biométricos elaborado en su 21ª reunión del 2-4 febrero de 2005.

La captación del dato dactiloscópico de una persona con una discapacidad (por ejemplo, una polidactilia) convierte el dato dactiloscópico en dato especialmente protegido obligando desde la misma fase de recogida a la implantación de medidas de seguridad de nivel alto de conformidad con lo exigido por el RLOPD.

El GPD 29 bajo el epígrafe "*Impossibility of enrolment*" en su Dictámen núm. 3/2007, ya citado en páginas anteriores,[254] hace referencia al hecho de exclusión en la participación o adhesión a un sistema de un grupo de la población. Estima el GPD 29 en este Dictámen que alrededor del 5% de la población, al no disponer de huellas dactilares legibles, no pueden participar en el proceso de solicitud de un visado; en definitiva, quedan fuera del sistema. Sobre un volumen aproximado anual de veinte millones de solicitudes de visado, estamos hablando de que cerca de un millón de personas se ven explulsadas del sistema al no poder físicamente incorporar a él. Estos individuos no deberían ser víctimas de una carencia del sistema técnico que no puede leer sus huellas. En efecto, no deberían verse estigmatizados por la ilegibilidad de sus huellas. Por ello, dada la posibilidad real de exclusión se recomienda en la tercera conlusión del

[254] Disponible en http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp134_en.pdf [Fecha de consulta: 12/09/2018].

Dictámen que el proceso de solicitud de visado esté siempre informado por el respeto de la dignidad humana y los derechos fundamentales[255].

2.3.2. Revelación inútil pero inevitable de datos de salud.

Aunque en muchos sistemas no sea acorde con la finalidad del tratamiento, en éste se revelan datos sobre enfermedad o discapacidad de los usuarios. Veremos cómo en las huellas dactilares, los perfiles de ADN[256] o en las muestras celulares hay una base física que en distinto grado puede afectar su obtención o extracción del cuerpo humano a los derechos de la personalidad apuntados bien sean la dignidad, la integridad. Aunque en el caso de la huella en poco afecta o al menos así lo ha entendido la jurisprudencia nacional, como veremos. Cuestión distinta es la información que como elemento inmaterial se deriva de la huella o del perfil o de la muestra en cuyo tratamiento posterior, automatizado o no, interviene otro ámbito de protección, el del derecho a la autodeterminación informativa, que se verá en el siguiente epígrafe.

Podríamos concluir afirmando que en el tratamiento de datos biométricos, y en concreto dactiloscópicos, por la parte del cuerpo a la que afectan, sobre la que no cabe apreciar un especial recato en su exhibición, no cabe apreciar vulneración del derecho a integridad corporal, ni a la intimidad corporal, con las salvedades apuntadas en relación con determinados grupos de presonas que por sus características físicas especiales, o bien, quedan por ello fuera del sistema o el simple hecho de incorporarse al sistema afecta a su integridad moral y/o intimidad corporal. Cuestión distinta son los debates jurídicos que suscita el tratamiento de los datos biométricos en relación con el derecho fundamental a la protección de datos personales, que entrañan mayor relevancia y que apuntaremos a continuación.

---

[255] Ibíd., "3. *With regard to the inclusion of biometric data and the possible use of fingerprints in connection with visa applications, account should be taken of human dignity and fundamental rights implications*".

[256] El Consejo de Europa ya advierte del potencial discriminatorio del Genoma humano y así el artículo 11 del Convenio Europeo sobre los derechos humanos y la biomedicina establece: "Artículo 11. No discriminación. Se prohíbe toda forma de discriminación de una persona a causa de su patrimonio genético". Convenio Europeo sobre los derechos humanos y la biomedicina: Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina. http://www.colmed2.org.ar/images/code04.pdf [Fecha de consulta: 12/09/2018].

2.4. La autodeterminación informativa en la captación del dato biométrico dactiloscópico.

En el momento de la recogida del dato dactiloscópico, el derecho fundamental a la protección de datos de carácter personal, o también llamado derecho a la autodeterminación informativa, tiene un papel fundamental en lo que se refiere a los requisitos jurídicos que deben presidir el proceso de recogida o captación aludido. Es el principio de calidad (art. 4 LOPD) y en la nueva LO 3/2018 podemos ubicarlo como principio de exactitud (art. 4), el que preside esta fase recopilatoria y, en virtud de él, únicamente queda autorizada la recogida de datos personales cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas que fundamentan esa recogida. El principio de calidad en el momento de la recogida se entiende a través de tres subcriterios o subprincipios: la adecuación, la pertinencia y la proporcionalidad. O como bien lo expresa López Aguilar, la licitud del tratamiento ha de basarse en "… los criterios de necesidad y de proporcionalidad como sustrato de la licitud del tratamiento de datos, en conjugación con el principio de finalidad legítima del tratamiento de datos y, en su caso, del acceso"[257]. A todos ellos aludiremos más adelante. De momento, es imprescindible delimitar el concepto de dato de carácter personal y determinar si el dato biométrico dactiloscópico reúne las características de ese concepto.

2.4.1. La formulación constitucional: El artículo 18.4 CE.

Tal y como apuntamos en la primera parte de este capítulo, el principal debate jurídico que suscita el tratamiento de datos biométricos, y en particular el de los datos dactiloscópicos, es en relación con el derecho fundamental a la protección de datos. Es decir, la legitimidad de algunos tratamientos de datos biométricos se debe estudiar a la luz de principios como los de finalidad y proporcionalidad, puesto que sólo respetando estos principios cabe aceptar la limitación al derecho fundamental a la protección de datos que el tratamiento de datos biométricos puede suponer o entrañar. Para todo ello, deberemos analizar: 1º cómo el tratamiento de datos biométricos es un tratamiento de

[257] Cfr. Sentencia TJUE, caso *Gaskin c. Reino Unido*, 7 de julio de 1989. LÓPEZ AGUILAR, J. F., op. cit., p. 561.

datos personales y supone una limitación al derecho fundamental aludido y, 2º la legitimidad del tratamiento depende de si la vulneración al derecho fundamental es ajustada a los principios y derechos de la protección de datos y, en especial, a los principios apuntados de finalidad y proporcionalidad. En este contexto, juega un papel determinante el artículo 18. 4 CE, artículo de una trascendental importancia en esta materia y que, de hecho, en el Preámbulo de la LO 3/2018, es calificado de "anclaje" en "el reconocimiento de un sistema de garantía de los derechos digitales"[258]. La vigente Ley Orgánica de protección de datos personales comienza su Preámbulo estableciendo como base constitucional de la protección de las personas físicas, en relación con el tratamiento de sus datos personales, este artículo 18.4 CE. Como bien ha puesto de relieve la doctrina, la CE desde un enunciado de limitación (negativo) y a la vez instrumental, en el sentido de servidor de otros derechos (honor e intimidad), configura el punto de arranque del que ha llegado a ser un derecho fundamental autónomo, y que incluso para algunos autores, como Ull Pont, es un derecho fundamental de libertad en el sentido de cauce de ejercicio libre, pleno, de cualquier otro derecho frente a la informática[259]. Así, en nuestro Derecho positivo el libre y pleno ejercicio de los derechos por el individuo, la información y el tratamiento automático de ésta se relacionan entre sí de tal modo que hacen surgir un nuevo derecho de libertad individual en el entorno automatizado. Se puede considerar un nuevo derecho porque otros, ya conocidos y afianzados en el ordenamiento como intimidad u honor, sin aquél no alcanzan a cubrir o proteger un área de libertad de las personas cuya existencia se ha evidenciado o revelado al tratar sus datos automáticamente. Por ello, el dato de carácter personal, como elemento sobre el que se basa el tratamiento automático de la información, es amparado por la CE que configura en torno a él un derecho con rango de derecho fundamental[260].

[258] BOE, 6 de diciembre de 2018, Sec.I. Pág. 119795, IV.

[259] Para Ull Pont la CE, en su artículo 18.4, configura un derecho fundamental de libertad para el individuo para ejercer cualquier derecho cuando éste se enfrente al uso de la información de forma automática. Consideramos que esta misma visión amplia, incluso podríamos calificar de "panteística", es la que plantea la nueva LO 3/2018 al considerar al artículo 18.4 CE "anclaje" de los nuevos derechos digitales. ULL PONT, E., op. cit. p. 47.

[260] Conviene señalar desde este momento inicial la diferencia entre la configuración de un derecho como derecho fundamental y la consideración de un derecho como principio rector de la política social y económica. Como veremos, el derecho a la protección de datos es un derecho fundamental tanto en Derecho interno como europeo, como también lo es el derecho a la vida y a la integridad física. Los derechos fundamentales tienen una vertiente prestacional, objetiva, que por ejemplo en el caso del derecho a la vida se concreta en la labor activa de los poderes públicos en garantía del mantenimiento de la vida y la integridad física a través de la atención sanitaria. Pero el derecho a la protección de la salud no es un derecho fundamental sino un principio rector de la política social y económica que, en definitiva,

La Ley Fundamental de Bonn y el Tribunal Constitucional Federal alemán han configurado un derecho general de libertad sobre una interpretación que el propio Tribunal hizo del derecho al libre desarrollo de la personalidad establecido en el artículo 2.1 de la Ley Federal. La Constitución confiere, no solo derechos a determinadas libertades o derechos frente a determinadas discriminaciones, sino que en opinión de Alexy[261] reconoce la existencia de un derecho general de libertad, de cuyo análisis cabría plantear el fundamento del derecho a la protección de datos personales. Este derecho general de libertad "puede extenderse -más allá de la protección de acciones- a la protección de situaciones y posiciones jurídicas del titular del derecho fundamental. Protege entonces, no solo su hacer, sino también su ser fáctico y jurídico. (…) el derecho general de libertad se ha convertido en un derecho exhaustivo de libertad general frente a intervenciones[262]".

Ya hemos visto que el artículo 18.1 CE garantiza el derecho a la intimidad personal. Ahora nos detendremos en su apartado 4. Este apartado dispone que la ley limitará el uso de la informática para garantizar la intimidad personal de los ciudadanos; la LOPD es la que reguló tal derecho fundamental, estableciendo a través de su articulado un conjunto de garantías a favor de los interesados, para el uso adecuado y legítimo de los

---

lo que supone es una directriz que orienta al legislador positivo, al juez y a los poderes públicos en su actuación. Ello supone que, por ejemplo, el derecho a la salud, solo puede ser alegado en la medida y con el contenido en que haya sido desarrollado por una ley no teniendo, como tal principio rector o directriz, una aplicación inmediata. Sin embargo, el derecho a la protección de datos como derecho fundamental que es sí tiene una vertiente objetiva *ex constitutione* exigible a los poderes públicos y un contenido esencial sin necesidad de estar a expensas del desarrollo legislativo posterior. Cfr. TRONCOSO REIGADA, A., *La protección de datos personales…,* op. cit., p. 1104. Así mismo, es muy esclarecedora la exposición del Magistrado Jiménez de Parga en su voto particular a la Sentencia del Pleno del TC 290/2000 al decir que él parte de: "[..] una distinción tripartita: valores superiores, constitucionalizados en el artículo primero de la Constitución, que, no obstante, carecen de especificaciones respecto a los supuestos en que deben ser aplicados: orientan la interpretación y aplicación de las normas. En segundo lugar, principios generales del derecho, no recogidos en el texto de la Constitución, o acogidos como principios rectores, los cuales informan el ordenamiento constitucional, además de ser faros en la tarea de interpretación y aplicación, pudiendo ser normas subsidiarias. En tercer lugar, pero en posición prevalente, los principios constitucionalizados, reconocidos y protegidos por la Constitución, que son los fundamentos mismos del sistema jurídico-político, a partir de los cuales se despliega todo el aparato de normas. Estos principios constitucionales y constitucionalizados poseen la fuerza vinculante de las normas jurídicas, son fuente normativa inmediata, en el sentido profundo de no necesitar de la interposición de regla, o circunstancia alguna, para alcanzar su plena eficacia.
Con estos principios constitucionales, de aplicación directa, y el apoyo de determinados derechos expresamente reconocidos en la Constitución de 1978, así como en textos internacionales, es posible extender la tutela a ciertos derechos de singular relieve e importancia en el actual momento de la historia. Tal es el derecho fundamental de libertad informática." TC Pleno, S 30-11-2000, nº 290/2000, BOE 4/2001, de 4 de enero de 2001, rec. 236/1993; 226/1993; 201/1993; 219/1993.

[261] ALEXY, R., op. cit., pp. 331 y ss.

[262] Ibíd, p. 334.

datos personales; actualmente es la LO 3/2018 la que se ocupa de ello. En la interpretación de este artículo 18.4, el Tribunal Constitucional viene estableciendo que tal precepto contempla "un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama la informática" (STC 254/1993, de 20 de julio, FJ 6, doctrina que se reitera en las SSTC 143/1994, de 9 de mayo, FJ 7: " […] se ha afirmado que, ya que "los datos personales que almacena la Administración son utilizados por sus autoridades y servicios", no es posible "aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión" (STC 254/1993, fundamento jurídico 7.). En consecuencia, habría que convenir en que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta"[263].

La nueva LO de protección de datos destaca en su Preámbulo dos de las Sentencias que el TC ha dictado, en este largo camino ya de configuración del derecho fundamental que nos ocupa; estas Sentencias son la 94/1998, de 4 de mayo, y la 292/2000, de 30 de noviembre.

Pero, sin duda, destaca con luz propia la importantísima sentencia del pleno del TC, de fecha 30-11-2000, núm. 290/2000, BOE 4/2001, de 4 de enero de 2001, rec. 236/1993; 226/1993; 201/1993; 219/1993, que establece una doctrina, seguida por muchas otras sentencias posteriores, en relación con lo que denomina un "haz de facultades" que confiere a su titular el derecho fundamental a la protección de datos. Derecho fundamental que "garantiza a la persona un poder de control y disposición sobre sus datos personales", pues "confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus

[263] TC, Sala 1ª, S 09-05-1994, nº 143/1994, BOE 140/1994, de 13 de junio de 1994, rec. 3192/1992. Véanse, asimismo, Sentencias 11/1998, de 13 de enero, FJ 4; 94/1998, de 4 de mayo, FJ 6, y 202/1999, de 8 de noviembre, FJ 2).

datos personales a conocer los mismo y, para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos" (Fundamento de Derecho Séptimo); la misma sentencia del TC concluye que "el derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos, de suerte que es sobre dichos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia del derecho fundamental aquí considerado por parte de las Administraciones Públicas competentes" (FJ 7). Merece ser destacado el voto particular emitido por el Magistrado D. Manuel Jiménez de Parga y Cabrera, al que presta su adhesión el Magistrado D. Rafael de Mendizábal Allende, en esta Sentencia. En él recoge la necesidad de reconocer de modo explícito la existencia de "[…] un derecho fundamental, el derecho de libertad informática, que no figura en la Tabla del texto de 1978". Puesto que, sigue diciendo, "[…] una de las tareas importantes de los Tribunales Constitucionales es extender la tutela a determinadas zonas del Derecho no expresamente consideradas en las correspondientes Constituciones, cuando, como ocurre en el presente caso, es necesario hacerlo para que no queden a la intemperie, sin techo jurídico alguno, intereses esenciales de los ciudadanos". El Fundamento tercero del voto particular recuerda que "la STC 254/1993, FJ 6, mencionó, por vez primera en nuestra jurisprudencia, la libertad informática, entendida como un derecho fundamental "en sí mismo"". Y apunta que otra base para la construcción del derecho fundamental la puso el artículo 18.4 de la Constitución. Ahora bien, dice Jiménez de Parga, "a mi entender, la libertad informática, en cuanto derecho fundamental no recogido expresamente en el texto de 1978, debe tener como eje vertebrador el art. 10.1 CE, ya que es un derecho inherente a la dignidad de la persona. Tal vinculación a la dignidad de la persona proporciona a la libertad informática la debida consistencia constitucional". Y sigue mencionando como cimientos de la "libertad informática" otros preceptos constitucionales (18.1; 20.1; 10.2) no reduciendo así al artículo 18.4 el único "cimiento" del nuevo derecho fundamental.

El artículo 18.4 CE, asumiendo la tensión existente entre informática e intimidad o, lo que es lo mismo, entre el uso masivo e invasivo de la informática y la salvaguarda de la

vida privada, ha proporcionado los cimientos del posterior edificio de la protección jurídica del dato de carácter personal. Literalmente este artículo 18.4 establece: *"*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*"*[264]. Es nada menos que uno de los derechos comprendidos entre los de mayor protección en la Constitución el que ha marcado el punto de arranque de este nuevo derecho. En su formulación inicial, a través del citado artículo 18.4, el enfoque atendía a una protección defensiva de la intimidad frente al ataque de la informática. Una protección negativa en la que la informática aparecía teñida de un carácter de riesgo que, sin ser un planteamiento erróneo, sin embargo, no agota todo el contenido del derecho a la protección de datos que, sin duda, tiene una vertiente positiva de ejercicio de la libertad personal, de control del ciudadano-individuo sobre sus datos[265].

Arzoz Santisteban[266] habla de una doble dimensión, instrumental y autónoma, del derecho fundamental consagrado en el artículo 18.4. En su dimensión instrumental el art. 18.4 es garantía de otros derechos fundamentales como el honor y la intimidad y así lo reconoce la STC 254/1993, en su Fundamento Jurídico 6, sin perjuicio de su carácter autónomo, al afirmar:

> "(…)
> Dispone el art. 18.4 C.E. que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona,

[264] Como señala Sempere Rodríguez, este apartado 4 del artículo 18 presentó otras redacciones, en concreto, en el anteproyecto (B.O.C., de 5 de enero de 1978) decía: "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos" y este texto se mantuvo en el informe de la ponencia (B.O.C., 17 de abril de 1978). La redacción definitiva añadiendo "…y el pleno ejercicio de sus derechos" se produjo en el Dictamen de la Comisión del Congreso (B.O.C., 1 de julio de 1978). SEMPERE RODRÍGUEZ, C., op. cit. p. 427.

[265] En este sentido, el TC, en su Sentencia 292/2000, de 30 de noviembre, define, en su Fundamento Jurídico 7º, el derecho a la autodeterminación informativa como el: "poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso". Este derecho a la autodeterminación encarna el carácter positivo o la vertiente positiva del derecho a la protección de datos. TC Pleno, S 30-11-2000, nº 292/2000, BOE 4/2001, de 4 de enero de 2001, rec. 1463/2000.

[266] ARZOZ SANTISTEBAN, X., op.cit., p. 127.

de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática".

El primer problema que este derecho suscita es el de la ausencia, hasta un momento reciente, en todo caso posterior a los hechos que dan lugar a la presente demanda, de un desarrollo legislativo del mismo. Ahora bien, a esa ausencia de legislación no se pueden enlazar las desmesuradas consecuencias que postula el Abogado del Estado. Aun en la hipótesis de que un derecho constitucional requiera una interpositio legislatoris para su desarrollo y plena eficacia, nuestra jurisprudencia niega que su reconocimiento por la Constitución no tenga otra consecuencia que la de establecer un mandato dirigido al legislador sin virtualidad para amparar por sí mismo pretensiones individuales, de modo que sólo sea exigible cuando el legislador lo haya desarrollado. Los derechos y libertades fundamentales vinculan a todos los poderes públicos, y son origen inmediato de derechos y obligaciones, y no meros principios programáticos. Este principio general de aplicabilidad inmediata no sufre más excepciones que las que imponga la propia Constitución, expresamente o bien por la naturaleza misma de la norma (STC 15/1982, fundamento jurídico 8º).
(…) .”

Es evidente que se expresa la doble dimensión del derecho recogido en el artículo 18.4 CE, por un lado, servidora de otros derechos y, por otro, de total autonomía al poder contemplar un nuevo derecho, el derecho a la libertad informática.

El Tribunal Constitucional en esta Sentencia es contundente: cabe reconocer un derecho autónomo[267] a la libertad frente a la informática. Por tanto, es innegable su dimensión autónoma derivada de la existencia de un bien jurídico independiente que resulta amparado. Este bien jurídico puede formularse como el control del flujo de información, o "de un uso ilegítimo del tratamiento mecanizado de datos" sobre un individuo. Difícilmente se puede hablar de un derecho de libertad frente al tratamiento mecanizado de datos personales sin que exista un poder de control del individuo sobre esos datos.

En definitiva, el dato de carácter personal recibe, a través de la ubicación en su génesis en el artículo 18.4 CE, la máxima protección que el ordenamiento jurídico español otorga a un bien o a un derecho de la personalidad. Y así, de esta formulación constitucional se deriva un derecho de toda persona equiparable al derecho a la vida o a la libertad.

La Constitución española del 78 es una de las primeras en introducir la protección de los datos frente al uso de la informática. Es en los años 70 cuando se comienza a plantear, por la doctrina especializada y en leyes incipientes, los peligros que puede entrañar el archivo y uso ilimitado de los datos informáticos. Posteriormente se especificaría y configuraría el concepto de dato de carácter personal y su protección frente a su tratamiento automatizado o no. Una primera interpretación llevó a considerar este derecho como una especificación del derecho a la intimidad, pero el Tribunal Constitucional ha interpretado que se trata de un derecho independiente, aunque obviamente estrechamente relacionado con aquél (SSTC 254/1993, de 20 de julio y 290/2000, de 30 de noviembre). La jurisprudencia del TC ya estableció en 1993 sin ambages que el derecho reconocido en el artículo 18.4 de la CE es un derecho autónomo, se trata de la libertad frente a potenciales agresiones a la dignidad y a la libertad proveniente del uso ilegítimo de la informática. El Alto Tribunal además señaló la vinculación directa de este derecho para los poderes públicos sin necesidad de desarrollo normativo (STC 254/1993)[268]. Y, es más, el TC en su Sentencia 292/2000[269]

[267] Sobre el art. 18.4 CE como derecho constitucional autónomo, véase PARDO FALCÓN, J., "Artículo 18.4. La protección de datos", en Rodríguez-Piñero, M. y Casas Baamonde, M. E. (Dir.), *Comentarios a la Constitución española*, Tomo I, Conmemoración del XL Aniversario de la Constitución, Madrid, Wolters Kluwer, BOE, TC y Ministerio de Justicia, 2018, pp. 563-566.

[268] Sentencia de 20 de julio de 1993 que resuelve el recurso de amparo nº 1827/90, a la que el magistrado Miguel Rodríguez-Piñero y Bravo-Ferre formula un voto particular. Ponente magistrado: Fernando García-Mon y González Regueral.

afirma que la protección de los datos se extiende a todos los datos sean éstos calificables de "íntimos" o no. Son los todos los datos de la personalidad los protegidos.

En concreto, la STC 94/1988 señaló que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención. Este derecho se halla estrechamente vinculado con la libertad ideológica, pues evidentemente el almacenamiento y la utilización de datos informáticos puede suponer un riesgo para aquélla, no solamente por lo que se refiere a 'datos sensibles', entre los que se encuentran los de carácter ideológico o religioso sobre los cuales según indica el artículo 16 CE nadie estará obligado a declarar, sino también por su posible utilización ajena a las finalidades para los que fueron recabados (SSTC 11/98, de 13 de enero; 44 y 45/1999, de 22 de marzo, entre otras, en relación con la libertad sindical), o la inclusión de datos sin conocimiento del afectado (STC 202/1999, de 8 de noviembre). Otro riesgo puede provenir por efectuarse accesos indebidos a ficheros ajenos (STC 144/1999, de 22 de julio, en torno a una indebida utilización por parte de una Junta Electoral de Zona de datos incluidos en el Registro Central de Penados y Rebeldes). Los derechos del artículo 18 CE, al encontrarse en la Sección 1ª del Capítulo II del Título I de la Constitución, están sometidos a reserva de ley orgánica (art. 81 CE), que en todo caso deberá respetar su contenido esencial, y vinculan a todos los poderes públicos (art. 53.1 CE), y, entre las garantías jurisdiccionales podrá recabarse la tutela de los tribunales ordinarios mediante un procedimiento basado en los principios de preferencia y sumariedad y, subsidiariamente, la tutela del Tribunal Constitucional mediante un recurso de amparo (art. 53.2 CE)[270].

Tal y como nos recuerda Murillo de la Cueva[271], los derechos fundamentales son "instrumentos que el Derecho pone a disposición de las personas para que puedan

[269] Sentencia 292/2000, de 30 de noviembre de 2000 del TC. Recurso de inconstitucionalidad respecto de los artículos 21.1 y 24.1 y 2 de la LOPD.
[270] Cfr. ELVIRA PERALES, A., op. cit.
[271] Cfr. LUCAS MURILLO DE LA CUEVA, P., "El derecho fundamental a la protección…, op. cit., pp. 21 y ss.

satisfacer sus necesidades básicas"; necesidades derivadas de las condiciones de convivencia y que si no se satisfacen la convivencia deviene imposible. Resulta muy relevante la ubicación en el texto constitucional del artículo 18.4 entre los artículos 14 a 19 y 20, que gozan de una protección reforzada, como ya hemos apuntado. Como también hemos apuntado, la condición de derecho fundamental de este derecho reconocido en el artículo 18.4 hace que la ley que lo desarrolle deba respetar su contenido esencial y para interpretar cuál es ese contenido esencial es de singular importancia, como así lo indica el art. 10.2 CE, atender a la Declaración Universal de Derechos Humanos[272], al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[273] y al Convenio Europeo[274] para la protección de los Derechos Humanos y Libertades Fundamentales de 1950.

Dada la articulación de este derecho, con la expresa mención a la informática, no es posible encontrar antecedentes directos en textos constitucionales anteriores, al menos así lo considera Sempere Rodríguez[275]. Sin embargo, este antecedente inmediato lo encontramos fuera de nuestras fronteras, en concreto como indica este mismo autor, en el artículo 35 de la Constitución Portuguesa de 2 de abril de 1976, con arreglo al cual: *"*1: Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanografiados acerca de ellos y la finalidad a la que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización. 2: No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos. 3: Se prohíbe atribuir un número nacional único a los ciudadanos"[276].

[272] El artículo 12 de la Declaración Universal de Derechos Humanos establece que: "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honor o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias y ataques*".* En este mismo sentido se pronuncia el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, suscrito en Nueva Cork el 19 de diciembre de 1966 (BOE de 30 de abril de 1977).
[273] Celebrado en Estrasburgo el 28 de enero de 1981 y ratificado por España el 27 de enero de 1984.
[274] Suscrito por España el 24 de noviembre de 1977. Con arreglo al art. 8 del Convenio Europeo: "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y libertades de los demás".
[275] SEMPERE RODRÍGUEZ, C., op. cit. pp. 425 y ss.
[276] Ibíd., p. 427.

En estado embrionario, el texto de la constitución portuguesa contiene los dos aspectos, positivo y negativo, del haz de facultades derivadas del derecho fundamental que, en origen, se formula dentro del derecho a la intimidad y posteriormente evoluciona al derecho autónomo a la protección de datos de carácter personal. En el apartado 1 de este artículo 35 se recogen algunas de las denominadas facultades positivas del individuo que consisten en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, todo ello en garantía de la vida privada de las personas y de su reputación. En este texto de la Constitución portuguesa se contienen las bases de los poderes que otorga al individuo el derecho a la protección de datos. En su aspecto funcional, el derecho fundamental otorga al individuo un poder de control sobre sus datos personales; un poder jurídico que puede imponer a terceros deberes de hacer o de no hacer. Entre los deberes de hacer, este derecho obliga a terceros a que se requiera el previo consentimiento para la recogida y uso de los datos, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. Y entre los deberes de no hacer se incardinarían los poderes negativos de prohibición. Se configura, con todo ello, un poder de disposición del individuo sobre sus datos personales.

En el estudio de este artículo 18.4 CE es necesario mencionar los derechos de la personalidad, ya que la formulación del precepto referencia a ellos la limitación que la Ley debe ejercer sobre el uso de la informática. Estos derechos de la personalidad, como ya se expuso anteriormente, admiten dos perspectivas de análisis, la civilista y la constitucional, que han de ser tenidas en cuenta. En el epígrafe anterior se ha hecho referencia a la cuestión de si el tratamiento, en el sentido de extracción, de la base física de las huellas dactilares, de los perfiles de ADN o de las muestras celulares pueden afectar a la dignidad humana y a derechos fundamentales como el honor, intimidad personal, propia imagen e integridad física. Una vez confirmado que, de un elemento físico del cuerpo humano, bien sean huellas, perfiles o muestras, hay una fase previa de extracción de la que dimana información del individuo, es el momento de analizar los ámbitos de protección de esa información frente a su tratamiento sea automatizado o no y las cuestiones que plantea su almacenamiento o conservación. Es el elemento inmaterial, la información, que se extrae de la persona la que en su tratamiento puede afectar al derecho fundamental a la autodeterminación informativa que ahora se estudia. El elemento material del dato biométrico dactiloscópico encuentra su ámbito jurídico de

protección en los derechos de la personalidad y fundamentales antes apuntados y el elemento inmaterial, en el sentido de la información extraída, en el derecho de autodeterminación informativa.

Aunque cabe sostener que el derecho a la protección de datos es un derecho autónomo, como afirma Piñar Mañas[277], ya que su formulación en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea es tajante: "Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan", no es menos cierto que también cabe sostener, siguiendo a Troncoso Reigada, que: "La protección de datos personales, a la vez que es un derecho autónomo, es un instrumento de garantía de otros derechos fundamentales ya que la informática puede ser utilizada para limitar el pleno ejercicio de los derechos…, el derecho fundamental a la protección de datos personales no debe ser visto como un derecho absolutamente independiente sino vinculado con el derecho a la intimidad…"[278]. Sin duda, gran parte de los datos protegidos por este derecho autónomo son datos íntimos, aunque éstos evidentemente no agotan el objeto de protección del derecho. La protección de los datos biométricos dactiloscópicos, entonces, no es solo control y poder de disposición sobre dichos datos, sino que también alcanza la protección de una vida privada, y/o incluso íntima, que puede verse afectada con el tratamiento de dichos datos. En este punto, y desde la perspectiva de las obligaciones que para el Estado se derivan para dar contenido al derecho de control del individuo, merece mención la opinión de Villaverde Menéndez: el Estado está sometido a dos deberes respecto de los individuos; por una parte "un deber positivo de protección de la intimidad de los individuos cuando lo que se pretenda es acceder a la información relativa a datos personales por alguien que no sea el afectado"[279]; y, por otra parte, un deber negativo, de abstención. En este segundo ámbito el Estado "no puede impedir el acceso de cualquier interesado a la información sobre la existencia y fin de los ficheros automatizados, si lo hiciera vulneraría el derecho a recibir información del artículo 20.1.d. […][280]". Es indudable que esta es una de las raíces de las que entronca el deber de transparencia de las Administraciones Públicas respecto de los ciudadanos.

[277] PIÑAR MAÑAS, J.L., "El derecho fundamental a la protección…", op. cit., p. 31.
[278] TRONCOSO REIGADA, A., *La protección de datos personales…,* op. cit., p. 1106.
[279] VILLAVERDE MENENDEZ, I., "Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993", *Revista Española de Derecho Constitucional*, Año 14 nº 41, agosto 1994, Madrid, Centro de Estudios Constitucionales, 1994, p. 222.
[280] Ibíd.

2.4.2. Evolución legislativa y jurisprudencial: del Derecho a la privacidad y a la autodeterminación informativa al Derecho a la protección de datos.

No aportamos nada nuevo recordando que el desarrollo de las tecnologías de la información ha generado en las últimas tres décadas una amenaza a la intimidad de los individuos. Lo ponía de manifiesto la exposición de motivos de la antigua LORTAD al decir que antes el tiempo y el espacio defendía nuestra privacidad, pero ahora ya estos baluartes de antaño han devenido insuficientes o directamente inexistentes habida cuenta de la globalidad o unicidad en la que todo ocurre. Las personas a menudo perdemos el control sobre el torrente de datos que genera nuestra actividad diaria. Nuestro día a día deja, de forma consciente o inconsciente, una multitud de datos sobre nuestra identidad, salud, actividad laboral, relaciones personales, familiares y un largo etc que puede o no pasar a incorporarse a una base de datos. Todos estos datos una vez analizados, disgregados, combinados o recompuestos generan nueva información sobre nosotros mismos. Por eso la informática en los primeros estadios del desarrollo legislativo sobre la materia es entendida como una amenaza a la intimidad de los individuos. Pero también es cierto que hoy en día las exigencias del Estado del bienestar con una sanidad pública universal, un control fiscal de toda la ciudadanía, la seguridad nacional, requieren la captación, almacenamiento y tratamiento de grandes volúmenes de datos. Esta dualidad de amenaza y oportunidad ya la evidenció la LORTAD indicando la necesidad de delimitar una nueva frontera de la intimidad y del honor que permitiera la protección frente a la acumulación de datos.

Antes del nacimiento del derecho específico a la protección de datos de carácter personal este derecho de las personas se tutelaba a través del derecho a la intimidad recogido en textos internacionales y Constituciones nacionales. Tanto la Declaración Universal de los Derechos Humanos de 1948 como el Convenio de Roma de 1950 reconocen el derecho al respeto a la vida privada. Así el artículo 8 del CEDH dice expresamente: **"**Derecho al respeto a la vida privada y familiar. 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya

una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás[281]*"*.

El concepto de "vida privada" del Convenio se ha considerado por Lezertua[282], como concepto coincidente o sin posibilidad de distinción del de "intimidad personal". Sin embargo, el TEDH ha optado por un concepto abierto y amplio de "vida privada" incluyendo en su contenido garantías de la autonomía personal de tal forma que ha entendido que este artículo 8 ofrece una protección más amplia que únicamente el derecho a la privacidad. El TEDH siempre ha sostenido, y así lo reitera en su sentencia de 4 de diciembre de 2008 en el caso S. y *Marper* contra Reino Unido, que la noción de «vida privada» es una noción amplia, sin una definición exhaustiva que cubre la integridad física y moral de la persona (Sentencias *Pretty* contra el Reino Unido, núm. 2346/2002, ap. 61, TEDH 2002-III[283] e Y.F. contra Turquía, núm. 24209/1994, ap. 33, TEDH 2003-IX). Engloba, por tanto, numerosos aspectos de la identidad física y social de una persona (Sentencia *Mikulic* contra Croacia, núm. 53176/1999, ap. 53, TEDH 2002-I[284]). También algunos elementos como, por ejemplo, la identificación sexual, el nombre, la orientación sexual y la vida sexual pertenecen a la esfera personal que

[281]Disponible en http://www.derechoshumanos.net/Convenio-Europeo-de-Derechos-Humanos-CEDH/articulo8CEDH.htm [Fecha de consulta: 29/04/2018].

[282] LEZERTUA, M., "El derecho a la vida privada y familiar en la jurisprudencia del Tribunal Europeo de Derechos Humanos*",* en *Perfiles del derecho constitucional a la vida privada y familiar,* Cuadernos de Derecho Judicial, Madrid, Consejo General del Poder Judicial, 1996, pp. 52 y ss.

[283] Párrafos 57-78, alegación de violación del artículo 8 de la Convención. Se alega el derecho recogido del artículo 8.1 de respeto a la vida privada y familiar considerándolo como un derecho de autodeterminación que engloba el derecho a tomar deciciones sobre el propio cuerpo. El párrafo 61 recoge el concepto amplio de vida privada que abarca la integridad física y psicológica de una persona, y así dice: "*As the Court has had previous occasion to remark, the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person (see X and Y v. the Netherlands, judgment of 26 March 1985, Series A no. 91, p. 11, § 22)."* https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%22CASE%20OF%20PRETTY%20v.%20THE%20UNITED%20KINGDOM\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-60448%22]} [Fecha de consulta: 21/09/2018].

[284] El párrafo 53 incluye en el concepto de vida privada, además de la integridad física y psicológica de una persona, ciertos aspectos de su identidad física y social y en cierto grado el derecho a relacionarse con otros seres humanos, del siguiente modo: "*Private life, in the Court's view, includes a person's physical and psychological integrity and can sometimes embrace aspects of an individual's physical and social identity. Respect for "private life" must also comprise to a certain degree the right to establish relationships with other human beings (see, mutatis mutandis, Niemietz v. Germany, judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29)".* https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22mikulic%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-60035%22]} [Fecha de consulta: 21/09/2018].

protege el artículo 8 (véase, entre otras, Sentencias *Bensaid* contra Reino Unido, núm. 44599/1998, ap. 47, TEDH 2001-I[285] y las referencias citadas en la misma y *Peck* contra Reino Unido, núm. 44647/1998, ap. 57, TEDH 2003-I). Además del nombre, la vida privada y familiar puede englobar otros medios de identificación personal y vinculación a una familia (Sentencia *Burghartz* contra Suiza, 22 febrero 1994, ap. 24, serie A núm. 280-B). La información relativa a la salud de una persona constituye un elemento importante de su vida privada (Sentencia Z contra Finlandia, 25 febrero 1997, ap. 71[286], Repertorio de sentencias y resoluciones 1997-I). Así mismo, la identidad étnica de una persona es para el Tribunal un elemento relevante de su vida privada (véase, concretamente, el artículo 6 de la Convención sobre protección de datos, que incluye los datos de carácter personal que revelan el origen racial, junto a otra información sensible sobre la persona, entre las categorías particulares de datos que no pueden ser conservados sin las garantías apropiadas). En todo caso, y como acertadamente sostiene Santolaya[287], el bien jurídico protegido es "la necesidad de garantizar la intimidad o vida privada", en el sentido ya definido por la Resolución 428 (1970) de la Asamblea Parlamentaria del Consejo de Europa entendiéndola como "el derecho de vivir la vida de cada uno con un mínimo de interferencia. Comprende la vida privada, la familia, la vida en el domicilio, la integridad física y moral, el honor y la reputación, el evitar ser colocado bajo una falsa luz, la no revelación de hechos irrelevantes o embarazosos, la publicación no autorizada de fotografías privadas, así como la protección de la divulgación de información dada y recibida por el individuo de manera confidencial…"[288].

[285] El párrafo 47 expresa como elementos tales como la identificación de género, el nombre, la orientación sexual o la vida sexual, la salud mental son parte crucial en la vida privada de los individuos: *"[…] The Court has already held that elements such as gender identification, name and sexual orientation and sexual life are important elements of the personal sphere protected by Article 8[…]Mental health must also be regarded as a crucial part of private life associated with the aspect of moral integrity.*" https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22bensaid%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-59206%22]} [Fecha de consulta: 21/09/2018].

[286] La sentencia dice textualmente: *"*El respeto al carácter confidencial de las informaciones sobre la salud constituye un principio esencial dentro del sistema jurídico de todos los Estados parte del Convenio. Resulta fundamental no sólo para proteger la vida privada de los enfermos, sino, igualmente, para preservar su confianza en el cuerpo médico y en los servicios de salud en general*".* https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-163986%22]} [Fecha de consulta: 21/09/2018].

[287] SANTOLAYA, P., "El derecho a la vida privada y familiar (un contenido notablemente ampliado del derecho a la intimidad)", en *La Europa de los Derechos: El Convenio Europeo de Derechos Humanos,* Madrid, Centro de Estudios Políticos y Constitucionales, 2014, p. 430.

[288] Ibíd., p. 430.

Pero ese derecho a la intimidad o vida privada experimenta una evolución por mor de la intervención de la informática y el valor económico atribuible a los datos personales hacia un derecho independiente a la protección de datos. Ya hemos apuntado como la Constitución portuguesa de 1976 fue la primera en referirse específicamente a la protección de datos personales. Las Constituciones de Alemania e Italia se aprobaron tras las II Guerra Mundial y, por ello, no previeron ninguna disposición en relación con la informática. En concreto, en Alemania, la Ley Fundamental de Bonn de 1949 (*Bonner Grundgesetz*)[289], establece en su artículo 2.1. "Todos tienen derecho al libre desarrollo de su personalidad, siempre que no vulneren los derechos de otros y no atenten al orden constitucional o a la ley moral. 2. Todos tienen derecho a la vida y a la integridad física. La libertad de la persona es inviolable. Sólo podrán ser afectados estos derechos en virtud de una ley*".* No hay un reconocimiento expreso del derecho a la intimidad, aunque el derecho a la protección de datos ha encontrado un adecuado desarrollo a través de las interpretaciones de su Tribunal Constitucional y de la doctrina que ubican el nuevo derecho fundamental a la protección de datos personales dentro del reconocimiento constitucional de la dignidad de la persona y del libre desarrollo de la personalidad[290]. En el caso de Italia, ocurre algo similar no se reconoce un derecho a la intimidad y de ahí, como señala Troncoso, que el *diritto a la riservatezza* para unos autores se derive de la interpretación de distintos preceptos constitucionales, para otros es un principio no escrito y, por último, para otros autores es la consecuencia de los derechos de libertad personal[291]. En Austria, la Ley Constitucional Federal de 1929 (*Bundes-Verfassungsgesetz in der Fassung*), tampoco reconoció un derecho a la intimidad.

En las reformas constitucionales que se fueron produciendo a partir de los años ochenta, como la Ley Fundamental del Reino de los Países Bajos revisada en 1983, la Constitución de Finlandia, tras la reforma de 1980, o la Constitución de Suecia de 1994, se recogen referencias expresas a la protección de los datos de carácter personal. Sin

[289] Aprobada en la fecha indicada en la ciudad renana de Bonn por el Consejo Parlamentario (*Parlamentarischer Rat*), constituido meses antes con el beneplácito y bajo la supervisión de las autoridades de ocupación.
[290] El Tribunal Constitucional Federal alemán ha sentado las bases del derecho a la autodeterminación informativa en su Sentencia de 15 de diciembre de 1983.
[291] TRONCOSO REIGADA, A., *La protección de datos personales…,* op. cit., p. 51.

embargo, la Constitución de Bélgica se limita a reconocer el derecho al respeto de la vida privada[292].

Siguiendo con este recorrido de la evolución legislativa en el reconocimiento del derecho a la protección de datos es obligada la mención de la Ley de protección de datos aprobada en el *land* de Hesse en el año 1970 y la Ley de protección de datos en Suecia de 1972. Así mismo, son destacables textos previos y preparatorios para el futuro reconocimiento del derecho fundamental a la protección de datos como la Comunicación de la Comisión titulada "Una política comunitaria de informática" de noviembre 1973 y la Resolución del Parlamento Europeo de 8 de mayo de 1979. El texto de la resolución formado por 14 proposiciones y 17 recomendaciones tiene una vocación maximalista puesto que abarca a ficheros manuales y automatizados, datos de las personas físicas y de las personas jurídicas o grupos de personas y propone un sistema de control a priori de ficheros a través de la autorización o declaración previa[293]. También es relevante la Recomendación de la OCDE, de 23 de septiembre de 1980 sobre "Flujo Internacional de Datos"[294]. Y por fin se llega al Convenio 108 del Consejo de Europa, de 28 de enero de 1981, el cual fue una norma incorporada al Derecho español por la vía prevista en el artículo 96 CE y a la vez sirvió como criterio de interpretación de los derechos fundamentales. Se culmina este proceso con la aprobación de la Directiva 95/46/CE[295]. Esta Directiva se hizo necesaria a fin de armonizar todas las leyes de protección de datos que en Europa se habían ido aprobando al albur del Convenio 108. El objeto de la Directiva queda establecido en el Artículo 1: "1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la Presente Directiva, la protección de las libertades y los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. 2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1*".* Posteriormente la Directiva

[292] Ibíd., p. 50.
[293] HEREDERO HIGUERAS, M., *La Directiva Comunitaria de Protección de los Datos de Carácter Personal*, Pamplona, Aranzadi, 1997, p. 20.
[294] Recomendación, aprobada por el Consejo de la OCDE el 23 de septiembre de 1980, Documentación Informática, Serie amarilla/Tratados internacionales núm. 2, Madrid, Presidencia del Gobierno/Servicio central de publicaciones, Servicio Central de Informática, 1982.
[295] Esta Directiva fue precedida de la propuesta de Directiva de 1990 y de la propuesta modificada de 1992.

97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997[296], relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones se remitía a la Directiva 95/46/CE en lo referente a la necesidad de respetar en las comunicaciones electrónicas y en el comercio electrónico el derecho fundamental a la protección de datos personales. La Directiva 97/66/CE fue derogada por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002[297], relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas en la que de forma expresa se hace referencia al derecho fundamental a la protección de datos personales como derecho autónomo. Así también se hace referencia a este derecho fundamental en la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, de "conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE"[298]. Por último, la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000[299], relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, se remite a la Directiva 95/46/CE en lo referente al tratamiento de datos personales, no haciendo ninguna modificación al respecto. Ahora bien, en esta evolución, brevemente comentada, tanto a nivel nacional como europeo, el año 2000 representa lo que Piñar Mañas califica de "giro copernicano"[300] en la protección de datos. Como señala este autor, la protección de datos pasa a tener la consideración de un "verdadero derecho fundamental autónomo eindependiente del Derecho a la intimidad[301]". El 7 de diciembre de ese mismo año es proclamada la carta de los Derechos Fundamentales de la Unión Europea en la Cumbre de Niza que recoge en su artículo 8 el Derecho de toda persona a la protección de los datos de carácter personal que le conciernan. Y por su parte nuestro TC dicta dos importantes Sentencias el mismo día 30 de noviembre, la 290/2000 y la 292/2000 (ya comentadas), configurando el Derecho a la protección de datos como un derecho autónomo e independiente del derecho a la intimidad y privacidad, incluso del

[296] *DOCE*, Serie L, nº 24, de 30 de enero.
[297] *DOCE*, Serie L, nº 201, de 31 de julio.
[298] Hay que tener en cuenta que la Sentencia del TJUE de 8 de abril de 2014 en el llamado Asunto *Digital Rights Ireland y Seitlinger y otros* (asuntos acumulados C-293/12 y C-594/12) ha afectado a la invalidación de la Directiva 2006/24/CE. Cfr. LÓPEZ AGUILAR, J. F., op. cit. p. 562.
[299] *DOCE*, Serie L, nº 178/1, de 17 de julio.
[300] PIÑAR MAÑAS, J.L., "El derecho fundamental a la protección…", op. cit., p. 30.
[301] Ibíd., p. 31.

derecho a la autodeterminación informática o informativa puente entre intimidad y protección de datos. El TC en la sentencia 292/2000 determina, en su FJ séptimo, que el Derecho fundamental a la protección de datos consiste en un poder de disposición y control sobre los datos personales que confiere una serie de facultades al individuo que se extienden desde el poder de decisión de a quién proporcionar esos datos hasta saber quién los tiene o la facultad de consentir su recogida, o de oponerse a su posesión, entre otras.

El devenir de los tiempos ha traído la modificación abierta y total de la Directiva 95/46/CE por la PRPD. Esta propuesta de Reglamento General de Protección de Datos de 25 de enero de 2012 establecía en su artículo 1 como objeto y objetivos: *"*1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos. 2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. 3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales*."* En términos totalmente coincidentes se expresa el vigente RGPD. La Directiva 95/46/CE quedó derogada al publicarse en el Diario Oficial de la Unión Europea, el 4 de mayo de 2016, el RGPD. Aprobado ya este Reglamento es una norma con alcance general, siendo de obligado cumplimiento todos sus artículos y directamente aplicable en cada Estado miembro. Ha quedado derogada, así, la Directiva 95/46/CE y el RGPD, según su artículo 99, comenzó a aplicarse el 25 de mayo de 2018. Con el RGPD la normativa de protección de datos ha pasado de ser una regulación formalista, en el sentido de estar en gran medida basada en el cumplimiento de formalidades administrativas (declaración e inscripción de ficheros y tratamientos, redacción y actualización de documentos de seguridad, contratos con el encargado del tratamiento, carteles informativos…), a una regulación que atiende a la protección sustantiva[302], del fondo no tanto de la forma, en la que nuevos conceptos se implantan con fuerza como el análisis de impacto en la privacidad, la adopción responsable y comprobable (*accountable*) de medidas adaptadas a los riesgos detectados, el denominado principio de *accountability* o responsabilidad

[302] ÁLVAREZ RIGAUDIAS, C., "El poder del usuario digital*",* en *Hacia un nuevo derecho europeo de protección de datos,* Valencia, Tirant lo Blanch, 2015, p. 279.

del artículo 24 RGPD. Con gran nitidez el Preámbulo de la Ley 3/2018 habla de este principio, que denomina "principio de responsabilidad activa", y dice refiriéndose al RGPD: "… la mayor novedad que presenta el RGPD es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan"[303]. Este principio, no obstante, es más conocido en la tradición anglosajona que en la española. En nuestra tradición jurídica estamos más habituados a que las normas reguladoras nos prohíban y nos sancionen más que nos establezcan objetivos abstractos que tenemos que alcanzar. Es probable que el RGPD sea un ejemplo de la evolución en la madurez jurídica de las leyes que va de la mano de la madurez de la cuidadanía. En todo caso, este principio de responsabilidad activa no es común en nuestro ordenamiento y, hasta ahora, no estábamos acostumbrados a él. Tanto el RGPD, como la Ley Orgánica 3/2018, convierten a todos los responsables del tratamiento, y en general a todos los implicados en el mismo, en colaboradores necesarios para alcanzar los objetivos de la norma basados en el interés colectivo de los ciudadanos. Con el nuevo Reglamento, por ejemplo, ya no hay necesidad de inscribir los ficheros, si bien es necesario que los responsables y encargados lleven un registro de las actividades del tratamiento que estará a disposición de las autoridades de control (artículo 30). El RGPD dará lugar a la desaparición en España del Registro general de ficheros de la AEPD.

En lo que se refiere al Derecho comunitario originario, no existe una proclamación expresa del derecho fundamental a la protección de datos como derecho autónomo hasta la aprobación en el Tratado de Niza del año 2000 de una Carta de Derechos Fundamentales de la Unión Europea[304] y la Constitución europea aprobada por el Tratado de Roma de 29 de octubre de 2004. Todo ello ha sido completado con la jurisprudencia del TJUE que interpretando los derechos de los artículos 7 y 8 CDFUE ha establecido una doctrina claramente favorable a la privacidad del individuo basada en la garantía de los principios europeos de la reserva de Ley, la necesidad,

[303] BOE 6 diciembre 2018. Sec I, p. 119797, párrafo V.
[304] *DOCE* de 18 de diciembre de 2000 (2000/C 364/01).

proporcionalidad y legitimidad de la finalidad y la limitación temporal en la conservación y retención de los datos.

Ya en Derecho español hemos de partir del artículo 18.4 CE desarrollado por la antigua LORTAD que en su artículo Primero establecía: "Objeto.- La presente Ley Orgánica, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos". Después la LOPD estableció en su Artículo 1: "Objeto.- La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar." Vemos claramente la diferencia con el vigente RGPD, el cual abiertamente habla como su objeto de la protección del derecho autónomo e independiente, de otros derechos fundamentales, de la protección de los datos personales. Y esto no quiere decir que derechos fundamentales como honor, intimidad personal y familiar no queden amparados por el RGPD, que sin duda sí se protegen, pero ya sin necesidad de ser el vehículo imprescindible para alcanzar la protección de los datos de carácter personal que por sí solos representan un ámbito autónomo. En este sentido, el art. 1 LO 3/2018, proclama como su objeto "adaptar el ordenamiento jurídico español al RGPD y garantizar los derechos digitales de la ciudadanía conforme a lo que manda el art. 18.4 CE.

Por lo que respecta a la evolución jurisprudencial y, en concreto, al Tribunal Constitucional español son destacables, entre otras ya citadas, la STC 11/1998, de 13 de enero, la STC 292/2000 y la STC 96/2012, de 7 mayo. Esta última Sentencia[305], ha representado un avance en la interpretación de la aplicación del Derecho a la protección de datos, ya que su indudable contenido independiente de otros derechos fundamentales ha de ser alumbrado por la aplicación del juicio de proporcionalidad que describe con claridad esta Sentencia.

[305] Tribunal Constitucional Sala 1ª, S 7-5-2012, nº 96/2012, BOE 134/2012, de 5 de junio de 2012, rec. 8640/2010.

En su Fundamento de Derecho Sexto reafirma el carácter autónomo del derecho a la protección de datos con respecto al derecho a la intimidad al disponer aquél de su ámbito de protección propio, y así dice: “[..] el Tribunal Constitucional ha perfilado las singularidades del derecho a la protección de datos, indicando expresamente que "su objeto es más amplio que el del derecho a la intimidad" (STC 292/2000, FJ 6), puesto que "el derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado" (STC 292/2000, FJ 6). En consecuencia, el objeto de protección del derecho fundamental a la protección de datos que se deriva del art. 18.4 CE "no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que, por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos" (STC 292/2000, FJ 6)”.

Y en el Fundamento de Derecho Séptimo concreta las facultades que el derecho a la protección de datos confiere a los individuos al decir: “[…] el derecho a la protección de datos atribuye a su titular, tal y como ha reiterado este Tribunal "un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ 7 EDJ 1993/7394)" (STC 292/2000, FJ 6 EDJ 2000/40918).

Por tanto, el contenido del derecho fundamental a la protección de datos otorga a su titular un poder de disposición y de control sobre los datos personales que se concreta jurídicamente "en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos" (STC 292/2000, FJ 7 EDJ 2000/40918). Así, la cesión de datos personales a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, supone una nueva posesión y uso que requiere el consentimiento del interesado, y ello porque si se priva a la persona de las facultades de disposición y control sobre sus datos personales, se la estará también privando del derecho fundamental consagrado en el art. 18.4 CE EDL 1978/3879 (STC 292/2000, FJ 7), de donde se infiere que cuando el Juez, en el seno de un procedimiento de medidas preliminares, solicita un fichero informático que contiene un conjunto de datos personales, con la finalidad de hacérselos llegar a una asociación que pretende iniciar un proceso para la defensa de los intereses colectivos de consumidores y usuarios, al objeto de concretar a los integrantes del grupo de afectados, está limitando el contenido del derecho fundamental a la protección de datos protegido por el art. 18.4 CE y, en consecuencia, deberán darse los presupuestos habilitantes necesarios para que dicha injerencia en el derecho fundamental pueda calificarse de constitucionalmente legítima.”

En el Fundamento de Derecho Décimo se explica en qué consiste el juicio de proporcionalidad que debe llevarse a cabo para evaluar si una medida, una actuación, restringe un derecho fundamental : “ […] para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en

sentido estricto).” Definitivamente, en este caso, la medida sometida al juicio de proporcionalidad por el TC no superó dicho juicio, otorgándose el amparo al recurrente.

2.4.2.1. Objeto de la protección.

El derecho reconocido en el artículo 18.4 de la CE “[…] protege la totalidad de los datos de carácter personal, no solo de los materialmente calificables como “íntimos” (art. 18.1 CE). Son, pues, todos los datos de la personalidad (STC 292/2000)[306], e independientemente de la ciudadanía española o la condición de extranjero”[307].

En este mismo sentido, ya hemos hecho referencia a la STC 96/2012, de 7 mayo, que declara que el objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino que abarca a cualquier tipo de dato personal. Incluso se extiendo a los datos personales públicos, es decir, los accesibles al conocimiento de cualquiera, pero que por ese simple hecho “no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos” (STC 292/2000, Fj 6).

En definitiva, el art. 18.4 CE, “consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona” (STC 11/1998, de 13 de enero, Fj 5). Y con esta STC 96/2012, por una parte, se consolida la Jurisprudencia ya marcada en la anterior Sentencia, STC 292/2000, ampliando el ámbito de la protección, ya que, no sólo se protegen los datos íntimos de la persona, sino que también se protegen los accesibles al conocimiento de cualquiera, sean de cualquier condición íntima o no. Y, por otra parte, es destacable la configuración del poder de disposición la persona que tiene un derecho de control de flujo de sus datos. Y todo ello culmina con el artículo 1.2 RGPD, que proclama como su objeto la protección de los derechos y libertades fundamentales de las personas físicas “[…] y, en particular, su derecho a la protección de los datos personales”.

[306] Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
[307] LÓPEZ AGUILAR, J. F., op. cit. p. 560.

2.4.2.2. Contenido de la protección. El principio de proporcionalidad en el tratamiento del dato dactiloscópico.

No debemos perder de vista la definición que la LOPD, en su artículo 3 apartados b), incluía de fichero como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso" y en el apartado c) de tratamiento de datos como "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias". El RGPD recoge ambas definiciones en el artículo 4 en el apartado 2) tratamiento y en el apartado 6) fichero. La definicición de tratamiento es más amplia que en la LOPD anterior. En concreto, el artículo 4. 2) «tratamiento» reza: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;" La definición recoge un concepto amplio omnicomprensivo de cualquier operación automatizada o no sobre datos personales estén éstos aislados o sean conjuntos o volúmenes grandes. El artículo 4.6) define el fichero haciendo hincapié en la estructura que es el elemento diferenciador de un fichero respecto de un conjunto desesturcturado, caótico de datos. Define el RGPD el fichero como: "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;*"* Ambas definiciones nos dan el ámbito en el que los principios de la protección de datos han de desplegar su eficacia. Sin fichero o sin tratamiento no habría base material para la aplicación de los principios. Debemos tener en cuenta que la primera norma a respetar en el uso-tratamiento de los datos de carácter personal es la prohibición de dicho uso salvo autorización o habilitación. Y las tres bases habilitantes de ese uso son: la primera el consentimiento, la segunda la habilitación legal y la tercera el interés legítimo

prevalente sobre la afectación a la esfera individual. Estas tres reglas habilitantes no son acumulativas, sino que juegan o trabajan por separado. Ahora bien, de no contar con ninguna de ellas, es decir, si ninguna concurre en el tratamiento, éste se puede concluir que es ilegítimo. Y junto a estas tres bases habilitantes, los principios de minimización, finalidad y seguridad, completan el marco habilitador del tratamiento. Así en relación con los datos biométricos se plantea la cuestión de si su tratamiento, la huella dactilar o palmar, por ejemplo, se puede considerar excesivo para el fin que lo motiva. Para realizar esta evaluación es imprescindible atender al principio de proporcionalidad recogido con anterioridad en el artículo 4.1 LOPD y, actualmente, como se ha subrayado en distintos momentos, en cierto modo asumido por el principio de exactitud de los datos del art. 4 LO 3/2018.

Por este motivo, la LO 3/2018, en relación con el tratamiento de datos establece en su art. 6 "éste ha de estar basado en el consentimiento del afectado, que, como ya establece el RGPD, es una manifestación de voluntad libre, específica, informada e inequívoca"; asimismo, habla de tratamiento en su art. 8, entendiendo que solo podrá considerarse como tal si está fundado en el cumplimiento de una obligación legal exigible al responsable en los términos previsto en el art. 6.1.c RGPD, previendolo así una norma de derecho de la UE o una norma con rango ley. Asimismo, el tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

Sin perjuicio del análisis que más adelante haremos, podemos ahora apuntar que la AEPD ha tratado la proporcionalidad del uso de la huella dactilar en su informe jurídico 368/2006[308] en relación con el establecimiento de un sistema de control para gestionar las ausencias y retrasos de los alumnos de un centro escolar. La Agencia analiza la cuestión partiendo del citado artículo 4.1 evaluando si el tratamiento de la información biométrica de huella dactilar es excesivo respecto al fin que motiva ese tratamiento. Así mismo la respuesta de la Agencia se efectúa a la luz de la Directiva 95/46/CE, entonces vigente, y teniendo en cuenta el Documento de trabajo del Grupo del artículo 29 de 1 de agosto de 2003. Pues bien, tomando en consideración todo ello: el "principio de fines",

[308] Agencia Española de Protección de Datos. Gabinete Jurídico. *Proporcionalidad del tratamiento de la huella dactilar de alumnos de un colegio. Informe 368/2006.* Disponible en https://www.aepd.es/informes/historicos/2006-0368.pdf [Fecha de consulta: 23/11/2018].

la "proporcionalidad" y la "legitimidad" la AEPD concluye calificando de "desproporcionado" el uso de la huella dactilar como medio de control de acceso de los alumnos al centro escolar. Es el "principio de fines" el que ilumina el juicio de porprocionalidad y, en consecuencia, de legitimidad de un determinado tratamiento. Ahora bien, la cuestión no queda completa si no tenemos en cuenta el más reciente informe 0065/2015[309] del Gabinete Jurídico de la misma AEPD. En este informe de 2015, la Agencia toma muy en consideración dos cuestiones: por una parte el hecho de la calificación como datos sensibles, o especialmente protegidos, de los datos biométricos por el, todavía por entonces, proyecto de nuevo Reglamento de la Unión Europea y, por otra parte, el nuevo Dictamen 2/2009 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas), adoptado el 11 de febrero de 2009 por el GPD 29 (Documento WP160). Se somete de nuevo a la consideración de la Agencia la legalidad de un sistema de control biométrico del acceso al comedor de los alumnos de un centro. El sistema funcionaría de la siguiente manera: los datos correspondientes al algoritmo de la huella digital se almacenarían encriptados en el sistema y estarían asociados a un "número de matrícula" distinto del correspondiente a los datos de identificación de los alumnos. De este modo, el sistema funcionaría haciendo coincidir la lectura de la huella dactilar con el algoritmo encriptado, no identificativo. En principio la Agencia, tomando en cuenta la Directiva 95/46/CE y el Documento de trabajo de 1 de agosto de 2003 del GrPD 29, podría haber considerado desproporcionado el uso de la huella como medio de control del acceso al comedor del centro; sin embargo, tiene en cuenta otras cuestiones. Primero, tiene en consideración que el documento de trabajo de referencia es del año 2003 y desde entonces la evolución de las nuevas tecnologías ha sido enorme y sobre todo en lo referente a la seguridad de la información. Y segundo, y fundamental, el criterio del GPD 29 ya había cambiado. Así quedó expresado en el Dictamen 2/2009 sobre la protección de los datos personales de los niños, que hemos citado más arriba. En este documento se señala que:

> " a**)** Datos biométricos – acceso a la escuela y al comedor
>
> A lo largo de los años se ha incrementado el control de acceso en las escuelas. Este control de acceso puede consistir en recoger a la entrada datos biométricos como las impresiones dactilares, el iris o el contorno

[309] Agencia Española de Protección de Datos. Gabinete Jurídico. *Informe 0065/2015*. Disponible en https://www.aepd.es/informes/historicos/2015-0065.pdf [Fecha de consulta: 23/11/2018].

> de la mano. En algunas situaciones, estos medios pueden ser desproporcionados con respecto al objetivo y tener efectos excesivamente molestos.
>
> En cualquier caso, también deberá aplicarse el principio de proporcionalidad a la utilización de estos datos biométricos.
>
> Se recomienda especialmente que los representantes legales dispongan de medios sencillos para oponerse a la utilización de datos biométricos de los niños. Si los representantes ejercen su derecho de oposición, a los niños se les proporcionará una tarjeta o cualquier otro medio de acceso al cenro escolar".

Planteada así la cuestión, la Agencia vuelve a enfocar su respuesta acudiendo al principio de proporcionalidad. Por ello recurre a "la necesidad de valorar si en el supuesto planteado se cumplirían los presupuestos necesarios para apreciar la existencia de proporcionalidad en el tratamiento"[310]. La Agencia, para aplicar este juicio de proporcionalidad se basa en el triple criterio de juicio de idoneidad, de necesidad y de proporcionalidad en sentido estricto, que tanto la doctrina del TC como el TEDH, han establecido. Pero la Agencia no se detiene aquí, sino que dá un paso más y hace referencia al principio de minimización de los datos; "es decir, que el dato sólo sea objeto de tratamiento, en tanto éste resulte completamente imprescindible para el cumplimiento de la finalidad perseguida"[311]. El uso del dato para la finalidad para la que fue concebido es baluarte para su defensa. En base a ello, la Agencia propone un sistema de mantenimiento de la huella dactilar en poder del propio alumno, en una tarjeta inteligente, evitando la incorporación del dato biométrico al sistema. De tal forma que la comparación en el acceso al comedor se produzca entre la huella leída en ese momento y la almacenada en la tarjeta que porta el propio individuo. El sistema almacena la información del individuo, pero no su huella dactilar, minimizándose así la injerencia de la medida en la privacidad de la persona y alcanzándose el objetivo perseguido. Por ello concluye la Agencia "[…] que solo sería ajustado al principio de proporcionalidad un sistema de reconocimiento dactilar que, por una parte, y como en el supuesto planteado, quede reducido a determinadas dependencias del centro, particularmente el comedor y, por otra, permita que los medios de verificación, en este

[310] Ibíd., p. 5.
[311] Ibíd., p. 6.

caso el algoritmo de la huella dactilar del alumno, permanezcan en su poder y no sean incorporados al sistema, que sólo incluirá los datos referentes a la identificación del alumno que accede al comedor, al producirse una verificación positiva del mismo"[312]. En definitiva, la Agencia está planteando un sistema de autenticación frente a un sistema de identificación, propiamente dicho, que supondría una mayor injerencia en la privacidad del menor.

Pero no podemos continuar sin detenernos ahora en los principios de la protección de datos. La Directiva 95/46 recogía en sus artículos 6 a 11 (ambos inclusive), dentro del Capítulo II referente a las condiciones generales para la licitud del tratamiento de datos personales, en las cuatro primeras secciones de dicho capítulo, el germen de lo que posteriormente la LOPD denominó principios de la protección de datos y la vigente Ley Orgánica 3/2018 denomina con la misma terminología "principios de protección de datos" (art. 4 al 10, ambos inclusive). Así la Directiva recogió en cuatro secciones toda la evolución que hasta ese momento había experimentado la protección de los datos personales fijando las bases o principios de un tratamiento lícito; la Sección I. Principios relativos a la calidad de los datos abarcaba el artículo 6; la Sección II. Principios relativos a la legitimación del tratamiento de datos, comprendía el artículo 7; la Sección III. Categorías especiales de tratamientos englobaba el artículo 8. Tratamiento de categorías especiales de datos y el artículo 9. Tratamiento de datos personales y libertad de expresión; por último, la Sección IV. Información al interesado abarcaba el artículo 10. Información en caso de obtención de datos recabados del propio interesado y el artículo 11. Información cuando los datos no han sido recabados del propio interesado.

Estas cuatro secciones de la Directiva, posteriormente, se desarrollaron en los nueve principios de la protección de datos de la LOPD, a saber: Calidad de los datos; Derecho a información en la recogida de datos; Consentimiento del afectado; Datos especialmente protegidos; Datos relativos a la salud; Seguridad de los datos; Deber de secreto; Comunicación de datos y Acceso a los datos por cuenta de terceros. Estos nueve principios de la protección de datos se recogían en el Título II de la LOPD, artículos 4 a 12 ambos inclusive. Por su parte, la PRGPD recogía los principios en su

[312] Ibíd., p. 7.

Capítulo II; el artículo 5 establecía los principios relativos al tratamiento de los datos personales, que corresponden a los principios relativos a la calidad de los datos del artículo 6 de la Directiva 95/46/CE. No obstante, se añadían algunos elementos como, por ejemplo, el principio de transparencia al establecerse que los datos personales deberán ser: "a) tratados de manera lícita, leal y transparente en relación con el interesado". Así mismo, se incorporaban otros elementos como la aclaración del principio de minimización de datos y el establecimiento de una responsabilidad general del responsable del tratamiento de datos. Derivado de todo ello, es el vigente artículo 5.1.a) del RGPD que recoge, de manera casi coincidente, el principio de transparencia: "1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);". Ahora bien, este artículo 5 debe ponerse en relación con el artículo 12 del mismo RGPD, que impone al responsable del tratamiento el deber de facilitar al interesado toda la información relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso[313]. Es indudable, como pone de manifiesto el Preámbulo de la LO 3/2018, que el Reglamento general "procede a reforzar la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios". Por tanto, la normativa interna no podrá entrar en contradicción con las normas del Reglamento, lo más que podrá hacer aquélla es especificar o restringir éstas. El citado Preámbulo, con una extrema claridad, distingue entre la vertiente positiva y la negativa del principio de seguridad jurídica. La positiva "… obliga a los Estados miembros a integrar el ordenamiento europeo en el interno". Y la negativa "… implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo". El RGPD en su capítulo II, artículos 5 a 11 (ambos inclusive), recoge bajo el epígrafe "Principios" en el artículo 5, los "Principios relativos al tratamiento"; artículo 6, "Licitud del tratamiento"; artículo 7, "Condiciones para el consentimiento"; Artículo 8, "Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información"; Artículo 9, "Tratamiento de categorías especiales de datos personales"; Artículo 10,

[313] SAN JOSÉ i AMAT, C., "Los principios del Reglamento (UE) General de Protección de Datos (1)", en *Factor GDA*, 7 de marzo de 2017, disponible en: https://esaged.wordpress.com/2017/03/07/los-principios-del-reglamento-ue- general-de-proteccion-de-datos-1/ [Fecha de consulta: 05/11/2017], citado por GARCÍA-CUEVAS ROQUE, E., op. cit., p. 70.

“Tratamiento de datos personales relativos a condenas e infracciones penales” y Artículo 11, “Tratamiento que no requiere identificación”. Todo ello ha llevado a que, por su parte, la vigente LO 3/2018, dedique su Título II a los principios de la protección de datos, en siete artículos (del 4 al 10), estableciendo las bases para un tratamiento lícito, herencia de todo el bagaje anterior, y que se concretan en: exactitud de los datos (art. 4); deber de confidencialidad (art. 5); tratamiento basado en el consentimiento del afectado (art. 6); consentimiento de los menores de edad (art. 7); tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos (art. 8); categorías especiales de datos (art. 9) y tratamiento de datos de naturaleza penal (art. 10).

Volviendo a la Directiva 95/46/CE, debemos considear que, basado en su artículo 7 (principio del consentimiento y de la necesidad), el artículo 6 establecía los criterios que ha de seguir el tratamiento lícito. El tratamiento para el cumplimiento de una obligación jurídica o para el cumplimiento de una misión de interés público exige como fundamento jurídico el Derecho de la Unión o la legislación de un Estado miembro. Se especificaban, así, más en profundidad los criterios del interés, y la observancia de las obligaciones jurídicas y el interés público. Por su parte, el artículo 7 aclaraba las condiciones para que el consentimiento sea válido como fundamento jurídico para el tratamiento lícito, estableciendo el apartado 1 de la PRGPD: “El responsable del tratamiento asumirá la carga de la prueba de que el interesado ha dado su consentimiento para el tratamiento de sus datos personales para determinados fines*”*. La versión definitiva de este apartado 1 del artículo 7 del RGPD, con el mismo contenido, aunque con diferente expresión, dice: 1.“Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales”.

El artículo 8 establece nuevas condiciones para la licitud del tratamiento de los datos personales de los niños en relación con los servicios de la sociedad de la información que se les ofrecen directamente, y así dispone: “1. A efectos del presente Reglamento, en relación con la oferta directa de servicios de la sociedad de la información a los niños, el tratamiento de los datos personales relativos a los niños menores de 13 años solo será lícito si el consentimiento ha sido dado o autorizado por el padre o tutor del niño. El responsable del tratamiento hará esfuerzos razonables para obtener un consentimiento verificable, teniendo en cuenta la tecnología disponible.” El artículo 8.1

ha variado su redacción final en el RGPD siendo actualmente más restrictiva: "Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años". Así, el Estado español a través de la vigente LO 3/2018, en el artículo 7.1, establece que: "El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento." El apartado 2 de este artículo 7, concluye: "El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela". Hay que tener en cuenta que el artículo 6.1 a) del RGPD se refiere al tratamiento legitimado por el consentimiento dado por el interesado para áquel habiéndose especificado sus fines. Ahora bien, en todo caso el consentimiento, directo o completado pot el tutor o titular de la patria potestad, habrá de ser de mayores de 13 de años.

Es el artículo 9 RGPD, -que la LO 3/2018 también recoge en el mismo número del precepto-, el dedicado al "tratamiento de categorías especiales de datos personales", estableciendo, por una parte, una prohibición general del tratamiento de estas categorías y, por otra, las excepciones a esta norma general, inspirándose en el artículo 8 de la Directiva 95/46/CE. La prohibición general cambió, se amplió en la Propuesta, con respecto a la de la Directiva, incluyendo los datos genéticos y decía: "1. Queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, la religión o las creencias, la afiliación sindical, así como el tratamiento de los datos genéticos o los datos relativos a la salud, la vida sexual, las condenas penales o medidas de seguridad afines". Pero, definitivamente, el RGPD en este artículo 9.1 recoge una prohibición general que alcanza también a una categoría de datos biométricos y determina: *"*Quedan prohibidos el tratamiento de datos personales

que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física". El apartado 2 de este artículo 9 recoge diez circunstancias que actúan a modo de excepciones a la prohibición general del apartado 1; el apartado 4 del artículo 9 deja una cláusula abierta para que los Estados miembros, si lo consideran oportuno, puedan introducir condiciones adicionales; incluso habla de "limitaciones" con respecto al tratamiento, entre otros, de datos biométricos. Entendemos que la normativa nacional de protección de datos puede reforzar la protección de los datos biométricos limitando su tratamiento. Pero no consideramos que ello haya ocurrido, ya que nuestra normativa nacional representada por la reciente LO 3/2018, de 5 de diciembre, nos dice en su artículo 9.1. que, "a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico". No hay una mención expresa, ni velada, a los datos biométricos dirigidos a identificar de una manera unívoca a una persona física. Por ello, entendemos cabe sostener que el solo consentimiento del afectado basta para levantar la prohibición de tratamiento.

Por último, el artículo 10 de la PRGPD aclaraba que el responsable del tratamiento no está obligado a obtener información adicional para identificar al interesado con el único fin de cumplir las disposiciones del Reglamento, diciendo: "Si los datos sometidos a tratamiento por un responsable no le permiten identificar a una persona física, el responsable no estará obligado a hacerse con información adicional con vistas a identificar al interesado con la única finalidad de cumplir lo dispuesto en el presente Reglamento". Actualmente, es el artículo 11.1 RGPD el que recoge este principio respecto de los tratamientos que no requieren identificación, aunque con un matiz distinto: *"*Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, éste no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento". Este último principio-aclaración no es en absoluto baladí y puede ser relevante en tratamientos de huellas dactilares con fines de autenticación en los que no se llega a identificar al

individuo, por lo que resultaría de aplicación este artículo 11. No obstante, no debemos perder de vista que el tratamiento siempre se refiere a personas identificadas o identificables; desde el momento en que se pierda esta condición *sine quanon* para aplicar la legislación específica de protección de datos, ya no tiene sentido plantearse su aplicación.

Centrándonos en los principios que contemplaba la LOPD, comenzaremos por el principio de calidad del artículo 4. Este principio de calidad de los datos implica que solo está permitida la recogida y el tratamiento de datos personales cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. La LO 3/2018 recoge como primer principio de la protección de datos, el ya mencionado de la exactitud (art. 4: "conforme al art 5.1.d. RGPD los datos serán exactos y, si fuere necesario, actualizados"); por tanto, no hace sinónimos los conceptos de exactitud y actualización, aunque estén íntimamente relacionados, ya que un dato no actualizado es imposible que sea un dato exacto. Ahora bien, no todos los datos actualizados por el mero hecho de estar actualizados, son exactos. Estos conceptos de exactitud y actualización llenaban de contenido al antiguo principio de calidad de los datos. Debemos precisar, por último, en relación con este principio de exactitud que, como dispone el RGPD, la inexactitud de los datos ha de ser suprimida o rectificada, no siendo imputable al responsable del tratamiento, siempre que éste haya adoptado todas las medidas razonables que estén a su alcance (art. 4.2 LO 3/2018).

La Directiva 95/46/CE también recogía este principio en su artículo 6. Es un principio básico en materia de protección de datos y así se recoge en numerosas Sentencias de la Audiencia Nacional, tales como la Sentencia de 25 de mayo de 2001, 5 de abril de 2001.

El principio de calidad debe respetarse tanto en el momento de la recogida de los datos, como en el momento del tratamiento, en el mantenimiento del fichero y en el momento de la cancelación del dato, ya que un dato que haya dejado de ser necesario o pertinente, por tanto, deviene ilícito, debe ser cancelado. La jurisprudencia de nuestro TC estableció, desde sus inicios (SSTC 11/98, de 13 de enero; 202/99, de 8 de noviembre;

290/2000, de 30 de noviembre)[314], el derecho de cancelación de los contenidos ilícitos. Derecho que posteriormente se ha visto reforzado con la configuración del nuevo derecho al olvido.

La calidad en la recogida de los datos exige atender a tres criterios fundamentales: el criterio o principio de adecuación, el criterio de pertinencia y el criterio de proporcionalidad. El criterio de adecuación, conforme establecían los artículos 4.1 LOPD y 8.2 RLOPD, exige que los datos de carácter personal solo pueden ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento. El hecho de que la LO 3/2018 no recoja con toda su extensión la definición del principio de calidad –que sí recogía la LOPD-, a nuestro juicio no es causa suficiente para considerar fuera del ámbito de la interpretación y adaptación de la normativa de protección de datos, a un caso concreto, este concepto de calidad al que nos referimos.

El criterio o principio de pertinencia supone que solo está permitida la recogida y el tratamiento de datos personales cuando sean pertinentes o necesarios en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Y el tercer criterio de calidad en la recogida hace referencia a la proporcionalidad resultando de interés su estudio en relación con la recogida de huellas dactilares. El RGPD utiliza otra terminología, pero hace referencia a los mismos conceptos. Ahora, el artículo 5 concreta los principios relativos al tratamiento en los siguientes: licitud, lealtad y transparencia en el tratamiento respecto al interesado; limitación de la finalidad que implica que los datos deban recogerse con fines determinados, explícitos y legítimos; minimización de datos, es decir, recoger los datos que sean necesarios para los fines para los que se van a tratar; exactitud, los datos deben ser exactos y actualizados y, por último, la responsabilidad proactiva que implica que el responsable del tratamiento debe ser capaz de cumplir todo lo indicado anteriormente y además demostrarlo.

El principio de proporcionalidad valora la adecuación entre la necesidad de recogida de un dato y la finalidad de la misma. Ello lleva a que, si valorada la finalidad de la

[314] Cfr. LÓPEZ AGUILAR, J. F., op. cit., p. 561.

recogida ésta puede ser suplida por la realización de una actividad distinta, sin alterar la finalidad, hay que elegir esa última actividad. Es evidente que, para la evaluación del cumplimiento de este principio, es necesario una determinación clara de los fines para los que se recogen y tratan los datos. De igual manera, se puede predicar del principio de exactitud (art. 4 LO 3/2018), el cual tiene que estar necesariamente conectado con los fines del tratamiento; de otro modo, no se podrá evaluar si el dato es inexacto o no.

En relación con este tema resulta de interés el ya citado informe del gabinete jurídico de la AEPD 368/2006, que analiza la proporcionalidad del tratamiento de la huella dactilar de alumnos de un colegio. La consulta que se planteó a la Agencia era la adecuación a la LOPD de la instauración de un sistema de control basado en la obtención de la huella dactilar de los alumnos de un colegio con el fin de gestionar las ausencias y retrasos de éstos. El registro de la huella permitiría el control de la entrada y salida de los alumnos en el centro escolar. Para resolver la cuestión la Agencia partió del análisis de la incidencia de los datos biométricos en el ámbito de aplicación de la LOPD. La Agencia hace un interesante razonamiento en relación con los datos biométricos que reproducimos:

> "Son datos biométricos aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión. Así se emplean para tales fines las huellas digitales, el iris del ojo, la voz, etc.
> Por su parte, el artículo 3 a) LOPD definía los datos de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables". En este sentido, debe indicarse que, si bien el procesamiento de los datos biométricos no revela nuevas características referentes al comportamiento de las personas, sí permite, lógicamente, su identificación, por lo que resulta evidente que, en caso de procederse a su tratamiento dicho tratamiento deberá ajustarse al RGPD y a la LO 3/2018.
>
> El artículo 4.1 LOPD indicaba que, sólo se podrán recoger datos de carácter personal para su tratamiento, así como someterlos a dicho tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades

determinadas, explícitas y legítimas para las que se hayan obtenido. En todo caso, como se contempla en el Preámbulo de la LO 3/2018, en su párrafo V, el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el art. 18.4 CE, se ejercerá con arreglo a lo establecido en el RGPD y en la nueva Ley.

El problema se planteará entonces en determinar si el tratamiento de la información biométrica de huella dactilar puede ser considerado excesivo para el fin que motiva dicho tratamiento, teniendo en cuenta que se efectuaría un tratamiento de datos de menores de edad para las finalidades a las que nos hemos referido al comienzo del presente informe.

A nuestro juicio, tal y como se ha venido indicando por el GPD 29 de la Directiva 95/46/CE, en el Documento de Trabajo sobre biometría, ya refernciado en páginas anteriores, la obtención de la huella dactilar como medio para identificar a los alumnos en el centro resulta excesivo y desproporcionado, para dicha finalidad.

“Con arreglo al artículo 6 de la Directiva 95/46/CE, los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. Además, los datos personales serán adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente (principio de fines). El cumplimiento de este principio implica en primer lugar una determinación clara de los fines para los que se recogen y tratan los datos biométricos.

Por otra parte, hace falta evaluar el cumplimiento de la proporcionalidad y de la legitimidad, teniendo en cuenta los riesgos para la protección de los derechos y libertades fundamentales de las personas y especialmente si los fines perseguidos pueden alcanzarse o no de una manera menos intrusiva.

No en vano, la proporcionalidad ha sido el criterio principal en casi todas las decisiones adoptadas hasta ahora por las autoridades encargadas de la protección de datos sobre el tratamiento de datos biométrico.

El uso de la biometría plantea también el tema de la proporcionalidad de cada categoría de datos a la luz de los fines para los que se tratan dichos datos. Los datos biométricos sólo pueden usarse de manera adecuada, pertinente y no excesiva, lo cual supone una estricta valoración de la necesidad y proporcionalidad de los datos tratados. En este sentido, la CNIL francesa ha rechazado el uso de huellas digitales en el caso del acceso de los niños a un comedor escolar, pero ha aceptado con el mismo fin el uso de los resultados de muestras de las manos. La autoridad portuguesa de protección de datos ha tomado recientemente una decisión desfavorable sobre la utilización de un sistema biométrico (huellas digitales) por parte de una universidad para controlar la asiduidad y puntualidad del personal no docente".

En consecuencia, entendemos que resulta desproporcionado -y, por ello, contrario a lo que disponía el artículo 4.1 LOPD (y, actualmente, el título II LO 3/2018), la utilización de la huella dactilar como medio para controlar el acceso de los alumnos al centro escolar y tal finalidad puede conseguirse, sin duda, de una manera menos intrusiva en relación con los derechos de los alumnos".

En definitiva, la AEPD considera desproporcionada la utilización de la huella dactilar para controlar el acceso de los alumnos al colegio porque la finalidad puede conseguirse de una manera menos intrusiva en los derechos de aquéllos.

Llegados a este punto, resulta muy interesante "la biometría en los teléfonos inteligentes de los particulares"[315]; en un contexto de generalización de los mecanismos de

[315] Texto original en francés. Disponible en https://www.cnil.fr/fr/biometrie-dans-les-smartphones-loi-informatique-et-libertes-exemption-ou-autorisation [Fecha de consulta: 27/05/2018]. En este contexto, la CNIL ha analizado la configuración de varios dispositivos de mercado con respecto a la regulación y su doctrina biométrica. El reconocimiento biométrico integrado en estos dispositivos puede funcionar de acuerdo con dos tipologías de configuración, que no generan los mismos riesgos para la vida privada de los individuos, ni el mismo marco legal:

- Dispositivos biométricos cuya plantilla se almacena en el dispositivo, bajo el control exclusivo del individuo. Muchos dispositivos móviles incorporan dispositivos biométricos que funcionan de manera autónoma, en un entorno completamente compartimentado dentro del dispositivo que impide que los datos biométricos en sí sean accesibles fuera del enclave. En estos casos, la plantilla biométrica se almacena en el dispositivo, en una especie de "caja" hermética, y nunca deja esta "caja". En la práctica, cuando el usuario se autentica, el dedo en el lector del dispositivo se compara con la plantilla biométrica registrada previamente. El servicio o la aplicación que utiliza este modo de autenticación recibe solo información sobre el éxito o el fracaso de la comparación entre el dedo presentado y la plantilla. En estos casos, la CNIL considera que los tratamientos implementados en la iniciativa y bajo el control exclusivo de la persona interesada, pueden estar cubiertos por la exención doméstica registrada en el artículo 2 -2-c de la RGPD.

autenticación biométrica en los teléfonos inteligentes, es de vital importancia aclarar las condiciones en que estas operaciones de procesamiento de datos biométricos están o no sujetas a obligaciones de protección de datos, que, desde luego, a nuestro juicio, lo están. Aquí el individuo debe mantener un control. La CNIL ha aclarado las condiciones en que estas operaciones de procesamiento de datos biométricos están o no sujetas a obligaciones de protección de datos. Sabemos que los dispositivos biométricos están estrictamente regulados por la Ley de protección de datos y el RGPD. El 28 de marzo de 2019, la CNIL francesa publicó "un reglamento modelo que especifica las obligaciones de las organizaciones que desean adquirir dispositivos biométricos con el fin de controlar el acceso a las instalaciones, aplicaciones y herramientas de trabajo". El reglamento modelo "biometría en el lugar de trabajo" es una continuación de las posiciones anteriores de la CNIL en esta área. Especifica a las organizaciones cómo encuadrar su tratamiento de datos biométricos de control de acceso a las instalaciones, las aplicaciones o las herramientas de trabajo y es de carácter vinculante. Por lo tanto, los organismos que implementan estos tratamientos deben respetar las indicaciones dadas en los reglamentos modelo.

Sabemos que los fabricantes de este sector han introducido en los últimos modelos de dispositivos móviles un mecanismo de autenticación de huellas digitales, además del código de acceso. Estos dispositivos permiten, en particular, simplificar el desbloqueo de los teléfonos inteligentes. Y comienza ya utilizarse en algunos centros de trabajo y Unviersidades para controlar las entradas y salidas de empleados y alumnos. El problema radica en que, al estar integradas en dispositivos de forma predeterminada, estas características biométricas son utilizadas por muchos proveedores de servicios y aplicaciones en línea, incluso para la autenticación de prepago.

En efecto, la biometría "en un contexto profesional, puede ser el control de acceso a las instalaciones, computadoras o aplicaciones; (…) los datos biométricos permiten reconocer automáticamente a las personas y confiar en una realidad biológica

- Dispositivos biométricos que operan desde servidores remotos. En otros casos, los dispositivos de autenticación basados en reconocimiento biométrico interactúan con servidores remotos controlados por un tercero. La organización en cuestión (ya sea el proveedor de la aplicación, el dispositivo, etc.) debe realizar una evaluación de impacto de la protección de datos (DIP). Es probable que el procesamiento de datos previsto genere un alto riesgo para los derechos y libertades de los interesados, particularmente en vista de la sensibilidad de los datos procesados y la naturaleza innovadora de las tecnologías utilizadas. Esta evaluación de impacto (AIPD) debe enviarse a la CNIL para consultas si el nivel de riesgo residual sigue siendo alto.

permanente, de la que no pueden liberarse. A diferencia de una credencial o contraseña, no es posible descartar una característica biométrica o cambiarla. El mal uso de tales datos puede tener graves consecuencias para los derechos y libertades de las personas"[316].

Pero, volviendo a los razonamientos que realiza la AEPD, sin embargo, ésta sí considera proporcionada la inclusión de la fotografía de los trabajadores en la tarjeta identificativa en su Informe 266/2006. La consulta que se planteó a la Agencia cuestionaba si la inclusión de una fotografía en las tarjetas identificativas de los trabajadores resultaba conforme a lo dispuesto en la LOPD. La Agencia ya trató en otro informe de 12 de mayo de 2006, la inclusión de la fotografía de los empleados en las tarjetas identificativas mientras ejercían sus funciones en la empresa. Este informe considera proporcional el tratamiento a la finalidad que lo motiva. Se reproduce, por su interés, un fragmento del mismo:

> *"*La consulta plantea si resulta adecuado a las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, la inclusión (...) la fotografía, además del nombre y los dos apellidos, en las tarjetas identificativas que los trabajadores deben llevar en lugar visible mientras estén ejerciendo sus funciones en la empresa.
>
> (...)
>
> Con carácter general el artículo 4.1 de la Ley Orgánica 15/1999, que consagra el denominado principio de proporcionalidad en el tratamiento, establece que "los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido". De ello se desprende la necesidad de que el tratamiento de un determinado dato de carácter personal, (como sería, en este caso, los datos de los trabajadores afectados, toda vez que para su inclusión en la tarjeta de identificación será necesaria la realización de una o varias de las actividades definidas como de tratamiento de datos por el artículo 3 c) de la mencionada Ley), deberá ser proporcionado a la finalidad que lo motiva.

[316] Texto original en francés, disponible en: https://www.cnil.fr/fr/le-controle-dacces-biometrique-sur-les-lieux-de-travail [Fecha de consulta: 27/05/2018].

De este modo, si dicha finalidad pudiera ser suplida por la realización de una actividad distinta al citado tratamiento, sin que dicha finalidad sea alterada o perjudicada, debería optarse por esa última actividad, dado que el tratamiento de los datos de carácter personal supone, tal y como consagra nuestro Tribunal Constitucional, en Sentencia 292/2000, de 30 de noviembre, una limitación del derecho de la persona a disponer de la información referida a la misma.

(...)

Igual argumentación cabe aplicarse a la inclusión en las tarjetas identificativas de la fotografía del trabajador, no pudiendo la misma considerarse excesiva a los efectos previstos en el artículo 4.1 de la Ley Orgánica 15/199**9**.

Por otra parte, en cuanto a la legitimación para el tratamiento de los datos en el marco del desempeño de una relación laboral, el artículo 6.2 de la Ley Orgánica 15/1999 dispone que "No será preciso el consentimiento cuando los datos de carácter personal (...) se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento".

En el presente supuesto, la finalidad que justifica la inclusión (...) la fotografía de los trabajadores en sus tarjetas es precisamente garantizar su identificabilidad en el desempeño de sus funciones, por lo que el tratamiento de los datos puede considerarse amparado por el citado artículo 6.2 de la Ley Orgánica, sin que sea necesario recabar el consentimiento de los afectados, sin perjuicio del necesario cumplimiento del deber de informar a los mismos en los términos exigidos por el artículo 5.1 de la Ley Orgánica 15/1999, que parece haberse cumplido en este caso, según parece deducirse de la consulta.

En consecuencia, y teniendo en cuenta lo señalado en la consulta, (...) cabe considerar que el tratamiento de los datos del Documento Nacional de Identidad y la fotografía de los trabajadores se encontraría amparado por la Ley Orgánica 15/1999".

Considera, entonces, adecuado el tratamiento consistente en el uso de la tarjeta con la foto del trabajador mientras éste está en la empresa trabajando, porque permite comprobar si la actividad del mismo se adecúa a las funciones que tiene en la empresa, encontrándose, además, todo ello entre las finalidades legítimas y necesarias para el normal desarrollo de la relación laboral que une a empleado y empleador.

En este mismo sentido y línea argumental, continúa la Agencia en el Informe 266/2006 no considerando excesiva, a los efectos previstos en el artículo 4.1, la inclusión de la fotografía, puesto que, a la finalidad de identificabilidad del trabajador, a efectos de seguridad, se une la finalidad de evitar una usurpación de su personalidad por terceras personas, asegurándose así la integridad de las instalaciones. En definitiva, se trata de finalidades legítimas y el tratamiento proporcionado a las mismas y, además, conforme al artículo 6.2 de la LOPD no era preciso el consentimiento del trabajador porque los datos tratados se refieren a las partes de un contrato, el contrato de trabajo. Se reproduce, por su interés, parte de este informe:

> *"*De este modo, si para el adecuado desarrollo de la actividad de los trabajadores, enmarcada en su relación laboral, resulta necesario, por motivos de seguridad, proceder a su identificación a través de la fotografía incorporada a su tarjeta, no sería preciso recabar el consentimiento de los mismos para proceder al tratamiento de aquélla.
>
> En cuanto al deber de información, los escritos adjuntos a la consulta vienen a señalar que se van a incorporar a las nuevas tarjetas la fotografía de los empleados, como necesidad ineludible por razones de seguridad (escrito de 10 de febrero de 2006), añadiendo el escrito de 28 de marzo de 2006 que "la fotografía es un dato personal del dossier de cada empleado, y por tanto, sujeto, como el resto de los datos, a la normativa que regula la Protección de Datos Personales".
>
> Del tenor de estas comunicaciones parece desprenderse la referencia al tratamiento de la fotografía y su inclusión en el "dossier de cada empleado", para fines de seguridad.
>
> Habría que completar la información con la indicación de quién es el responsable del fichero y del modo de ejercicio de los derechos de acceso, rectificación, cancelación u oposición, pudiendo considerarse en lo demás adecuada la información remitida".

Por tanto, la Agencia únicamente puntualiza respecto al tratamiento tomado en consideración que, en cumplimiento del deber de información o, lo que es lo mismo, del principio de información en la recogida de los datos, exige indicar al trabajador ante quién puede ejercitar los derechos que la Ley le otorga.

Más reciente el informe 073667/2018 de la AEPD que se emite acerca de la incidencia que en el ámbito de la investigación biomédica pudiera producir la plena aplicación del RGPD, hace referencia a datos de salud y recoge una serie de consideraciones respecto al consentimiento que entendemos aplicables a los datos biométricos dactiloscópicos. En nuestro derecho la Ley 14/2007, de 3 julio, de Investigación Biomédica, basa en el consentimiento la protección del titular de estos datos. Para la AEPD, el RGPD y la LOPD -(no estaba todavía en vigor la LO 3/2018)-, no sólo mantienen inalterado el régimen contenido en la normativa reguladora de la investigación biomédica, sino que permiten realizar una interpretación más flexible del alcance que puede darse al consentimiento prestado de conformidad con la misma. "De todo ello se derivaría que los requisitos de especificidad y carácter inequívoco para la prestación del consentimiento no deben ser interpretados en el ámbito de la investigación científica de un modo restrictivo, limitado a una concreta investigación de la que se facilite toda la información disponible, sino que cabe considerar que concurren en los supuestos en los que el consentimiento se presta en relación con un determinado campo de investigación, pudiendo extenderse en el futuro ese consentimiento, sin que ello lo vicie en modo alguno, incluso a <<finalidades>> o áreas de investigación que ni siquiera hubieran podido determinarse en el momento en que se prestó, sin que sea necesario recabar un nuevo consentimiento del sujeto fuente, teniendo en cuenta los beneficios para los individuos y la sociedad en su conjunto que pueden derivarse de tal investigación no prevista"[317]. Entendemos que, teniendo en cuenta el "hermanamiento" al incluirse en la misma categoría de datos, según el artículo 9.1 del RGPD, los datos biométricos dirigidos a identificar de manera unívoca a una persona física y los datos relativos a la salud, las consideraciones relativas al consentimiento efectuadas respecto a las muestras biológicas son plenamente aplicables a los datos objeto de nuestro estudio. Desprendiéndose así de este Informe de la AEPD una nueva dimensión del principio del consentimiento. Quede ahora apuntada aquí esta idea, sin perjucio de volver sobre este fundamental principio del consentimiento más adelante.

[317] Agencia Española de Protección de Datos. Gabinete Jurídico. INFORME: 073667/2018. https://www.aepd.es/media/informes/2018-0046-investigacion-biomedica.pdf [Fecha de consulta:05/10/2018].

2.4.2.3. Derechos del titular de los datos

El derecho fundamental a la protección de datos tiene un contenido esencial que viene constituido por los derechos de acceso, rectificación, cancelación y oposición[318]. Y junto a estos derechos el derecho de impugnación de valoraciones basadas éstas únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de la personalidad (que se recogía en el art. 13 de la LOPD) y el derecho de consulta al Registro General de Protección de Datos del artículo 14 de la LOPD, configuran las armas de defensa de su privacidad del titular de los datos. Actualmente, estos derechos han pasado a recogerse en el título III, como derechos de las personas (arts. 11 a 18 LO 3/2018). Este conjunto de derechos constituye un arma esgrimible frente a titulares de ficheros y/o tratamientos públicos o privados. Junto a estos derechos citados, el nuevo derecho al olvido –derecho de supresión- de los contenidos lesivos adquiere especial importancia en la defensa de la privacidad del individuo (art. 17 RGPD y art. 15 LO 3/2018). Ya el TJUE ha diseñado una jurisprudencia protectora de la privacidad frente a la responsabilidad de "los motores de búsqueda". De hecho, nuestro TS ha aplicado esta doctrina en su Sentencia TS4132/2015, de 15 de octubre de 2015[319]. Según esta Sentencia del TS las "hemerotecas digitales" no tienen obligación de cancelar ni bloquear el acceso a informaciones "veraces" en sus buscadores internos, aunque esta información corresponda a hechos del pasado, pero lo que sí deben responsabilizarse es de la "anonimización" externa. Se admite, así, la indexación interna de la "hemeroteca digital" pero no la externa que puedan realizar motores de búsqueda generales. Para el Tribunal Supremo prohibir la indexación interna supondría un sacrificio desproporcionado de la libertad de información del artículo 20.1.d) CE. Es destacable la reciente sentencia del TC de 4 de junio de 2018, la cual ha venido a otorgar amparo a

[318] El derecho de oposición está resultando ser el gran ignorado en entornos de *Big Data* donde la recolección masiva de datos y su procesamiento automatizado para crear un modelo que muestre las correlaciones entre las variables objeto de análisis y la posterior aplicación del modelo a personas determinadas, hace necesaria la paresencia del ejercicio de este derecho de oposición. Sin embargo, la toma de decisiones automáticas en función de los modelos desarrollados que afectan directamente a personas que no tienen ni siquiera conocimiento de ser objeto de esa toma de decisiones deja, en muchas ocasiones, en entredicho si privacidad. Y ello es así porque el derecho a oponerse a un tratamiento solo puede ejercitarse si la persona es consciente de que las deciosnes que le van a afectar se toman de forma automatizada. Pero muchos de los procesos analíticos de datos masivos, de donde surgen los modelos, se desarrollan sin conocimiento de los individuos a los que se aplicarán posteriormente dichos modelos. Cfr. CORTÉS VÉLEZ, J. J., "Privacidad y seguridad en el universo digital" en *El Derecho*, Lefebvre ELDERECHO.COM http://tecnologia.elderecho.com/tecnologia/internet_y_tecnologia/Privacidad-seguridad-universo-digital_11_1265680001.html [Fecha de consulta:28/08/2018].

[319] Cfr. LÓPEZ AGUILAR, J. F., op. cit., p. 562.

los recurrentes en el mismo asunto ventilado por la arriba citada sentencia del Tribunal Supremo. La diferencia es que el Tribunal Constitucional plantea el alcance del derecho al olvido no frente a quien permite localizar información en Internet (el buscador) sino frente a quien la ha colgado efectivamente en la Red (el editor)[320]. Debemos aclarar que los hechos de los que conoce el Tribunal Constitucional ocurrieron mucho tiempo atrás y se refieren a personas que no se pueden considerar personajes públicos. El TC considera el derecho al olvido un derecho fundamental al integrarse en el derecho a la protección de datos o libertades informáticas que sin duda tienen dicho carácter fundamental. Ello le hace aplicable la jurisprudencia relativa a los límites de los derechos fundamentales. Y para resolver este conflicto, como advierte Piñar Mañas, la importancia del factor tiempo juega un papel transcendental. Y esto es así porque el mero transcurso del tiempo parece haber producido en un hecho una pérdida de su interés público informativo y haberse transformado en un interés simplemente histórico, importante sin duda, pero ya en otro ámbito para, por ejemplo, la formación de la cultura o la actividad investigadora. Y es por ello por lo que el TC, al distinguir esta doble dimensión, informativa o investigadora, prohíbe, en su Fundamento Jurídico 8, indexar los datos personales de nombres y apellidos de los recurrentes por el motor de búsqueda interno del editor[321].

Centrándonos en el RGPD, los derechos de los titulares de datos biométricos dactiloscópicos se concretan en los artículos 12 a 23, ambos inclusive, que conforman el capítulo III del Reglamento. Estos derechos se han visto reforzados y ampliados con la aprobación del RGPD con respecto a los establecidos en la anterior Directiva y en la anterior Ley nacional (LOPD). Es indudable, como así afirma Troncoso Reigada, que "[…] los derechos de acceso, rectificación, cancelación y oposición que forman parte, como ha determinado la jurisprudencia constitucional, del contenido esencial del derecho fundamental a la protección de datos personales a la luz de la opinión generalmente admitida de lo que este derecho significa- sin los cuales este derecho no es reconocible como perteneciente a su tipo previo- y sin cuyo ejercicio los intereses

[320] PIÑAR MAÑAS, J.L., *El derecho al olvido y las hemerotecas digitales*, Newsletter RedAbogacía Nº 64 – Julio 2018, Sección Actualidad TIC. Disponible en https://www.abogacia.es/2018/07/23/el-derecho-al-olvido-y-las-hemerotecas-digitales/?lang=es [Fecha de consulta: 01/08/2018].
[321] Tribunal Constitucional. Sala Primera. Sentencia 58/2018, de 4 de junio de 2018 (BOE núm. 164, de 7 de julio de 2018).

jurídicos que dan vida a este derecho resultan desprotegidos"[322]. El RGPD comienza la enumeración de los derechos del interesado por la alusión a la transparencia de la información, que ha de vertebrar todas las comunicaciones entre el responsable del tratamiento y el interesado. La información que facilite el responsable al interesado deberá realizarse "en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo […]". Sigue indicando este artículo 12 que "La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos". El Reglamento está haciendo referencia a la información que debe fluir del responsable al interesado en la recogida, por ejemplo, de sus huellas dactilares. Otra cuestión será el derecho de acceso posterior del interesado a esos datos ya tratados que, si atendemos a la configuración de esta información, referente a las huellas dactilares es muy probable que sea facilitada por medios electrónicos al referirse a una plantilla o algoritmo que requiera esta forma de comunicación. Siguiendo con este derecho de información, el apartado 7 del artículo 12 añade una precisión respecto a la posible información que puede facilitar el responsable, al establecer: "La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente". El Reglamento, en este artículo 12 y bajo la denominación general del epígrafe de "Transparencia de la información […]", hace hincapié en este principio de la transparencia que debe presidir las relaciones entre responsables de los tratamientos e interesados. Es cierto que este derecho de información en la recogida y, como acertadamente señala Tronco Reigada, el mismo derecho de acceso "[…] ha sido un medio para introducir en el ordenamiento jurídico una mayor transparencia administrativa y un mejor acceso a la información en manos de la Administración Pública -al menos para el titular de los datos-"[323]. No debemos olvidar que estamos hablando de diferentes derechos: por una parte, emerge el derecho de información -que difiere si los datos se han obtenido directamente del interesado o no-; junto a él se configura con gran precisión el derecho facultad del interesado de acceso posterior a sus datos y en pie de igualdad con los anteriores se encuentra el derecho de acceso a archivos y registros administrativos reconocido en nuestra Constitución en el artículo

[322] TRONCOSO REIGADA, A., *La Protección de Datos...*, op. cit., p. 548.
[323] Ibíd., p. 549.

105.b); en el artículo 13 d) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Merece la pena detenerse en este momento en el informe 0324/2009 de la AEPD que atañe a cuestiones que pueden, en un determinado caso, ser conexas como son: información en la recogida, acceso a datos por un tercero y relaciones de responsable y encargado del tratamiento. En relación con la información que debe facilitarse al interesado, titular de los datos, podemos hacer referencia al informe 0324/2009 sobre acceso al dato de huella dactilar de la AEPD. Este informe aborda, sobre el supuesto de hecho de implantación de un sistema de control del horario de trabajadores, la cuestión del acceso por terceros a los datos de huella dactilar. En los hechos en cuestión los trabajadores pertenecían a dos administraciones u órganos públicos diferentes, por una parte, una mancomunidad y, por otra, una de las comunidades que componen aquélla y se daba la circunstancia de que los trabajadores de la comunidad prestarían sus servicios en el edificio de la mancomunidad. En definitiva, se planteaba a la Agencia un acceso a datos de huella dactilar por una administración, la mancomunidad, que no es la responsable inicial de los mismos, la comunidad empleadora. Y este acceso requeriría el consentimiento de los trabajadores desde el momento en que se está planteando realmente una cesión o comunicación de datos entre administraciones. Pues bien, planteadas las cosas en estos términos, la respuesta de la AEPD en este informe es considerar la existencia de una relación de encargado del tratamiento y responsable entre ambas administraciones, así, "la comunidad encargaría el tratamiento del dato de la huella dactilar de sus trabajadores, a la mancomunidad con la finalidad específica de control horario de trabajo, para lo cual, deberán ambas empleadoras suscribir el contrato previsto en el artículo 12 de la Ley Orgánica 15/1999, y en el Capítulo III del Título II del Reglamento que la desarrolla […][324]". Esta situación ha quedado regulada en el actual artículo 28 del RGPD (y también art. 28 LO 3/2018) que define la figura del encargado del tratamiento, rigiéndose la actuación de éste por un contrato "u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la

[324] Agencia Española de Protección de Datos. Gabinete Jurídico. Informe 0324/2009. Disponible en https://www.aepd.es/informes/historicos/2009-0324.pdf [Fecha de acceso: 19/10/2018].

finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable." También creemos que este supuesto de hecho podría haberse enfocado en lugar de hacerlo desde la prespectiva de la existencia de un encargado del tratamiento, por la vía del derecho de información en la recogida de los artículos 13.1 e); f) y 14.1 e); f) LOPD; es el actual art. 11 LO 3/2018, relativo a la transparencia e información al afectado, dando cumplimiento al deber de información establecido en el art. 13 RGPD.

En relación con el derecho de acceso, que se concreta en el artículo 15 RGPD (y art. 13 LO 3/2018), como el derecho del interesado "a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales", no difiere en lo sustancial del régimen jurídico del derecho de acceso al resto de datos personales. No obstanto, quizá, como hemos apuntado más arriba, deba facilitarse dicho acceso en soporte electrónico. En todo caso es aplicable lo dispuesto en el apartado 3. del citado artículo 15 que dispone que: "El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. […] Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común". El apartado 3 del artículo 15, pero en este caso, de la anterior LOPD, establecía un límite formal al derecho de acceso al establecer que "sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto". Un inciso tal, puede encontrarse en el art. 13.3 LO 3/2018, en virtud del cual, "a los efectos establecidos 12.5 RGPD, se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de 6 meses, a menos que exista causa legítima para ello". Entendemos que deben interpretarse conjuntamente ambos artículos, Reglamento y LOPD, en el sentido de que, caso de que el interesado solicite una copia en intervalo inferior a doce meses el responsable podrá percibir un canon basado en los costes administrativos; con arreglo a la nueva ley, el derecho de acceso se puede entender otorgado si el responsable facilita al afectado un sistema de acceso remoto a tales datos personales y, eso sí, si el afectado elige un medio distinto al que se le ofrece, que suponga un coste desproporcionado, el afectado deberá asumir el exceso de costes que su elección comporte (art. 13.4 LO 3/2018)

Así mismo, el RGPD reconoce en el artículo 16 el derecho de rectificación que "es prácticamente un derecho absoluto siempre que se trate de un dato erróneo o incompleto y se aporte la documentación justificativa que muestra claramente el error o la inexactitud del dato personal […]"[325]. A este derecho de rectificaión en el nuevo Reglamento le acompaña un derecho a completar los datos que obran en poder del responsable del tratamiento.

El derecho de cancelación se enuncia como derecho de supresión ("derecho al olvido") en el artículo 17 RGPD, ya mencionado. Este derecho a la supresión de los datos se activa bajo la presencia de determinadas circunstancias, como son que: a) los datos personales ya no sean necesarios si atendemos a los fines para los que fueron recogidos; b) el interesado retire el consentimiento en que se basa el tratamiento (un consentimiento explícito con fines específicos); c) el interesado se oponga al tratamiento; d) los datos personales hayan sido tratados ilícitamente; e) cuando hayan de suprimirse los datos personales para cumplir una obligación legal; f) los datos personales de los niños. Ahora bien, este derecho de supresión cede en determinados casos como son en todos aquellos en que el tratamiento sea necesario: a) para ejercer el derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal; c) por razones de interés público en el ámbito de la salud pública; d) con fines de archivo en interés público.

El artículo 18 RGPD recoge el nuevo derecho a la limitación del tratamiento. Es un derecho que tiene el interesado frente al responsable. Para poder ejercitarlo ha de cumplirse alguna de las siguientes condiciones: que el interesado haya impugnado la exactitud de sus datos personales y solicite la limitación durante el tiempo que el responsable necesite para verificar la exactitud de los mismos; que el tratamiento sea ilícito y en lugar de solicitar la supresión el interesado haya optado por la limitación; el responsable no necesite los datos para los fines del tratamiento pero el interesado los necesite para la formulación, ejercicio o defensa de reclamanciones; y en caso de ejercicio del derecho de oposición al tratamiento por parte del interesado en el interin en el cual se dilucida qué interés prevalece, o como dice el Reglamento, qué "motivos legítimos" prevalecen, si los del interesado o los del responsable.

[325] TRONCOSO REIGADA, A., *La Protección de Datos...*, op. cit., p. 559.

Por último, el Derecho de oposición lo recoge el artículo 21 del RGPD. La LOPD mencionaba este derecho en el artículo 17 y se desarrollaba en los artículos 34 a 36 del RLOPD; hoy, lo contempla el art. 18 LO 3/2018.

2.4.3. El dato dactiloscópico como dato de carácter personal.

La aproximación al concepto de dato biométrico se llevará a cabo desde una perspectiva jurídica y, en concreto, desde el concepto de dato de carácter personal, analizando si el dato biométrico se puede considerar, o no, un dato de carácter personal, resultando para ello imprescindible delimitar primero el concepto de dato de carácter personal. Aunque, sin duda, cabría plantear el análisis del dato biométrico desde otras perspectivas, técnica, policial, psicológica o social, que harían surgir otras muchas y muy diversas cuestiones en relación con el tratamiento de datos biométricos de individuos[326], nosotros nos limitaremos a la perspectiva jurídica.

Por tanto, la primera tarea consistirá en delimitar el concepto de dato de carácter personal, ya que, de su delimitación, cabrá deducir lo que puede considerarse incluido dentro de sus límites y lo que habrá de considerarse fuera de ellos. Y, en definitiva, si el dato biométrico es o no dato de carácter personal, y le es de aplicación la legislación sobre protección de datos. Como veremos a continuación, la normativa de protección de datos no siempre es aplicable a la tutela de los datos de un individuo. Hay datos personales, referidos a una persona, que sin embargo no reúnen las características que permite predicar de ellos la "etiqueta" de dato de carácter personal. Por todo ello, la delimitación del concepto de dato de carácter personal reviste tanta importancia.

[326] Consideramos especialmente interesante e incisivo el comentario que Arzoz Santisteban hace respecto a las medidas de vigilancia estatales de la esfera privada que junto al control de las telecomunicaciones y los datos biométricos pueden hacer derivar peligros para las estructuras democráticas actualmente establecidas. Aunque también cabe afirmar, desde el punto de vista opuesto, que existen peligros sociales que estriban en un Estado que minusvalora el miedo de la población a la criminalidad y que no hace todo lo posible para combatirla. Un ejemplo de ello podrían ser los episodios de vandalismo extremo y violencia en la calle protagonizados por centenares de jóvenes en agosto de 2011 en el Reino Unido. Cfr. ARZOZ SANTISTEBAN, X., op. cit., p. 27.

Ya en 1981[327], el Convenio 108 del Consejo de Europa plasmó la necesidad de reforzar la protección jurídica de los individuos frente a la amenaza proveniente de los tratamientos automatizados de datos personales. El Convenio nació con la vocación de armonizar el derecho a la protección de los datos de los individuos y la libre circulación de las informaciones a través de las fronteras, reduciendo su ámbito al tratamiento automatizado. El artículo 1 establecía que: *"*El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física, sean cuales fueran su nacionalidad o su residencia, el respeto a sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona*"*. Y, a continuación, en el artículo 2 define los datos de carácter personal como: "cualquier información relativa a una persona física identificada o identificable*"*. Es importante reseñar el potencial unificador de la normativa sobre protección de datos a nivel internacional que podía desplegar este Convenio. Ello deriva del carácter abierto a la adhesión al Convenio para Estados no miembros del Consejo de Europa[328]. Esa vocación armonizadora apuntada por el Convenio 108[329], fue recogida explícita y claramente por el artículo 1, apartados 1 y 2, de la Directiva 95/46/CE. El artículo 1.1 planteaba como objeto de la Directiva: "(…) la protección de las libertades y los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales*"*. Pero el apartado 2, de este mismo artículo 1, añadía lo que para Heredero Higueras[330], es el verdadero objeto de la ya derogada Directiva y que jerárquicamente prevalece sobre el primero que es, ahora ya sí, facilitar la libre circulación de los datos personales entre los Estados miembros superando las posibles

[327] Hay que tener en cuenta que, con anterioridad al Convenio 108, ya desde 1974, existía una inquietud en Europa en orden a la elaboración de una Directiva de protección de datos. De hecho, desde 1970, en el *land* de Hesse, y desde 1972, en Suecia, existían leyes de protección de datos. Por su parte, la Comisión de las Comunidades Europeas, en noviembre de 1973 publicó la comunicación que con el título *"*Una política comunitaria de informática*"* planteaba la preocupación del tratamiento automatizado de los datos personales en el ámbito de los derechos y libertades de los individuos. No es hasta el 8 de mayo de 1979 cuando el Parlamento Europeo aprueba una Resolución con una serie de Recomendaciones y el informe *Bayerl* que contenía los antecedentes y justificación de cada una de dichas recomendaciones. En esta Resolución de 1979 se encuentra el germen de la -que iba a ser entonces- futura Directiva de protección de datos. Cfr. HEREDERO HIGUERAS, M., op. cit., pp. 17 y ss.

[328] Actualmente de las 46 Partes Contratantes del Convenio 108, 45 son Estados miembros del Consejo de Europa y hay un Estado no europeo, Uruguay que se adhirió en 2013. Marruecos está en proceso de formalización de su adhesión. Cfr. Agencia de los Derechos Fundamentales de la Unión Europea (FRA). *Manual de legislación europea…*, op. cit., p. 17.

[329] Discrepa de esta opinión Heredero Higueras, para quien el Convenio persigue la protección de las personas frente al tratamiento automatizado incontrolado de sus datos de carácter personal. HEREDERO HIGUERAS, M., op. cit., p. 69.

[330] Ibíd., p. 70.

disparidades existentes en sus legislaciones internas. Establecía este artículo 1.2. *"*Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1*."*. Es relevante, desde este momento inicial, destacar la importancia de este fin de la Directiva, pues en lo que nunca debe convertirse la legislación de protección de datos es en un obstáculo a la circulación de los datos sino, muy al contrario, en la garantía de un tráfico de datos respetuoso con los derechos individuales.

A continuación, la aproximación a la delimitación del concepto de dato de carácter personal la realizaremos teniendo como guía el derecho positivo y a través de los siguientes cuatro elementos: Primero: Dato de carácter personal como "toda información sobre una persona"; Segundo: información extractada registrada en soporte físico que la haga susceptible de tratamiento. El concepto de fichero de datos; Tercero: Exclusiones de datos de personas jurídicas, especialidad en el empresario individual y el profesional, y de personas fallecidas y Cuarto: Inclusiones en el concepto de dato de carácter personal de la dirección IP.

2.4.3.1. Titular del dato: la persona física.

Desde los orígenes de la regulación de la protección de datos ha sido siempre el individuo, la persona física, la protegida. Ahora, el RGPD, en su considerando primero, así lo reconoce diciendo expresamente:

> *"*La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*"*

> Y el Preámbulo de la LO 3/2018 (párrafo I)[331] nos deleita con el reconocimiento de la protección de las personas físicas en relación con el tratamiento de datos personales como un derecho fundamental recogido en el art. 18.4 CE.

Pero pasando ya propiamente al concepto de dato de carácter personal la Directiva 95/46/CE establecía un concepto amplio definiéndolo así en su artículo 2 a):

> «"datos personales": toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».

Así pues, el concepto de dato de carácter personal va unido a la identificación o, en palabras de Piñar Mañas, "(…) es el que entrelaza sin fisuras la privacidad y el derecho a la identidad"[332]. Si un dato no se puede asociar a "una persona, identificada o identificable", no es dato de carácter personal, con los efectos de aplicabilidad de la legislación específica. Si el dato se asocia, no a una, sino a un grupo o grupos de personas o a varias personas dentro de un grupo o de distintos grupos, no es dato de carácter personal.

Esto es así porque el objetivo de las normas incluidas en la citada Directiva era proteger a las personas como individuos. Tanto el artículo 1 de la Directiva 95/46/CE como el artículo 1 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la

[331] En dicho párrafo, el preámbulo de la ley no deja pasar la ocasión para señalar que, tanto la STC 94/1998, de 4 de mayo, como la STC 292/2000, de 30 de noviembre, ya señalaron que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre los mismos, siendo éste "un derecho autónomo e independiente, que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso".

[332] PIÑAR MAÑAS, J.L., "Concepto de dato de carácter personal*"* en Troncoso Reigada, A. (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de carácter personal*, Cizur Menor, Civitas, 2010, p. 184.

intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), determinaban que el principal objetivo de las normas que contienen es proteger las libertades y los derechos fundamentales[333] de las personas físicas y, en particular, su derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. Este objetivo no podría cumplirse si los datos no son atribuibles a una persona por ausencia de objeto de protección. En este sentido, el Considerando 26 de la Directiva 95/46/CE advertía que para determinar si una persona es identificable y, así, convertir en dato de carácter personal la información relativa a ella hay que tener en cuenta el conjunto de medios que pueden ser razonablemente utilizados por el responsable del tratamiento, o por cualquier otra persona, para identificar al interesado. Si esos medios fueran desproporcionados habría que concluir que la persona no es identificable. Ni el legislador nacional ni el europeo determina quién debe ser el que establezca la asociación ni cómo o con qué medios ha de hacerse únicamente, como expone Nicolás Jiménez[334], si esa posibilidad de asociación existe el dato se incluye ya en el ámbito de aplicación de los principios de la protección de los datos de carácter personal. Por lo expuesto, la cualificación del dato como dato de carácter personal deriva de la posibilidad de la relación o vinculación con una persona concreta, si esa vinculación no es posible podemos estar ante un dato personal pero no ante un dato de carácter personal. Esta distinción es apreciada por Heredero Higueras[335], ya que un dato puede ser personal porque se refiere a características, cualidades, aspectos de una persona humana[336], pero si no es posible establecer una relación o

[333] La Directiva y las normas de protección de datos personales sobrepasan, sin excluirlo, el ámbito, más reducido, de protección del respeto a la intimidad, a la vida privada y familiar para abarcar la protección de las libertades y los derechos fundamentales de las personas físicas en general. En este sentido, es importante señalar que el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea consagra la protección de los datos de carácter personal como un derecho independiente, autónomo, distinto del derecho al respeto a la vida privada, que se recoge en su artículo 7.

[334] NICOLÁS JIMÉNEZ, P., *La protección jurídica…,* op. cit., p. 65.

[335] HEREDERO HIGUERAS, M., op. cit., p. 73.

[336] En este mismo sentido el artículo 2.1. del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de datos personales relativa a la prevención, investigación, detección o enjuiciamiento de infracciones penales aprobado por DECISIÓN (UE) 2016/2220 del CONSEJO de 2 de diciembre de 2016. Según el citado artículo 2 del conocido como *Umbrella Agreement* "Se entenderá por «datos personales» toda información referida a una persona física identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante referencia, en particular, a un número de identificación o a uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social". Disponible en: https://www.boe.es/doue/2016/336/L00001-00013.pdf Consulta 25/09/2017.

vinculación con un individuo concreto, no es un dato de carácter personal y no le es de aplicación la normativa específica de protección para datos de este carácter[337].

La definición del artículo 2 a) de la Directiva, que hemos reproducido, recoge una serie de instrumentos que, directa o indirectamente, pueden determinar la identidad de un individuo. No ha de entenderse que se trata de una enumeración cerrada, sino más bien una enumeración *ad exemplum* donde caben otros medios para identificar, por eso el texto definitivo del artículo recoge la expresión "en particular", no cerrando la lista en un *numerus clausus*, sino más bien convirtiéndola en un *numerus apertus*. De este modo, la vinculación del dato con una persona concreta, convirtiéndolo en dato de carácter personal, puede establecerse de manera directa con el nombre y apellidos o bien indirectamente con un número de teléfono fijo o móvil, la matrícula de un coche, el número de la Seguridad Social, el DNI, un cargo ocupado por la persona, su imagen, su voz, las huellas dactilares o las características genéticas (ADN)[338]. En todo caso, nuestro ADN es una especificación larguísima. Las características genéticas de una persona pueden informar, por ejemplo, de determinados riesgos de salud, como cierta propensión a determinados riesgos cardiovasculares, pero, *a priori*, no permiten identificar al individuo en cuestión. Una cuestión distinta es analizar la información genética que hay que reunir para poder identificar a una determinada persona. En este sentido, el GPD 29, en su Dictamen 4/2007[339] sobre el concepto de datos personales, considera identificable a la persona cuando, aunque no se la haya identificado todavía, sea posible hacerlo a partir de los denominados identificadores, bien sea de forma directa o indirecta; identificadores, que directamente permiten la identificación de una persona son, sin duda, su nombre y apellidos, pero también la imagen de su rostro. Más dudoso es considerar como identificador directo el patrón de su huella dactilar ya que éste debe de combinarse con otros identificadores porque, aunque la huella dactilar sea única de cada individuo y, por tanto, le identifique, no es directamente asociable a un

[337] Así resulta, como se ha expuesto, del Considerando 26 de la Directiva que dice textualmente: *"*(…)*;* que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado*;* (…) *"*.

[338] Herederos Higueras enumera como medios indirectos para establecer la vinculación con una persona un elemento biométrico como son las huellas dactilares constituyendo instrumentos indudables de identificación de los individuos. Cfr. HEREDERO HIGUERAS, M., op. cit., p. 74.

[339] Grupo de Trabajo del artículo 29. Dictamen 4/2007 sobre el concepto de datos personales adoptado el 20 de junio 01248/07/ES WP 136. Página 6. Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

nombre y apellidos[340]. Cabría, no obstante, plantear que el patrón de huella dactilar, o de cualquier otro elemento biométrico, al ser único se puede considerar como un identificador único universal[341] del que extraer, asociados a él, datos personales del individuo que cobran relevancia en el ámbito de la protección de datos. No en vano, el RGPD, al definir en su artículo 4 punto 14) los datos biométricos, cita expresamente *ad exemplum* a las "[…] imágenes faciales o datos dactiloscópicos;". Por ello entendemos que el nuevo Reglamento considera al dato dactiloscópico identificador del individuo y, por ende, dato de carácter personal. Por su parte la AEPD, en su Memoria del año 1999, hace mención a esta cuestión bajo el epígrafe "Tratamiento de la huella digital de los trabajadores"[342]. La AEPD resuelve la cuestión del tratamiento de la huella dactilar de los funcionarios de una Corporación Local en base a la normativa, por entonces vigente, es decir, la LORTAD. La AEPD parte de considerar a los datos biométricos como: "[…] aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión (tales como las huellas digitales, el iris del ojo, la voz, etc.)". A la luz del artículo 3 a) LORTAD, que definía los datos de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables", la Agencia concluye que los datos biométricos son datos de carácter personal ya que permiten la identificación de las personas y, por tanto, su tratamiento debe acomodarse a la LORTAD. Dá un paso más la Agencia y se plantea si ese tratamiento puede considerarse excesivo respecto del fin que lo legitima atendiendo al principio de proporcionalidad. Y es aquí donde la Agencia emite su opinión sobre la naturaleza del dato biomátrico, al decir que es dato de carácter personal y al no contener ningún aspecto concreto de la personalidad limitando su función a

[340] Troncoso advierte que los datos biométricos aun generando una plantilla, un algoritmo informatizado, que es único lo cierto es que por sí solo no identifica a una persona. Este autor afirma que: " […] cuando los datos biométricos, como una plantilla, se almacenan de manera que el responsable del tratamiento o cualquier otra persona no pueden identificar al interesado, dichos datos no tienen la consideración de datos personales. La identificabilidad de la persona depende de la disponibilidad de otros datos". Cfr. TRONCOSO REIGADA, A., *La protección de datos…*, op. cit., (Nota al pie núm. 115), p. 220.

[341] La preocupación por el uso de identificadores universales está específicamente recogida en el apartado 7 del artículo 8 de la Directiva 95/46 que dice: "Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento". La Directiva deja a criterio de los Estados el cauce legal, ley o reglamento, y las condiciones en las que un identificador de carácter general pueda utilizarse, no prohibiendo, en todo caso, su tratamiento.

[342] *Memoria de la Agencia Española de Protección de Datos 1999*. "3.2.1.3. Tratamiento de la huella digital de los trabajadores por el empresario". Disponible en: https://www.aepd.es/media/memorias/memoria-AEPD-1999.pdf [Fecha de consulta: 10/10/2018].

identificar a un sujeto considera que: "[…] su tratamiento no tendrá mayor trascendencia que el de los datos relativos a un número de identificación personal, a una ficha que tan solo pueda utilizar una persona o a la combinación de ambos". Consideramos que, en este punto, la Agencia generaliza en exceso al decir que el dato biométrico no contiene ningún aspecto concreto de la personalidad porque incluso hasta una huella dactilar puede revelar aspectos de la personalidad del individuo (un desgaste excesivo puede revelar datos sobre el trabajo u ocupaciones de su titular) que éste tiene derecho a que permanezcan protegidos. En lo referente al tratamiento inconsentido hay que tener en cuenta que dicho tratamiento queda dentro del ámbito del desarrollo de una relación estatutaria que vincula al funcionario con la Administración y, por ello, cabe dicho tratamiento inconsentido al amparo del, entonces, artículo 6.2 LORTAD, después recogido en el artículo 6.2 LOPD y, actualmente, en los artículos 6.1. b), c), e), f) del RGPD y 6 de la LO 3/2018; esta nueva ley advierte que el tratamiento inconsentido puede derivarse de que ese tratamiento tenga una pluralidad de finalidades y no se haya otorgado el consentimiento para todas ellas, deviniendo, entonces, en inconsentido una finalidad a la que no se haya hecho referencia.

El tratamiento queda, no obstante, sometido al resto de disposiciones de la ley y en concreto el derecho de información en la recogida por el que los funcionarios deberían haber sido informados previamente de los extremos que recogía el artículo 5.1 LOPD y recogen los art. 13 RGPD y 11 LO 3/2018; cuando los datos personales son obtenidos del afectado, el responsable debe facilitar a dicho afectado una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a información adicional, siendo la información básica que debe de facilitarle en el momento la identidad del responsable del tratamiento y de su representante, la finalidad del tratamiento y la posibilidad de ejercer los derechos del titular.

En relación con los identificadores indirectos, el citado Dictamen 4/2007 afirma que son elementos que indirectamente permiten distinguir a la persona del resto y, en este sentido, establece:

> "hay que combinar el nombre y apellidos de la persona con otros datos (fecha de nacimiento, nombres de los padres, dirección o una fotografía de su rostro) para evitar toda confusión con otras personas del mismo nombre

> y apellidos. (…) Así pues, a través de los identificadores la información original se asocia con una persona física que puede ser distinguida de otros individuos.
>
> Por su parte, cuando hablamos de 'indirectamente' identificadas o identificables, nos estamos refiriendo en general al fenómeno de las 'combinaciones únicas', sean éstas pequeñas o grandes. En los casos en que, a primera vista, los identificadores disponibles no permiten singularizar a una persona determinada, ésta aún puede ser 'identificable', porque esa información combinada con otros datos (tanto si el responsable de su tratamiento tiene conocimiento de ellos como si no) permitirá distinguir a esas personas de otras. Aquí es donde la Directiva se refería a 'uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social'. El nuevo Reglamento añade el elemento propio de la identidad genética como medio indirecto para determinar la identidad de una persona. Algunas de esas características son tan únicas que permiten identificar a una persona sin esfuerzo (…), pero una combinación de detalles pertenecientes a distintas categorías (edad, origen regional, etc.) también puede ser lo bastante concluyente en algunas circunstancias, en especial si se tiene acceso a información adicional de determinado tipo. (…)".

En los párrafos transcritos, el GPD 29 distingue, por un lado, un sistema de identificación indirecta de personas a través de combinaciones de detalles. La combinación de distintos aspectos característicos de una persona permite obtener lo que el grupo denomina "combinaciones únicas". Estas combinaciones únicas permiten ya la identificación de un individuo y convierten en datos de carácter personal todos los datos combinados. De este método de identificación indirecto, por combinación, convierte en dato de carácter personal información que, por separado, deslavazada, no lo es. Por otro lado, el Dictamen que venimos comentando, llama la atención sobre identificación de personas sin acudir a su nombre y apellidos, sino a través de un identificador único asignado en un fichero informatizado. Y cómo no, en Internet, una dirección IP es un identificador único de máquina y, por extensión, de los comportamientos de la persona que la maneja que puede llevar a incluir a esa persona en una categoría sin, ni siquiera, conocer su nombre y apellidos. Con todo ello, el concepto de datos de carácter personal,

y de tratamiento de datos personales, queda ampliado, encontrándose las situaciones enunciadas, bajo el amparo de protección de la Directiva 95/46.

El RGPD recoge todo este bagaje doctrinal, legislativo y jurisprudencial y en su artículo 4.1 define los datos personales como:

> "[…] toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;"

Y en el apartado 14 de este mismo artículo 4 incluye a los datos biométricos sin ambages en la categoría de datos personales diciendo:

> "[…] datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;"

Al llegar a este punto, conviene señalar que, si bien la identificación a través del nombre y apellidos es en la práctica lo más habitual, esa información puede no ser necesaria en todos los casos para identificar a una persona. Así, puede suceder cuando se utilizan otros 'identificadores' para singularizar a alguien. Efectivamente, los ficheros informatizados de datos personales suelen asignar un identificador único a las personas registradas para evitar toda confusión entre dos personas incluidas en el fichero. También en Internet, las herramientas de control de tráfico permiten identificar con facilidad el comportamiento de una máquina y, por tanto, la del usuario que se encuentra detrás. Así pues, se unen las diferentes piezas que componen la personalidad del individuo con el fin de atribuirle determinadas decisiones. A estos

identificadores hace expresamente referencia el RGPD en su artículo 4.1. al decir: "[…] en particular mediante un identificador […] un identificador en línea […]". Sin ni siquiera solicitar el nombre y la dirección de la persona es posible incluirla en una categoría, sobre la base de criterios socioeconómicos, psicológicos, filosóficos o de otro tipo, y atribuirle determinadas decisiones puesto que el punto de contacto del individuo (un ordenador) hace innecesario conocer su identidad en sentido estricto. En otras palabras, la posibilidad de identificar a una persona ya no equivale necesariamente a la capacidad de poder llegar a conocer su nombre y apellidos. La definición de persona física identificada o identificable refleja este hecho.

El TJUE se ha pronunciado en este sentido al considerar que "la conducta que consiste en hacer referencia, en una página *web*, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un tratamiento […] de datos personales en el sentido del artículo 3, apartado 1, de la Directiva 95/46". En el siguiente epígrafe nos aproximaremos al concepto de tratamiento, dejando únicamente aquí apuntado este criterio.

A nuestro entender, tanto en su momento la Directiva en su artículo 2, como actualmente el RGPD en su artículo 4.1., enumeran una serie de elementos de identificación sin clasificarlos de forma rígida en directos o indirectos. Es la doctrina y, también, el GPD 29 en el Dictamen al que más arriba se ha hecho referencia, los que consideran, entre otras, las características de la identidad física, fisiológica o psíquica de un individuo elementos que indirectamente pueden determinar su identidad; si bien, entendemos, que un elemento físico como es la imagen de una persona la identifica directamente. En cualquier caso, es tan amplia la lista de identificadores a la que el GPD 29 se refiere, donde hasta los números asignados a una máquina por las herramientas de control de tráfico en Internet pueden convertir en tratamiento de datos personales el efectuado en dicho ordenador, que cabría sostener, como así lo hacemos, que uno solo de esos elementos específicos como la imagen del rostro de una persona, es por sí solo identificador directo válido que permite convertir un simple dato personal, asociado a dicha imagen, en un dato de carácter personal al que es de aplicación la legislación de

protección de datos[343]. Y viene a corroborar esta interpretación el artículo 4.14. del RGPD que incluye como dato personal, en la categoría de dato biométrico, la imagen facial. Otra cuestión es si el patrón de huella dactilar o de iris, un patrón de comportamiento en el uso del teclado, por sí solos identifican directamente a un individuo. Entendemos que no se pueden considerar identificadores directos, pero sí indirectos[344] pues al ser únicos pueden considerarse identificadores únicos del individuo como si de su DNI vital se tratara. Como veremos más adelante, el número del Documento Nacional de Identidad debe considerarse, por sí solo, dato de carácter personal.

Siguiendo con el análisis del concepto de dato de carácter personal utilizado en la Directiva 95/46/CE, y también en el RGPD, éste es un concepto tan lato, tan amplio, que abarca "toda información"[345] entendiendo por tal todo tipo de afirmaciones sobre una persona. Así, datos personales no son exclusivamente los referidos a la vida íntima, o privada[346] o familiar de un individuo sino también todos aquellos datos referidos a sus relaciones laborales, económicas, profesionales o sociales, en general. En este sentido, la STC 292/2000, de 30 de noviembre, en su Fundamento Jurídico 6º, en relación al objeto de amparo constitucional declara que, no son solo los que cabría denominar datos íntimos los protegidos, sino que la protección es más amplia porque el concepto de dato de carácter personal lo es. Reproducimos, en parte, este Fundamento Jurídico por su trascendencia en la materia que nos ocupa:

[343] En todo caso no se debe olvidar que la Directiva, conforme a lo dispuesto en su artículo 3, es aplicable al tratamiento de datos de carácter personal no a los datos aisladamente considerados.
[344] Opinión, muy fundada, en contra es la expresada por TRONCOSO REIGADA, A., *La protección de datos…*, op. cit. p. 220.
[345] Como expone Heredero Higueras, la definición no detalla el tipo de información en que puede consistir un dato. La enmienda 12ª del Parlamento Europeo propuso la siguiente definición: "cualquier conjunto de datos personales, redes de datos, perfiles, sistemas integrados de sonido, imágenes, datos numéricos o textos, centralizados o repartidos en diversos emplazamientos, que sean objeto de un tratamiento automatizado o no, o que, sin serlo, estén estructurados y sean accesibles dentro de una recopilación organizada según criterios determinados con objeto de facilitar su utilización o interconexión". Este autor continúa diciendo que esta enmienda ha de ser considerada en relación con la enmienda 14ª que proponía suprimir la definición de fichero. HEREDERO HIGUERAS, M., op. cit., pp. 71-72.
[346] Además, hay que tener en cuenta que el concepto de vida privada y familiar es también sumamente amplio como así ha afirmado el TEDH en la Sentencia del asunto *Amann*/Suiza de 16 de febrero de 2000 en el apartado 65: «[…] el término "vida privada" no debe interpretarse restrictivamente. En especial, el respeto por la vida privada comprende el derecho a establecer y a desarrollar relaciones con otros seres humanos; además, no hay ninguna razón de principio que justifique la exclusión de actividades de una naturaleza profesional o empresarial de la noción de la "vida privada" […]. Esta interpretación amplia se corresponde con la del convenio del Consejo de Europa de 28 de enero de 1981 […]».

"La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.

[…]

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona,

pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (SSTC 73/1982, de 2 de diciembre, FJ 5; 110/1984, de 26 de noviembre, FJ 3; 89/1987, de 3 de junio, FJ 3; 231/1988, de 2 de diciembre, FJ 3; 197/1991, de 17 de octubre, FJ 3, y en general las SSTC 134/1999, de 15 de julio, 144/1999, de 22 de julio, y 115/2000, de 10 de mayo), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ 7)"[347].

[347] Tribunal Constitucional Pleno, S 30-11-2000, nº 292/2000, BOE 4/2001, de 4 de enero de 2001, rec. 1463/2000. EDJ 2000/40918 STC Pleno de 30 de noviembre de 2000. https://online.elderecho.com/seleccionProducto.do;jsessionid=9AD2FDB026DF4D82AFD26ADE672376C2.TC_ONLINE03?producto=PA#pestana_jurisprudencia Base de datos on-line de la editorial Lefebvre El Derecho. [Fecha de consulta: 16/04/2018].

El TC recoge lo que en la doctrina más especializada se ha denominado "la tipología de datos personales", que permite distinguir tres grupos de datos[348]: los referentes al corazón de la intimidad de un individuo, los referentes a su vida privada y los referentes a su vida pública. Son tres grupos que, a modo de círculos concéntricos desde el centro, lo más íntimo, al círculo más externo, lo más conocido, determinan diferentes niveles de acceso y protección. Abarcando los tres grupos de datos es como el derecho a la protección de datos despliega toda su potencialidad y afirma su carácter autónomo con respecto al derecho a la intimidad. Ésta es protegida y rebasada, siendo el derecho a la protección de datos garantía de otras libertades públicas y derechos fundamentales de las personas físicas.

Este análisis se ve corroborado y ampliado con el manifestado por el WP-DP del artículo 29 en el citado Dictamen 4/2007 al afirmar que, dato personal es todo tipo de información sobre una persona abarcando información objetiva y también opiniones, evaluaciones o informaciones subjetivas. El ámbito de las informaciones subjetivas no podía quedar fuera del concepto de dato personal y de la protección jurídica dispensada por la Directiva. Reproducimos, por su claridad y amplitud en la descripción de los distintos componentes que abarca el concepto de dato de carácter personal, el análisis recogido en este Dictamen 4/2007, que afirma:

> "La expresión <<toda información>> utilizada en la Directiva indica claramente la voluntad del legislador de dar un sentido amplio al concepto 'datos personales'. Esta redacción exige una interpretación amplia.
> Desde el punto de vista de la naturaleza de la información, el concepto de datos personales incluye todo tipo de afirmaciones sobre una persona. Por consiguiente, abarca información 'objetiva' como, por ejemplo, la presencia de determinada sustancia en su sangre, pero también informaciones, opiniones o evaluaciones 'subjetivas'. (…)"

[348] En el grupo central más íntimo se encuentran los datos especialmente protegidos, ideología, afiliación sindical, religión o creencias con mayores restricciones para su tratamiento, y los datos de salud, raza o vida sexual, también especialmente protegidos. Estos datos, aunque no son identificativos, al afectar a la esfera más íntima de la persona tienen un gran potencial discriminador. Un segundo grupo, amplio, lo constituirían los datos privados que no se quieren hacer públicos y el tercer grupo vendría constituido por los datos profesionales, laborales y económicos. TRONCOSO REIGADA, A., *La protección de datos…,* op. cit. pp. 780 y ss.

"Para que esas informaciones se consideren 'datos personales', no es necesario que sean verídicas o estén probadas. De hecho, las normas de protección de datos prevén la posibilidad de que la información sea incorrecta y confieren al interesado el derecho de acceder a esa información y de refutarla a través de los medios apropiados.

Desde el punto de vista del contenido de la información, el concepto de datos personales incluye todos aquellos datos que proporcionan información cualquiera que sea la clase de ésta. Por supuesto esto incluye la información personal considerada 'datos sensibles' en el artículo 8 de la Directiva a causa de su naturaleza particularmente delicada, pero también otras categorías más generales de información. El término 'datos personales' comprende la información relativa a la vida privada y familiar del individuo *stricto sensu,* pero también la información sobre cualquier tipo de actividad desarrollada por una persona, como la referida a sus relaciones laborales o a su actividad económica o social. El concepto de 'datos personales' abarca, por lo tanto, información sobre las personas, con independencia de su posición o capacidad (…)".

"Desde el punto de vista del formato o el soporte en que la información está contenida, el concepto de datos personales incluye la información disponible en cualquier forma, alfabética, numérica, gráfica, fotográfica o sonora, por ejemplo, desde este punto de vista, el concepto incluye la información conservada en papel, así como la información almacenada en una memoria de ordenador, utilizando un código binario, o en una cinta de video, por ejemplo. Se trata de una consecuencia lógica de la inclusión en su ámbito de aplicación del tratamiento automático de datos personales. En particular, los datos que consisten en sonidos e imágenes están calificados como datos personales desde este punto de vista, en la medida en que pueden contener información sobre una persona. A este respecto, la referencia particular a los datos consistentes en sonidos e imágenes del artículo 33[349] de la Directiva debe ser entendida como la confirmación de

[349] "Artículo 33: "La Comisión estudiará, en particular, la aplicación de la presente Directiva al tratamiento de datos que consistan en sonidos e imágenes relativos a personas físicas y presentará las propuestas pertinentes que puedan resultar necesarias en función de los avances de la tecnología de la información, y a la luz de los trabajos de la sociedad de la información." Este párrafo segundo del artículo

> que esta clase de datos entra en efecto en su ámbito de aplicación (siempre y cuando se cumplan las restantes condiciones) y de que la Directiva se aplica a ellos. (…). Por otra parte, para que la información sea considerada como datos personales no es necesario que esté recogida en una base de datos o en un fichero estructurado. También la información contenida en un texto libre en un documento electrónico puede calificarse como datos personales, siempre que se cumplan los otros criterios de la definición de datos personales. El correo electrónico, por ejemplo, contiene datos personales".

En consecuencia, la expresión "toda información" ciertamente es amplia, abarca información objetiva, subjetiva, verdadera o no, íntima o pública, referente a personas capaces o incapaces y en cualquier formato que se presente. Podemos afirmar que la definición de la Directiva es terminante y no deja lugar a dudas que, es a las personas a las que se refiere dicha información, las cuales son personas físicas, no jurídicas[350]. En este mismo sentido se pronuncia el Considerando (14) del RGPD[351].

Y en nuestro Derecho interno, la LOPD ofrecía una definición de dato de carácter personal en su artículo 3 a) como: *"*cualquier información concerniente a personas físicas identificadas o identificables[352]*"*. Por su parte, el art. 2 LO 3/2018 dispone que

---

33 fue agregado como respuesta a las preocupaciones manifestadas por la CNIL, en relación al tratamiento de imágenes y sonido. Cfr. HEREDERO HIGUERAS, M., op. cit., p. 232.

350 El Considerando 24 de la Directiva establecía: "Considerando que las legislaciones relativas a la protección de las personas jurídicas respecto del tratamiento de los datos que las conciernan no son objeto de la presente Directiva;"

351 Considerando (14) "La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto". En nuestra opinión esta es una redacción mejorada a la incluida en el Considerando (12) de la Propuesta de Reglamento (PRGPD) que decía: "La protección otorgada por el presente Reglamento se refiere a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de datos personales. Por lo que respecta al tratamiento de datos relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto, nadie puede invocar la protección del presente Reglamento. Ello también es de aplicación cuando el nombre de la persona jurídica incluya los nombres de una o más personas físicas".

352 Como desarrollo del concepto de persona identificable en relación con la delimitación del concepto de dato de carácter personal resulta de interés el artículo 5.1.o) del RLOPD, que establecía: *"*1. A los efectos previstos en este Reglamento, se entenderá por: (…) o) Persona identificable: Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados". Como es lógico la normativa referenciada sigue el concepto marcado por el artículo 2.a) de la Directiva 95/46/CE, que consideraba identificable a "toda persona cuya identidad pueda determinarse, directa o indirectamente, en

"la presente ley se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

La definición es muy amplia y, como indica Vizcaíno Calderón, únicamente cabría entender que, "quedan fuera del ámbito de la Ley los ficheros de datos personales en los que no estén identificadas personas y en el bien entendido que tampoco sean identificables por cualquiera de los medios actuales y, previsiblemente, futuros (…)"[353]. Tanto este autor como Ortí Vallejo[354] referencian el concepto de dato de carácter personal a la identificación.

Por su parte el RLOPD, definía en su artículo 5.1. f) los datos de carácter personal como*:* "Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"[355].

---

particular mediante un número de identificación o uno o varios elementos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social". En relación con la determinación de la identidad, el Considerando 26 de la propia Directiva advertía que para determinar si una persona es identificable, hay que considerar el conjunto de medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar al interesado. Un ejemplo práctico puede ilustrar el concepto "identificable": puede que un dato personal no permita identificar a una persona en general, pero sí dado un conjunto reducido de personas. Así la altura de 1 metro 90 no sirve para identificar a un español en concreto, no es un dato de carácter personal, pero dado un conjunto específico de personas, por ejemplo, los alumnos del grupo de 1ºde la ESO del colegio "x, entonces sí hace identificable al individuo porque solo hay una persona del grupo con esa altura lo que lo convierte en dato de carácter personal. Por conexión datos que por separado no tienen el carácter de personales se convierten en personales: la persona de 1º de la ESO del colegio "x" de 1,90 de altura.

[353] VIZCAÍNO CALDERÓN, M., *Comentarios a la Ley Orgánica de Protección de Datos de carácter personal*, Madrid, Civitas, 2001, p. 71.

[354] Ortí Vallejo sostiene, haciendo un comentario al artículo 3 a) de la antigua LORTAD, que un fichero de sonidos de una persona como por ejemplo los pulsos cardiológicos si permite la identificación del individuo, ha de considerarse sujeto a la Ley "(…) pese a que, en rigor, no se trate de un dato personal". Discrepamos en esta última afirmación ya que si la identificación es posible ese hipotético fichero de pulsos cardiológicos es un fichero de datos personales, y en concreto, de datos biométricos. Cfr. ORTÍ VALLEJO, A., *Derecho a la intimidad e informática, (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*, Granada, Comares, 1994, p. 73.

[355] Esta definición de dato de carácter personal tiene su antecedente inmediato en el artículo 1.4 del Real Decreto 1332/1994, de 20 de junio, que quedó derogado por el Real Decreto 1720/2007 (RLOPD), que consideraba dato de carácter personal: "toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable". El artículo 1.5 de este Real Decreto 1332/1994 cerraba el concepto de dato personal vinculando la identificación del afectado a "cualquier elemento que permita determinar, directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada".

La definición vuelve a ser lo suficientemente amplia como para entender comprendida en ella información en formato[356] digital y/o analógico[357], bien se trate de textos, imágenes o sonidos. Y si atendemos a lo dispuesto en el apartado o), de este mismo artículo 5.1 del Reglamento, al definir persona identificable se refiere a cualquier información referida a los múltiples aspectos que conforman la identidad de un individuo desde algo tan específico como su identidad física o fisiológica, a algo tan amplio como su identidad cultural. En definitiva, el contenido de la información, sea en formato digital o analógico, de texto, gráfica o acústica, siempre que se refiera a una persona, puede abarcar un espectro tan amplio como su físico, sus características fisiológicas, psíquicas, económicas, culturales o sociales. Es, por tanto, desde este encuadre de información concerniente, referida, a una persona física en todos los aspectos que conforma su identidad desde el que nos aproximaremos a la delimitación del concepto de dato biométrico, que, en principio, puede considerarse incluido, sin gran esfuerzo, en ese ámbito de la identidad personal. La información puede encontrarse en uno u otro formato, ser un sonido, una representación gráfica o fotográfica, una representación tipográfica o un algoritmo digital, es indiferente, sólo su capacidad de conexión con un individuo es lo absolutamente imprescindible. En este sentido, la información que proporciona el dato biométrico tiene, como veremos más adelante, esa capacidad de unión unívoca con la persona a la que pertenece.

Es muy significativa la definición de datos personales que contenía, en su artículo 4 apartado 2), la que fue PRGPD, que escuetamente utilizaba la expresión: "toda información relativa a un interesado". Esta propuesta traslada al concepto de interesado la delimitación del contenido de dato personal ya que define a aquél, en este mismo artículo 4 apartado 1), como: "toda persona física identificada o que pueda ser identificada, directa o indirectamente, por medios que puedan ser utilizados

[356] El GPD 29 ya ha puesto claramente de manifiesto cómo el soporte en que la información esté contenida no es obstáculo para su protección. De hecho, el formato del dato personal es muy amplio abarcando la forma alfabética, numérica, gráfica, fotográfica o sonora. Así la Directiva 95/46/CE recogía en su considerando 14: «considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos». Cfr. Grupo de Trabajo del artículo 29. Dictamen 4/2007 sobre el concepto de datos personales Adoptado el 20 de junio 01248/07/ES WP 136, p. 8. Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm [20 de marzo 2016].

[357] Prácticamente ya no se emplean registros analógicos, por ejemplo, las fotografías, las voces, las firmas se guardan ya todas en formato digital, salvo el poco registro que quede en papel, discos de vinilo, cintas de cassete, etc.

razonablemente por el responsable del tratamiento o por cualquier otra persona física o jurídica, en particular mediante un número de identificación, datos de localización, identificador en línea o uno o varios elementos específicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;"

Lo expuesto hasta ahora es aplicable a esta definición de la propuesta de Reglamento (PRGPD), pero cabría añadir dos notas nuevas que a nuestro parecer contiene esta definición con respecto al artículo 2 de la Directiva 95/46/CE: primero, se incluye en la propia definición de dato personal la referencia al responsable del tratamiento[358] o al que de *facto* lleve a cabo el proceso de identificación y, segundo, entre los identificadores se añaden los datos de localización, el identificador en línea y elementos de la identidad genética.

Por consiguiente, y a la luz de la normativa interna y europea citada, ni la naturaleza de la información, objetiva o subjetiva, ni su carácter veraz o falso, ni el ámbito íntimo, familiar, económico, laboral, o social a que se refiera, ni el formato o soporte en que se incorpore, son criterios válidos de delimitación del concepto de dato personal porque éste es tan amplio que abarca todos esos componentes. Ahora bien, si ese dato personal

[358] Entendemos que esta referencia expresa al responsable del tratamiento, o al que de hecho lleve a cabo la identificación, responde a la tendencia que en la actualidad presenta la protección de datos en Europa. Para acercarnos al nuevo rumbo de la protección de datos es muy ilustrativo el Dictamen 3/2010 sobre el principio de responsabilidad adoptado el 13 de julio de 2010 por el grupo de trabajo de protección de datos del artículo 29 (00062/10/ES, GT 173) http://ec.europa.eu/justice/policies/privacy/index_en.htm En este Dictamen, desde un enfoque de progreso en la práctica de la protección de datos, se hace referencia a la arquitectura jurídica general de dicha protección que ha de basarse en la responsabilidad. Así el GPD 29 en sus conclusiones dice que: "(…) está convencido de que el aumento no solo de los riesgos sino del valor de los datos personales en sí abundan en la necesidad de reforzar el papel y la responsabilidad de los responsables del tratamiento de datos. (…) Para estimular en la práctica la protección de datos (…) los responsables del tratamiento de datos apliquen medidas adecuadas y eficaces para garantizar el cumplimiento de los principios y obligaciones de la Directiva de protección de datos, demostrándolo ante las autoridades que se lo soliciten*"*. El papel y las funciones del responsable del tratamiento aumentan al constituir el pilar básico en la construcción de la nueva estructura general de protección de datos que, sin variar en esencia lo que constituyen los principios de dicha protección, necesita en la práctica que el modo en que se ejercen las competencias sobre un tratamiento y el modo en que esto puede comprobarse esté delimitado al atribuirse a una persona responsable. Como, así mismo, dice el GPD 29 en este Dictamen: "(…) Competencia y responsabilidad son dos caras de la misma moneda y sendos elementos esenciales de la gobernanza. Solo cuando la responsabilidad funciona en la práctica puede desarrollarse la confianza suficiente". Entendemos que la mención en la propia definición de interesado al responsable del tratamiento responde a este principio de responsabilidad *(accountability)* que ha de impregnar toda la protección de datos.

no es atribuible a una persona física concreta o por concretar, identificada o identificable[359], no será dato de carácter personal y no será objeto de nuestro interés.

2.4.3.1.1. Exclusiones.

En relación con las exclusiones se debe hacer mención a las personas jurídicas, al empresario individual, al profesional y a las personas fallecidas. Con respecto al concepto de persona física, que hemos calificado de cimiento de la estructura de la protección de datos de carácter personal, solo sus datos, los datos de la persona física, del hombre con independencia de su nacionalidad, sexo, raza o residencia, serán protegibles por esta normativa específica. Pero si sólo atenderemos a los datos de las personas físicas[360], qué ocurre con los datos de las personas jurídicas[361], o con los datos del empresario individual o del profesional y con los datos de personas físicas fallecidas. Sin perder la perspectiva del objeto de nuestro estudio, el dato personal

[359] El Dictamen 4/2007 del WP-DP al analizar el concepto de persona identificable establece: "De modo general, se puede considerar 'identificada' a una persona física cuando, dentro de un grupo de personas, la 'distingue' de todos los demás miembros del grupo. Por consiguiente, la persona física es 'identificable' cuando, aunque no se la haya identificado todavía, sea posible hacerlo (que es el significado del sufijo 'ble'). Así pues, esta segunda alternativa es, en la práctica, la condición suficiente para considerar que la información entra en el ámbito de aplicación del tercer componente. La identificación se logra normalmente a través de datos concretos que podemos llamar 'identificadores' y que tienen una relación privilegiada y muy cercana con una determinada persona. Cabe citar como ejemplos su apariencia exterior, es decir su altura, el color del cabello, la ropa, etc., o una cualidad de la persona que no puede percibirse inmediatamente, como su profesión, el cargo que ocupa, su nombre, etc. La Directiva menciona esos 'identificadores' en la definición de 'datos personales' del artículo 2 cuando establece que 'se declarará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. (…) el que determinados identificadores se consideren suficientes para lograr la identificación es algo que depende del contexto de la situación de que se trate. Un apellido muy común no bastará para identificar a una persona –es decir, para aislarla- dentro del conjunto de la población de un país, mientras que es probable que permita la identificación de un alumno dentro de una clase. Incluso una información auxiliar, como, por ejemplo, 'el hombre que lleva un traje negro', puede identificar a alguno de los transeúntes que esperan en un semáforo. Así pues, el que se identifique o no a la persona a la que se refiere una información depende de las circunstancias concretas del caso". Parece claro, en principio, que podemos calificar de 'identificadores' los elementos físicos o fisiológicos de un individuo, base del dato biométrico, dependiendo, eso sí, de las circunstancias que rodeen a dicho dato.

[360] El artículo 6 de la Declaración Universal de los Derechos Humanos hace referencia al concepto de persona física y afirma: "todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica". Este concepto de personalidad jurídica de los seres humanos ha de entenderse como capacidad de la persona, como individuo, para ser sujeto de relaciones jurídicas desde su nacimiento hasta su muerte.

[361] Algunas legislaciones como la de Austria, Italia, Luxemburgo, Dinamarca y Alemania, en algunos supuestos, consideran datos de carácter personal los referidos a las personas jurídicas. Este es un elemento claro de divergencia en la legislación y en la aplicación de la normativa de protección de datos en los Estados de la Unión Europea. TRONCOSO REIGADA, A., *La protección de datos…*, op. cit., p. 180.

biométrico, difícilmente predicable de una persona jurídica, pero, por qué no de un empresario individual o de un profesional; se hace necesaria la adecuada comprensión y análisis de estos ámbitos.

Ya el artículo 1 de la antigua LORTAD dejaba fuera de su marco protector a los datos de las personas jurídicas[362]. Pero cuál es el fundamento de excluir los datos de las personas jurídicas del ámbito de protección, aplicación, de la legislación de protección de datos. Aquí la respuesta viene por la exclusión expresa que hace la letra de la ley. El ámbito subjetivo de aplicación de la LOPD tampoco amparaba a las personas jurídicas porque la protección de los datos personales se refiere a la intimidad personal y familiar y una persona jurídica, una empresa, no tiene un ámbito de intimidad reconocido. Es más, la Directiva y la LOPD protegían un ámbito más amplio que el estricto de la intimidad, protegen la privacidad[363] de los individuos atribuible únicamente a las personas físicas. La privacidad se genera en torno a las manifestaciones del libre desarrollo de la personalidad que únicamente es predicable de los individuos, de los seres humanos. Así el artículo 1 de la LOPD en relación al objeto de la Ley establecía:

> "La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".

Una regulación tal no se recoge en la LO 3/2018 de un modo tan detallado.

---

[362] Orti Vallejo, en sus comentarios al artículo 1 de la LORTAD, destacaba la relevancia de la STC 214/1991 de 11 de noviembre, que insistió en que el concepto de honor que contempla la CE "no se refiere a las personas jurídicas, respecto a las cuales solo puede hablarse de dignidad, prestigio o autoridad moral. O sea, tienen derecho, pero no es de los de naturaleza fundamental, ni es un derecho de la personalidad, del que sólo gozan personas físicas. Esta concepción del Tribunal Constitucional, significaría que el hipotético honor de las personas jurídicas (prestigio lo denomina) no tendría protección constitucional y, por ende, protección dimanante de las Leyes que desarrollan este derecho." En definitiva, concluye este autor que las personas jurídicas carecen de derechos de la personalidad y por ello no les ampara la legislación específica de protección de datos. Ello no obsta, como sigue exponiendo Orti Vallejo, que el prestigio y el secreto de los datos de las personas jurídicas no goce de protección en otros ámbitos del ordenamiento jurídico como por ejemplo a través del artículo 1902 del Código civil. Cfr. ORTÍ VALLEJO, A., op. cit., pp. 74 y 75.

[363] La Exposición de Motivos de la antigua LORTAD señalaba a la privacidad y no la intimidad como eje de la protección considerándola como "un conjunto más amplio, más global, de facetas de la personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado".

Aquel artículo 1 LOPD, que fue desarrollado por el artículo 2 en sus apartados 2 y 3 del RLOPD, el cual recogía unas exclusiones en el ámbito objetivo de aplicación que ayudaban a delimitarlo, establecía:

> "2. Este Reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.
> 3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal".

Claramente el Reglamento excluía de su ámbito de aplicación a los datos de las personas jurídicas y, a nuestro entender, también excluía de forma clara a los datos de profesionales, en cuanto a su actividad profesional, y en general, los relativos a la actividad empresarial de un individuo. Entendemos, con Aparicio Salom[364], que el concepto de empresario abarca el ejercicio de una actividad tanto empresarial, artística, como profesional. Pero, además, el citado artículo 2.3., excluía los datos de contacto de las personas que prestan servicios en las empresas, ya sean empleados o colaboradores[365], bien entendido que la exclusión se refiere únicamente a los datos

[364] Aparicio Salom resuelve la posible cuestión de si existe, o no, distinción entre empresario y profesional. Para ello acude al concepto legal de empresario recogido en el artículo 80 de la Ley 39/1988, de 28 de diciembre, Reguladora de las Haciendas Locales que establece: "Se considera que una actividad se ejerce con carácter empresarial, profesional o artístico cuando suponga la ordenación por cuenta propia de medios de producción y de recursos humanos o de uno de ambos, con la finalidad de intervenir en la producción de bienes o servicios". Por tanto, este concepto de empresario engloba la actividad de empresarios y de profesionales. En definitiva, unos y otros, son personas que ordenan medios de producción o recursos humanos para producir bienes o servicios. Cfr. APARICIO SALOM, J., op. cit., pp. 50 y 51.

[365] En relación con esta exclusión de aplicación del Reglamento a los datos del personal de contacto en una empresa es relevante el Informe de la AEPD 2008/0078 que en la interpretación del artículo 2.2. del RLOPD dice: "En consecuencia, la Agencia ha venido señalando que en los supuestos en que el tratamiento del dato de la persona de contacto es meramente accidental en relación con la finalidad del tratamiento, referida realmente a las personas jurídicas en las que el sujeto presta sus servicios, no resulta de aplicación lo dispuesto en la Ley Orgánica 15/1999, viniendo el Reglamento a plasmar este principio.
No obstante, nuevamente, es necesario que el tratamiento del dato de la persona de contacto sea accesorio en relación con la finalidad perseguida. Ello se materializa mediante el cumplimiento de dos requisitos: El primero, que aparece expresamente recogido en el Reglamento será el de que los datos tratados se limiten

expresamente enumerados, es decir: nombre, apellidos, las funciones o puestos desempeñados, dirección postal o electrónica, teléfono y número de fax profesionales. Por consiguiente, y como indica Piñar Mañas, el tratamiento del dato del DNI, del empleado o colaborador, no quedaría excluido de la aplicación del Reglamento, y además la finalidad para la que tales datos pueden ser tratados, sigue diciendo este autor, es exclusivamente "como datos de contacto en las actividades propias de las relaciones empresariales o profesionales, no para otras finalidades distintas" [366].

Por consiguiente, si bien es cierto que la exclusión de los datos de la persona jurídica, de la empresa, es clara si los datos se refieren a una persona que ejerce individualmente una actividad empresarial o profesional, la ley matiza y solo los excluye de su ámbito de protección si hacen referencia a la persona única y exclusivamente en su calidad de comerciante, industrial o naviero y, cabría añadir, en su calidad de profesional.

A este respecto, es muy ilustrativo el Informe Jurídico 42/2008 de la AEPD que interpretó estos apartados 2 y 3 del artículo 2 del RLOPD de la siguiente manera:

> "A la vista de lo que se ha venido indicando cabe considerar que los datos referidos a los empresarios individuales y que aparecen exclusivamente ligados a su actividad comercial o mercantil, o que identifican, aún con su

---

efectivamente a los meramente necesarios para identificar al sujeto en la persona jurídica a la que presta sus servicios. Por este motivo, el Reglamento impone que el tratamiento se limite a los datos de nombre y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, teléfono y número de fax profesionales.
De este modo, cualquier tratamiento que contenga datos adicionales a los citados se encontrará plenamente sometido a la Ley Orgánica 15/1999, por exceder de lo meramente imprescindible para identificar al sujeto en cuanto contacto de quien realiza el tratamiento con otra empresa o persona jurídica.
Por ello, no se encontrarían excluidos de la Ley los ficheros en los que, por ejemplo, se incluyera el dato del documento nacional de identidad del sujeto, al no ser el mismo necesario para el mantenimiento del contacto empresarial. Igualmente, y por razones obvias, nunca podrá considerarse que se encuentran excluidos de la Ley Orgánica los ficheros del empresario respecto de su propio personal, en que la finalidad no será el mero contacto, sino el ejercicio de las potestades de organización y dirección que a aquél atribuye las leyes.
El segundo de los límites se encuentra, como en el supuesto contemplado en el artículo 2.3, en la finalidad que justifica el tratamiento. Como se ha venido indicando reiteradamente, la inclusión de los datos de la persona de contacto debe ser meramente accidental o incidental respecto de la verdadera finalidad perseguida por el tratamiento, que ha de residenciarse no en el sujeto, sino en la entidad en la que el mismo desarrolla su actividad o a la que aquél representa en sus relaciones con quienes tratan los datos.
De este modo, la finalidad del tratamiento debe perseguir una relación directa entre quienes traten el dato y la entidad y no entre aquéllos y quien ostente una determinada posición en la empresa. De este modo, el uso del dato debería dirigirse a la persona jurídica, siendo el dato del sujeto únicamente el medio para lograr esa finalidad".

[366] PIÑAR MAÑAS, J.L., "Concepto de dato…", op. cit., p. 196.

nombre y apellidos un determinado establecimiento o la marca de un determinado producto o servicio, como consecuencia de la existencia de una libre decisión empresarial adoptada en este sentido, no se encuentran sometidos a la protección conferida por la Ley Orgánica 15/1999. Éste es el criterio recogido por el artículo 2.3 del Reglamento de desarrollo de la Ley Orgánica 15/1999.

Al propio tiempo, el tratamiento ha de llevarse a cabo en el ámbito empresarial. Quiere ello decir que, a los efectos del tratamiento de los datos, la finalidad perseguida por quien trata el dato es la de recabar y mantener información sobre la empresa y no sobre el comerciante que la ha constituido.

Así, el tratamiento de los datos del empresario individual, con las limitaciones que se han venido señalando, para mantener una relación comercial con el mismo, podría encontrarse amparado por el artículo 2.3 del Reglamento, en conexión con las normas de la Ley Orgánica 15/1999 que se han venido indicando.

Sin embargo, no podrá considerarse amparado por el precepto, y en consecuencia excluido de la aplicación de la Ley orgánica 15/1999, el tratamiento de los datos del comerciante llevado a cabo no con la finalidad de mantener una relación empresarial con el establecimiento u organización que el mismo hubiera creado, sino para conocer la información del propio sujeto organizado en forma de empresa, siendo el destinatario del tratamiento no la empresa sino el propio empresario en tanto, por ejemplo, que consumidor individual.

En consecuencia, de lo que ha venido indicándose cabrá extraer dos conclusiones determinantes del alcance de lo dispuesto en el artículo 2.3 del Reglamento:

-Cabrá considerar que la legislación de protección de datos no es aplicable en los supuestos en los que los datos del comerciante sometidos a tratamiento hacen referencia únicamente al mismo en su condición de comerciante, industrial o naviero; es decir, a su actividad empresarial.

- Al propio tiempo, el uso de los datos deberá quedar limitado a las actividades empresariales; es decir, el sujeto respecto del que pretende llevarse a cabo el tratamiento es la empresa constituida por el comerciante

> industrial o naviero y no el empresario mismo que la hubiese constituido. Si la utilización de dichos datos se produjera en relación con ámbito distinto quedaría plenamente sometida a las disposiciones de la Ley Orgánica".

Como pone de manifiesto Aparicio Salom[367], y se desprende del informe transcrito, la AEPD optó por un criterio "finalístico" a la hora de determinar la aplicabilidad de la normativa sobre protección de datos al tratamiento de los datos referidos a los empresarios individuales. Así, si el tratamiento se efectúa en consideración a la empresa y tiene por finalidad exclusivamente analizar la actividad empresarial o profesional, no era aplicable la LOPD. Pero si el tratamiento también se realiza en consideración a la esfera privada del individuo, que ejerce esa actividad empresarial, teniendo por finalidad abarcar su vida privada, la LOPD era plenamente aplicable. En este sentido el Dictamen 4/2007 del WP-DP al analizar la palabra "sobre", incluida en la definición de dato de carácter personal, hace referencia al elemento "finalidad" y determina: "También la presencia de un elemento 'finalidad' puede ser lo que determine que la información verse 'sobre' determinada persona. Se puede considerar que ese elemento 'finalidad' existe cuando los datos se utilizan o es probable que se utilicen, teniendo en cuenta todas las circunstancias que rodean el caso concreto, con la finalidad de evaluar, tratar de determinada manera o influir en la situación o el comportamiento de una persona". Por tanto, habrá que atender a las circunstancias que rodean cada caso concreto, pero si los datos del empresario individual se utilizan con la finalidad de evaluar o influir en la situación o comportamiento del empresario como individuo, sin duda, no era de aplicación el régimen tuitivo de la LOPD puesto que como persona debe ver amparado su derecho a la protección de datos, y todo ello atendiendo al Considerando 2 de la Directiva 95/46/CE que establecía: "los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos;".

La LO 3/2018 recoge expresamente, en el art. 19, esta cuestión: "se presume amparado en lo dispuesto en el art. 6.1. f) el tratamiento de los datos de contacto y también de la

[367] APARICIO SALOM, J., ob. cit., p. 55.

función o puesto desempeñado de las personas físicas que presten sus servicios en una persona jurídica". La misma presunción opera para el tratamiento de datos relativos a empresarios individuales y profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no para entablar una relación como personas físicas.

En cuanto a los datos biométricos de las personas jurídicas, es evidente que no existen puesto que no podemos hablar de datos referentes a ellas porque no hay un cuerpo físico, no hay características físicas ni fisiológicas que mensurar, pero sí cabría hablar de datos biométricos del empresario individual, del comerciante o del profesional o del representante de la empresa. En el caso de los datos personales biométricos, objeto de nuestro estudio, habrá, por consiguiente, que atender a la finalidad del tratamiento de dichos datos, ya que si ésta es recabar y mantener información sobre la empresa y no sobre el comerciante que la ha constituido no será de aplicación la nueva ley. En principio, podemos afirmar que el dato biométrico al consistir en la mensuración de las características físicas, fisiológicas o de comportamiento del empresario o del profesional no se refiere a su condición de comerciante, industrial o naviero, es decir, a su actividad empresarial sino a las características de su cuerpo con independencia de la actividad a la que lo dedique. Así, por ejemplo, su huella dactilar será la misma ejerciendo su actividad mercantil o profesional que registrándose en la recepción de un hotel en sus vacaciones, por tanto, sólo la finalidad para la que se ha registrado esa huella será la que delimite el carácter personal, o no, del dato. Volvemos así al criterio finalístico para determinar la aplicabilidad de la normativa de protección de datos. Por ello, y siguiendo la interpretación dada por la Agencia al citado artículo 2.3 del Reglamento y atendiendo a las dos conclusiones que extrae, recordemos: la legislación de protección de datos no es aplicable en caso de que los datos del comerciante hagan referencia únicamente a su actividad empresarial y segundo, y fundamental, el uso de esos datos se limite a la actividad empresarial, es decir, que el sujeto respecto del que se lleva a cabo el tratamiento es la empresa, solo un tratamiento de datos biométricos que reúna ambas condiciones quedará excluido. En definitiva, un tratamiento de huella dactilar del empresario cuya finalidad sea el control de acceso a la empresa para el ejercicio de la actividad, sí podría quedar excluido, pero siempre que el tratamiento se limite a la actividad empresarial. El tratamiento de esos mismos datos con fines ajenos al desarrollo de dicha actividad quedaría plenamente dentro del ámbito de aplicación de la LOPD, ahora de la LO 3/2018.

Siguiendo con el análisis jurídico del concepto de persona titular de los datos ya hemos visto ha de tratarse de una persona física, identificada o identificable, y cabría preguntarse ¿viva? Si los datos se refieren a una persona que ha fallecido ¿ya no están amparados por la normativa específica de protección de datos? Esta es una cuestión que merece detenerse a estudiar.

Si atendemos a lo dispuesto en el artículo 32 del vigente Código Civil la personalidad civil se extingue por la muerte de las personas, en consecuencia, los derechos inherentes a la personalidad del individuo se extinguirían con su muerte. De hecho, el Dictamen 4/2007 del WP-DP al analizar el concepto de "persona física" hace referencia al concepto de personalidad[368] jurídica, en el sentido de capacidad de la persona para ser sujeto de relaciones jurídicas, y atribuye esta capacidad solo a las personas físicas vivas y así dice:

> "Al concepto de persona física se hace referencia en el artículo 6 de la Declaración Universal de los Derechos Humanos, en el que se afirma que 'todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica'. Los ordenamientos jurídicos de los Estados miembros, en general en su orden civil, delimitan con mayor precisión el concepto de personalidad de los seres humanos, entendida como la capacidad de que están dotadas las personas para ser sujetos de relaciones jurídicas, desde su nacimiento hasta su muerte. Los datos personales son, por lo tanto, datos relativos a seres vivos identificados o identificables en principio. (…)
>
> En principio, la información relativa a personas fallecidas no se debe considerar como datos personales sujetos a las normas de la Directiva, ya

[368] Este mismo Dictamen también se refiere al concepto de *'personalidad pretérita'* que debe entenderse como información sobre personas fallecidas. Si bien es verdad esta 'personalidad pretérita' se encuentra bajo otro ámbito de protección, en concreto el que le otorga el derecho a la propia imagen y el derecho al honor, lo cierto es que, por ejemplo, la obligación de confidencialidad del personal médico no termina con la muerte del paciente, sino que la legislación sobre el derecho a la propia imagen y al honor también ofrece protección a la memoria de los muertos. De hecho la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen otorga protección frente a las intromisiones que supongan una vulneración de los derechos al honor y a la intimidad que subsiste con posterioridad a la muerte de las personas y no impide el ejercicio de las acciones por las personas designadas en el testamento, su cónyuge, ascendientes, descendientes o hermanos que viviesen al tiempo de su fallecimiento o, a falta de todas ellas, el Ministerio Fiscal.

> que los difuntos dejan de ser personas físicas para el Derecho civil. Sin embargo, en determinados casos los datos de los difuntos aún pueden recibir indirectamente una cierta protección."

Este mismo hilo argumental utilizó la AEPD en su Informe Jurídico 61/2008 analizando las causas de exclusión del régimen de protección de datos a los datos de fallecidos afirmando que:

> "Así, la Agencia ha analizado si la muerte de las personas da lugar a la extinción del derecho a la protección de datos, ya que el artículo 32 del Código Civil dispone que 'la personalidad civil se extingue por la muerte de las personas', lo que determinaría, en principio, la extinción con la muerte de los derechos inherentes a la personalidad.
>
> En este sentido, se ha indicado en el informe de 23 de mayo de 2003, a la luz de lo señalado en la STC 292/2000, de 30 de noviembre, que 'si el derecho fundamental a la protección de datos ha de ser considerado como el derecho del individuo a decidir sobre la posibilidad de que un tercero pueda conocer y tratar la información que le es propia, lo que se traduce en la prestación de su consentimiento al tratamiento, en el deber de ser informado y en el ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición, es evidente que dicho derecho desaparece por la muerte de las personas, por lo que los tratamientos de datos de personas fallecidas no podrían considerarse comprendidos dentro del ámbito de aplicación de la Ley Orgánica 15/1999"

No obstante ser esta la base del planteamiento, el GPD 29, en el citado Dictamen 4/2007, admite un margen de actuación al legislador nacional que puede ampliar las disposiciones de la legislación interna sobre protección de datos a algunos aspectos referentes al tratamiento de los datos de personas fallecidas siempre que exista un interés legítimo que lo justifique[369]. En este sentido, el Dictamen hace referencia a un

[369] En Portugal la legislación sobre protección de datos se aplica a las personas fallecidas en base a una interpretación de dicha legislación y del Código Civil hecha por la autoridad de protección de datos. En Luxemburgo está autorizado a familiares cercanos el acceso a la información de la última enfermedad del difunto. Francia admite la posibilidad de que los familiares requieran al responsable del fichero para que

supuesto de hecho en el que, indirectamente, el dato de salud de una persona fallecida puede ser objeto de protección pues afecta a una persona viva. El dictamen reconoce que:

> "(…), la información sobre personas fallecidas también puede hacer referencia a personas vivas. Por ejemplo, la información de que Menganita, ya fallecida, era portadora del gen de la hemofilia indica que su hijo Fulano también puede sufrir la misma enfermedad, pues dicha enfermedad está ligada a un gen contenido en el cromosoma X. Así pues, cuando se considere que la información proporcionada por los datos sobre una persona fallecida también se refiere al mismo tiempo a una persona viva, constituyendo datos personales sujetos a la Directiva, los datos personales del difunto podrán disfrutar indirectamente del amparo de las normas de protección de datos.

Este supuesto de datos de salud de personas fallecidas podría ser extrapolable, en algún caso, a datos biométricos de una persona fallecida, por ejemplo, en caso de huellas dactilares, o información del iris de fallecidos que evidencien una enfermedad de carácter hereditario.

Pero, en todo caso, la cuestión está en estudiar si directamente estos datos de fallecidos pueden gozar del amparo de la legislación de protección de datos sin acudir a supuestos indirectos de protección en atención a la repercusión de dichos datos sobre personas vivas.

Expresamente, en nuestro Derecho interno, el artículo 2.4 del RLOPD abordó el tema de la siguiente manera:

> "Este Reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el

rectifique haciendo constar el fallecimiento. TRONCOSO REIGADA, A., *La protección de datos…,* op. cit., p. 180.

óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos".

A nuestro entender, este artículo debe ser interpretado en relación con los apartados 3 y 5 del artículo 4 de la LOPD que establecían que:

"3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
(…)
5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados".

La LO 3/2018 contempla, en su art. 3.1, "las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse al responsable o encargado del tratamiento, al objeto de solicitar el acceso a los datos personales de aquélla, y, en su caso, su rectificación o supresión". Añade, como excepción que "los familiares o herederos no podrán acceder a los datos del causante ni rectificarlos o surprimirlos, si la persona fallecida lo ha prohibido expresamente o así lo establece una ley".

No en todos los casos, pero sí en la mayoría, una vez fallecida una persona ya no es necesario, ni pertinente, que sus datos sigan apareciendo en ficheros o tratamientos que eran pertinentes mientras esa persona estaba viva. Desde esta base de razonamiento, aunque es cierto que la LO 3/2018 no protege a las personas fallecidas, podemos afirmar que para poder dar cumplimiento al principio de la calidad de los datos es necesario reconocer a los herederos del fallecido un derecho de cancelación de datos inexactos; derecho este de cancelación que plantea no pocas cuestiones, como veremos a continuación, y que como exige el Reglamento para su ejercicio exigirá la acreditación suficiente del óbito que entendemos se llena con la aportación de un certificado literal de fallecimiento.

A su vez, en relación con la cancelación[370] de los datos, y en los mismos términos que el artículo 4.5 LOPD, se expresaba el artículo 8.6 RLOPD que establecía que:

> "Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la cual hubieran sido recabados o registrados.
> No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.
> Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento".

Por consiguiente, lo cierto es que se plantea, por el citado artículo 2.4 del RLOPD, un derecho nuevo a favor de terceras personas, herederos del finado titular de los datos, que plantea problemas respecto del carácter esencialmente personalísimo de los derechos reconocidos al afectado o interesado por la LOPD. Así, ahondando un poco más en la cuestión de la naturaleza jurídica de este derecho, que el artículo 2.4 RLOPD atribuía a los herederos, la AEPD en su citado Informe 61/2008 afirma:

> "Sin embargo, la regla contenida en el mencionado precepto establece un supuesto excepcional para que los herederos del finado u otras personas que cumplan los requisitos que el mismo establezca puedan instar la cancelación de los datos. Así, añade el segundo inciso del artículo 2.4 del Reglamento que 'No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

[370] Los derechos de rectificación y cancelación, en su formulación dada por el artículo 16.2 de la LOPD rezaba de la siguiente manera: "Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos".

> El precepto citado tiene por objeto conciliar el carácter personalísimo del ejercicio de los derechos de acceso, rectificación, cancelación y oposición con la posibilidad de que el responsable conozca efectivamente el hecho mismo del óbito y pueda proceder, en su caso, a la cancelación de los datos. Se evitan así situaciones, como la planteada en el presente informe, que pudieran llegar a resultar incluso dolorosas para los allegados a un fallecido y que se derivarían del hecho de desconocerse esta circunstancia por parte de quien trata los datos sin que ello implique en ningún caso el ejercicio por los herederos de derechos que la Ley Orgánica 15/1999 reserva exclusivamente al causante ya fallecido"

Por su parte, la LO 3/2018 no contempla como tal el derecho de cancelación, si bien, sigue recogiendo el derecho de rectificación (art. 14), el derecho de supresión (art. 15) y el derecho de oposición (art. 18).

La AEPD acude a un criterio de simple pragmatismo para hacer posible, como hemos visto, el cumplimiento efectivo del principio de calidad de los datos incorporados a un tratamiento. Salvaguardando el carácter personalísimo del ejercicio del derecho de cancelación la Agencia otorgó a este artículo 2.4 del RLOPD el carácter de un derecho de comunicación de las personas allegadas al fallecido, también previsto en la nueva Ley, tal y como hemos visto con anterioridad. Así la AEPD termina afirmando que:

> "De este modo, la reclamación que podrá ser dirigida por las personas allegadas al fallecido no supondrá en la práctica el ejercicio del derecho de cancelación, regulado por el artículo 16 de la Ley Orgánica 15/1999, sino que tendrá por objeto comunicar al responsable la inexactitud del contenido del fichero, debiendo proceder a la cancelación de los datos correspondientes al fallecido".

Este derecho de comunicación de los allegados al fallecido es aplicable, en principio sin excepciones, a la cancelación de datos biométricos dactiloscópicos del fallecido no apreciando la existencia de un régimen específico diferente al régimen general expuesto en lo que a la cancelación de datos dactiloscópicos de finados se refiere. Decimos en principio sin excepciones porque en el ámbito público, mediando un interés público

prevalente, sí que cabrían estas excepciones siendo legalmente admisible la conservación de, por ejemplo, perfiles de ADN reveladores de la misma información que una huella dactilar.[371] La conservación de perfiles de ADN y huellas dactilares ha sido estudiado por la jurisprudencia comunitaria y por nuestro TC. La conservación de datos personales en general, y específicamente el ADN no codificante o la huella dactilar, tiene consecuencias en la vida privada de las personas. Y la conservación de datos como el ADN codificante, generador y fuente de un gran número de datos, aún tiene más claras consecuencias. Así lo han expresado con meridiana claridad tanto el Tribunal Constitucional en su STC 199/2013, de 5 de diciembre, como el TEDH en su Sentencia de 4 de diciembre de 2008, caso S. y *Marper v*. Reino Unido, "la cantidad de información personal contenida (en las muestras celulares) conduce a considerar que su conservación constituye en sí misma una lesión del derecho a la vida privada, de suerte que poco importa que las autoridades extraigan o utilicen solo una pequeña parte de tal información para la creación de perfiles de ADN". Porque "el mero hecho de que las autoridades públicas conserven o memoricen datos de carácter personal, cualquiera que sea la manera en la que hayan sido obtenidos, tiene unas consecuencias directas en la vida privada de la persona afectada". Por tanto, la cancelación de datos dactiloscópicos de una persona, aunque ya esté fallecida, puede verse limitado por un interés público que haga prevalecer la conservación a la cancelación.

[371] El preámbulo de la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN, recoge una de estas excepciones ya que dice: "El articulado de la presente Ley comienza determinando lo que constituye su objetivo fundamental, que no es otro que la creación de una base de datos en la que, de manera única, se integren los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado en los que se almacenan los datos identificativos obtenidos a partir de los análisis de ADN que se hayan realizado en el marco de una investigación criminal, o en los procedimientos de identificación de cadáveres o de averiguación de personas desaparecidas.
En relación con su integración orgánica, la base de datos policiales sobre identificadores obtenidos a partir del ADN dependerá del Ministerio del Interior a través de la Secretaría de Estado de Seguridad.
A continuación, la Ley incorpora una importante novedad, ya que posibilita que para determinados delitos de especial gravedad y repercusión social -así como en el caso de los patrones identificativos obtenidos en los procedimientos de identificación de restos cadavéricos o de personas desaparecidas, o cuando el titular de los datos haya prestado su consentimiento para la inscripción-, los resultados obtenidos a partir del análisis de las muestras biológicas del sospechoso, detenido o imputado, sean inscritos y conservados en la base de datos policial, a fin de que puedan ser utilizados en esa concreta investigación, o en otras que se sigan por la comisión de alguno de los delitos para los que la propia Ley habilita la inscripción de los perfiles de ADN en la base de datos.
Esta regulación contiene una salvaguarda muy especial, que resulta fundamental para eliminar toda vulneración del derecho a la intimidad, puesto que sólo podrán ser inscritos aquellos perfiles de ADN que sean reveladores, exclusivamente, de la identidad del sujeto -la misma que ofrece una huella dactilar- y del sexo, pero, en ningún caso, los de naturaleza codificante que permitan revelar cualquier otro dato o característica genética." Por tanto, se permite el almacenamiento y conservación de perfiles de ADN no codificante en una base de datos policial que al igual que una huella dactilar son reveladores de la identidad del sujeto mediando un interés general superior de averiguación de las circunstancias de un hecho delictivo y persecución del delincuente. LO 10/2007; BOE 242/2007, de 9 de octubre de 2007 Ref Boletín: 07/17634.

2.4.3.2. Soporte del dato: soporte físico susceptible de tratamiento. El concepto de fichero.

Con las notas apuntadas hasta ahora, se ha delimitado el concepto jurídico de dato de carácter personal como información, objetiva o subjetiva, atribuible a una persona física, que se somete a un tratamiento estructurado, manual o automatizado, y con una finalidad del tratamiento no exclusivamente personal o doméstica.

Si estas son las notas que, en general, permiten delimitar el concepto de dato de carácter personal habrá, más adelante, que concretar aquéllas que delimitan el concepto de dato de carácter personal biométrico[372], sin olvidar que únicamente el análisis del dato biométrico interesa a este estudio si es predicable de él su carácter personal, en el sentido arriba apuntado.

Ahora bien, podemos calificar de elemento delimitador del dato personal su carácter de información extractada, en el sentido de extraída de la fuente, y susceptible de acceso mediante un proceso determinado ya sea una herramienta informática o una consulta manual ordenada. El Dictamen 4/2007, al que venimos haciendo referencia, y en relación precisamente a los datos biométricos, apunta lo que califica como una particularidad de dichos datos pero que, a nuestro entender, hace referencia a un concepto general extrapolable a los datos personales en genérico, nos referimos a la distinción entre fuente de datos y datos propiamente dichos. Así, el Dictamen indica:

> "Las muestras de tejido humano (al igual que las muestras de sangre) son fuentes a partir de las cuales se extraen datos biométricos, pero no son en sí mismas datos biométricos (…). Por lo tanto, la extracción de información de las muestras supone la obtención de datos personales, a los que se aplican las normas de la Directiva."

[372] Resulta evidente, por lo que hasta aquí hemos expuesto, que el dato personal biométrico, si no es atribuible a una persona o individuo concreto, no es objeto de este estudio. Como tampoco lo son los datos biométricos que no se refieran a personas sino a otros seres vivos del mundo animal o vegetal.

Partiendo de esta distinción entre fuente de dato y dato propiamente dicho, reviste interés la opinión de Aparicio Salom[373], que analizando esta distinción, llega a afirmar que la mera imagen de un individuo es fuente de información pero no es dato personal aun; datos serán los que se extraigan realmente de dicha imagen y se conserven en un soporte legible. Aun siendo el criterio unánime en contra, Aparicio Salom sostiene que las imágenes tomadas, por ejemplo, mediante sistemas de videovigilancia no constituyen un tratamiento de datos porque éstos han de ser extraídos de la imagen que, como fuente o continente, los contiene. Este análisis, en todo caso, nos sirve para avanzar al siguiente elemento determinante de la aplicabilidad de la normativa de protección de datos que es el concepto de tratamiento que entronca con lo que antes hemos denominado información extractada.

Por consiguiente, la vinculación a una persona de la información extraída, extractada, de una fuente que se encuentre en un soporte físico que la haga susceptible de tratamiento es lo que determina la aplicación de la normativa específica de protección de datos. Sin información extraída, dato, atribuible a un individuo concreto no se puede hablar de dato de carácter personal, y sin su incorporación a un soporte físico independiente tampoco hay posibilidad de aplicar toda la legislación de protección de datos que analizamos. De aquí y, como ya hemos apuntado anteriormente, siguiendo a Piñar Mañas, podríamos deducir la estrecha imbricación entre el concepto de privacidad e identidad que se encuentra en el centro de la doctrina de la protección de datos. Sin correlación entre derecho a la privacidad y derecho a la identidad la protección de datos no es posible. En palabras de Piñar Mañas, "(…) los datos personales (…) definen y configuran la identidad de las personas"[374] afirmación que, si bien es aplicable en general a los datos personales lo es, aun si cabe, con mayor claridad en los datos biométricos, como veremos más adelante.

Ya hemos afirmado que el concepto de tratamiento se utiliza en la delimitación del ámbito objetivo de aplicación de la normativa específica de protección de datos. Así lo recogían el artículo 3 de la Directiva 95/46 y la LOPD. El artículo 2.1 LOPD, en lo referente a este ámbito objetivo de aplicación de la Ley, establecía que la legislación sobre datos de carácter personal es de aplicación a los datos de carácter personal

[373] APARICIO SALOM, J., op. cit., pp. 59 y ss.
[374] PIÑAR MAÑAS, J.L., "Concepto de dato…", op. cit., p.186.

registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Y en lo referente al concepto de dato de carácter personal, ya hemos visto que el artículo 3 a) LOPD definía el dato de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables". Por su parte, el artículo 1.4 del ya derogado RD 1332/1994, consideraba a los datos de carácter personal como: "toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable". Una definición coincidente, en lo esencial, con esta última se recogía en el artículo 5.1 f) RLOPD.

De nuevo, recordamos en este punto que la LO 3/2018 no recoge el concepto de fichero y únicamente se refiere a "tratamientos" concretos; así, en el título IV (arts. 19 a 27), establece disposiciones aplicables a tratamientos, tales como, datos de contacto de empresarios individuales y profesionales liberales, sistema de información crediticia, tratamiento relacionados con la realización de determinadas operaciones mercantiles, tratamientos con fines de videovigilacia, sistemas de exclusión publicitaria, sistemas de información de denuncias internas, tratamientos de datos en el ámbito de la función estadística pública, tratamiento de datos con fines de archivo en interés público por parte de las Administraciones públicas y tratamiento de datos relativos a infracciones y sanciones administrativas.

Pues bien, sobre la base del concepto de dato de carácter personal se construye el concepto de fichero, que ahora nos ocupa, ya que éste se forma por la acumulación de aquéllos, eso sí, una acumulación estructurada. Como bien exponía el Considerando 27 de la Directiva: "Considerando que la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves de elusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los

elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva". De aquí que sea la estructura y no el carácter automatizado o no de dicha estructura la raíz de la definición de fichero de datos personales del artículo 2 c) de la Directiva. Vemos, en definitiva, que es la estructura, la organización con arreglo a criterios específicos que permita el acceso posterior a los datos almacenados, la determinante en la delimitación del ámbito de aplicación de la Directiva. Un conjunto de carpetas sin estar sometidas a un criterio de ordenación, por muy básico que éste sea, que permita el acceso posterior a los datos contenidos en ellas, queda fuera del ámbito de aplicación de la legislación de protección de datos.

Siguiendo este planteamiento, el artículo 3 b) LOPD definía el concepto de fichero como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso". Indudablemente incluye los ficheros manuales, no automatizados.

Así pues, son tres conceptos los que han de ser delimitados y manejados en la aplicación de la normativa sobre protección de datos personales: primero el concepto dato de una persona física, segundo el de tratamiento y, por último, el concepto de fichero. Bien entendido que estos tres pilares delimitadores se cimentan por una parte en la persona titular de los datos que ha de ser una persona física identificada o identificable y, por otra, en el propio dato extraído, extractado, de la fuente que lo contiene. Como ya ha quedado apuntado, si los datos no se pueden atribuir a una persona física concreta y no están extraídos de su fuente no son datos personales y no es aplicable la normativa específica. En palabras de Piñar Mañas, "(…) los datos se consideran relevantes sólo en la medida en que se den tales circunstancias. Un dato o conjunto de datos no sometidos a tratamiento o no susceptibles del mismo, o que no estén destinados a ser incluidos en un fichero, quedan fuera del ámbito de aplicación, y,

por tanto, de protección de la legislación de protección de datos[375]". En la nueva Ley, el concepto clave o fundamental es el de "tratamiento".

Llegamos así a cerrar un primer tramo en este camino de aproximación al ámbito de aplicación de la legislación de protección de datos y, así mismo, de delimitación del concepto de dato de carácter personal, al encerrar éste en las lindes de información atribuible a una persona determinada, extractada y registrada en un soporte físico que la haga susceptible de un tratamiento. Por obvio, no es menos importante destacar que si el dato de carácter personal extractado no está mantenido, soportado, registrado en un medio físico (con independencia del código en que se exprese: binario, analógico, etc…) que permita su tratamiento, o uso posterior, la normativa específica a la que nos venimos refiriendo no será aplicable. Así lo recogía el artículo 2.1 LOPD cuando establecía en relación al ámbito de aplicación: "La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado". En relación con este artículo cabría un doble comentario inicial: primero con este ámbito de aplicación el mandato constitucional contenido en el artículo 18.4 CE, de limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos, se ha visto superado y ampliado. Ello se debe, como ya hemos apuntado y veremos a continuación, al imperativo definido en la Directiva 95/46/CE que ampliaba su ámbito a los ficheros y tratamientos no automatizados. Y, en segundo lugar, en este artículo 2.1 no se menciona expresamente el concepto de fichero, expresándose con total coincidencia el artículo 2.1. RLOPD al regular el ámbito objetivo de aplicación del mismo. Ley y Reglamento acudían al término fichero para la delimitación del ámbito de aplicación por exclusión al referirse, en el artículo 2.2 y 3 LOPD y artículo 2.2 y 4 RLOPD, a ficheros específicos que quedan excluidos. Sin embargo, la Directiva 95/46/CE, en su artículo 3.1, al referirse a su ámbito de aplicación, lo delimitaba de forma positiva, acudiendo a los conceptos de tratamiento, total o parcialmente automatizado, y de fichero:

[375] PIÑAR MAÑAS, J.L., "Concepto de dato…", op. cit., pp. 186 y 187.

"1. Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

Vemos cómo expresamente la Directiva incluía los tratamientos no automatizados en su ámbito de aplicación. Posteriormente la delimitación se realiza de forma negativa en el apartado 2., estableciendo que:

"2. Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales:

- efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los Títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal;

- efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas".

La Directiva, en este artículo 3, a diferencia de la legislación interna, introducía expresamente el concepto de fichero, de trascendental importancia en la aplicación de la legislación de protección de datos y, así mismo, establece exclusiones de su ámbito de aplicación bajo el doble criterio de la finalidad[376] de la actividad y el tipo de tratamiento. Así, por un lado, los tratamientos efectuados en el ejercicio de actividades

[376] El criterio de la finalidad del tratamiento como delimitador del propio concepto de dato de carácter personal es destacado por Aparicio Salom que analiza como en la práctica se han planteado supuestos en los que aun estando ante datos personales éstos no afectan a la intimidad del individuo porque las características que concurren en el tratamiento lo hacen ajeno a dicha intimidad. Pensemos en los datos de profesionales y comerciantes que según criterio de la Agencia Española de Protección de Datos: "los profesionales y los comerciantes individuales (estos dos últimos sólo en los estrictos términos señalados en el párrafo que antecede, esto es, cuando sus datos hayan sido tratados tan sólo en su consideración de empresarios) quedan fuera del manto protector de la Ley Orgánica 15/1999". En este mismo sentido, la misma Agencia ha utilizado el criterio de la finalidad del tratamiento como delimitador de la aplicación de la normativa de protección de datos excluyendo su aplicación en un supuesto en que aun concurriendo un error en un dato éste era meramente circunstancial respecto del resto de datos del fichero y, por tanto, no imputaba información esencial a una persona, conforme a la finalidad de dicho tratamiento. APARICIO SALOM, J., op. cit., pp. 77 y ss.

no comprendidas en el ámbito del Derecho comunitario y los tratamientos efectuados en el ámbito doméstico están exentos y, por otro lado, los tratamientos no automatizados sin estructura, tampoco quedan dentro del ámbito de aplicación. Al excluir, por el tipo de tratamiento, todos aquellos que se lleven a cabo de forma manual no estructurada y, por otra parte, todos aquellos que por la finalidad del tratamiento se lleven a cabo en actividades exclusivamente personales o domésticas efectuadas por una persona física, deja reducidos los tratamientos concernidos a los automatizados, o no, que se destinen a ser incluidos en un fichero siempre que dicho fichero no se lleve a cabo dentro de una actividad exclusivamente doméstica o de las expresamente excluidas. El tratamiento manual (no automatizado) de datos personales entraba dentro del ámbito de aplicación de la Directiva, conforme a este artículo 3, si los datos están contenidos en un fichero o su destino es la inclusión en un fichero. Para algunos autores, el concepto de tratamiento[377] pasa a jugar un papel importante en la delimitación del ámbito de aplicación de la normativa sobre protección de datos, ya que esta normativa es aplicable si el dato de carácter personal ha sido sometido a un tratamiento automatizado, esté o no incorporado a un fichero, o si el tratamiento, no automatizado, sí incluye la incorporación de aquél a un fichero. Por eso, siguiendo esta tendencia a dotar de mayor relevancia al concepto de tratamiento, la LOPD lo utilizaba como delimitador de su ámbito de aplicación. La nueva Ley aclara que no será de aplicación a los tratamientos excluidos del ámbito del RGPD, a los tratamientos de datos de personas fallecidas y a los tratamientos sometidos a la normativa sobre protección de materias clasificadas (art. 2.2 LO 3/2018).

Sin embargo, el RGPD, en su Capítulo I, (Disposiciones Generales), artículo 2.1. volvía a definir su ámbito de aplicación material coincidiendo con la definición de la derogada Directiva 95/46/CE, estableciendo:

[377] Davara Rodríguez, tras analizar comparativamente el ámbito de aplicación fijado por el artículo 2 de la antigua LORTAD y el establecido también por el artículo 2 de la LOPD, afirma que: "(…) el tratamiento de los datos ha adquirido una fuerza interpretativa mayor y, sin dejar de ser importante, el concepto de fichero no es ya un eje tan determinante en la protección como lo era antes". DAVARA RODRÍGUEZ, M.A., "El concepto de fichero en la normativa sobre protección de datos", en Troncoso Reigada, A. (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de carácter personal*, Cizur Menor, Civitas, 2010, p. 215.

"El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero."

Igual que en la Directiva derogada, la delimitación del ámbito material de aplicación en el RGPD se realiza también de forma negativa al establecer el artículo 2.2:

"El presente Reglamento no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;

b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;

c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención[378]."

Por consiguiente, en la delimitación del concepto de dato de carácter personal, han de considerarse las condiciones en las que éste se encuentra soportado que han de ser tales que lo hagan susceptible de tratamiento. Y, así mismo, a fin de analizar la aplicabilidad de la normativa sobre protección de datos, también hay que tener en cuenta estos conceptos fundamentales, que venimos citando, de tratamiento de datos personales y de fichero de datos personales.

En relación con el "tratamiento", el artículo 2 b) de la Directiva 95/46/CE lo definía como:

[378] Más adelante analizaremos el denominado "*Umbrella Agreement*" que entró en vigor en febrero de 2017, como acuerdo alcanzado entre la UE y EE.UU. para la protección de los datos personales de los europeos en supuestos de transmisión de estos datos a los EE.UU. en el ámbito de la prevención, investigación, detección y enjuiciamiento de infracciones penales.

"cualquier operación o cualquier conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;"

El mismo artículo 2 en el apartado c) definía fichero de datos personales como:

"todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;"

Por su parte, la LOPD definía en su artículo 3 b) y c) fichero y tratamiento de datos, respectivamente como:

"b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

3. Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".

La PRGD, en su artículo 4. 3) definía el tratamiento como:

"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, efectuadas o no mediante procedimientos automatizados, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, supresión o destrucción".

Por último, la misma propuesta de Reglamento en su artículo 4. 4) definía el fichero como:

> "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".

En términos casi coincidentes ha quedado definitivamente fijado el concepto de tratamiento en el artículo 4. 2) del RGPD, que añade la "limitación" como una operación incluida en el concepto de tratamiento y así se pronuncia:

> "«tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;"

La definición de fichero recogida en el RGPD, en su artículo 4.6, es sincrética y amplia a la vez, haciendo expresamente mención a la organización centralizada o descentralizada del mismo, como ya lo hacía la propuesta. Así lo define como:

> "«fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;"

En un análisis comparativo de la definición de tratamiento recogida en la Directiva, LOPD y PRGPD podemos apreciar que los tres textos normativos, con términos casi coincidentes, daban contenido al concepto de tratamiento aludiendo a una pléyade de operaciones que podríamos agrupar u ordenar en cuatro momentos o fases cronológicamente distintas: primera, inicial, comprende operaciones de recogida, registro y extracción; segunda, de tratamiento propiamente dicho, abarca la organización, estructuración, conservación, elaboración, modificación, adaptación y grabación; tercera, de uso, con operaciones de consulta, utilización, cesiones,

comunicación por transmisión, difusión, cualquier forma de acceso o habilitación de acceso, cotejo, interconexión, transferencias y, por último, la cuarta de supresión, destrucción, cancelación y bloqueo. El RGPD incluye las operaciones de limitación que pueden afectar a la tercera fase de uso y/o también a la cuarta fase de supresión. Cabe citar algunas diferencias entre los cuatro textos como, por ejemplo, en la fase inicial la propuesta de Reglamento y el RGPD son los únicos que mencionan la operación de extracción que, ya hemos dicho, consideramos fundamental para distinguir entre dato y fuente del dato. En la segunda fase, la Propuesta (PRGPD) hace hincapié en la organización haciendo mención expresa al término estructuración. Las operaciones de la tercera fase están descritas de manera casi coincidente, salvo en la PRGPD, que incluye no solo el acceso sino cualquier forma de habilitación de acceso ampliando así su ámbito y salvo la mención de las operaciones de limitación ya apuntadas. Por último, en la última fase de cancelación, la PRGPD no incluía el concepto de bloqueo.

Estas cuatro fases señaladas no son necesariamente de desarrollo secuencial en el tiempo, ya que una operación de consulta será tratamiento de datos y le será de plena aplicación la legislación tuitiva en la materia con independencia de que vaya precedida de la recogida o registro de los datos consultados por el mismo autor de la consulta.

El RLOPD en su artículo 5 apartados k), l), m) y n) definía por separado los conceptos de fichero, ficheros de titularidad privada, ficheros de titularidad pública y fichero no automatizado en los siguientes términos:

> "k) Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
> l) Ficheros de titularidad privada: Los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las Corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

m) Ficheros de titularidad pública: Los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

n) Fichero no automatizado: Todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica"[379].

La definición de fichero recogida en el artículo 5 k) coincidía con la recogida en la LOPD, salvo que el RLOPD hacía hincapié en que ese conjunto organizado de datos debe permitir el acceso con arreglo a criterios determinados. Por tanto, el acceso se destaca con respecto a otras características del fichero como pueden ser la modalidad de su creación, almacenamiento u organización.

Centrándonos, en primer lugar, en el concepto de fichero, en un análisis comparativo la Directiva lo definía como conjunto estructurado y la LOPD como conjunto organizado. Si añadimos a estas definiciones normativas la reproducida por Davara Rodríguez, recogida en el Diccionario Enciclopédico de Tecnología en el área de conocimiento de *software* básico, el fichero se define como:

"conjunto de datos relacionados entre sí, considerados como una unidad, al que se da un nombre simbólico mediante el cual es posible identificarlo y manipularlo. Por regla general, los ficheros se organizan como un conjunto de registros o líneas cuya longitud puede ser fija o variable. Los registros se

[379] Cabe apuntar que de conformidad con la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, su artículo 7.2 establece que: "(…) no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real".

componen de un conjunto de campos cuyo formato puede ser numérico, alfanumérico, etc., y de longitud fija o variable"[380].

Este autor[381] recogiendo, además de la reproducida, otras definiciones de fichero, concluye que en todas ellas el común denominador es la existencia de un conjunto de datos organizado o estructurado. Así mismo, la Exposición de Motivos de la antigua LORTAD, promulgada para proteger la privacidad poniendo límite al uso de la informática y otras técnicas de tratamiento automatizado de los datos de carácter personal, en su apartado II decía que: "(…) partiendo de que su finalidad es hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos, la Ley se nuclea en torno a los que convencionalmente se denominan 'ficheros de datos': Es la existencia de estos ficheros y la utilización que de ellos podría hacerse la que justifica la necesidad de la nueva frontera de la intimidad y del honor". Aquí, el concepto de fichero se destaca como elemento de riesgo para los derechos de la personalidad puesto que el acopio de datos y su posterior tratamiento reviste peligro en cuanto esos datos se incorporan a ficheros, es decir, en cuanto medie una estructura u organización. Así lo recoge claramente el artículo 4.6 RGPD, al concretar en el conjunto estructurado de datos el concepto de fichero. Ambos conceptos, fichero y tratamiento, delimitan las posibilidades de despliegue de la protección de datos personales en el Derecho nacional y europeo.

Por consiguiente, vemos que en la base de todas estas definiciones bien sea a través de los conceptos de conjunto de datos relacionados, organizados o estructurados, se está advirtiendo sobre la existencia de lo que se ha venido en denominar 'poder informático' que Vizcaíno Calderón describe como la capacidad que proporciona la técnica

[380] DAVARA RODRÍGUEZ, M.A., "El concepto de fichero…", op. cit., p. 216.

[381] Davara distingue entre los conceptos de fichero lógico, físico y jurídico que, aunque, como advierte, no son conceptos normativos sino meramente explicativos o didácticos, ayudan a interpretar algunas disposiciones legales. Estos conceptos hacen referencia el primero a aquel fichero que resulta de la organización interna del sistema de información correspondiente. El segundo, el fichero físico, se refiere a la ubicación física ya que todo fichero está ubicado en un sistema de información concreto o, si es un fichero manual, está en un lugar determinado. Y, por último, el fichero jurídico que se determina por la finalidad para la que se tratan los datos personales que contiene. Este concepto de fichero jurídico puede inferirse del artículo 81.8 RLOPD que disponía: "A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad". Ibíd., p. 219.

informática "para confrontar y agregar los datos más diversos hasta el punto de transformar informaciones dispersas en una información organizada, remontándose así de los actos más banales del individuo a sus más íntimos secretos, con posibilidad de encontrar inmediatamente y de comunicar con la misma rapidez las informaciones así obtenidas"[382]. La información organizada se convierte en un potencial factor de agresividad a la privacidad del individuo porque de la propia organización u orden de los datos se desprende la configuración de un retrato de la persona con toda la información relacionada que le pertenece. La información inconexa, sin relacionar, sin ordenar y sin ningún criterio de organización en su almacenamiento, impidiendo su posterior acceso, no reviste peligro para la intimidad y privacidad de la persona, la situación contraria indudablemente sí es peligrosa[383].

De hecho, este criterio de estructura y organización es el que también presidía la definición de fichero no automatizado del artículo 5 n) RLOPD reproducido más arriba.

2.4.3.3. Inclusiones en el concepto de dato de carácter personal.

Tanto el GPD 29 en el dictamen 4/2007, como la jurisprudencia de la Audiencia Nacional en España, la AEPD y la doctrina han venido analizando y configurando un elenco de informaciones concretas que cabe incluir en el concepto de dato de carácter personal. Recogemos, a continuación, algunas de ellas ya que los criterios utilizados para la inclusión o exclusión de estas informaciones del concepto de dato de carácter personal pueden orientar, a su vez, la delimitación del dato personal biométrico.

[382] VIZCAÍNO CALDERÓN, M., op. cit., p. 34.

[383] Piñar Mañas, consciente de este peligro, advierte como: "Nunca antes como hoy había sido posible, utilizando las tecnologías que están ya al alcance de casi cualquiera, invadir la privacidad de las personas hasta los límites a los que se está llegando. Pensemos que hoy es posible conocer los contenidos de los correos electrónicos, de las llamadas efectuadas o recibidas mediante teléfonos móviles; que pueden tratarse para múltiples finalidades los datos genéticos; que el uso de datos biométricos está casi a la orden del día; que las nuevas tecnologías pueden afectar grave e intensamente a los derechos fundamentales e incluso pueden condicionar el contenido de las normas jurídicas; que mediante dispositivos de radiofrecuencia es posible no sólo controlar las ventas en un centro comercial sino también localizar personas; que la capacidad de los ordenadores personales y sus funcionalidades se incrementan constantemente implicando riesgos potenciales para la privacidad y para la protección de datos personales; que cada vez son más los casos en que se exigen tratamientos de datos y transferencias internacionales, así como retenciones de datos en aras de la seguridad ciudadana; que la sociedad corre el riesgo de verse sometida a una videovigilancia constante…". PIÑAR MAÑAS, J. L., "Consideraciones introductorias sobre el derecho fundamental a la protección de datos de carácter personal", *Revista Jurídica General*, Boletín del Ilustre Colegio de Abogados de Madrid nº 35, 3ª época, febrero 2007, pp. 13-14.

En primer lugar, en relación con los números de teléfono se pueden realizar las siguientes consideraciones. En opinión de Piñar Mañas, es indudable que el número de teléfono es un dato personal "pues constituye información sobre personas" [384]. Pero la cuestión radica, como acertadamente puntualiza este autor, en si el número de teléfono por sí solo es, o no, dato de carácter personal; es decir, ¿un número telefónico sin ninguna otra información adicional que lo acompañe es por sí solo un dato de carácter personal? Este autor para abordar esta cuestión considera relevante analizar, no solo el Informe 285/2006 de la AEPD, sino también, los fundamentos de derecho de la Sentencia de 17 de septiembre de 2008 (rec. 353/2007) de la Audiencia Nacional.

Partiendo del Informe 285/2006, éste afirma que el número de teléfono es un dato personal "cuando resulte adscrito al concreto titular del mismo o se asocie a datos identificativos adicionales como pueden ser la dirección*".* En este Informe la Agencia sigue la Sentencia de la Audiencia Nacional de 8 de marzo de 2002 que estableció que "para que exista un dato de carácter personal (en contraposición con dato disociado) no es imprescindible una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados*".* Esta Sentencia está haciendo referencia al concepto de persona identificable y en este sentido afirma que "para determinar si una persona es identificable, hay que considerar el conjunto de los medios que pueden ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona".

Por otra parte, la Sentencia de 17 de septiembre de 2008, también de la Audiencia Nacional, estimó el recurso presentado por una empresa, prestadora de servicios de descargas a teléfonos móviles, contra una sanción que le había sido impuesta por la AEPD al considerar que dicha empresa no contaba con el consentimiento del titular de los datos, número de móvil, para el tratamiento de los mismos. El procedimiento ante la AEPD se inició con la presentación de una denuncia por el titular de los datos alegando que solicitó la descarga de un tono anunciado en televisión y posteriormente recibió durante varios meses tonos o politonos por los que se le cobró, pero que realmente no

[384] Id., "Concepto de dato…", pp. 203-204.

había solicitado, teniendo grandes problemas para darse de baja del servicio de descarga. Para la prestación de este servicio la empresa sancionada únicamente trataba el dato relacionado con el número de teléfono móvil del usuario y la facturación se hacía a través del operador de telefonía correspondiente a cada usuario. Por tanto, la empresa prestadora del servicio de descargas única y exclusivamente gestionaba el dato del teléfono móvil sin llegar a conocer o tratar ningún otro dato personal. Sobre la base de estos hechos la AEPD sancionó a la empresa y, sin embargo, la Audiencia Nacional considera, en esta sentencia, que la Agencia no ha probado que la existencia del número por sí solo haga al titular identificable, y por tanto no se le puede aplicar la LOPD. De esta sentencia se pueden extraer varias conclusiones, primera: el número de teléfono móvil no es en sí mismo y por sí solo un dato de carácter personal. Es necesario para convertirlo en dato de carácter personal que haga al usuario del mismo identificado o identificable. Y segunda: la AEPD se excedió en sus funciones al aplicar la normativa de protección de datos a hechos ajenos al objeto de esta norma ya que la valoración de la validez de un contrato o la información que debe contener un anuncio exceden de los supuestos a los que resulta aplicable la LOPD. Esta Sentencia que venimos comentando establece en su fundamentación jurídica que si no se acredita "que a través del número de teléfono móvil se haya identificado al titular del mismo o que a partir del citado número fuese posible tal identificación", hay que concluir "que el citado número de teléfono ayuno de otras circunstancias que identifiquen o pudiesen permitir identificar al titular del mismo impide que pueda encajarse en la definición legal de dato de carácter personal[385]."

Posteriormente, la AEPD ,en su Informe Jurídico 0575/2008, recoge la doctrina de esta Sentencia de la Audiencia Nacional y afirma que: "Siguiendo esta doctrina jurisprudencial, el número de teléfono móvil por si mismo, esto es, sin el concurso de otros datos que contribuyan a identificar a su propietario, no tiene el carácter de dato personal, en consecuencia, la aplicación de las prescripciones contenidas en la LOPD vendrá determinada por la asociación de dicho número con otros datos que permitan establecer la identidad de su titular".

[385]Ibíd., p. 204.

Habrá que valorar, entonces, caso por caso para determinar si existe o no nexo de unión entre el dato, teléfono móvil, y la persona física titular del mismo y considerar si el establecimiento de ese nexo de unión exige esfuerzos desproporcionados lo que llevaría, si es así, a no considerarlo datos de carácter personal.

Cabría preguntarse si lo dicho respecto de los teléfonos móviles ¿es aplicable también a un número de teléfono fijo? ¿Y respecto de un número IP[386] o el DNI? En principio cabría apuntar que el criterio para determinar si se trata o no de datos personales es el mismo, es decir, si en cada caso concreto es posible establecer un nexo de unión entre el dato, teléfono fijo, y la persona este dato puede considerarse dato de carácter personal. Se puede afirmar que, únicamente en el caso de los teléfonos móviles, el uso es más personal, a diferencia de una línea de teléfono fija donde el titular puede ser el cabeza de familia y los usuarios varias personas pertenecientes a la familia o a su entorno. Respecto a la dirección IP o número IP, el TJUE tiene declarado que son datos de carácter personal las denominadas IP estáticas[387]. En concreto en el apartado 51 de la sentencia de 24 de noviembre de 2011, *Scarlet Extended* (C‑70/10, EU:C:2011:771), el TJUE estimó, en esencia, que las direcciones IP de los usuarios de Internet son datos protegidos de carácter personal, ya que permiten identificar concretamente a esos usuarios. Lo que posteriormente se ha planteado es si las direcciones IP dinámicas (provisionales de cada sesión) también son datos de carácter personal. Y el TJUE ha determinado que sí lo son. El Tribunal de Justicia, en respuesta a una cuestión planteada por el Tribunal Supremo Alemán (*Bundesgerichsthof*) que remitió la citada cuestión en los siguientes términos: si la IP dinámica de un ordenador obtenida por el titular de la web puede ser considerada un dato personal, en el caso de que el proveedor de acceso a internet tenga los datos adicionales necesarios para identificar a un usuario; a esta cuestión, así planteada, la Sala Segunda del Tribunal de Justicia en Sentencia de 19 de

[386] "Las direcciones IP son secuencias de números que se asignan a los ordenadores conectados a Internet para que estos puedan comunicarse entre sí a través de esa red". Párrafo 15 Sentencia del Tribunal de Justicia (Sala Segunda), en el asunto C‑582/14, en el procedimiento entre Patrick Breyer y Bundesrepublik Deutschland, de 19 de octubre de 2016. ECLI:EU:C:2016:779. http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=295403 [Fecha de consulta: 28/08/2018].

[387] "[…] los ordenadores de los usuarios de Internet reciben de los proveedores de acceso a Internet una dirección IP «estática» o una dirección IP «dinámica», es decir, una dirección IP que cambia con ocasión de cada nueva conexión a Internet. A diferencia de las direcciones IP estáticas, las direcciones IP dinámicas no permiten relacionar, mediante ficheros accesibles al público, un ordenador concreto y la conexión física a la red utilizada por el proveedor de acceso a Internet". Ibídem, Párrafo 16 Sentencia del Tribunal de Justicia (Sala Segunda), asunto C‑582/14.

octubre de 2016, contesta que sí es dato de carácter personal. En concreto el párrafo 44 de la sentencia dice textualmente: "El hecho de que la información adicional necesaria para identificar al usuario de un sitio de Internet no esté en poder del proveedor de servicios de medios en línea, sino del proveedor de acceso a Internet de ese usuario, no parece que pueda excluir que las direcciones IP dinámicas registradas por el proveedor de servicios de medios en línea constituyan, para éste, datos personales, […]".

En cuanto al dato D.N.I., como cualquier otro dato de carácter personal, para considerarlo como tal debe contener una información y poder vincular esa información a una persona física determinada. Este puede ser el punto de partida, pero hay que tener en cuenta la regulación específica en esta materia.

En el RD 1553/2005, que regula la expedición del DNI, se establece que: "El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior que goza de la protección que a los documentos públicos y oficiales otorgan las Leyes. Su titular estará obligado a la custodia y conservación del mismo. Dicho documento tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo. A cada Documento Nacional de Identidad, se le asignará un número personal que tendrá la consideración de identificador numérico personal de carácter personal". Por otra parte, el NIE está regulado en el Real Decreto 2393/2004, que aprueba el Reglamento de la Ley Orgánica 4/2000, sobre derechos y libertades de los extranjeros en España y su integración social, en cuyo articulado dice: "El número personal será el identificador del extranjero, que deberá figurar en todos los documentos que se expidan o tramiten, así como en las diligencias que se estampen en su pasaporte o documento análogo".

A la luz de esta regulación, se ha producido una evolución en el criterio mantenido por la AEPD en esta materia. Como señala Piñar Mañas[388], inicialmente la AEPD en la Resolución de 20 de abril de 2005 dictada en el procedimiento E/00561/2004 afirmó que "(…) aunque en principio es criterio de esta Agencia Española de Protección de Datos que el número del DNI, por sí solo, no constituye un dato de carácter personal, sí

[388] PIÑAR MAÑAS, J.L., "Concepto de dato…", op. cit., p. 204.

lo será en cuanto resulte adscrito al concreto titular del mismo". En este mismo sentido, se pronunció la Audiencia Nacional en la Sentencia de 27 de octubre de 2004. Sin embargo, posteriormente la AEPD ha cambiado su opinión y en el Informe 0334/2008, teniendo en cuenta la regulación de los Reales Decretos 1553/2005 y 2393/2004, considera que una base de datos en la que, aunque solo se recojan el DNI o el NIE, "queda plenamente sometida a la Ley Orgánica y su Reglamento de desarrollo, debiendo de adoptarse todas las medidas en dichas normas previstas, dado que son números cuya finalidad es identificar a las personas físicas".

2.5. Aproximación al concepto de dato biométrico y dato biométrico dactiloscópico. Acomodación del mismo al concepto de dato de carácter personal.

Llegados a este punto, establecer con la mayor exactitud posible el concepto de dato biométrico de carácter personal, para sobre dicha base determinar si le es o no de aplicación la normativa de protección de datos, es una cuestión trascendental.

Siguiendo el Dictamen 4/2007 del GPD 29, ya citado, los datos biométricos se pueden definir como: "propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son al mismo tiempo atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad"[389].

La definición transcrita abarca un conjunto de datos tan amplio que oscilan desde las propiedades biológicas del individuo o características fisiológicas, como las huellas dactilares, la estructura facial, la voz, hasta simples tics o características comportamentales como pueden ser la caligrafía, las pulsaciones en teclado, la manera de hablar o de caminar. Ahora bien, ese amplio abanico de datos sólo será dato de carácter personal, en el sentido que hemos delimitado anteriormente, si confluyen dos notas características: la primera y fundamental, es atribuible a una única persona y la segunda, es mensurable, es decir, se puede someter a un procedimiento de medición,

[389] Grupo de Trabajo del artículo 29. Dictamen 4/2007 sobre el concepto de datos personales, op. cit., p. 9. Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm [20 marzo 2016].

que lo convierte en dato extractado a los efectos de poder ser sometido a un tratamiento estructurado, con incorporación a un fichero automatizado o no.

Algunos autores, como Vizcaíno Calderón[390] o Aparicio Salom, circunscriben los datos biométricos a determinados aspectos físicos de la persona sin tomar en consideración otra categoría de datos biométricos que son los referidos al comportamiento. Aparicio Salom entiende que*:* "(…) el procesado de datos biométricos y su vinculación con la identidad de los ciudadanos no tiene mayor trascendencia respecto de la intimidad que los métodos de personalización más tradicionales y menos exactos que se emplearon con anterioridad, ya que no revelan nada de la personalidad del individuo, salvo el ADN"[391]. Destacamos esta afirmación, aunque discrepamos de ella, porque llama la atención sobre la razón de ser de este estudio. Si realmente el dato biométrico no contiene ninguna información adicional del individuo efectivamente, sin negarle su carácter de dato personal, su análisis podría quedar circunscrito al cumplimiento del principio de calidad de los datos que se recogía en el artículo 4.1 de la LOPD (no especificado en la nueva Ley como tal, sino a través del principio de exactitud), en el sentido de que solo podrá ser recogido para su tratamiento cuando sea adecuado, pertinente y no excesivo en relación con el ámbito y las finalidades para las que se haya obtenido. Pero a nuestro entender, esta es una visión parcial del tema porque el dato biométrico, o algunos datos biométricos y entre ellos la huella dactilar, puede contener

[390] Este autor reproduce la opinión de la Agencia Española de Protección de Datos en relación con la incidencia de los datos biométricos en el ámbito de aplicación de la Ley. Partiendo de entender por datos biométricos únicamente "(…) aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren en dichos aspectos y que, una vez procesados, permiten servir para identificar al individuo en cuestión (iris del ojo, voz, huellas digitales…)." Afirma que:
"(…) si bien el procesado de los datos biométricos no revela nuevas características referentes al comportamiento de las personas, sí permite su identificación por lo que, caso de procederse a su tratamiento, deberá éste ajustarse a la Ley de Protección de Datos. (…) Entendió la Agencia que estos datos biométricos, datos de carácter personal, no contienen aspectos concretos de la personalidad, limitando su función a identificar un sujeto cuando la información se vincula a éste, por lo que su tratamiento no tendrá mayor trascendencia que el de los datos relativos a un número de identificación personal, a una ficha que tan sólo pueda utilizar una persona o a la combinación de ambos". Entendemos que esta es una visión parcial del concepto de datos biométricos ya que: primero, algunos datos biométricos de características físicas pueden revelar aspectos del comportamiento del individuo y, segundo y fundamental, existe toda una categoría de datos biométricos comportamentales referidos precisamente a algunos aspectos del comportamiento de la persona en los que dicho comportamiento es sometido a cuantificación, análisis, tratamiento técnico y puede servir para identificar al individuo. Estos datos comportamentales tienen relevancia normativa recogiéndose en el artículo 13 LOPD el derecho de las personas a la impugnación de valoraciones de su comportamiento y, sí mismo, mereciendo los conjuntos de datos que permitan evaluar determinados aspectos de la personalidad o del comportamiento la adopción de medidas de seguridad de nivel medio, como expresamente así dispone el artículo 81.2 f) RLOPD. Cfr. VIZCAÍNO CALDERÓN, M., op. cit., p. 73.
[391] APARICIO SALOM, J., op. cit., p. 85.

información adicional y de tan alta sensibilidad como la relativa a la salud de su titular. Como veremos en la segunda parte de este estudio, el análisis del dato biométrico, y en concreto el dato biométrico dactiloscópico, se abordará distinguiendo un elemento material y un elemento inmaterial. El elemento material, fuente del dato biométrico, bien sea el conjunto de surcos y valles de la huella, o las características del óvalo facial, o del iris de un individuo es distinto de la información contenida en ese conjunto de surcos y valles que incluso puede revelar información sobre los hábitos ocupacionales o profesionales de la persona si se aprecian corrosiones o desgastes anormales o, incluso proporcionar información sobre la salud, o revelar deformidades congénitas[392]. Por consiguiente, entendemos que el elemento inmaterial, la información inmanente en el soporte material-físico propiamente dicho, sí puede revelar nuevas características referentes a la intimidad y privacidad del individuo y sí puede contener aspectos concretos de su personalidad no limitándose su funcionalidad a identificar a un sujeto.

La AEPD, en el párrafo quinto de su Informe Jurídico número 0368/2006[393], define a los datos biométricos como: "[…] aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión […]". En el mismo sentido, se incluye esta definición en el Informe 0324/2009 de la AEPD. El Informe de 2006 recoge una consideración que es asumida en toda su extensión por el posterior Informe de 2009, que a continuación reproducimos expresamente, y con la que humildemente discrepamos por razones que veremos más adelante. Estos informes indican lo siguiente:

> "[…] En el caso planteado, tratándose del tratamiento de la huella digital, la información contenida en dicho dato no contiene ningún aspecto concreto de la personalidad y tan sólo cuando dicha información se vincula a la identidad de una persona es posible

[392] De Antón enumera respecto de deformidades congénitas que pueden revelarse en el tratamiento de datos dactiloscópicos la falta de dedo índice, la polidactilia, la sindactilia, la ectrodactila y la anquilosis. Cfr. DE ANTÓN Y BARBERÁ, F., op. cit., p. 122.

[393] Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/calidad/common/pdfs/2006-0368_Proporcionalidad-del-tratamiento-de-la-huella-dactilar-de-alumnos-de-un-colegio.pdf [Fecha de consulta: 23/02/2016].

> identificarla con toda certeza, de modo que los datos que se recaban no pueden considerarse de mayor trascendencia que los relativos a un número personal, a una ficha que tan solo pueda utilizar una persona o a la combinación de ambos.
>
> […] Además, en lo atinente a las medidas de seguridad en el tratamiento, debe señalarse que, teniendo en cuenta lo que se ha indicado en cuanto al dato biométrico de la huella digital, el mismo no puede ser considerado en modo alguno dato especialmente protegido o sensible, por lo que resultarán de aplicación al tratamiento las medidas de seguridad de nivel básico, previstas en el Reglamento de Seguridad, aprobado por Real Decreto 994/1999, de 11 de junio."

Sin embargo, consideramos que la huella digital puede contener aspectos concretos de la personalidad del individuo incluso datos de salud que hacen que estos datos pasen a la categoría de datos sensibles.

La PRGPD definía, a los efectos del citado Reglamento, en su artículo 4 apartado 11) los datos biométricos como: "cualesquiera datos relativos a las características físicas, fisiológicas o conductuales de una persona que permitan su identificación única, como imágenes faciales o datos dactiloscópicos;".

El documento de trabajo sobre biometría del año 2003, del GPD 29,[394] utiliza una terminología que conviene acotar en su contenido a los fines que nos ocupan.

Por una parte, se hace referencia al concepto de "elemento biométrico" que al ser universal, único y permanente en cada persona lo hace susceptible de servir a los fines de identificación y/o autenticación de aquélla. Y ejemplifica, como elementos biométricos el ADN, la retina y las huellas digitales.

Por otra parte, se utilizan los términos de "datos físicos y fisiológicos" como datos estables en el individuo y, el concepto de "datos comportamentales" como datos

[394] Documento del Grupo de Trabajo del artículo 29 WP 80, 12168/02/ES, op. cit., pp. 3 y ss.

dinámicos. Tanto a unos, físicos, como a otros, comportamientos, se los denomina datos biométricos o muestras biométricas.

Referidas a la medición de estos datos, cabe distinguir, a su vez, entre "técnicas fisiológicas" y "técnicas comportamentales". Las primeras se basan en la medición de aspectos físicos y fisiológicos de la persona y las segundas miden aspectos del comportamiento de una persona, por ejemplo, su forma de caminar. El término de "sistema biométrico", también utilizado, abarcaría a unas u otras técnicas apuntadas.

Pasando a la operativa básica de uno de estos sistemas biométricos, el documento en cuestión hace referencia a la extracción de rasgos específicos del individuo a partir de los datos biométricos para elaborar una "plantilla biométrica". A continuación, esta plantilla se define como "la medida biométrica registrada de una persona". Lo que se almacena es la plantilla en formato digitalizado y no el propio elemento biométrico.

En definitiva, esta fase inicial en el tratamiento de datos biométricos, denominada "fase de inscripción" a la que ya hemos hecho referencia en el Capítulo I, es de singular importancia, porque en ella confluyen tres elementos: los datos brutos que antes hemos denominado elemento biométrico o datos físicos o de comportamiento, los algoritmos de extracción y protección que en cada caso utilice el sistema biométrico en cuestión y las plantillas. Y decimos que es singular esta fase porque cabe determinar a partir de qué momento resultaría aplicable la normativa sobre protección de datos de carácter personal, tanto europea como nacional de desarrollo.

Así, si los datos brutos revelan información del individuo que pueda considerarse sensible en el sentido que lo contemplaba el artículo 8 de la Directiva 95/46/CE, le es plenamente aplicable al proceso, o fase de inscripción, desde su inicio la prohibición establecida en dicho artículo. El apartado 1. del citado artículo 8 establecía que: "Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad", a no ser que se den determinadas circunstancias habilitantes[395].

[395] Circunstancias que aparecían recogidas en el apartado 2 de este artículo 8 que establecía: "2. Lo dispuesto en el apartado 1 no se aplicará cuando: a) el interesado haya dado su consentimiento explícito a

El RGPD, en su art. 4.14, nos proporciona una definción de datos biométricos: "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

De lo expuesto cabría deducir dos consideraciones: para el GPD 29 la normativa de protección de datos es aplicable a los sistemas biométricos y, segundo, el punto inicial de aplicación lo determina el carácter sensible o no del dato bruto que haya de tratar el sistema. Si los datos físicos, los surcos y valles de la huella revelan un dato de salud, sensible, desde ese momento de captura de esos datos físicos es de aplicación lo dispuesto en el citado artículo 8; entendiendo "sensible"[396] en el sentido determinado por el citado artículo 8 de dato de salud, origen racial, vida sexual. Pero si esos datos brutos no revelan información sensible, ¿es aplicable la Directiva? O aun siendo aplicable ¿lo es en un momento posterior a la fase de inscripción? Todas estas cuestiones se abordarán más adelante.

2.6. Requisitos en la captación del dato biométrico.

2.6.1. El principio de calidad.

dicho tratamiento, salvo en los casos en que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o d) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial".

[396] Como acertadamente comenta Heredero Higueras, los datos a que se refería este artículo 8 de la Directiva 95/46/CE, tanto para la doctrina como para el legislador, han sido objeto de una especial preocupación, ya que pueden ser utilizados para adoptar decisiones discriminatorias respecto a los individuos. No obstante, la doctrina mayoritaria entiende que no hay datos sensibles *per se* sino dependiendo del contexto en el que se tratan y, sin embargo, el legislador de la mayoría de los Estados miembros, con alguna excepción, aceptan la existencia de una categoría de datos sensibles *per se*. Cfr. HEREDERO HIGUERAS, M., op. cit., p. 116.

El principio de calidad ha experimentado un especial desarrollo en relación a un tipo muy específico de datos que son los relativos a la solvencia patrimonial y crédito de una persona. El artículo 38 RLOPD, establecía los requisitos para el tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés[397]. Aunque no exista una reglamentación tan concreta y específica respecto a los datos biométricos dactiloscópicos lo cierto es que el principio de calidad en su triple vertiente de principio de adecuación, pertinencia y proporcionalidad establece límites y cauces por los que ha de desarrollase la captación del dato dactiloscópico. En todo caso, el requisito previo para la utilización ajustada a la legalidad del dato biométrico, en general, y del dato dactiloscópico, en particular, es una definición clara de los fines para los que se recaba y trata. Sin un fin claro, y jurídicamente ajustado al ordenamiento, no existe apoyo jurídico para recabar y tratar datos. Es decir, no solo es necesario el establecimiento de unos fines claros, sino que también es imprescindible que esos fines no contraríen el ordenamiento; por ejemplo, una captación de datos cuya única finalidad sea el conocimiento de aquellos individuos con alteraciones en su huella dactilar no encuentra acomodo en Derecho.

Así, el mencionado principio de adecuación, de conformidad con el artículo 4.1 LOPD y 8.2 RLOPD, establecía que los datos de carácter personal solo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas. Por su parte, el criterio o principio de pertinencia hace referencia a que la recogida de los datos sea

[397] Estos requisitos son los siguientes: "1.- Sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, siempre que concurran los siguientes requisitos: a) Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el RD 303/2004 de 20 febrero 2004 Real Decreto 303/2004, de 20 de febrero, por el que se aprueba el Reglamento de los comisionados para la defensa del cliente de servicios financieros..
b) Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.
c) Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.
2. No podrán incluirse en los ficheros de esta naturaleza datos personales sobre los que exista un principio de prueba que de forma indiciaria contradiga alguno de los requisitos anteriores. […]
3. El acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento de los requisitos establecidos en este artículo […]." EDC 2014/30693 Requisitos.
http://online.elderecho.com/seleccionProducto.do?producto=A#presentar.do%3Fnref%3D7DE077E5%26producto%3DQ. [Fecha de consulta: 10 septiembre de 2017].

necesaria para el ámbito y las finalidades determinadas, explícitas y legítimas para la que se hayan obtenido. Por último, el criterio de proporcionalidad evalúa la existencia de ésta en un ejercicio de ponderación entre el hecho de la recogida y la finalidad que la motiva. Adecuación a la finalidad, pertinencia en correlación con la necesidad y proporcionalidad en relación a los riesgos para la privacidad del individuo que se generan con la recogida y tratamiento, son los tres pilares de la calidad. Así, por ejemplo, la AEPD (Informe 368/2006), aplicando este principio, tiene declarado que la utilización de la huella dactilar como medio para controlar el acceso de los alumnos al centro escolar es una medida desproporcionada y, por ende, contraria al art. 4 LOPD, ya mencionado. La finalidad de control de acceso al centro escolar puede alcanzarse a través de medios menos intrusivos. Sin embargo, la misma AEPD (Informe 266/2006) no considera desproporcionada la medida de inclusión de la fotografía de los trabajadores en la tarjeta identificativa que éstos llevan en su puesto de trabajo. La Agencia considera que la medida es proporcional a la finalidad que precisamente es poder identificar al trabajador en el ejercicio de sus funciones.

En este análisis de la base jurídica para la recogida-captación del dato dactiloscópico es importante la aportación del GPD 29, que afirma con rotundidad que los datos biométricos sólo pueden tratarse si existe dicha base jurídica. Y esta base se conforma tras el análisis de múltiples aspectos que el Grupo concreta en el estudio del propósito (finalidad), la proporcionalidad, la precisión, la minimización de datos y el periodo de conservación[398].

En cuanto al propósito la utilización de medidas de seguridad basadas en captación de huella dactilar no es, a priori, una finalidad o un propósito ilícito. Ahora bien, el GPD 29 en el Dictamen 3/2012, de referencia, advierte con gran acierto que la captación de una característica biométrica, con el fin de garantizar un nivel de seguridad adecuado a la criticidad de los datos que alberga un sistema puede no resultar efectiva porque muchos datos biométricos pueden captarse sin el conocimiento del interesado. Por eso, cuanto mayor sea el nivel de seguridad que sea necesario aplicar es menor la capacidad de los datos biométricos para alcanzar ese objetivo. No obstante, creemos que en el caso del dato dactiloscópico la captación de la huella dactilar es difícil que se produzca sin el

[398] Grupo de Trabajo del artículo 29. Dictamen 3/2012 sobre la evolución de las tecnologías biométricas. 00720/12/ES. WP193, adoptado el 27 de abril de 2012, op. cit., p. 7 y ss.

conocimiento del interesado. Por tanto, puede considerarse como una finalidad adecuada la captación de la huella dactilar para la autenticación de personas en el acceso a tratamientos de datos personales[399].

En lo referente a la proporcionalidad en el mismo sentido que el informe 368/2006 de la AEPD, arriba aludido, el GPD 29 considera que la instalación en un gimnasio de un sistema biométrico centralizado basado en la recogida de impresiones dactilares a fin de permitir el acceso a las instalaciones y servicios conexos únicamente a los clientes que hayan abonado su cuota es una medida desproporcionada en relación con la finalidad de control de acceso al recinto y control de la gestión del cobro de cuotas. La desproporción se deriva del hecho de que esas finalidades pueden ser atendidas sin necesidad de acudir al tratamiento del dato dactiloscópico.

En lo que respecta a la precisión, ésta exige que los datos biométricos sean exactos y pertinentes en relación con la finalidad para la que se recogieron. Esta exigencia de exactitud despliega sus efectos no solo en la captación o recogida del dato al establecer el vínculo entre el dato biométrico y la persona a quien pertenece, sino también, en el almacenamiento o registro a fin de evitar la usurpación de identidad. Esta exigencia de exactitud bien puede desembocar, como acertadamente apunta el GPD 29[400], en un identificador único que haría directamente aplicable a los datos biométricos lo que disponía, en su artículo 8.7[401] la Directiva 95/46/CE. Por otra parte, el principio de calidad en la recogida exige respetar un principio que el GPD 29 denomina de "minimización de datos", referente a una recogida no excesiva que cobra especial relevancia en el ámbito de los datos biométricos, ya que éstos, con frecuencia, contienen más información de la necesaria para la finalidad a la que se destinan (identificación o

[399] Lo que no tendría justificación alguna, en opinión del GPD 29, es el tratamiento de fotografías publicadas en internet, en las redes sociales, en aplicaciones de puesta en común o de gestión de fotos en línea con la finalidad exclusiva de extraer plantillas biométricas para reconocer a las personas de las imágenes automáticamente (reconocimiento facial). La extracción de las plantillas para el reconocimiento automático es una finalidad nueva para la que hay que recabar el consentimiento del titular de la imagen. El interesado ha de consentir que las fotografías en las que aparece puedan tratarse para etiquetarle automáticamente y además este reconocimiento automático de personas debe a su vez responder a una finalidad legítima y respetuosa con la protección de datos. Cfr. Grupo de Trabajo del artículo 29. Dictamen 3/2012. Ibíd., p. 8.

[400] En el capítulo I ya apuntamos el carácter único del dato biométrico y la generación de una plantilla o imagen también únicas que favorecerían la conformación de dicho dato como un identificador único. Ibíd., p. 10.

[401] "Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento".

bien autenticación) y para la búsqueda de correspondencias. Este principio de minimización despliega su efecto no solo en la recogida, sino que debe aplicarse en el tratamiento, la transmisión y el almacenamiento de la información necesaria para la finalidad. Para finalizar la calidad exige respetar un período de conservación de los datos biométricos que no exceda del necesario para atender a los fines para los que esos datos fueron recogidos. Aquí el GPD 29 vuelve a precisar la directa relación entre finalidad de la recogida y mantenimiento del dato biométrico; si la finalidad desaparece el dato debe ser suprimido.

2.6.2. El derecho/deber de información.

En el momento de la recogida del dato personal biométrico dactiloscópico se plantea una situación reversible de derecho/deber de información en la que el titular de los datos tiene un derecho de información que representa un deber para el responsable del tratamiento[402]. Éste tiene la obligación de informar de acuerdo con lo que disponía el art. 5 de la LOPD, es decir, informar de la existencia de un fichero o tratamiento, del carácter obligatorio o facultativo de las respuestas o del hecho de la recogida misma del dato dactiloscópico, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercicio de los derechos de acceso, rectificación, cancelación y oposición y de la identidad y dirección del responsable del tratamiento. Y el art.11 LO 3/2018 hace referencia a una información básica que el afectado debe recibir, y a la que ya hemos aludido.

Este deber de información se mantiene aún incluso en aquellos casos en que no es necesario el consentimiento del titular de los datos para su captación. El incumplimiento del deber de información hace ilegítimo el tratamiento posterior. En relación al deber de información, es digno de mención el criterio que ha mantenido la AEPD en relación a aquellos casos en los que son los propios titulares de los datos los que por propia

[402] Conviene precisar que. aunque la LOPD (art. 3 d) y el RLOPD (art. 5.1.q) definían de forma conjunta al responsable del fichero o tratamiento no son conceptos sinónimos. El responsable del tratamiento lo define de forma clara la Directiva 95/46/CE en su art. 2 d) como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; […]". La fijación de los fines y los medios del tratamiento corresponde al responsable del tratamiento pudiendo recaer la condición de responsable del fichero en otra persona distinta, toda vez que el concepto de tratamiento no es coincidente con el de fichero.

iniciativa facilitan voluntariamente sus datos para, por ejemplo, poder acceder a algún servicio. En este específico caso, en el que el titular revela sus datos al responsable del fichero porque tiene un específico interés en hacerlo, cabría considerarlo un supuesto de excepción[403].

Muy relevante es la STS, (Sala 2ª, S 14-10-2005, nº 1311/2005, rec. 739/2005), por un doble motivo: por la interpretación que hace el Tribunal del principio de información en la recogida y por el hecho de la obtención de datos personales de un elemento físico del cuerpo humano, en este caso restos de saliva.

La sentencia considera la prueba de ADN realizada sobre unos restos de saliva del acusado. Se trata, por tanto, de la obtención de datos personales relevantes en el proceso penal derivados de un elemento físico del acusado, en este caso, sin su consentimiento. La Sala 2ª desestima el recurso de casación porque la toma de muestras de ADN se lleva a cabo por razones de puro azar y a la vista de un suceso totalmente imprevisible, como fue que el procesado escupiera en el suelo; los restos de saliva escupidos se convierten así en un objeto procedente del sospechoso, pero obtenido de forma totalmente inesperada. Además, continúa la Sala, la Ley de Protección de Datos excluye de su ámbito de aplicación los ficheros y tratamientos establecidos con fines de investigación del terrorismo y formas graves de delincuencia organizada. Esta sentencia a su vez fue recurrida ante el Tribunal Constitucional dictándose la STC, Pleno de 5 diciembre 2013 (J2013/253497), que desestima el recurso interpuesto contra la STS Sala 2ª de 14 octubre 2005.

Brevemente, los hechos se resumen en la comisión por el acusado de un acto de violencia callejera (*kale-borroka*), recogiendo la policía del lugar de los hechos una camiseta de la que se obtuvieron restos genéticos que, posteriormente, fueron comparados con los restos de saliva obtenidos del acusado resultando coincidentes. La Audiencia Nacional, como Tribunal de instancia, condenó al acusado*:* "(…) como responsable penal en concepto de autor material de un delito de daños terroristas, con la concurrencia de la circunstancia modificativa de la responsabilidad criminal de disfraz,

[403] En este sentido, puede consultarse Sentencia de la Audiencia Nacional de 28 de septiembre de 2006 (recurso 000018/2005).

a la pena de seis años de prisión, privación del derecho de sufragio pasivo por el mismo tiempo e inhabilitación absoluta por seis años más, y al pago de las costas del juicio; debiendo indemnizar a la entidad bancaria <<Caja de Ahorros C.>>, en la suma de 17.199,21 euros". La representación procesal del condenado preparó e interpuso recurso de casación ante la Sala 2ª del Tribunal Supremo basándolo, entre otros, en los siguientes motivos: por resultar lesionado el derecho a la intimidad del artículo 18.1 CE, por resultar lesionado el derecho a la autodeterminación informativa del artículo 18.4 CE y por vulneración de la presunción de inocencia del artículo 24.2 CE. La defensa centra su recurso en la ausencia de garantías en la toma de muestras genéticas indubitadas, ya que éstas se obtienen de los restos de un esputo que el acusado realiza cuando sale de una de las celdas de la Comisaría y que es recogido por la policía. El alto Tribunal analiza la situación a la luz del derecho a la intimidad y del derecho a la autodeterminación informativa considerando no existe vulneración de ninguno de ellos. Reproducimos, por su claridad expositiva, parte del Fundamento Primero de la Sentencia (destacamos con subrayado lo más relevante a nuestro juicio):

"(…)

Toda la argumentación se centra en torno a la forma en que se realiza la toma de muestras orgánicas al acusado. No parece discutirse la pertenencia de las prendas encontradas en el lugar de los hechos y sobre todo las huellas genéticas que se observan en la camiseta que se usó a modo de pasamontañas para tapar el rostro mientras se ejecutaban los hechos que son objeto de enjuiciamiento en el presente procedimiento.

Suscita, con carácter general, si la <<huella genética>>, una vez analizada y codificada, constituye un <<indicador identificativo no sólo de la persona sino de sus posibles patologías>> con la consiguiente lesión o deterioro de sus derechos a la intimidad.

Profundizando en argumentos legales, mantiene que los laboratorios de la Ertzainza y los bancos de datos genéticos derivados del ADN, no se ajustan a las previsiones de la Ley Orgánica de 13 de diciembre de 1999 de Protección de Datos de Carácter Personal EDL 1999/63731. Reconoce que la Ertzainza regula los protocolos de actuación en estos casos en virtud de una Orden de 2 de septiembre de 2003 EDL 2003/64065. No obstante, insiste en que la forma de recogida de datos solo se puede hacer a través de la información facilitada libremente por el interesado, en virtud del derecho de autodeterminación

informativa, después de un consentimiento suficientemente informado o, en su caso, en virtud de requerimiento judicial.

En consecuencia, sostiene que se produce el efecto cascada previsto en el artículo 11, 1º de la Ley Orgánica del Poder Judicial EDL 1985/8754. En su opinión el vicio inicial insubsanable, arrastra o acaba con su virtualidad probatoria y su utilización como prueba de cargo. Advierte que, los peritos analizaran la prueba que les llega, anonimizada, ya que ignoraban su procedencia y además había sido obtenida subreptíciamente.

2.- Como pone de relieve el propio recurrente no nos encontramos ante la obtención de muestras corporales realizada de forma directa sobre el sospechoso, sino ante una toma subrepticia derivada de un acto voluntario de expulsión de materia orgánica realizada por el sujeto objeto de investigación, sin intervención de métodos o prácticas incisivas sobre la integridad corporal.

En estos casos, no entra en juego la doctrina consolidada de la necesaria intervención judicial para autorizar, en determinados casos, una posible intervención banal y no agresiva. La toma de muestras para el control, se lleva a cabo por razones de puro azar y a la vista de un suceso totalmente imprevisible. Los restos de saliva escupidos se convierten así en un objeto procedente del cuerpo del sospechoso, pero obtenido de forma totalmente inesperada. El único problema que pudiera suscitarse es el relativo a la demostración de que la muestra había sido producida por el acusado, circunstancia que en absoluto se discute por el propio recurrente, que sólo denuncia la ausencia de intervención judicial.

"Res nullius"

3.- Las previsiones de la Ley de Enjuiciamiento Criminal (artículo 363 y 778.3º EDL 1882/1) regulan, con rango legal, la obtención de muestras biológicas del sospechoso cuando sean necesarias e indispensables para la determinación de su perfil de ADN, procurando que la necesaria decisión motivada del juez se ajuste a los parámetros de proporcionalidad y razonabilidad.

4.- El primer aspecto que se denuncia es el relativo a la posible afectación de la intimidad del acusado ya que los perfiles genéticos no solo sirven para la identificación de personas, sino que pueden almacenar datos relativos a la salud que son eminentemente sensibles. No cuestionamos esta alegación que

admitimos, con carácter general, por su indudable base científica, pero, en el caso presente, se obtuvieron solamente para la identificación a través de una muestra aleatoria y con fines de investigación de un delito. No consta en las actuaciones que el proceso posterior de almacenamiento incluya datos más allá de los necesarios para las labores de investigación policial.

En todo caso, si el almacenamiento de datos excesivos e innecesarios perjudica o contraviene la normativa de la Ley de Protección de Datos EDL 1999/63731 será competencia de la Agencia de Protección de Datos investigar el fichero y reducirlo a los términos previstos por la ley. Todo ello para nada afecta a la identificación previa realizada con criterios adecuados, lo que hace innecesaria la autorización judicial al no suponer invasión corporal alguna. Es más, la Orden de 2 de septiembre de 2003 del Departamento de Interior Vasco EDL 2003/64065, limita su finalidad a las actividades de policía científica orientadas a relacionar personas con el espacio físico de la infracción penal.

5.- En cuanto a la autodeterminación o "habeas data" informativa creemos que se saca de contexto y no se ajusta a la realidad de lo sucedido en el caso presente. La autodeterminación en la facilitación de los datos es un presupuesto imprescindible que forma parte del derecho fundamental a la libertad y se complementa con otras garantías procesales.

Ahora bien, una vez más, hemos de repetir que la forma en que se recoge la muestra es absolutamente inesperada como pudiera suceder si se encuentra en una colilla, un cepillo de dientes o en un vaso en el que haya bebido el sospechoso.

La Carta de los Derechos Fundamentales de la Unión Europea efectivamente, en su artículo 8 EDL 1979/3822, proclama que toda persona tiene derecho a la protección de los datos de carácter personal y que sólo podrán ser recogidos mediante su consentimiento o en virtud de otro fundamento legítimo previsto por la ley.

Si relacionamos este precepto con el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales EDL 1979/3822 se llega a la conclusión de que la salvaguarda de la intimidad permite la injerencia prevista por la ley o cuando se trate de medidas aceptables en una sociedad democrática para la prevención del delito.

La Ley de 13 de diciembre de 1999 de Protección de Datos EDL 1999/63731 excluye de su ámbito de aplicación los ficheros y tratamientos establecidos con fines de investigación del terrorismo y formas graves de delincuencia organizada. En todo caso, el hipotético incumplimiento del registro constituye una irregularidad administrativa que en modo alguno supone la vulneración de un derecho fundamental que lleve aparejada la nulidad absoluta del análisis practicado.

La orden de 2 de septiembre de 2003 por la que se regulan los ficheros automatizados de datos personales por el Departamento de Interior del Gobierno Vasco EDL 2003/64065, establece un indiscutible marco de regulación de la recogida de muestras genéticas. De modo impecablemente legal, respeta el principio de autodeterminación de la persona previo consentimiento informado o, en su caso en virtud de requerimiento judicial. Una vez mas insistiremos en que todo el protocolo seguido para tomar muestras espontáneas y ajenas a cualquier compulsión personal se ha cumplido de forma escrupulosa.

El recurrente admite que los protocolos de obtención, método de tratamiento de la muestra, clase de análisis realizado e incluso su conservación, se ha ajustado a las previsiones establecidas por orden de la misma unidad policial que actúa. La impugnación de sus resultados sólo era posible sometiendo a una discusión técnico-científica el resultado del análisis y su comparación con la muestra obtenida, en el lugar del delito sobre una prenda que pertenecía a la persona que se vincula directamente con su participación en los hechos delictivos. Esta prueba contradictoria no ha sido solicitada.

Por lo expuesto el motivo debe ser desestimado".

2.6.3. **Motivo legítimo para la captación. El consentimiento**.

Hasta hace poco, se afirmaba con rotundidad que el consentimiento era la piedra angular de todo el edificio de la protección de datos. Lo cierto es que todo está cambiando y los medios a través de los que se obtiene el consentimiento en la nueva era digital no protegen adecuadamente la privacidad ni atienden los mínimos exigidos por el RGPD. El consentimieno puede definirse como toda manifestación de voluntad, libre, específica, inequívoca e informada y alcanzar todos esos atributos en el entorno digital

cotidiano no es fácil. Por tanto, el consentimiento está relacionado con el principio de información antes aludido.

La obtención previa del consentimiento del interesado supone disponer de la legitimación para tratar sus datos personales. La LOPD no exigía ninguna forma concreta en el otorgamiento del consentimiento, lo que sí exigía es que éste fuera inequívoco, es decir, indubitado. Y, sin dudar, la nueva Ley establece que el consentimiento ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyéndose el consentimiento tácito; en el caso de que el consentimiento sea necesario para una pluralidad de finalidades, es necesario que conste de manera precisa e inequívoca para todas ellas (art. 6 LO 3/2018).

Por tanto, un consentimiento inequívoco bien puede ser expreso, presunto, por actuaciones concomitantes, o tácito, derivado de la propia inacción. En la mayoría de los tratamientos, el consentimiento es tácito, salvo en los tratamientos de datos de salud, origen racial y vida sexual en que debe ser expreso y en los tratamientos de datos de ideología, afiliación sindical, religión y creencias en que debe ser expreso y por escrito. A la luz de lo descrito en capítulos anteriores, el consentimiento para el tratamiento del dato dactiloscópico habrá de ser expreso y, por tanto, consistir en una declaración de voluntad de forma clara e inequívoca al ser potencialmente revelador de datos de salud o de vida sexual.

Ahora bien, si esto es así no podemos olvidar la claridad con la que el Considerando (32) se refiere al consentimiento al decir que debe darse mediante un "acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen". Sin embargo, este acto afirmativo no se produce con claridad en la nueva era digital. El RGPD, a modo de ejemplo, cita expresamente la declaración por escrito, que puede ser por medios electrónicos, o bien una declaración verbal, como formas de este acto afirmativo. Lo que el Reglamento excluye del concepto de consentimiento son: "el silencio, las casillas ya marcadas o la inacción". Así, el artículo 4 11) deja definido el consentimiento como: "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;". El artículo 7

RGPD especifica aún más las características del consentimiento dejando que recaiga la carga de probar su existencia sobre el responsable del tratamiento. Si el consentimiento se otorga en el contexto de una declaración escrita, debe distinguirse claramente del resto de asuntos y la revocabilidad del consentimiento debe quedar siempre garantizada.

2.6.4. Especialidad en la recogida de los datos sensibles.

Nos detenemos en la fase de captación de los datos merecedores de una especial protección o datos sensibles porque, como veremos a continuación, el dato biométrico dactiloscópico puede revelar información sensible del individuo que éste tiene derecho a que goce de una especial protección. Sabemos que la regla general del consentimiento del titular de los datos para el tratamiento de sus datos de carácter personal no quiebra cuando se trata de los datos especialmente protegidos o datos sensibles a los que se refería el artículo 7 de la LOPD y se refiere el artículo 9 RGPD, bajo la denominación de "tratamiento de categorías especiales de datos personales", y artículo 9 LO 3/2018. De hecho, la normativa europea regula estos datos prohibiendo su tratamiento. Así el citado artículo 9 RGPD, en su apartado 1. afirma: "Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física".

Ahora bien, esta prohibición general puede quedar sin efecto al concurrir al menos una de las diez circunstancias que incluye a continuación el apartado 2. del mismo artículo 9. La primera de estas circunstancias la recoge el apartado a) no siendo así de aplicación el apartado 1. cuando "a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;".

Se plantean dos cuestiones que merecen, a nuestro entender, detenernos en ellas: el concepto de consentimiento explícito y la "prohibición absoluta "de tratamiento al no poder ser levantada por el consentimiento del interesado.

Es importante tener en cuenta que quienes traten datos personales especialmnte protegidos deben realizar, de acuerdo con el nuevo RGPD, un análisis de riesgos y si el tratamiento implica un riesgo alto, como es de suponer en el caso de este tipo de datos, es obligatorio realizar una evaluación de impacto, como también recoge la LO 3/2018. Nos detendremos en este punto siguiendo las guías prácticas que al efecto ha elaborado la AEPD de análisis de riesgos y de evaluaciones de impacto en la protección de los datos sujetas al RGPD.

Los datos relativos al origen racial, a la salud y a la vida sexual requieren el consentimiento expreso para su tratamiento, pero no necesariamente éste ha de constar por escrito. No obstante, el hecho de que no sea imprescindible el consentimiento por escrito no exime al responsable del fichero o del tratamiento a que acredite que cuenta con una manifestación de voluntad libre, inequívoca y específica para dicho tratamiento lo cual es más complejo si ésta no consta por escrito. Siendo, por tanto, el consentimiento por escrito la mejor manera de acreditar ese consentimiento expreso que la ley exige.

3. La conservación del dato dactiloscópico y la seguridad de los datos.

Las principales cuestiones jurídicas suscitadas por el tratamiento de datos biométricos están relacionadas con el derecho fundamental a la protección de datos que venimos comentando porque, sin dificultad, se puede afirmar que los datos biométricos son datos de carácter personal. Y estas cuestiones jurídicas se suscitan en la captación, en lo que se refiere al principio de finalidad que debe inspirar todo el proceso de recogida, ya que el dato biométrico debe ser adecuado, pertinente y no excesivo con respecto a la finalidad legítima para la que se recaba, pero también en la fase posterior de almacenamiento y nuevos accesos o reutilización del dato. Y es incluso en esta fase posterior de almacenamiento o conservación donde se plantean cuestiones aún más relevantes. En ambas fases se despliega el derecho de control del flujo de datos. Así, el

TEDH en el caso S y *Marper* contra el Reino Unido dictó Sentencia, el 4 de diciembre de 2008 en la que diferencia entre los procesos de extracción y de conservación de huellas dactilares, perfiles de ADN y muestras biológicas. Como acertadamente señala Correa (*et al*), el Reino Unido cuenta con una base de datos nacional de ADN (*Nacional DNA Database,* NDNAD*)* de las más desarrolladas de Europa, incluso del mundo. Como indican estos autores "el tratamiento de material biométrico como prueba en investigaciones penales está regulado por la Ley de Evidencia Policial y Criminal de 1984 (*Police and Criminal Evidence Act,* PACE*).* Esta ley fue sustancialmente modificada por la POFA, que en su parte 1 capítulo 1 regula la destrucción, retención y uso de material probatorio" [404]. El TEDH puso al descubierto en esta Sentencia que los problemas que plantea la conservación de estos datos y muestras superan a los que plantea la extracción. Y esto es así, entre otras cuestiones, porque, por ejemplo, la conservación de muestras biológicas plantea cuestiones de orden ético por la gran cantidad de información que pueden llegar a revelar de la persona en posteriores accesos.

Debemos tener en cuenta, antes de analizar la problemática jurídica de la conservación del dato dactiloscópico a la luz de la Sentencia del caso *Marper*, que el CEDH ha instaurado un sistema de control y de supervisión de los derechos humanos basado en un órgano de naturaleza jurisdiccional, el TEDH. Hasta 1998 existían básicamente dos órganos de control, la Comisión Europea de Derechos Humanos y el Tribunal, pero tras la entrada en vigor del Protocolo nº 11 al Convenio en noviembre de 1998, que prevé la supresión de la Comisión como filtro de las demandas, todas ellas se plantean directamente ante el Tribunal. El control del cumplimiento del Convenio por parte de los Estados se lleva a cabo a través de tres cauces o vías: los informes, las demandas interestatales y las demandas individuales. La primera vía, la de los informes, se inicia a requerimiento del Secretario General del Consejo de Europa, y en ella el Estado miembro debe explicar la manera en que su Derecho interno asegura la aplicación efectiva de las disposiciones del Convenio. La segunda vía, la de las demandas interestatales, se trata de una denuncia de uno o varios Estados miembros contra otro

[404] CORREA, M., (*et al*), *La construcción de estándares legales para la vigilancia en América latina. Parte II: Reglas comparadas a nivel global*, América Latina, Derechos digitales, 2018, pp. 42-43. Texto disponible en: https://creativecommons.org/licenses/by/4.0/deed.e [Fecha de consulta: 25/04/2019], pp. 40 ss.

por incumplimiento del Convenio. Por último, las demandas individuales, constituyen el mecanismo más importante mediante el que cualquier persona, ONG o grupo de particulares que se consideren víctima de una violación de sus derechos humanos puede plantear una demanda ante el TEDH. Además de esta función contenciosa el Tribunal Europeo también lleva a cabo una función de carácter consultivo en todos los asuntos relativos a la interpretación y aplicación del CEDH que le sean sometidos.

La jurisprudencia del TEDH es amplia en materia de protección de datos de carácter personal y también en relación con los datos de huella dactilar. Las decisiones de los Jueces del Tribunal de Estrasburgo en materia de privacidad y tratamiento de datos personales se han convertido en auténtica fuente del Derecho no solo comunitario sino interno. La noción de vida privada que maneja el TEDH dimana del texto del artículo 8 de la Convención Europea de los Derechos del Hombre y las Libertades Fundamentales firmado en Roma, 4.XI.1950. No obstante, al ser muy amplia esta noción ha permitido al TEDH interpretar este artículo 8 de forma evolutiva. En el mismo sentido, la amplitud con la que han sido formulados otros derechos en la Convención ha permitido igualmente al Tribunal considerar otros derechos humanos no explícitamente codificados como el derecho a la integridad psicológica o el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior. De hecho, el Tribunal ha llegado "a atribuir al principio de vida privada el valor de aglutinador de todos los derechos y las libertades que le pertenecen al hombre en cuanto ser humano"[405]. Este Derecho al respeto a la vida privada y familiar quedó formulado en el artículo 8 del Convenio, tras la modificación efectuada por las disposiciones del Protocolo n° 14 (STCE n° 194) que entraron en vigor el 1 de junio de 2010, como sigue: "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

[405] SOLINAS, C., "Tutela de la persona y tratamiento de los datos personales. Derecho interno y jurisprudencia del Tribunal Europeo de los Derechos Humanos y de las Libertades Fundamentales", en *Protección de Datos Personales en la Sociedad de la Información y la Vigilancia*, Madrid, LA LEY, 2011, p. 143.

Volviendo al citado caso S y *Marper* contra el Reino Unido, el TEDH plantea la diferencia entre los procesos de extracción y de conservación de huellas dactilares, perfiles de ADN y muestras biológicas. No podemos negar que tanto la extracción como la conservación son una forma de tratamiento, tal y como lo definía el artículo 2 b) de la Directiva 95/46, el artículo 3 LOPD, el vigente artículo 4 RGPD y los artículos 6, 8 y 10 de la vigente Ley Orgánica 3/2018. Ahora bien, como ya hemos apuntado, las cuestiones y controversias que genera la conservación superan a la extracción. En relación con la toma de muestras "se establece en general que el material biométrico no puede ser tomado sin el consentimiento apropiado, salvo que se cumpla con los requisitos de la ley; en el caso de huellas dactilares o de su pisada, la persona debe estar detenida tras su arresto por un delito, y sus huellas no han sido tomadas en el curso de la investigación por la policía (arts. 61-61A PACE)"[406]. Centrándonos en el caso, se trata de dos ciudadanos británicos, el señor S y *Michael Marper*, que presentan ante el Tribunal, en virtud de la legitimación activa que les confiere el artículo 34[407] del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su reclamación por considerar afectado o vulnerado su derecho al respeto a la vida privada y familiar. La demanda la presentan los dos ciudadanos británicos contra el Reino Unido por la conservación en los registros policiales de sus huellas dactilares, muestras biológicas y ADN después de haber sido absueltos o retirados los cargos de los delitos de los que eran sospechosos. Una vez dicho esto, y en lo referente al *Iter* procesal, conviene hacer mención a que en virtud del artículo 30[408] del Convenio la Sala declinó su competencia en favor de la Gran Sala.

La Sentencia aborda el derecho al respeto a la vida privada y familiar y a la protección de datos de carácter personal en supuestos de conservación de huellas dactilares,

[406] CORREA, M. (*et al*), op. cit., p. 41.
[407] ARTÍCULO 34. Demandas individuales. El Tribunal podrá conocer de una demanda presentada por cualquier persona física, organización no gubernamental o grupo de particulares que se considere víctima de una violación por una de las Altas Partes Contratantes de los derechos reconocidos en el Convenio o sus Protocolos. Las Altas Partes Contratantes se comprometen a no poner traba alguna al ejercicio eficaz de este derecho. http://www.echr.coe.int/Documents/Convention_SPA.pdf. [Fecha de consulta: 17/03/2016]
[408] "Artículo 30. Inhibición en favor de la Gran Sala. Si el asunto pendiente ante una Sala plantea una cuestión grave relativa a la interpretación del Convenio o de sus protocolos, o si la solución dada a una cuestión pudiera ser contradictoria con una sentencia dictada anteriormente por el Tribunal, la Sala podrá inhibirse en favor de la Gran Sala, mientras no haya dictado sentencia, salvo que una de las partes se oponga a ello".

muestras biológicas y ADN en el registro policial de sospechosos que han sido absueltos o sus causas archivadas. Como veremos, el TEDH en esta Sentencia considerará una medida desproporcionada la prevista por la ley con carácter general e indiscriminado con la finalidad de la detección y prevención del delito. Habría, en todo caso, que guardar un justo equilibrio entre los intereses públicos y privados. Ese carácter general e indiscriminado encierra un grave riesgo de estigmatización de las personas no culpables que son tratadas como culpables sin aplicárseles la presunción de inocencia. Es indudable que, el mantenimiento de las huellas dactilares de una persona en un registro policial de personas absueltas de una imputación penal o con causas archivadas, sitúa a esas personas en un punto de salida, o si se quiere, de inicio de una investigación policial distinto al resto de individuos. Los criterios de necesidad y de proporcionalidad han marcado y siguen marcando la línea que delimita la licitud del tratamiento de datos. Todo ello en conjunción con el principio de la finalidad legítima del tratamiento y/o acceso[409].

En lo que se refiere al procedimiento, el asunto tiene su origen en dos demandas (núms. 30562/2004 y 30566/2004) dirigidas contra el Reino Unido de Gran Bretaña e Irlanda del Norte, que dos ciudadanos británicos, los señores S. («el primer demandante») y *Michael Marper* («el segundo demandante») presentaron ante el Tribunal, en virtud del artículo 34 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales («el Convenio»), el 16 de agosto de 2004. Los demandantes se quejan, en virtud de los artículos 8 y 14 del Convenio, de que las autoridades conservasen sus huellas dactilares, muestras celulares y perfiles genéticos tras concluir, mediante la absolución y el archivo, respectivamente, las acciones penales entabladas contra ellos. Tanto uno como otro demandante pidieron que se destruyesen sus respectivas huellas digitales y muestras de ADN. La policía no accedió a la destrucción en ninguno de los dos casos. Ante esta negativa los demandantes accionaron judicialmente ante la jurisdicción británica, en concreto, el Tribunal administrativo que desestimó su solicitud. Los demandantes apelaron y en segunda instancia el Tribunal de apelación confirmó la decisión del Tribunal administrativo.

[409] Cfr. LÓPEZ AGUILAR, J. F., op. cit., p. 561.

Los recurrentes llegaron a la Cámara de los Lores y también esta Cámara desestimó su recurso al considerar que, en la conservación para posteriores accesos de las huellas digitales y muestras obtenidas de los sospechosos, prima la finalidad de esclarecer o determinar la autoría o grado de participación en un delito. Los demandantes siempre mantuvieron en sus sucesivos recursos ante instancias nacionales que la conservación de huellas digitales y muestras de ADN hacía recaer sospechas sobre personas que habían sido absueltas. En definitiva, la cuestión de la estigmatización de los individuos está sobre la mesa porque personas que han resultado absueltas tienen que soportar que sus huellas y/o perfiles se mantengan almacenados en una base de datos para posteriores comparaciones.

La Cámara de los Lores desestimó, por tanto, la queja de los demandantes según la cual la conservación de sus huellas digitales y muestras los sometía a un trato discriminatorio contrario al artículo 14[410] del Convenio en relación al conjunto de personas que no había tenido que prestarse a que la policía tomara sus huellas dactilares y muestras biológicas en el marco de una instrucción.

Entrando ya en los Fundamentos de Derecho de la Sentencia, ésta comienza por determinar si la conservación por las autoridades de las huellas dactilares, muestras celulares y perfiles de ADN de los demandantes puede considerarse una injerencia en la vida privada de los interesados. Ante los argumentos contrapuestos de las partes el Tribunal resuelve acudiendo a los Principios generales del Derecho. En cuanto a la aplicación al caso de autos de los citados principios generales, hay que comenzar por determinar si las tres categorías de datos conservados por las autoridades son o no datos de carácter personal. Sin reservas, el Tribunal señala, de entrada, que las tres categorías de información personal conservadas por las autoridades respecto a los dos demandantes, a saber, las huellas dactilares, los perfiles de ADN y las muestras celulares, constituyen datos de carácter personal en el sentido de la Convención sobre la protección de datos puesto que se refieren a personas identificadas o identificables.

[410] ARTÍCULO 14. Prohibición de discriminación. El goce de los derechos y libertades reconocidos en el presente Convenio ha de ser asegurado sin distinción alguna, especialmente por razones de sexo, raza, color, lengua, religión, opiniones políticas u otras, origen nacional o social, pertenencia a una minoría nacional, fortuna, nacimiento o cualquier otra situación. *Convenio Europeo de Derechos Humanos.* http://www.echr.coe.int/Documents/Convention_SPA.pdf. [Fecha de consulta: 17/03/2016].

El Tribunal recuerda una distinción entre la conservación de las huellas dactilares y la de las muestras celulares y los perfiles de ADN, debido a que la información personal contenida en estas dos últimas categorías se presta en mayor medida a posteriores utilizaciones (*Van der Velden* contra Países Bajos [dec.], núm. 29514/2005, TEDH 2006–...). Por tanto, la cuestión de la lesión del derecho de los demandantes al respeto de su vida privada ha de examinarse separadamente en cuanto a la conservación de sus muestras celulares y perfiles de ADN y la de sus huellas digitales.

En primer lugar, el Tribunal señala que "las muestras celulares contienen mucha información sensible de la persona, concretamente sobre su salud […]".

Como colofón de toda la argumentación expuesta "el Tribunal concluye que la conservación tanto de las muestras celulares como de los perfiles de ADN de los demandantes se considera una lesión del derecho de estos últimos al respeto de su vida privada, en el sentido del artículo 8.1 del Convenio".

Por lo que respecta a las huellas digitales el Tribunal afirma que "es patente que las huellas dactilares no contienen tanta información como las muestras celulares o los perfiles de ADN". Y aquí deben tenerse en cuenta las normas sobre retención y uso, ya que "por regla general, la ley permite la retención de las muestras hasta el fin de la investigación penal, o hasta la conclusión de los procedimientos contra la persona que se inicien tras dicha investigación (art. 63E PACE). Además, la ley establece otros casos excepcionales para la retención: investigaciones pendientes, reincidencia, consentimiento del comisionado, seguridad nacional, entrega voluntaria, entre otras (arts. 63F-63O PACE).

Los requisitos para usar el material retenido son: (i) interés de seguridad nacional; (ii) propósitos de investigación terrorista; (iii) prevención o detección de crimen, investigación de un delito o la conducción de una persecución penal; (iv) identificación de persona fallecida o de la persona de la que proviene el material (art. 63T PACE)"[411].

[411] No obstante, las normas sobre destrucción existen y disponen que: "las muestras biométricas deben ser destruidas si el oficial jefe de la policía considera que: (i) la toma de las muestras fue ilegal; (ii) la toma de las muestras fue realizada a una persona durante un arresto que fue ilegal o se basó en una identidad equivocada; (iii) cualquier otro caso donde no haya una autorización para retener dicho material. En

En base a esta normativa la retención y uso posterior de las huellas dactilares goza de un régimen más amplio, que el referido a perfiles de ADN y muestras celulares, siendo la prevención o detección del crimen la justificación alegada y admitida para su mantenimiento o retención.

En otro asunto, el denominado *Kinnunen*, "la Comisión consideró que la conservación tras la detención del demandante de sus huellas dactilares y fotografías, no se consideraba una injerencia en su vida privada puesto que tales elementos no contenían ninguna apreciación subjetiva susceptible de ser rebatida. […]". Es destacable esta decisión porque llama la atención sobre el verdadero punto crítico de la cuestión que es si la persona puede rebatir o no la información que sobre ella se ha almacenado y efectivamente no cabe contra-argumentación sobre datos que son objetivos.

El TEDH "considera que el enfoque adoptado por los órganos del Convenio respecto a las fotografías y muestras de voz se ha de aplicar también a las huellas dactilares. [...]".

La conservación de las huellas dactilares es, por lo tanto, susceptible de atentar contra la vida privada.

En segundo lugar, el Tribunal sigue su argumentación analizando el "fin legítimo" y el Tribunal reconoce, "que la conservación de datos relativos a las huellas dactilares y genéticas persigue una finalidad legítima: la detección y, en consecuencia, la prevención del delito. Mientras que la extracción inicial está destinada a vincular a una persona determinada con un delito concreto que se sospecha que ha cometido, la conservación persigue un objetivo más amplio, a saber, contribuir a la identificación de futuros delincuentes".

Y en tercer lugar, y en cuanto a la necesidad en una sociedad democrática y haciendo referencia a los Principios generales, el Tribunal añade: [Una injerencia se considera «necesaria en una sociedad democrática» para alcanzar un fin legítimo si responde a una «necesidad social imperiosa» y en particular, si es proporcionada al fin legítimo perseguido y si los motivos invocados por las autoridades nacionales para justificarla

general, las muestras deben ser destruidas, a más tardar, tras el transcurso de 6 meses desde que fueron tomadas (arts. 63D, 63R PACE). CORREA, M. (*et al*)., op. cit., p. 41.

parecen «pertinentes y suficientes». Si bien, corresponde, en primer lugar, a las autoridades internas juzgar si se cumplen todas estas condiciones, es el Tribunal quien tiene que resolver definitivamente la cuestión de la necesidad de la injerencia respecto a las exigencias del Convenio (Sentencia Coster contra el Reino Unido [GS], núm. 24876/1994, ap. 104, 18 enero 2001, y referencias citadas)].

Por tanto, la necesidad de una injerencia en la vida privada de los individuos se plantea en una sociedad democrática si hay una relación proporcional a un fin legítimo perseguido.

Y el Tribunal afirma rotundamente que [la protección de los datos de carácter personal juega un papel fundamental en el ejercicio del derecho al respeto de la vida privada y familiar consagrado por el artículo 8 del Convenio. Por tanto, la legislación interna debe ofrecer unas garantías apropiadas que impidan toda utilización de datos de carácter personal que no sea conforme a las garantías previstas en dicho artículo (ver, *mutatis mutandis*, Sentencia Z contra Finlandia, previamente citada, ap. 95). La necesidad de disponer de tales garantías se hace sentir aún más cuando se trata de proteger los datos de carácter personal sometidos a un tratamiento automático, en particular cuando estos datos son utilizados con fines policiales. El derecho interno ha de asegurar, concretamente, que estos datos sean pertinentes y no excesivos en relación a las finalidades para las que son registrados y que se conserven bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado (preámbulo y artículo 5 del Convenio sobre la protección de datos y principio 7 de la Recomendación R[87]15 del Comité de Ministros destinada a reglamentar el uso de los datos de carácter personal en el sector de la policía). El derecho interno ha de contener también garantías que protejan eficazmente los datos de carácter personal registrados contra los usos impropios y abusivos (ver, en particular, el artículo 7 del Convenio sobre la protección de datos). Las consideraciones que preceden sirven muy especialmente cuando se trata de proteger unas categorías particulares de datos más sensibles (artículo 6 del Convenio sobre la protección de datos), concretamente los datos de ADN que, en la medida en que contienen el patrimonio genético de la persona, son de gran importancia tanto para ella misma como para su familia (Recomendación núm. R [92] 1 del Comité de Ministros sobre la utilización de los análisis de ADN en el

marco del sistema judicial penal).] El Tribunal aborda en este argumento el principio base de la protección de datos, el principio de la calidad de los datos aplicable plenamente al asunto.

[El interés de las personas afectadas y del conjunto de la comunidad de que se protejan los datos de carácter personal y, concretamente, los relativos a las huellas dactilares y genéticas, puede desaparecer ante el interés legítimo que constituye la prevención del delito (artículo 9 del Convenio sobre la protección de datos). Sin embargo, habida cuenta del carácter intrínsecamente privado de esta información, el Tribunal debe proceder a un examen riguroso de cualquier medida adoptada por un Estado para autorizar su conservación y utilización por las autoridades sin el consentimiento de la persona afectada (ver, *mutatis mutandis*, Sentencia Z contra Finlandia, previamente citada, ap. 96)].

Una vez expuestos los principios, pasando a la aplicación de los mismos, en el presente caso para el Tribunal, [no hay duda de que la lucha contra la criminalidad y, concretamente, contra el crimen organizado y el terrorismo, que constituye uno de los desafíos a los que han de enfrentarse actualmente las sociedades europeas, depende en gran medida de la utilización de técnicas científicas modernas de investigación e identificación.

[En el caso de autos, las huellas digitales y muestras celulares de los demandantes fueron extraídas y sus perfiles de ADN realizados en el marco de unos procedimientos penales por robo en grado de tentativa en el caso del primer demandante y por acoso a su pareja en el caso del segundo. Los datos fueron almacenados sobre la base de una Ley que autorizaba su conservación ilimitada en el tiempo, si bien el primer demandante había sido absuelto y la causa del segundo se había archivado definitivamente].

[El Tribunal debe examinar si la conservación permanente de las huellas dactilares y los datos de ADN de todas las personas sospechosas, pero no condenadas se funda en unos motivos pertinentes y suficientes].

En conclusión, el Tribunal estima que el carácter general e indiferenciado de la facultad de conservar las huellas dactilares, las muestras biológicas y los perfiles de ADN de las

personas sospechosas de haber cometido delitos pero que no han sido condenadas, tal y como se ha aplicado a los demandantes en el caso de autos, no guarda un equilibrio justo entre los intereses públicos y privados que concurren y que el Estado demandado ha superado cualquier margen de apreciación aceptable en la materia. Por tanto, la conservación en litigio se ha de considerar una lesión desproporcionada del derecho de los demandantes al respeto de su vida privada y no puede considerarse necesaria en una sociedad democrática. Por ello, el Tribunal consideró que existía violación del artículo 8 del Convenio.

Por tanto, el TEDH pone de manifiesto claramente en esta sentencia que el derecho a la vida privada resulta comprometido por la mera conservación y almacenamiento de muestras biológicas y perfiles de ADN. Una vez afirmada la existencia de injerencia en la vida privada el TEDH sitúa la cuestión en la justificación de la medida en términos compatibles con el CEDH.

El Tribunal, al abordar el estudio de la existencia de un fin legítimo que justificase la injerencia apreciada, se ocupa de remarcar oportunamente la diferencia existente entre la conservación de muestras biológicas y perfiles de ADN para la identificación de los autores de futuros hechos delictivos y otros supuestos en los cuales "la extracción inicial está destinada a vincular a una persona determinada con un delito concreto que se sospecha que ha cometido" (§ 100). El reproche del Tribunal Europeo de Derechos Humanos se dirige a la conservación indefinida por las autoridades policiales de muestras biológicas y perfiles de ADN de personas no condenadas con la finalidad de identificar a los autores de futuros hechos delictivos, a través del contraste del ADN obtenido a partir de muestras biológicas del sospechoso "con vestigios anteriores conservados en la base de datos" (&116). La censura se realiza, por tanto, a la conservación de los datos personales, pues el Tribunal Europeo de Derechos Humanos afirma que "se ha de considerar que el mero hecho de que las autoridades públicas conserven o memoricen datos de carácter personal, cualquiera que sea la manera en la que hayan sido obtenidos, tiene unas consecuencias directas en la vida privada de la persona afectada, tanto si se utilizan o no estos datos posteriormente" (§ 1 19)”.

4. Mención a la categoría de datos sensibles, especialmente protegidos, como ámbito de protección del dato biométrico-dactiloscópico.

Como ya mencionamos en el capítulo I, para el profesor Troncoso Reigada[412], de la amplia variedad de datos relativos a un individuo se pueden establecer tres grandes grupos en función de su mayor o menor cercanía a la dignidad de la persona: en el primer grupo, denominado por este autor zona *core*, se encuentran los datos especialmente protegidos, en el segundo grupo se encontrarían los datos íntimos y en el tercero los datos de la relaciones profesionales, laborales y económicas.

También se apuntó en la introducción de este estudio la posibilidad de que una persona pueda ser tratada de una forma diferente, discriminada, como consecuencia del tratamiento de sus datos personales que revelan una deformación congénita de polidactilia o sufrir discriminación por la presencia en un dactilograma de alteraciones patológicas provocadas por una enfermedad venérea. Nos referimos a datos personales que pueden ofrecer una "vulnerabilidad especial"[413] en un doble sentido: bien porque a partir de ellos se pueden adoptar decisiones discriminatorias, o bien porque su uso o revelación puede provocar a sus titulares unos perjuicios más graves que la revelación de otros datos personales no sensibles. Los sistemas biométricos de captación de huella dactilar o reconocimiento de la palma de la mano pueden revelar información personal sensible. Qué ámbito es el más adecuado para proteger estos datos de una persona es una cuestión que trataremos a continuación, partiendo de considerar que, *a priori*, la categoría de los datos sensibles o especialmente protegidos es la categoría más adecuada por la propia naturaleza de dichos datos, puesto que pueden revelar datos de salud, o si no son datos de salud, puede tratarse de datos de configuración física de la persona que al igual que los datos de salud pueden intervenir, como ya se ha apuntado, en su discriminación.

En efecto, en una visión amplia de los datos sobre la salud cabría "(…) incluir las informaciones relacionadas con el cuerpo humano, la sexualidad, la raza, el código genético, los antecedentes familiares, los hábitos de vida, de alimentación y consumo"[414]. Sin duda, un dato dactiloscópico revela información relacionada con el

[412] TRONCOSO REIGADA, A., *La protección de datos…*, op.cit. pp. 780 y ss.
[413] HEREDERO HIGUERAS, M., op. cit. p. 116.
[414] SÁNCHEZ-CARO, J., ABELLÁN, F., *Datos sobre la salud y datos genéticos, Su protección en la Unión Europea,* Granada, Comares, 2004, p. 15, citado por REBOLLO DELGADO, L., SERRANO PÉREZ, M. M., *Manual de protección,* op. cit., p. 234. Nos indica este autor, apoyándose también en la

cuerpo humano, y ya podríamos considerarlo dato de salud en sentido amplio. Pero, además, si queremos especificar aún más la categoría cabría hablar de datos biosanitarios, dentro de los cuales se encuadrarían los datos genéticos y los datos biométricos.

En definitiva, sea dentro de un concepto amplio de datos de salud, sin mayores especificaciones, o sea dentro de un subconjunto de datos biosanitarios los datos biométricos y los dactiloscópicos, en particular, son datos especialmente protegidos o datos sensibles.

Pero, remontándonos a la Recomendación aprobada por el Consejo de la Organización de Cooperación y Desarrollo Económico (OCDE) en sesión celebrada el 23 de septiembre de 1980, ya se consideró la existencia de datos especialmente sensibles en atención a diversos criterios como, por ejemplo, la manera en que hubieren de ser tratados, su naturaleza o el contexto en que hubieren de ser utilizados. Como anejo a esta Recomendación se expresaron una serie de Directrices que son parte integrante de aquélla. Estas directrices deben considerarse pautas mínimas susceptibles de ser completadas con medidas adicionales de protección de la intimidad y de las libertades individuales. A su vez, existen unos comentarios de detalle que siguen a las directrices y hacen referencia a ellas y que precisan el sentido de los debates que tuvieron lugar en el seno del grupo de expertos. De estos comentarios de detalle merece ser destacado el apartado 3: "Grados de sensibilidad de los datos", que indica que las directrices no deben ser aplicables de manera puramente mecánica, cualesquiera que sean los tipos de datos y de actividades de tratamiento, sino que, muy al contrario, hay que atender a las diversas tradiciones y las distintas actitudes del público en general. Es decir, que cabría hablar de las distintas "sensibilidades" de la población en concreto. El comentario hace expresa mención de los identificadores personales universales ya que, por ejemplo, en un país pueden ser considerados como inocuos y, sin embargo, en otro país ser considerados como algo delicado. Esta cuestión incide directamente sobre el problema de la dificultad de definir unos datos sensibles considerados universalmente como

doctrina científica, que se puede añadir a la lista, "los trastornos mentales, las enfermedades y las adicciones. Incluso podrían formar parte también del concepto de datos sobre la salud, las dificultades de aprendizaje, la ludopatía, los conflictos de pareja problemas de adaptación, desarraigo (…), es decir, todas aquellas informaciones relativas a un individuo que, en un contexto sanitario, pudieran afectar a la situación de salud presente, pasada o futura de la persona".

tales[415]. No obstante, esta dificultad se consideró deseable enumerar tipos de datos sensibles. Así se recoge en estos mismos comentarios, concretamente en el referido al principio de limitación de la colecta[416] (principio incluido dentro de la segunda parte de las mencionadas Directrices, relativa a los principios fundamentales a aplicar en el ámbito interno) que en legislaciones europeas ya existe el precedente de enumeración de estos datos incluyéndose en dicha enumeración los datos de raza, creencias religiosas y registros de condenas. Este principio de limitación de la colecta hace referencia a dos cuestiones: los "límites a establecer en la colecta de aquellos datos que deban ser considerados como especialmente sensibles" (bien por la manera en que hubieren de ser tratados, bien por su naturaleza o bien por el contexto en el cual hayan de ser utilizados) y las "condiciones que deban cumplir los métodos de colecta de datos". Y es precisamente en relación con la primera cuestión, sin perjuicio de la diversidad de opiniones, donde se consideró posible y deseable enumerar tipos o clases de datos sensibles *per se*[417] y, en su caso, limitar o incluso prohibir su recogida. El grupo de expertos indicó que cabía encontrar legislaciones europeas que consideraban como tipos de datos sensibles los relativos a la raza, creencias religiosas, registros de condenas, entre otros. Sin perjuicio de este planteamiento, se puso de manifiesto que también cabe sostener que ningún dato es intrínsecamente sensible, ontológicamente en esencia, privado o sensible, sino que puede llegar a serlo, o no, dependiendo del contexto en el que se trate o considere y del uso que de él se haga. Las Directrices no enumeran unos datos como sensibles pero el Grupo de expertos consideró diversos criterios de sensibilidad, es decir, criterios para predicar la sensibilidad de un dato, o un conjunto de datos, como por ejemplo "el riesgo de discriminación"[418]. En relación con los límites en la recogida de datos aquéllos deben hacer referencia a: 1º aspectos cualitativos de los datos lo que supone que de los datos se ha de poder extraer una información de calidad

[415] A comienzos de 1978, se creó dentro de la OCDE un grupo *ad hoc* de expertos presidido por el juez *Kirby* que entre otras cuestiones abordó la relativa a los datos sensibles afirmando que posiblemente en rigor no era posible definir un conjunto de datos considerados universalmente como sensibles. Cfr. "Flujo Internacional de datos. Recomendación adoptada por el Consejo de la OCDE el 23 de septiembre de 1980, por la que se formulan directrices en relación con el flujo internacional de datos personales y la protección de la intimidad y las libertades fundamentales", en *Documentación Informática*, Serie Amarilla, Tratados Internacionales nº 2. Presidencia del Gobierno, Madrid, Servicio Central de Publicaciones. Servicio Central de Informática, 1982, pp. 33 y ss.

[416] "Principio de limitación de la colecta de datos. Deberán ponerse límites a la colecta de datos de carácter personal, debiendo tales datos ser obtenidos por medios legítimos y leales y, en los casos en que fuere procedente, con el conocimiento o el consentimiento del interesado". Ibíd., p. 18.

[417] Contraria a la categorización de datos sensibles en sí mismos es la mayoría de la doctrina y así algún autor habla de que no hay datos "intrínsecamente neutros". Cfr. LUCAS, A., *Le droit de l`ìnformatique*, París, PUF, Themis, 1987, p. 76.

[418] Ibíd., p. 51.

y obtenerse en un entorno de información al titular; 2º la recogida de datos debe limitarse al mínimo posible para atender a la finalidad prevista.

Merece aquí también especial mención el Convenio 108 del Consejo de Europa, que en su artículo 6, regula lo que denomina "Categorías particulares de datos". Prohíbe el tratamiento automático de los datos personales que revelan el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, los datos de salud o la vida sexual o los datos sobre condenas penales, a menos que el derecho interno de cada país prevea garantías adecuadas.

Por tanto, es evidente la dificultad de establecer unos datos considerados como sensibles universalmente, por todos. Pero lo que sí es cierto es que un dato que pueda servir para discriminar a una persona es un dato sensible. Por este motivo, es importante precisar, qué se entiende por discriminación; qué datos pueden servir para discriminar a alguien y si los datos revelados tras la captación de una huella dactilar pueden llevar o desembocar en dicha discriminación. En esta tarea nos ayuda el TEDH, el cual, en su sentencia de 25 de enero de 1997, estableció en relación con las informaciones sobre la salud y su divulgación no consentida que ello podía tener "consecuencias desastrosas sobre la vida privada y familiar de la persona concernida y sobre su situación profesional, exponiéndola a su desaprobación y a un riesgo de exclusión"[419]. Son dos los componentes de la exclusión social: la divulgación de un dato personal y la desaprobación social que ello conlleva. En definitiva, la discriminación, nos dice el TEDH, lleva como componente intríseco el conocimiento de un dato/s de un individuo que por su carácter especialmente "pegado" a su configuración física o a sus comportamientos pueden provocar rechazo en la sociedad. Consideramos que los datos que puede llegar a revelar una huella dactilar, aunque solo sea en un bajo porcentaje de casos, puede desencadenar el proceso de exclusión al que hemos aludido.

Otra cuestión es si la lista de los datos sensibles es una lista abierta o cerrada. Esta cuestión se debatió en la fase de tramitación de la Directiva 95/46/CE, resolviéndose a favor del carácter de lista abierta. La enumeración que hacía la Directiva de las "categorías especiales de datos", o lo que es lo mismo, datos sensibles, cabría considerar

[419] Tribunal Europeo de Derechos Humanos: Sentencia Z.c. Finlandia, de 25 de febrero de 1997. Demanda nº 22009/93.

que no es una lista cerrada. Pero, en general, aunque no exista un impedimento explícito a la existencia de dicha lista abierta lo cierto es que su existencia haría muy difícil la armonización de legislaciones en el ámbito de aplicación de la Directiva si cada Estado miembro amplía la lista *ad libitum*. En todo caso, lo que sí cabe constatar es que actualmente las legislaciones no prohíben rígidamente el tratamiento de estos datos, sino que éste se condiciona al cumplimiento de unos requisitos determinados.

La Directiva 95/46/CE recogía en el apartado 1 de su artículo 8, "Tratamientos de categorías especiales de datos", la prohibición del tratamiento de seis determinadas categorías de datos personales, en concreto: los que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, datos relativos a la salud y a la sexualidad. Pero esta prohibición no se aplica en cinco situaciones diferentes que pueden concurrir en un tratamiento de forma cumulativa o aislada excluyendo cada una de ellas por separado la prohibición de tratamiento expuesta. Así, estas cinco situaciones son: primera, que el interesado haya dado su consentimiento; segunda, que el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral; tercera, que el tratamiento sea necesario para salvaguardar un interés vital del interesado; cuarta, que el tratamiento se realice por una asociación o fundación sin ánimo de lucro en desarrollo de su actividad legitima y se refiera a los miembros de esa institución y, quinta y última, se trate de datos hechos públicos por el propio interesado o que el tratamiento sea necesario en el seno de un procedimiento judicial para el reconocimiento, ejercicio o defensa de un derecho. Una sexta excepción a la prohibición se recoge en el apartado 3 de este artículo 8 únicamente respecto a los datos de salud si el tratamiento resulta necesario para la prevención o para el diagnóstico médico y se realiza por un profesional sanitario sujeto al secreto profesional. El artículo 8.5 prevé la ampliación de las excepciones al tratamiento de estos datos sensibles por motivos de interés general y siempre que lo prevea la legislación nacional o bien la autoridad de control.

Sin duda, la delimitación jurídica del concepto de dato sensible es fundamentalmente material, estando concretados, tanto en el RGPD como en la LO 3/2018, por todos aquellos que revelan o son susceptibles de revelar el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, los datos

de salud y los relativos a la sexualidad; de este modo, se ha unificado "la denominación bajo el generíco concepto de <<categorías especiales de datos personales>>, a los que de forma genérica, y, en principio, podemos identificar con un mayor grado de protección, además de no ser una lista cerrada, puesto que la normativa europea prevé la ampliación de las excepciones al tratamiento de estos datos por motivo de interés general y siempre que lo prevea la legislación nacional o bien la autoridad de control"[420].

La LOPD, bajo la denominación de datos especialmente protegidos, reproducía la regulación de la Directiva. El artículo 7 de la LOPD diferenciaba dos conjuntos de datos especialmente protegidos: aquellos que revelen la ideología, afiliación sindical, religión y creencias y como segundo grupo los que hacen referencia al origen racial, a la salud y a la vida sexual. El primer grupo de datos únicamente puede recogerse "con el consentimiento expreso y por escrito del afectado". Además, nadie puede ser obligado a declarar sobre su ideología, religión o creencia en consonancia con la libertad de conciencia reconocida en el artículo 16.2 CE. Se establece una excepción para los ficheros de los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, exigiéndose siempre el consentimiento para la cesión de estos datos.

El RLOPD, en el artículo 81.2 f) exigía la implantación de medidas de seguridad de nivel medio además de las de nivel básico a ficheros o tratamientos de datos de carácter personal "… que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos". Aunque bien es cierto que este apartado se está refiriendo a los datos destinados a evaluar determinados aspectos de la personalidad de un individuo, (artículo 13 LOPD), también consideramos que podrían tener cabida algunos datos biométricos que miden aspectos del comportamiento de una persona. En todo caso, el artículo 81.3. a), 81.5 y 81.6 del RLOPD establecían las medidas de seguridad de los datos

[420] REBOLLO DELGADO, L., SERRANO PÉREZ, M. M., *Manual de Protección…,* op. cit., p. 222.

especialmente protegidos. En el caso de los datos de ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual se han de aplicar junto a las medidas de nivel básico y medio, las de nivel alto. No obstante, se establece una excepción en relación con los ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastando la implantación de medidas de nivel básico cuando los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros. O bien, se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad. Así mismo, el artículo 81.6 establecía que también podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

La PRGPD recogía, en su artículo 9, el tratamiento de categorías especiales de datos personales en términos, en muchos puntos, coincidentes con la Directiva.

> "Artículo 9: Tratamiento de categorías especiales de datos personales
>
> 1. Queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, la religión o las creencias, la afiliación sindical, así como el tratamiento de los datos genéticos o los datos relativos a la salud, la vida sexual, las condenas penales o medidas de seguridad afines.
>
> 2. El apartado 1 no será aplicable si:
>
> a) el interesado ha dado su consentimiento para el tratamiento de dichos datos personales, sin perjuicio de las condiciones establecidas en los artículos 7 y 8, excepto cuando el Derecho de la Unión o la legislación de los Estados miembros disponga que la prohibición establecida en el apartado 1 no puede ser levantada por el interesado; o
>
> b) el tratamiento es necesario para cumplir las obligaciones y ejercer los derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que así lo autorice el Derecho de la Unión o la legislación de los Estados miembros que establezca las garantías apropiadas; o

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento; o

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a sus miembros, a antiguos miembros del organismo o a personas que mantengan contactos regulares con la fundación, la asociación o el organismo en relación con sus fines y siempre que los datos no se comuniquen fuera del organismo sin el consentimiento de los interesados; o

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos; o

f) el tratamiento es necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; o

g) el tratamiento es necesario para el cumplimiento de una misión de interés público, sobre la base del Derecho de la Unión o la legislación de los Estados miembros, que establecerán las medidas adecuadas para proteger los intereses legítimos del interesado; o

h) el tratamiento de datos relativos a la salud es necesario a efectos sanitarios y sin perjuicio de las condiciones y garantías contempladas en el artículo 81; o

i) el tratamiento es necesario con fines de investigación histórica, estadística o científica, sin perjuicio de las condiciones y garantías contempladas en el artículo 83; o

j) el tratamiento de datos relativos a condenas penales o medidas de seguridad afines se lleva a cabo bajo la supervisión de poderes públicos o si el tratamiento es necesario para cumplir una obligación jurídica o reglamentaria a la que esté sujeto el interesado o para desarrollar una tarea llevada a cabo por motivos importantes de interés público y siempre que lo autorice el Derecho de la Unión o la legislación de los Estados miembros que establezca las garantías apropiadas. Solo se llevará un registro completo de condenas penales bajo el control de los poderes públicos.

3. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios, las

condiciones y las garantías apropiadas para el tratamiento de las categorías especiales de datos personales contempladas en el apartado 1 y las excepciones establecidas en el apartado 2."

La PRGPD no recogía en este artículo 9 como una categoría especial de datos personales a los datos biométricos, pero en el artículo 33, al referirse a la "Evaluación de impacto relativa a la protección de datos", consideraba que determinadas operaciones de tratamiento entrañan riesgos específicos para los derechos y libertades de los individuos y, en concreto, el tratamiento de datos biométricos es una de ellas. La existencia de estos riesgos obliga al responsable, o al encargado del tratamiento, a realizar la "evaluación de impacto". Esta evaluación debe incluir " […] como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a los riesgos, y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de datos personales y a probar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas". Para realizar esta evaluación, el responsable deberá recabar la opinión de los interesados en relación con el concreto tratamiento previsto. Ahora bien, continuaba este artículo 33, que cuando el responsable sea una autoridad u organismo público y el tratamiento se efectúe en cumplimiento de una obligación legal, es decir, conforme al artículo 6.1.c) "el tratamiento es necesario para el cumplimiento de una obligación jurídica a la que está sujeto el responsable del tratamiento", no será aplicable esta evaluación de impacto.

El RGPD, en su Considerando (10), comienza reconociendo a cada Estado miembro un margen de maniobra en el establecimiento de las normas que rijan el tratamiento de categorías especiales de datos citando la terminología "datos sensibles" para referirse a ellos, no volviendo a utilizarla en el resto del texto. Para referirse a estos datos especialmente protegidos el RGPD utiliza la expresión: "categorías especiales de datos personales". Y es también el artículo 9 RGPD el dedicado a la regulación del "Tratamiento de categorías especiales de datos personales".

Aunque efectivamente partimos de una prohibición general de tratamiento de estas categorías especiales de datos, el mismo Considerando (51) reconoce la necesidad de

excepciones explícitas a dicha prohibición. Sin duda, cuando el interesado otorgue su consentimiento explícito la excepción se cumple. Pero el RGPD va más allá al admitir la excepción ante necesidades específicas y, en concreto, si nos encontramos detro del marco de actividades legítimas de asociaciones y fundaciones cuyo objetivo sea permitir o favorecer al ejercicio de las libertades fundamentales. A nuestro entender, no es angosto el camino que se abre así a las excepciones a la prohibición inicial al tratamiento. El Considerando (52) sigue recogiendo excepciones a la prohibición en este caso fundadas en la existencia de un interés público enumerando unos ámbitos en los que este interés puede estar presente como: "[…] la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud"[421]. Son ámbitos en los que bien el Derecho de la UE o de los Estados miembros pueden definir excepciones a la prohibición con las garantías apropiadas para proteger los datos personales y otros derechos fundamentales. La excepción en el ámbito de la salud puede presentar finalidades diversas, así, por ejemplo: "[…] con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos*".* Y, por último, se recoge una última excepción que el propio Reglamento califica de "a título excepcional", consistente en la necesidad de tratamiento de las categorías especiales de datos para la formulación, el ejercicio o la defensa de reclamaciones en un procedimiento judicial, administrativo o extrajudicial. En un procedimiento judicial, entendemos, habrá un tercero imparcial que vele por el cumplimiento de los límites de la excepción, pero en un procedimiento administrativo la propia Administración es parte interesada y ¿en un procedimiento extrajudicial? Cabe preguntarse qué considera el RGPD como procedimiento extrajudicial. Si consideramos un procedimiento arbitral podemos confiar en ese tercer garante. Pero en una reclamación extrajudicial entre partes en

[421] En este sentido de amenaza grave para la salud el Considerando (54) desarrolla el tratamiento sin consentimiento por razones de interés público en el ámbito de la salud pública que debe entenderse en el contexto del Reglamento (CE) n.o 1338/2008 del Parlamento Europeo y del Consejo, por tanto: "todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad […]".

conflicto ¿la excepción puede operar? Entendemos que no. En todo caso el "arca" de las excepciones se amplía considerablemente.

El Considerando (53) hace referencia dentro de estas categorías especiales de datos a los que "merecen mayor protección" que únicamente deben ser tratados con fines relacionados con la salud. Nos hace pensar en los datos de la zona que podríamos calificar de "más sensible" que, por ejemplo, en nuestra legislación interna la constituyen los datos de origen racial, salud y vida sexual. Pero esta zona altamente sensible o "más sensible" entendemos se ve ampliada en el articulado del RGPD, en concreto, en el artículo 9.1, ya que, junto al origen étnico o racial, la salud, la vida sexual o las orientaciones sexuales, recoge expresamente los datos genéticos y los "datos biométricos dirigidos a identificar de manera unívoca a una persona física". Y nos hace pensar en el reconocimiento por parte del RGPD de esta zona de mayor sensibilidad porque en el mismo artículo 9.4 se preveé que: "Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud". Merece destacar, a los fines de este estudio, que los datos biométricos se incluyen en esta zona altamente sensible.

Recordemos que el artículo 9.1 del RGPD prohíbe el tratamiento de categorías especiales de datos personales incluyendo en estas categorías a: "[…] datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física". En concreto, son ocho categorías especiales de datos. Ahora bien, el apartado 2. de este mismo artículo 9 recoge diez excepciones a la prohibición que son:

- consentimiento explícito del interesado salvo que el Derecho de la UE o de los Estados miembros no permita esta excepción;
- necesidad derivada del cumplimiento de obligaciones o ejercicio de derechos del responsable o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social;
- necesidad de proteger intereses vitales del interesado o de otra persona física;

- tratamiento efectuado por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro en el ámbito de sus actividades y la finalidad sea política, filosófica, religiosa o sindical respecto de sus miembros o exmiembros;
- comunicación pública previa hecha por el propio interesado;
- necesidad para la formulación, ejercicio o defensa de reclamaciones[422] o cuando los tribunales actúen en ejercicio de su función judicial;
- necesidad por razones de interés público esencial, sobre la base de una habilitación legal bien del Derecho de la UE o de los Estados miembros y atendiendo al principio de proporcionalidad respecto del objetivo perseguido, respetando lo esencial del derecho a la protección de datos y establecimiendo medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
- necesidad para fines de medicina preventiva o laboral, sobre la base una habilitación legal, en todo caso el tratamiento debe hacerlo un profesional sujeto a la obligación de secreto profesional o por cualquier otra persona también sujeta a la obligación de secreto;
- necesidad por razones de interés público en el ámbito de la sanidad pública, igualmente sobre la bese de una habilitación legal;
- necesidad con base en fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos con las garantías de habilitación legal, proporcionalidad entre tratamiento y fines, respeto en lo esencial al derecho a la protección de datos y medidas adecuadas y específicas de protección, antes aludidas.

Sin duda el elenco de excepciones es amplio, no injustificado, pero indudablemente amplio.

Las categorías especiales de datos tienen una regulación especial en el artículo 22.4 en relación con las decisiones individuales automatizadas que no pueden basarse en estas categorías de datos, salvo que el interesado haya dado su consentimiento explícito o estemos en presencia de razones de interés público esencial.

[422] No especifica el texto del artículo 9.2. f) RGPD, por lo que cabrían tanto judiciales como extrajudiciales en armonía interpretativa con el Considerando (52), ya mencionado.

El resto de menciones en el texto del RGPD a estas categorías especiales de datos vienen a ser adjetivas en relación a la obligación o no de adoptar medidas de seguridad. El artículo 30.5, en lo que se refiere a las obligaciones de registro del tratamiento, no se aplica a empresas u organizaciones con menos de 250 empleados salvo, entre otras excepciones, que el tratamiento incluya categorías especiales de datos. En este sentido de cumplimiento de formalidades el artículo 35.3.b) en el tratamiento a gran escala de categorías especiales de datos, será precisa la evaluación de impacto. Así mismo, la designación de un delegado de protección de datos será necesaria siempre que las actividades principales del responsable y del encargado del tratamiento sean categorías especiales de datos a gran escala. Es evidente que el RGPD identifica como una actividad de riesgo para la privacidad de la persona el tratamiento a gran escala de datos sensibles. También se recoge en el artículo 47.2.d) como necesario contenido de las normas corporativas vinculantes en un sector, empresa, grupo de empresas, etc… el tratamiento de estos datos.

En suma, a través de este epígrafe, hemos intentado situar el dato biométrico como una categoría específica de datos sensibles.

5. Breve referencia a los antecedentes legislativos de la regulación de la biometría en Norteamérica y la adaptación al RGPD en la Unión Europea

En este apartado haremos unas breves referencias, a modo casi de enumeración, de dos puntos interesantes para nuestro estudio, relacionados con las legislaciones sobre protección de datos. En primer lugar, citaremos la regulación de la biometría en EEUU, muy relevante, por cierto, en tres Estados; en segundo lugar, y por orden cronológico, la adaptación progresiva que han ido realizando los distintos países de la UE al nuevo RGPD.

En cuanto al primer punto, sabemos que el uso y regulación de la biometría comienza fundamentalmente en EEUU. Pues bien, el Estado de Illinois[423] cuenta desde el 10 de

[423] *Biometric Information Privacy Act*. (Source: P.A. 95-994, eff. 10-3-08.) http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004 [Fecha de consulta: 14/05/2019]

marzo de 2008 con la denominada *Biometric Information Privacy Act*[424]. Esta ley, breve en su extensión, sin embargo, recoge una serie de disposiciones de gran claridad en su formulación positiva que sin duda entendemos sirven de orientación en la materia. Se puede afirmar que esta Ley del Estado de Illinois es de las más estrictas leyes de privacidad en biometría en Estados Unidos. Merece destacar la (740 ILCS 14/15) Sec. 15. referente a la retención, almacenamiento, revelación y destrucción de identificadores biométricos. Previamente la ley en 740 ILCS 14/10) Sec. 10. definiciones, entiende comprendidos dentro de los identificadores biométricos a las huellas dactilares, entre otros, quedando excluidos el material biológico, imágenes del interior del cuerpo tomadas para combatir una enfermedad, fotografías, órganos donados o descripciones físicas del individuo. En definitiva, se restringen los identificadores biométricos a características permanentes del individuo que están mostrados al exterior y que permiten identificar a una persona. Por ello, sigue diciendo la ley en esta misma Sec. 10. que la información biométrica es aquella que con independencia de cómo se haya capturado, almacenado o tratado permite identificar a un individuo. Volviendo a lo dispuesto en la Sec. 15., ya aludida, las entidades en posesión de información biométrica y/o identificadores biométricos deben desarrollar una política de privacidad por escrito pública acomodada a dicha información que poseen. Esta política debe contener un plan o un programa de mantenimiento y, a la vez, de destrucción de forma permanente de los identificadores biométricos y/o información biométrica cuando el propósito inical para el que se recopilaron esos identificadores se ha cumplido; o bien, en todo caso, la ley establece un plazo de tres años desde la última interacción del individuo con la entidad detentadora de dicha información biométrica para que se produzca la destrucción, lo que ocurra primero de los dos escenarios propuestos. Esta política de privacidad es de obligado cumplimiento para la entidad. Podemos considerar que esta política de privacidad biométrica viene a ser el antecedente de los "Códigos de conducta" regulados por la sección 5ª del Capítulo IV del RGPD. La misma sec. 15

[424] Recientemente se ha dictado una Sentencia por la Corte Suprema del Estado de Illinois, en concreto el 25 de enero de 2019, siendo partes interesadas Stacy Rosenbach *as Mother and Next Friend of Alexander Rosenbach, Appellant, v. Six Flags Entertainment Corporation et al., Appellees.*
La Sentencia considera hechos ocurridos en mayo o junio de 2014 en un parque de entretenimiento de la empresa Six Flags Entertainment Cp. en Gurnee (Illinois) donde se utiliza el escaneo de las huellas dactilares como sistema de control de acceso a dicho parque. La Corte Suprema entiende que no se pueden recoger datos biométricos, como la huella dactilar de un individuo, sin informarle previamente sobre dicha recogida y tratamiento posterior y sin recabar su consentimiento, lo contrario es una violación de la *Illinois Biometric Information Privacy Act (BIPA)*. En esta Sentencia la Corte Suprema entiende que no es necesario demostrar un daño concreto como un fraude en la identidad para considerar la existencia de una violación de la BIPA. https://www.eff.org [08/05/2019].

establece que, en todo caso, el titular de la información biométrica debe ser informado previamente sobre el hecho de la recopilación y almacenamiento de la información biométrica. Queda prohibida la venta o la obtención de cualquier otro lucro, de la información biométrica y/o los identificadores biométricos. Por último, señalar que la sec. 20 de la ley otorga a cualquier persona agraviada por una violación de esta ley una acción ante el Tribunal estatal y ante el Tribunal del distrito federal.

Por su parte, la Ley de Identificadores Biométricos de Texas (*Biometric Identifier Statute*), replicada en el art. 503.001 de su Código de Comercio[425], establece que "una persona no puede capturar un identificador biométrico de un individuo para un propósito comercial a menos que la persona informe al individuo antes de capturar el identificador biométrico; y reciba el consentimiento de este para capturarlo.

La persona que posee un identificador biométrico de un individuo que es capturado para un propósito comercial no puede venderlo, arrendarlo o divulgarlo a otra persona a menos que:

(1) Consentimiento del individuo para fines de identificación en caso de desaparición o muerte de la persona.
(2) La divulgación complete una transacción financiera que el individuo solicitó o autorizó.
(3) Sea requerida o permitida por un estatuto federal o estatal.
(4) Sea hecha por una agencia policial con el propósito de hacer cumplir la ley en respuesta a una orden judicial".

Por último, la Ley de Privacidad Biométrica de Washington (*Biometric Privacy Act*, HB1493)[426] regula los identificadores biométricos en términos análogos al Estatuto de Texas. (Véase Anexo I, donde pueden encontrarse los textos norteamericanos).

[425] Puede encontrarse en https://codes.findlaw.com/tx/business-and-commerce-code/bus-com-sect-503-001.html [Fecha de consulta: 14/05/2019]. Cfr. CORREA, M. (*et al*) *La construcción de estándares legales para la vigilancia en América latina. Parte II: Reglas comparadas a nivel* global, América Latina, Derechos digitales, 2018, pp. 42-43. Texto disponible en: https://creativecommons.org/licenses/by/4.0/deed.e [Fecha de consulta: 25/04/2019].
[426] Disponible en https://app.leg.wa.gov/RCW/default.aspx?cite=19.375&full=true. [Fecha de consulta: 08/05/2019].

En cuanto al segundo punto, la adaptación al RGPD en la Unión Europea, han sido diversos los países que cuentan ya con una legislación adaptada al nuevo RGPD. De una forma algo inesperada, el legislador español, como ya hemos indicado en las primeras páginas, elaboró la LO 3/2018, a la que ya hemos hecho obligadas referencias. Pero no hemos sido los únicos.

En efecto, no podemos olvidar que tanto en España como en el resto de la UE estamos en un proceso de actualización de las respectivas normartivas internas. Comenzaremos haciendo referencia a este proceso en Alemania, ya que fue el primer país en adaptarse al RGPD. La fecha de aprobación de la denominada *Bundesdatenschutzgesetz*[427] fue julio de 2017. De este modo, Alemania se adelantó en un año a la obligatoriedad de la adaptación de la legislación interna al Reglamento. Siguiendo un orden cronológico, Austria, en abril de 2018, aprobó su ley interna de adaptación, la denominada *Austrian Data Protection Act (Datenschutzgeset)*[428].

Por su parte, Bélgica aprobó la nueva Ley de protección de datos en julio de 2018[429] y, en ese mismo mes de julio de 2018, Bulgaria modificó su antigua ley, aprobando la denominada *Personal Data Protection Act* (*Draft Bill)*[430].

En Chipre fue publicada la ley 125 (I/2018)[431]; Croacia promulgó su nueva Ley el 27 de abril de 2018, entrando en vigor en mayo de ese año[432]. Dinamarca, un mes después, aprobó la *Danish Data Protection Act* el 23 de mayo de 2018[433], entrando en vigor en ese mismo mes.

[427] Disponible en: https://dsgvo-gesetz.de/bdsg/ [Fecha de consulta: 17/02/2019]
[428] Disponible en: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html [Fecha de consulta: 17/02/2019].
[429] Disponible en: https://iapp.org/media/pdf/resource_center/Belgian/GDPR-law_FR-DUTCH.pdf [Fecha de consulta: 20/03/2019].
[430] Disponible en: https://www.parliament.bg/bg/laws/ID/78179 [Fecha de consulta: 20/02/2019].
[431] Disponible en: http://www.cygazette.com/Gazette.dll/%7BA732F24B-2FD0-4D3D-884D-258C507E2509%7D/AppPgView?YssueMo=4670&PageNo=0&AppNo=1&PartNo=1&IssueDate=2/1/2013 [Fecha de consulta: 05/03/2019].
[432] Disponible en: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html [Fecha de consulta: 10/04/2019].
[433] Disponible en: https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf [Fecha de consulta: 10/04/2019].

Eslovaquia se adelantó, aprobando su nueva ley 18/2018[434] el 30 de enero de dicho año, no entrando en vigor hasta mayo. Estonia aprueba el 12 de diciembre de 2018 su nueva Ley[435], que no entra en vigor hasta enero de 2019. Finlandia aprueba el 5 de diciembre de 2018 la Ley de protección de datos (*Tietosuojalaki)*[436] que entra en vigor el 1 de enero de 2019.

En el caso de Hungría[437], se modificaron distintas leyes y aún se esperan modificaciones sectoriales a fin de armonizar la legislación húngara al nuevo RGPD; en todo caso, la Ley que adaptó la legislación húngara a dicho Reglamento, entró en vigor el 26 de julio de 2018.

Irlanda aprobó la *Data Protection Act* en 2018 (a través de la Ley número 7 de 2018)[438]. Italia armonizó su marco normativo con el Decreto legislativo 101/2018, que entró en vigor el 19 de septiembre de 2018[439].

Tanto Letonia[440] como Lituania[441] aprobaron sus nuevas leyes de protección de datos, reemplazando las antiguas, entrando en vigor las nuevas en julio de 2018.

En el caso de Luxemburgo[442] se aprobaron dos leyes el 1 de agosto de 2018 para incorporar el RGPD y se realizaron varias enmiendas a leyes a fin de incorporar o adaptar la normativa nacional a la legislación europea.

Malta reemplazó su antigua ley por una nueva que entró en vigor el 28 de mayo de 2018[443]. Los países bajos tenían una ley de protección de datos que ya se adaptaba en

---

[434] Disponible en: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/2018/20180525 y https://www.dataprotection.gov.sk/uoou/sites/default/files/kcfinder/files/Act_122-2013_84-2014_en.pdf [Fecha de consulta: 17/02/2019].
[435] Disponible en: https://www.riigiteataja.ee/akt/104012019011 [Fecha de consulta: 20/03/2019].
[436] Disponible en: https://www.finlex.fi/fi/laki/alkup/2018/20181050 [Fecha de consulta: 05/03/2019].
[437] Disponible en: http://www.parlament.hu/irom41/00335/00335.pdf [Fecha de consulta: 03/02/2019].
[438] Disponible en: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html [Fecha de consulta: 10/02/2019].
[439] Disponible en: https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg [Fecha de consulta: 10/02/2019].
[440] Disponible en: https://likumi.lv/ta/id/300099-fizisko-personu-datu-apstrades-likums [Fecha de consulta: 15/03/2019].
[441] Disponible en: https://e-seimas.lrs.lt/portal/legalAct/It/TAP/952a77b0709011e8a76a9c274644efa9 [Fecha de consulta: 15/03/2019].
[442] Disponible en: http://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a686/jo [Fecha de consulta: 20/02/2019].

casi todos sus términos al nuevo RGPD, por lo que las autoridades decidieron para armonizar y mejorar la legislación promulgar la ley holandesa (*Uitvoeringswet AVG)*[444]; Polonia publicó dos proyectos de ley en septiembre de 2017: uno sobre la Ley de Protección de Datos personales y otro sobre la implementación de la protección de datos, cuya finalidad es modificar todo el conjunto de leyes de carácter sectorial. La primera ley fue aprobada el 10 de mayo y entró en vigor el 25 de mayo de 2018, mientras que la segunda se está debatiendo en estos meses de 2019[445].

Rumanía promulgó la Ley 190/2018 que entró en vigor el 31 de julio de 2018[446].
Suecia aprobó su Ley en 2018, entrando en vigor el 25 de mayo[447].

Reino Unido aprobó la Data Protection Act que entró en vigor el 25 de mayo de 2018.[448]

La República Checa[449] aún sigue debatiendo en su Cámara la Data Protection Act y lo mismo ocurre con Eslovenia[450] y con Grecia[451].

Uno de los países, entre otros, que no se ha adaptado es Portugal, siguiendo actualmente en debate la propuesta de ley 120/XII; sigue en vigor, entonces, la Ley de protección de datos personales 67/98 de 26 de octubre.

---

443 Disponible en: http://www.justicesservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29098&1=1 [Fecha de consulta: 03/02/2019]

444 Disponible en: https://zoek.officielebekendmakingen.nl/stb-2018-144.html [Fecha de consulta: 10/04/2019].

445 Disponible en: https://uodo.gov.pl/data/filemanager_pl/757.pdf [Fecha de consulta: 12/02/2019].

446 Disponible en: https://iapp.org/media/pdf/resource_center/Romanian_Data_Protection_Law_English_Translation.pdf y https://www.senat.ro/legis/PDF/2018/18L294FP.pdf [Fecha de consulta: 12/02/2019].

447 Disponible en: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling-lag-2018218-med-kompletterande-bestammelser_sfs-2018-218 [Fecha de consulta: 11/03/2019].

448 Disponible en: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [Fecha de consulta: 12/02/2019].

449 Disponible en: http://www.psp.cz/sqw/historie.sqw?t=138&o=8 [Fecha de consulta: 11/03/2019].

450 Disponible en: http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/mp.gov.si/novice/2018/ZVOP-2_NG_2_apr.pdf [Fecha de consulta: 20/02/2019]

451 Disponible en: http://www.opengov.gr/ministryofjustice/wp-content/uploads-downloads/2018/02/sxedio_nomou_prostasia_pd.pdf [Fecha de consulta: 20/02/2019].

Capítulo III. Algunos ámbitos públicos de aplicación de los sistemas biométricos: la identificación de los individuos por las Administraciones Públicas.

Podrá observarse que van a quedar reflejados solo algunos ámbitos de aplicación, a título de ejemplo, de los sistemas dactiloscópicos, no siendo nuestra intención abarcar tan amplio campo de trabajo. Esta última parte se ha incluido con la intención de mostrar la aplicación de estos sistemas, a través de algunos ejemplos. Sin duda, podrá ser objeto de una interesante investigación posterior.

Antes de adentrarnos en la breve referencia a algunos ámbitos públicos de aplicación de los sistemas biométricos, consideramos de interés hacer referencia a la identificación de los individuos en la legislación nacional. Así la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas[452], en su Capítulo II referente a la Identificación y firma de los interesados en el procedimiento administrativo, establece en el artículo 9 "Sistemas de identificación de los interesados en el procedimiento" los siguiente:

> "1. Las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente.
> 2. Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad. En particular, serán admitidos, los sistemas siguientes:
> a) Sistemas basados en certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación». A estos efectos, se entienden comprendidos entre los citados certificados electrónicos reconocidos o cualificados los de persona jurídica y de entidad sin personalidad jurídica.

[452] BOE 236/2015, de 2 de octubre de 2015 Ref Boletín: 15/10565.

b) Sistemas basados en certificados electrónicos reconocidos o cualificados de sello electrónico expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».

c) Sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan.

Cada Administración Pública podrá determinar si sólo admite alguno de estos sistemas para realizar determinados trámites o procedimientos, si bien la admisión de alguno de los sistemas de identificación previstos en la letra c) conllevará la admisión de todos los previstos en las letras a) y b) anteriores para ese trámite o procedimiento.

3. En todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo".

La propia Exposición de Motivos de la L 39/2015 EDL 2015/166690 considera que esta es «una de las novedades más importantes». Identificación y firma difieren fundamentalmente en cuanto a su uso en el procedimiento administrativo. En este sentido, la identificación es suficiente, «con carácter general», para realizar cualquier actuación prevista en el ordenamiento jurídico (art.11.1 EDL 2015/166690). La firma, en cambio, debe ser obligatoriamente exigida por las Administraciones Públicas a los interesados para que estos puedan formular solicitudes, presentar declaraciones responsables o comunicaciones, interponer recursos, desistir de acciones y renunciar a derechos (art.11.2 EDL 2015/166690). Por otra parte, la firma absorbe la identificación, como se deriva de la disposición contenida en el art.10.4 L 39/2015 EDL 2015/166690, según la cual: «Cuando los interesados utilicen un sistema de firma de los previstos en este artículo, su identidad se entenderá ya acreditada mediante el propio acto de la firma».

Respecto a la identificación, si el art.9.1 L 39/2015 EDL 2015/166690 impone a las Administraciones Públicas la obligación de verificar la identidad de los interesados en el procedimiento administrativo, el art.9.2 EDL 2015/166690 reconoce a estos el

derecho a identificarse electrónicamente «a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad».

En cuanto a la firma, el art.10.1 L 39/2015 EDL 2015/166690 establece que los interesados «podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento». Cabe destacar, que la L 39/2015, en su art.10.2 EDL 2015/166690, hace una referencia equívoca al «caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos» pues lo cierto es que no a todos los interesados, como hemos visto, les es dado optar a relacionarse de tal modo.

Especial mención merece el art.12.1 L 39/2015 EDL 2015/166690, en cuanto reconoce que las Administraciones Públicas «deberán garantizar que los interesados pueden relacionarse con la Administración a través de medios electrónicos, para lo que pondrán a su disposición los canales de acceso que sean necesarios, así como los sistemas y aplicaciones que en cada caso se determinen». Tal garantía parece que trasciende la regulación específica de la identificación y firma, por lo que no se acaba de entender muy bien su ubicación sistemática. Lo mismo sucede con el deber instrumental del anterior, el deber de asistencia en el uso de los medios electrónicos a los interesados, que se reconoce en el apartado siguiente. A este respecto, destacar que la asistencia se limita a «los interesados no incluidos en los apartados 2 y 3 del art.14 EDL 2015/166690 que así lo soliciten», en abierta contradicción con el derecho del mismo contenido que se reconoce, con carácter general, a las personas en el art. 13.b) de la Ley 39/2015 EDL 2015/166690. Por último, una especificación adicional de este deber de asistencia se contiene en el art.13.2 EDL 2015/166690, segundo párrafo, respecto de los interesados que no dispongan de medios electrónicos y que se concreta en que su identificación y firma por medios electrónicos «podrá ser válidamente realizada por un funcionario público mediante el uso del sistema de firma electrónica del que esté dotado para ello»[453].

[453] VILLAFÁÑEZ GALLEGO, R., "Los medios electrónicos en la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones Públicas", en *ELDERECHO.COM*, Lefevure, 8 de junio de 2016, disponible en: https://elderecho.com/los-medios-electronicos-en-la-ley-392015-de-1-de-octubre-del-procedimiento-administrativo-comun-de-las-administraciones-publicas [Fecha de consulta: 10/03/2019].

1. Los datos biométricos dactiloscópicos recabados y almacenados con fines públicos de control fronterizo.

La armonización a nivel internacional de la normativa sobre protección de datos de carácter personal se ha basado en tres pilares fundamentales: las líneas directrices de la OCDE, el Convenio 108 y la Directiva 95/46/CE, hasta la aprobación en 2016 del RGPD. Es ahora sobre la base del nuevo RGPD sobre la que habrá de sustentarse la protección jurídica al dato biométrico dactiloscópico, dado que es un dato de carácter personal.

1.1. Servicios públicos. Seguridad pública. El Sistema EURODAC.

En este epígrafe se hará referencia a aquellas bases de datos que contienen impresiones dactiloscópicas de gran interés para el presente estudio y otros posteriores.

1.1.1. Cuestiones previas.

Estas cuestiones giran en relación a la aplicabilidad de la normativa sobre protección de datos. Incorporamos en este punto del trabajo unas pinceladas en relación con las aplicaciones prácticas del tratamiento de los datos biométricos en el control de la seguridad pública. Así en este sentido mencionaremos ahora en primer lugar el Sistema Eurodac, al ser cronológicamente el primero en desarrollarse, para después mencionar el Sistema de Información sobre los Visados (VIS) y el nuevo *Umbrella Agreement* de control de la delincuencia internacional.

Desde el punto de vista de la protección de datos, resulta de interés analizar el funcionamiento del sistema Eurodac al incorporar una base de datos central con impresiones dactiloscópicas, a las que no dudamos en considerar datos biométricos[454].

[454] En este sentido la Agencia Española de Protección de Datos en informe de 28 de febrero de 2006 señaló: "Son datos biométricos aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión. Así se emplean para tales fines las huellas digitales, el iris del ojo, la voz, etc."

Creemos que es útil recordar aquí el concepto de fichero, recogido tanto en la Directiva europea como en nuestra legislación interna, como fundamentador de la aplicación del régimen jurídico específico de la protección de datos.

La mencionada base de datos central del sistema Eurodac sin duda podía encuadrarse dentro del concepto de fichero del art. 5 RDLOPD donde se definía como "Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".

Como es lógico, esta definición está en consonancia con la recogida en el artículo 2. Definiciones, de la Directiva 94/46/CE que establecía: "A efectos de la presente Directiva, se entenderá por:
(…)
c) «fichero de datos personales» («fichero»): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;
(…)".

No obstante, hay que tener en cuenta que de acuerdo con el artículo 3 de la Directiva, ésta se aplicaba a todo tratamiento automatizado de datos personales, estén o no contenidos en ficheros. Y siguiendo en este punto a Heredero Higueras[455], en relación con el tratamiento no automatizado, la Directiva se aplicaba sólo si los datos están contenidos en un fichero. Por tanto, el tratamiento no automatizado de datos que no están incorporados a ficheros, sino que consten en expedientes o carpetas, no es objeto de la Directiva.

Efectivamente, un tratamiento de datos no automatizado, y no encontrándose incorporados los datos a un fichero, está fuera del ámbito de la Directiva. Y en el mismo sentido, el elemento determinante para identificar un fichero sometido a la legislación sobre protección de datos, o un tratamiento no automatizado sometido a dicha legislación, reside en que se trate de información estructurada en la que resulte posible

[455] Cfr. HEREDERO HIGUERAS, M., op. cit., p. 85.

recuperar los registros relativos a un individuo determinado[456]. En definitiva, el concepto de fichero se revela como fundamentador de la aplicación de la legislación de protección de datos.

Pero en relación con el sistema Eurodac es importante tener en cuenta que puede existir un mismo fichero en distintos ordenadores. En este sentido, el Informe 368/2003 de la AEPD dice: «de lo establecido en la Directiva y en la propia Ley Orgánica parece desprenderse que el concepto de fichero no va directamente vinculado a la exigencia de que el mismo se encuentre en una única ubicación, sino que será posible la existencia de ficheros distribuidos en lugares geográficos remotos entre sí, siempre y cuando la organización y sistematización de los datos responda a una conjunto organizado y uniformado de datos, sometido a algún tipo de gestión centralizada.».

El GPD 29, en su Dictamen 3/2012, llama la atención sobre lo que denomina sistemas automáticos de identificación dactilar (SAID) utilizados con fines policiales destacando a nivel de la UE el sistema Eurodac y el Sistema de Información de Visados. Estos sistemas avanzados a gran escala (almacenan cerca de 70 millones de impresiones dactilares) plantean en su utilización importanes cuestiones jurídicas que han de resolverse en muchos casos teniendo en cuenta la necesidad de garantizar la proporcionalidad[457].

---

[456] En este sentido, es muy ilustrativa la Sentencia de la Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 16 de febrero de 2006 que establece: «Todo fichero de datos exige para tener esta consideración una estructura u organización con arreglo a criterios determinados. El mero acúmulo de datos sin criterio alguno no podrá tener la consideración de fichero a los efectos de la ley.
(…)
Es claro para este Tribunal que registro en soporte físico equivale a fichero en los términos de la ley. Basta la lectura completa de este artículo 2 y su comparación con el art. 3 de la Directiva del que trae causa, y que sirve para interpretarlo, para llegar a esa conclusión.
Pues bien, para que una actuación manual sobre datos personales (recogida, grabación, conservación, elaboración, modificación, bloqueo...) tenga la consideración de "tratamiento de datos personales" sujeto al sistema de protección de la Ley Orgánica 15/1999 es necesario que dichos datos estén contenidos o destinados a ser incluidos en un fichero, esto es, en un conjunto estructurado u organizados de datos con arreglo a criterios determinados. Si no es así, el tratamiento manual de datos personales quedará fuera del ámbito de aplicación de la ley, no será un "tratamiento de datos personales" según el concepto normativo que la ley proporciona.
En realidad, la existencia del "fichero" en el sentido legal es siempre precisa para que un tratamiento de datos personales esté sujeto al sistema de protección de la ley. En los casos de tratamiento automatizado de datos -siempre sometidos a la ley- es difícil imaginar la inexistencia de un fichero (aunque no se exija expresamente) puesto que los datos que se tratan mediante sistemas automatizados lo son siempre bajo unos criterios de estructura u organización previa.»
[457] GPD 29 Dictamen 3/2012, op. cit., p. 21.

1.1.2. Creación del sistema Eurodac[458].

Desde su creación en el año 2000, el sistema Eurodac, de comparación de impresiones dactilares de los solicitantes de asilo y extranjeros interceptados en el cruce irregular de una frontera exterior de la Comunidad Europea, ha planteado y plantea múltiples cuestiones prácticas entorno a la protección jurídica del dato biométrico de la huella de un individuo. Este sistema se inscribe en el ámbito del Derecho de asilo en la Unión Europea y se circunscribe al desarrollo del Convenio de Dublín de 1990[459]. En definitiva, Eurodac ayuda a los Estados miembros de la UE a determinar el país responsable de examinar una solicitud de asilo mediante la comparación de juegos de impresiones dactilares. Actualmente es el Reglamento (UE) No 603/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, el que regula este sistema. Fue publicado el 29 de junio de 2013 y es aplicable desde el 20 de julio de 2015 deroga el Reglamento 407/2002, de 28 de febrero (Ref. DOUE-L-2002-80409) y el Reglamento 2725/2000, de 11 de diciembre (Ref. DOUE-L-2000-82443). Así mismo, modifica el Reglamento 1077/2011, de 25 de octubre (Ref. DOUE-L-2011-82210).

La creación del sistema "Eurodac" para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín se efectuó por Reglamento (CE) Nº

[458] Reglamento (CE) Nº 2725/2000 del Consejo de 11 de diciembre de 2000, relativo a la creación del sistema "Eurodac" para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín. Reglamento (UE) No 603/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) no 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) no 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia (refundición). https://www.boe.es/buscar/doc.php?id=DOUE-L-2013-81287 [Fecha de consulta: 5 de julio de 2018].

[459] El Convenio de Dublín firmado por los Estados miembros de la UE tiene como finalidad la determinación del Estado responsable del examen de las solicitudes de asilo presentadas en los Estados comunitarios. Diario Oficial nº C254 de 19/08/1997. No obstante, hay que tener en cuenta que el Convenio de Dublín ha sido sustituido por el Reglamento 343/2003 del Consejo que en su Considerando 19 dice: "El Convenio de Dublín continúa vigente y aplicable entre Dinamarca y los Estados miembros vinculados por el presente Reglamento hasta tanto se celebre un acuerdo que permita la participación de Dinamarca en el presente Reglamento". Este Reglamento entró en vigor en marzo de 2003 y conforme con lo dispuesto en su artículo 29 "Será aplicable a las solicitudes de asilo presentadas a partir del primer día del sexto mes siguiente a su entrada en vigor y, desde esa fecha, se aplicará a toda petición de asunción de responsabilidad o de readmisión de solicitantes de asilo, sea cual sea la fecha en que haya sido cursada la petición. La determinación del Estado miembro responsable del examen de una solicitud de asilo presentada antes de dicha fecha se efectuará de conformidad con los criterios enunciados en el Convenio de Dublín".

2725/2000 del Consejo de 11 de diciembre de 2000. Hay que tener en cuenta, así mismo, el Reglamento (CE) 343/2003, de 18 de febrero[460], que establece los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de asilo presentada en uno de los Estados miembros por un nacional de un tercer país, y que sustituye al Convenio de Dublín.

El Reglamento 2725/2000 creó por primera vez en la Unión Europea un sistema automatizado común de identificación de la huella digital (AFIS), por ello dada su trascendencia pasamos a analizar la estructura del citado Reglamento.

Debemos partir del hecho que los Estados miembros, con anterioridad, en concreto, el 15 de junio de 1990, firmaron en Dublín el Convenio relativo a la determinación del Estado responsable del examen de las solicitudes de asilo presentadas en los Estados miembros de la Comunidades Europeas.

Para poder aplicar el citado convenio de Dublín es necesario determinar la identidad del solicitante de asilo o de las personas interceptadas en un cruce irregular de las fronteras exteriores de la Comunidad. En este punto se revela como de gran utilidad la tecnología de impresiones dactilares. También es necesario comprobar si los extranjeros ilegalmente presentes en territorio de la Comunidad han solicitado asilo en otro Estado miembro.

Por tanto, eran dos las aplicaciones prácticas perseguidas por las disposiciones del Reglamento 2725/2000, partiendo de la identificación del solicitante de asilo saber si es la primera vez que formula una solicitud o si por el contrario ya ha solicitado con anterioridad asilo en un Estado miembro. Ahora el Reglamento UE 603/2013 dentro de su Capítulo I artículo 1.1 recoge, en el mismo sentido, como doble finalidad de "Eurodac" "[…] ayudar a determinar el Estado miembro responsable, con arreglo al Reglamento (UE) nº 604/2013[461] del examen de las solicitudes de protección

[460] DOL 25 febrero 2003, núm. 50, [pág. 1, Núm. Págs. 10].

[461] Reglamento (UE) Nº 604/2013 del Parlamento Europeo y del Consejo de 26 de junio de 2013 por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida (Texto refundido). DOUE 29 de junio de 2013. L180/31-59. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013R0604&from=ES [Fecha de consulta: 9 de julio de 2018].

internacional presentadas en los Estados miembros por un nacional de un tercer país o un apátrida y, además, facilitar la aplicación del Reglamento (UE) nº 604/2013 en las condiciones establecidas en el presente Reglamento".

Sobre la base de que las impresiones dactilares son un elemento importante para determinar la identidad exacta de una persona, es necesario crear un sistema para comparar los datos dactiloscópicos de aquéllas.

Con este objetivo se creó Eurodac, sistema con una Unidad Central establecida en la Comisión que gestiona una base central informatizada de datos dactiloscópicos y, de este modo, gestiona los medios electrónicos de transmisión entre los Estados miembros y la base de datos central.

Para la puesta en funcionamiento de este sistema es necesario partir de la recogida de datos, es decir, recoger las impresiones dactilares de los mayores de 14 años solicitantes de asilo y de los extranjeros interceptados en el cruce irregular de una frontera exterior de un Estado miembro.

Se pueden así distinguir las siguientes fases en el tratamiento de los datos en el sistema Eurodac: 1. Recogida de los datos dactiloscópicos. 2. Transmisión de los datos a la unidad central. 3. Registro de los datos en la unidad. 4. Conservación en la unidad central. 5. Comparación de datos en la unidad. 6. Transmisión de los datos resultado de la comparación a los Estados miembros. 7. Bloqueo y supresión de los datos registrados.

El Reglamento 2725/2000 establecía un reparto de responsabilidades entre la Comisión y los Estados miembros, siendo aquélla responsable de la unidad central y éstos respecto al uso y seguridad de los datos. Los Estados miembros garantizarán la seguridad en el acceso a los datos registrados y su corrección, en definitiva, la calidad del dato.

Junto a este reparto de responsabilidades, que cabría calificar de contractual, se establecía una responsabilidad extracontractual de la Comunidad en relación con el funcionamiento del sistema Eurodac. Pero también se establecen normas específicas de responsabilidad extracontractual de los Estados miembros en relación con el funcionamiento del sistema.

La creación de este sistema a nivel comunitario en aplicación del principio de subsidiariedad recogido en el artículo 5 del Tratado constitutivo de la Comunidad Europea[462] es legítimo al no poder los Estados miembros lograr el objetivo de forma aislada. La comparación de impresiones dactilares a los efectos de aplicación de la política de asilo comunitaria no puede realmente llevarse a efecto sino es con una comparación centralizada de dichas impresiones recogidas en los distintos Estados. Por ello, tanto el principio de subsidiariedad como el de proporcionalidad aconsejan la adopción del sistema.

Como hemos destacado con anterioridad, los Estados miembros tienen en el sistema un ámbito de responsabilidad muy específico ya que son los únicos responsables de la identificación y clasificación de los resultados de las comparaciones que les ha transmitido la Unidad Central. Por tanto, como decíamos son los Estados responsables del uso y de la seguridad de los datos personales.

El Estado miembro recoge la impresión dactilar, la envía a la Unidad Central, ésta remite al Estado miembro el resultado de la comparación y el Estado debe clasificarla y en su caso proceder al bloqueo de los datos de personas admitidas y consideradas como refugiados.

Por tanto, las competencias encomendadas a los Estados miembros en materia de protección de datos son de relevancia puesto que pueden afectar al ejercicio de libertades individuales y es, por ello, que el Consejo se reserva determinadas competencias de ejecución en relación a la adopción de medidas que garanticen la seguridad y fiabilidad de tales datos. La Directiva 95/46/CE era aplicable al tratamiento de datos personales por los Estados miembros en el marco del sistema Eurodac. Pero además, en virtud del artículo 286 del Tratado[463], la Directiva de protección de datos se aplicaba también a las instituciones y organismos comunitarios.

---

[462] Versión Consolidada del Tratado Constitutivo de la Comunidad Europea. 24.12.2002 ES Diario Oficial de las Comunidades Europeas C 325/41. Artículo 5: La Comunidad actuará dentro de los límites de las competencias que le atribuye el presente Tratado y de los objetivos que éste le asigna.
En los ámbitos que no sean de su competencia exclusiva, la Comunidad intervendrá, conforme al principio de subsidiariedad, sólo en la medida en que los objetivos de la acción pretendida no puedan ser alcanzados de manera suficiente por los Estados miembros, y, por consiguiente, puedan lograrse mejor, debido a la dimensión o a los efectos de la acción contemplada, a nivel comunitario. Ninguna acción de la Comunidad excederá de lo necesario para alcanzar los objetivos del presente Tratado.

[463] Artículo 286: 1. A partir del 1 de enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de

1.1.3. Estructura del Reglamento (CE) Nº 2725/2000.

El Reglamento estaba estructurado en VII capítulos y consta de 27 artículos. En el capítulo I se recogen las disposiciones generales informadoras del resto del articulado. El capítulo II está dedicado a los solicitantes de asilo. El capítulo III a los extranjeros interceptados con ocasión del cruce irregular de una frontera exterior. El capítulo IV regula la situación jurídica de los extranjeros presentes ilegalmente en un Estado miembro. El capítulo V se dedica a los refugiados reconocidos. Y el capítulo VI se centra en la materia de mayor interés para nosotros al tratar la utilización de los datos, protección de los datos, seguridad y responsabilidad, abarcando los artículos 13 a 20. El VII y último capítulo recoge las disposiciones finales.

1.1.4. Finalidad de Eurodac.

Entre las disposiciones generales del Reglamento se encuentra la determinación de la finalidad del sistema. La determinación clara de la finalidad del sistema es una condición general para evaluar la licitud del tratamiento de datos personales[464].

---

aplicación a las instituciones y organismos establecidos por el presente Tratado o sobre la base del mismo.
2. Con anterioridad a la fecha indicada en el apartado 1, el Consejo establecerá, con arreglo al procedimiento previsto en el artículo 251, un organismo de vigilancia independiente, responsable de controlar la aplicación de dichos actos comunitarios a las instituciones y organismos de la Comunidad y adoptará, en su caso, cualesquiera otras disposiciones pertinentes. 24.12.2002 ES Diario Oficial de las Comunidades Europeas C 325/41.

[464] No debemos olvidar que la Directiva 95/46/CE, en relación con los principios relativos a la calidad de los datos, establecía, en su artículo 6: "1. Los Estados dispondrán que los datos personales sean: … b) recogidos con fines determinados, explícitos y legítimos y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas; c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente; d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados; e) conservados en una forma que permita la identificación del interesado durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos." Por tanto, la finalidad del tratamiento determina no solo la licitud de la recogida de datos, sino también, el tratamiento posterior y las condiciones del mantenimiento de los mismos. El principio de finalidad recogido en este artículo ha experimentado una evolución partiendo de las leyes de primera generación de los años 70. En un principio, se entendía por finalidad la ilicitud de usar para una finalidad distinta los datos recogidos para una finalidad determinada. De hecho, la ley de Francia, de 1978, y la de Luxemburgo, de 1979, tipificaron un delito de desviación de finalidad. Posteriormente el Convenio 108 cambió la concepción de este

Así pues, la finalidad de Eurodac es doble: por una parte, ayudar a determinar el Estado miembro responsable, con arreglo al convenio de Dublín, del examen de las solicitudes de asilo presentadas en los Estados miembros. Y, por otra parte, facilitar la aplicación del Convenio de Dublín.

Para cumplir estos fines Eurodac tiene la siguiente estructura: una Unidad Central y una base de datos central informatizada. A continuación, veremos cómo esta finalidad se ha visto ampliada con el nuevo Reglamento (UE) nº 603/2013.

1.1.5. El nuevo Reglamento Eurodac.

El nuevo Reglamento (UE) n° 603/2013 del Parlamento Europeo y del Consejo, para la aplicación efectiva del Reglamento (UE) n° 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) n° 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, aplicable desde el 20 de Julio de 2015, mejora el funcionamiento regular de Eurodac ya que fija nuevos plazos para la transmisión de datos sobre impresiones dactilares. También es destacable la reducción del tiempo transcurrido entre la toma de las impresiones y su envío a la Unidad Central de Eurodac. Y, por último, y no por ello menos relevante, el nuevo Reglamento asegura la total compatibilidad con la legislación más reciente en materia de asilo[465] y se ajusta mejor a los requisitos de protección de datos.

---

principio de finalidad considerando ilícito el uso posterior de los datos de manera incompatible con dichos fines. Cfr. HEREDERO HIGUERAS, M., op. cit., pp. 103 y ss.

[465] Directiva 2013/32/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre procedimientos comunes para la concesión o la retirada de la protección internacional (refundición) (aplicable desde el 21 de julio de 2015).

Directiva 2013/33/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por la que se aprueban normas para la acogida de los solicitantes de protección internacional (refundición) (aplicable desde el 21 de julio de 2015).

Directiva 2011/95/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, por la que se establecen normas relativas a los requisitos para el reconocimiento de nacionales de terceros países o apátridas como beneficiarios de protección internacional, a un estatuto uniforme para los refugiados o

Lo más relevante de este nuevo Reglamento es la ampliación de los usos legítimos del sistema. "Hasta la entrada en vigor del nuevo Reglamento la base de datos Eurodac solo podía utilizarse con fines de asilo. El nuevo Reglamento permite ahora que las fuerzas de policía nacionales y Europol comparen las impresiones dactilares vinculadas a investigaciones criminales con las contenidas en Eurodac. Ese ejercicio se llevará a cabo en circunstancias estrictamente controladas y únicamente con fines de prevención, detección e investigación de delitos graves y terrorismo. – Las salvaguardias específicas incluyen el requisito de comprobar en primer lugar todas las bases de datos de antecedentes penales existentes y el de limitar las búsquedas a los delitos más graves, como el asesinato y el terrorismo. – Además, antes de hacer una comprobación en Eurodac, los cuerpos de seguridad deben llevar a cabo una comparación de las impresiones dactilares con las del Sistema de Información de Visados (cuando esté permitido). – Los controles policiales no se harán con carácter sistemático, sino como último recurso y cuando se cumplan todas las condiciones de acceso. – Los datos recibidos de Eurodac no pueden, bajo ningún concepto, compartirse con terceros países" [466]. Efectivamente, como bien expone el Considerando (11) del vigente Reglamento "[…] Europol desempeña un papel clave para la cooperación entre los Estados miembros en el ámbito de la investigación penal transfronteriza en apoyo de la prevención, el análisis y la investigación de la delincuencia en toda la Unión. […]". El ámbito de aplicación del sistema ha experimentado un notable avance expansivo llevado de la mano de la capacidad de indentificación de personas que conlleva las huellas dactilares. En definitiva, no se puede obviar toda la capacidad histórica de lucha contra el crimen y la delincuencia que estos datos dactiloscópicos proporcionan. Así, el Considerando (14) continúa reconociendo que, aunque en un principio no fuera la finalidad de Eurodac, es evidente que la comparación de datos entre la huella latente encontrada en el escenario de un crimen y la base central es un mecanismo "[…] fundamental en el campo de la cooperación policial. La posibilidad de comparar una

---

para las personas con derecho a protección subsidiaria y al contenido de la protección concedida (refundición) (aplicable desde el 21 de diciembre de 2013).
Reglamento (UE) n° 604/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida(refundición). (Nuevo Reglamento de Dublín, aplicable desde el 1 de enero de 2014).

[466] Comisión Europea. *Un Sistema Europeo Común de Asilo*. Oficina de publicaciones de la Unión Europea 2014. http://ec.europa.eu/dgs/home-affairs/e-library/docs/ceas-fact-sheets/ceas_factsheet_es.pdf [Fecha de consulta: 11/05/2016].

impresión dactilar latente con los datos dactiloscópicos que se conservan en Eurodac, en los casos en que existan motivos razonables para creer que el autor del delito o la víctima pueden pertenecer a alguna de las categorías contempladas en el presente Reglamento, dotará a las autoridades designadas de los Estados miembros de un instrumento muy valioso a la hora de prevenir, detectar o investigar los delitos de terrorismo u otros delitos graves, cuando, por ejemplo, la única prueba disponible en la escena de un delito sean impresiones dactilares latentes". Esta comparación entre huella latente y base central tiene su limitación, que el Consierando (32) recoge al decir que sólo se debe permitir el acceso si la comparación con las bases de datos nacionales y con los sistemas automatizados de identificación dactiloscópica de todos los demás Estados miembros en virtud de la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza[467], no haya permitido establecer la identidad del sujeto de los datos.

1.1.5.1. Definición.

Los datos dactiloscópicos para el Reglamento son conforme los define su artículo 2.1.l) "los datos relativos a las impresiones dactilares de todos los dedos o, al menos, de los dedos índices, y si éstos faltan, las impresiones de todos los restantes dedos de una persona, o una huella dactilar latente". No se recoge a lo largo del Reglamento una especial protección en relación con personas que les falten los dedos índices que consideramos merecedoras de un mayor nivel de protección ya que esa falta de dedos índices las hace más vulnerables al ser más fácil su identificación. No olvidemos ue cualquier ellemto diferenciador en el dactilograma de un individuo lejos de dificultar su identificación lo que provoca es una mayor facilidad y, por ende, vulnerabilidad de la privacidad de dicho sujeto.

1.1.5.2. Arquitectura y legalidad del sistema.

Sigue existiendo una base central informatizada de datos dactiloscópicos, el denominado Sistema Central, y una infraestructura de comunicación entre el Sistema

[467] DO L 210 de 6.8.2008, p. 1.

Central y los Estados miembros que es una red virtual cifrada. Cada Estado miembro dispone de un único punto de acceso nacional. Ya el GPD 29 advirtió, en su documento de trabajo (WP80) de 2003 y en su Dictámen 3/2012 (WP193), del riesgo que conlleva la utilización de datos biométricos para fines de identificación en grandes bases de datos centralizadas ante los potenciales riesgos para los individuos afectados. El Grupo de Trabajo advierte del importante impacto en la dignidad humana de los interesados y las implicaciones en cuestión de derechos fundamentales de este tipo de sistemas centralizados. Y así el Reglamento, siguiendo al Grupo de Trabajo, tiene en cuenta el Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales y de la jurisprudencia del TEDH sobre el artículo 8 de Convenio. Y así se concluye "que cualquier interferencia con el derecho a la protección de datos solo podrá autorizarse si es conforme a la ley y si es necesaria, en una sociedad democrática, para proteger un interés público importante[468]".

1.1.5.3. Regímenes aplicables y protección de datos.

En los capítulos II, III y IV se establecen distintos regímenes dependiendo de si el solicitante lo es de protección internacional exclusivamente (C. II); si se trata de nacionales de terceros países o apátridas interceptados con ocasión del cruce irregular de una frontera irregular (C. III); o bien nacionales de terceros países o apátridas que se encuentran ilegalemente en un Estado miembro (C. IV). Por último, hay un régimen especial para personas que gozan de protección internacional (C. V).

En cualquiera de los regímenes, las normas de tratamiento y protección de datos se establecen en el Capítulo VII, estableciendo el artículo 23 que cada Estado miembro de origen responde: de la legalidad de la toma de las impresiones dactilares, de la legalidad de la transmisión al Sistema Central, de la exactitud y actualidad de los datos cuando se transmitan al Sistema Central, de la legalidad del registro, conservación, rectificación y supresión en el Sistema Central y de la legalidad en el tratamiento de los resultados de comparación de los datos dactiloscópicos transmitidos por el Sistema. Y, todo ello,

[468] Dictamen 3/2012 sobre la evolución de las tecnologías biométricas. 00720/12/ES WP193, adoptado el 27 de abril de 2012, p. 9.

sobre la base del mencionado interés público necesitado de protección que el TJUE ha puesto de manifiesto en reiterada jurisprudencia[469].

Se establece en el artículo 35 una prohibición de transferencia de datos a terceros países, organismos internacionales o particulares respecto de los datos personales obtenidos por un Estado miembro o Europol del Sistema Central Eurodac. Esta prohibición se entiende sin perjuicio del derecho de los Estados miembros a transferir dichos datos a los terceros países a los que se aplica el Reglamento (UE) n o 604/2013[470].

1.2. El Sistema de Información sobre los Visados (VIS). Control de la delincuencia internacional.

Partimos del Dictamen 10/2011 del GPD 29, WP 181, relativo a la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para prevención, detección, investigación y enjuiciamiento de los delitos terroristas y delitos graves[471], adoptado el 5 de abril de 2011.

De acuerdo con la propuesta, se recogerá una enorme cantidad de datos personales sobre todos los pasajeros que vuelen hacia o desde la UE, se trate o no de sospechosos. La recogida y el tratamiento de datos PNR en la lucha contra el terrorismo y la delincuencia grave no deben posibilitar el rastreo y la vigilancia de todos los viajeros. El

[469] Sentencia de 20 de mayo de 2003 en los asuntos acumulados C-465/00, C-138/01 y C-139/01 (Rechnungshof contra Österreichischer Rundfunk y otros), TEDH, sentencia de 4 de diciembre de 2008, nº 30562/04 y 30566/04 (S. y *Marper* contra Reino Unido) y sentencia de 19 de julio de 2011, nº 30089/04, 14449/06, 24968/07, 13870/08, 36363/08, 23499/09, 43852/09 y 64027/09 (*Goggins* y otros contra Reino Unido). Los demandantes reclamaban por la recolección y mantenimiento de sus huellas dactilares, entre otros datos, tras haber sido objeto de una investigación criminal sin que diera lugar a un procedimiento judicial posterior y el Tribunal uniendo todas las demandas considera que esta materia debe ser considerada bajo el amparo del Artículo 8 del Convenio estimado dichas demandas y reconociendo una compensación económica en concepto de "*legal expenses*", por otra parte, previamente ofrecida por el Gobierno Británico. https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22goggins%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-105719%22]} [Fecha de consulta:10/07/2018].

[470] En este Reglamento 604/2013 se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida.

[471] Disponible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp181_es.pdf [Fecha de consulta: 02/06/2016].

Grupo de Trabajo lo considera desproporcionado y, por ello, estima que recoger y retener todos los datos de todos los viajeros de todos los vuelos no se ajusta al artículo 8 de la Carta de los Derechos Fundamentales." … "El Grupo de Trabajo desearía también recordar que, en algunos Estados miembros, métodos similares de control solo son constitucionales y consiguientemente viables para la policía con autorización judicial y en circunstancias específicas, como una amenaza específica. El sistema PNR propuesto convertiría esta excepcionalidad en un instrumento corriente del trabajo policial". … "Implantar medidas que no supongan protección de los derechos y libertades de los viajeros solo es algo proporcionado cuando se hace como recurso temporal ante una amenaza específica, lo que no es el caso de esta propuesta. En la lucha contra el terrorismo y la delincuencia grave, la invasión de la intimidad de los viajeros debe ser proporcional a los beneficios".

La entrada en funcionamiento del sistema VIS de toma de datos biométricos para las solicitudes de visados *Schegen* se produjo el 15 de mayo de 2014, según consta en Sentencia del TSJ de Madrid[472], que enjuicia hechos ocurridos en el Consulado General de España en la Habana.

Por último, y en lo que se refiere al control de la delincuencia internacional, podemos afirmar que, en este ámbito, destaca la Sentencia del TJUE en el Asunto *Digital Ireland* de 8 de abril de 2014, que ha traído, como consecuencia, la negociación y firma del denominado *Umbrella Agreement*[473] para dar refuerzo a la protección de los datos personales de los europeos en las transmisiones de estos datos a los EEUU para la investigación de delitos y lucha contra el crimen por las *Law Enforcement Agencies*.

1.3. El denominado *Umbrella Agreement*.

En relación con la protección de los datos de los europeos en su transmisión a efectos de la investigación de los delitos y lucha contra el crimen, es de necesaria referencia el

[472] Fundamento de Derecho Primero Sentencia nº 389/2015de 30 de septiembre de 2015 TSJ Madrid Sala de lo Contencioso Administrativo, sección 3ª, recurso 733/2014. Base de datos El Derecho EDJ 2015/190436.

[473] Decisión (UE) 2016/2220 del Consejo de 2 de diciembre de 2016 relativa a la celebración, en nombre de la Unión Europea, del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de los datos personales en relación con la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales. Este acuerdo entró en vigor en enero de 2017. http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D2220&from=ES [Fecha de consulta: 25/09/2017].

llamado *Umbrella Agreement.* La Decisión (UE) 2016/2220 del Consejo de 2 de diciembre de 2016 relativa a la celebración, en nombre de la Unión Europea, del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de los datos personales en relación con la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales, acuerdo que entró en vigor el 1 de febrero de 2017, ha supuesto un nuevo ámbito de cobertura reforzado en la transmisión de los datos personales de los europeos a los EEUU dentro de la investigación de delitos y lucha contra el crimen.

2. Breve referencia a la cooperación judicial e investigación penal transfronteriza mediante intercambio de perfiles de ADN.

El 27 de mayo de 2005, siete Estados miembros de la UE (Bélgica, Alemania, España, Francia, Luxemburgo, Países Bajos y Austria) firmaron el denominado "Tratado de Prüm" (el Tratado) con el fin de mejorar la cooperación judicial y las investigaciones penales transfronterizas a través del intercambio de información. En concreto, se prevé el intercambio entre las partes contratantes de perfiles de ADN y datos dactiloscópicos, entre otros datos personales, con el fin de luchar más eficazmente contra el terrorismo, la delincuencia transfronteriza y la inmigración ilegal. Entró en vigor en España el 1 de noviembre de 2006[474]. Por el Supervisor Europeo de Protección de Datos se ha mostrado disconformidad[475] con la aprobación de este Tratado fuera del marco institucional de la Unión Europea, lo que supone la falta de participación del Parlamento Europeo, si bien es cierto los Parlamentos nacionales sí han tenido posibilidad de valorar el Tratado.

[474] Instrumento de ratificación de España del Convenio relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, hecho en Prüm el 27 de mayo de 2005. https://www.boe.es/boe/dias/2006/12/25/pdfs/A45524-45534.pdf [Fecha de consulta: 31/07/2018].

[475] El Supervisor emitió su Dictamen que se publicó en el DOUE serie C 116, de 17.5.2006. En concreto: "El SEPD no aprueba el proceso que conduce a dicho Tratado, fuera del marco institucional de la Unión Europea, y por lo tanto sin participación sustantiva de la Comisión. Además, ello significa ausencia de control democrático por parte del Parlamento Europeo y ausencia de control judicial por parte del Tribunal de Justicia y como resultado de todo ello menos garantías de que se equilibren de igual modo todos los intereses (públicos). Ello incluye la perspectiva de la protección de datos (…). Las instituciones de la Unión Europea no tienen la oportunidad de valorar -antes de que se establezca el sistema- el impacto de las elecciones políticas en la protección de datos personales".

Como acertadamente pone de manifiesto Dietrich Plaza[476], todas las materias relacionadas con visados, asilo, inmigración, libre circulación de las personas pertenecen al primer pilar comunitario, y la lucha contra el terrorismo, tráfico de personas, Europol (entre otras materias) pertenecerían al denominado "tercer pilar". En consecuencia, el Tratado se adopta al margen de la UE, pero está estrechamente relacionado con la UE. Por esta razón, durante el Consejo de Justicia y Asuntos de Interior del 15 de febrero de 2007, se acordó integrar partes del Tratado de Prüm en el ordenamiento jurídico de la UE mediante una Decisión basada en el tercer pilar. La finalidad de la Decisión Prüm era intensificar y acelerar el intercambio de información entre autoridades de los Estados miembros. Además, hay que tener en cuenta que el programa de la Haya[477] fijaba el 1 de enero de 2008 como la fecha a partir de la cual el intercambio de datos se base en el principio de disponibilidad. Este principio de disponibilidad significa que un agente de un Estado miembro que necesite información para poder llevar a cabo su trabajo, podrá obtener esta información de otro Estado miembro (la información se «pondrá a disposición»). Este es un principio, como bien destacan Martínez y Poza, que proporciona un instrumento innovador de intercambio transfronterizo de información policial[478]. Indudablemente este principio necesitaba una traducción normativa y la misma la constituye, entre otras, el Tratado de Prüm. Tratado que se incorpora al marco jurídico comunitario a través de las Decisiones JAI/615/2008 y JAI/616/2008[479]. El Tratado dedica su capítulo II, entre otros, a los datos

[476] "El concepto de "pilares" se utiliza en el Tratado de la Unión Europea para definir la arquitectura de la Unión. En concreto el primer pilar comunitario corresponde a las tres comunidades (CEE, EURATOM y CECA), el segundo pilar corresponde a la política exterior y de seguridad común (PESC), regulada en el Título V del Tratado de la Unión Europea, y finalmente el tercer pilar, a la cooperación policial y judicial en materia penal (regulada en el Título VI de TUE)". DIETRICH PLAZA, C., *El Tratado de Prüm en el marco de la regulación de protección de datos personales en la Unión Europea.* https://www.ugr.es/~redce/REDCE7/articulos/03cristinadietrichplaza.htm [Fecha de consulta: 31/07/2018].

[477] El Programa de La Haya para la consolidación de la libertad, la seguridad y la justicia en la Unión Europea, aprobado por el Consejo Europeo el 5 de noviembre de 2004. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=LEGISSUM:l16002&from=ES [Fecha de consulta: 30/07/2018].

[478] MARTÍNEZ PÉREZ, F. y POZA CISNEROS, M., *El Principio de Disponibilidad: Antecedentes Penales y Convenio de Prüm*, Nota de Servicio interior, Consejo General del Poder Judicial. Escuela judicial, Red Europea de Formación Judicial (REFJ), 5ª edición, 2013, p. 5. http://www5.poderjudicial.es/cvcp12-13/CVCP13-09-ES.pdf [Fecha de consulta: 01/08/2018].

[479] El Tratado fue seguido de un Acuerdo de ejecución administrativo y técnico de 5 de diciembre de 2006. Y paralelamente para aclarar las cuestiones complejas tanto de carácter jurídico como técnico se adoptó la Decisión 2008/615/JAI, y el Consejo, por mayoría cualificada y previa consulta al Parlamento, adoptó a su vez Decisión 2008/615/JAI, ambas de fecha de 23 de junio de 2008, con un amplio anexo técnico referido al intercambio automatizado de datos de ADN, datos dactiloscópicos y datos de matriculación de vehículos.

dactiloscópicos. En concreto se prevén unas normas de intercambio de estos datos que resumidamente, siguiendo a Matínez y Poza, pordemos concretar en las siguientes:

“ - Las Partes garantizan la disposición de índices de referencia relativos a los datos contenidos en los sistemas automatizados nacionales de identificación dactiloscópica creados para los fines de la prevención y persecución de los delitos. […] disponen ya de estos ficheros.

- Estos índices, no obstante, contendrán, exclusivamente, datos dactiloscópicos y una referencia, sin que incorporen datos que permitan identificar directamente a la persona concernida. Sin embargo, las denominadas "huellas abiertas” o índices de referencia que no pueden atribuirse a persona determinada, deben poder ser reconocidos como tales.

- Consulta automatizada de datos dactiloscópicos, con un sistema similar al previsto para los perfiles de ADN, también a través de puntos de contacto nacionales. La conexión definitiva de un dato dactiloscópico con un índice de referencia de la Parte Contratante que mantenga el fichero se efectuará por el punto de contacto nacional que realice la consulta sobre la base de los índices de referencia comunicados de forma automatizada que sean necesarios para la atribución definitiva.

- Si en el curso de la consulta automatizada, se comprueba la concordancia de datos dactiloscópicos, la transmisión de otros datos de carácter personal disponibles relativos a los índices de referencia y demás informaciones se efectuará con arreglo al derecho interno de la Parte Contratante requerida, incluidas sus disposiciones relativas a la asistencia judicial”[480].

Hay que tener en cuenta, como cuestión de relevancia, que el marco normativo aplicable a los Estados parte del Tratado de Prüm quedan vinculados, por lo que será aplicable en el derecho interno en materia de protección de datos y por las normas que en esta materia adopte la Unión Europea, en concreto por el RGPD. Así, por ejemplo, las consultas y transmisión de perfiles de ADN para su comparación, así como la transmisión de otros datos de carácter personal se regirán por el derecho interno de las partes, tal y como se concreta en los artículos 4 y 5 del Tratado, de la misma manera que la solicitud de una persona para que se examine la legalidad de un determinado tratamiento de datos o el derecho de las personas interesadas a la información e

[480] MARTÍNEZ PÉREZ y POZA CISNEROS, M., op. cit., p. 16.

indemnización de daños, se regirán por el derecho interno del Estado en el que se hagan valer estos derechos, como se precisa en los artículos 39 y 40 del Tratado. Esta remisión al derecho interno podría suponer en opinión de Dietrich Plaza "[…] diferencias en el ejercicio de los derechos concretos de una persona frente al tratamiento de datos por aplicación del Tratado, en función del Estado miembro en que se realice el tratamiento, ya que, entre las diferentes normas internas de protección de datos de cada país, podrían existir diferencias en este sentido, […]"[481]. Pero el RGPD ha venido a dar la uniformidad necesaria entre todos los Estados miembros en la aplicación y sustantividad de las normas de protección de datos personales.

Por último, en el ámbito de los perfiles de ADN reviste particular interés la jurisprudencia del TS de EE.UU., en concreto, la Sentencia de 2013, *Maryland v. King*, en la cual, la cuestión debatida está relacionada con la recogida de muestras de ADN: se plantea si es necesario o no una orden judicial para la toma de la muestra o es suficiente que se realice en sede policial. En esta Sentencia se tiende a solicitar orden judicial salvo casos específicamente regulados como, por ejemplo, en un control antidroga, de alcohol o en control de dopaje en el deporte.

3. La identidad digital y la biometría.

Llegados a este punto, es necesario plantear el almacenamiento de los datos dactiloscópicos con fines de identificación, en concreto, el DNI electrónico biométrico y pasaportes y documentos del mar.

Como paso previo a la descripción de los documentos electrónicos biométricos mencionados es conveniente aclarar sucintamente el concepto de identidad digital.

La identidad digital puede abordarse desde una doble perspectiva: la identidad digital, que vamos a denominar, comportamental basada en el comportamiento que cada individuo desarrolla en la Red y la identidad digital en el sentido de credencial que nos permita acceder a recursos, servicios, registros públicos y privados. En esta segunda

[481] DIETRICH PLAZA, C., op. cit., p. 6.

perspectiva cabría incluir la identidad digital fisiológica que en nuestra opinión resolvería el problema de la suplantación de la identidad digital, problema manifestado en el entorno electrónico al igual que en el entorno presencial. Así, hemos distinguido entre tres identidades digitales: la identidad digital comportamental, la identidad digital como credencial de cada individuo y la identidad fisiológica digital, con incorporación del dato biométrico.

En el entorno digital, como en el presencial, disponer de una identidad única, exclusiva y excluyente es imprescindible para el desenvolvimiento de la vida de relación. La gestión de la identidad digital en un entorno digital globalizado plantea nuevos retos, nuevos problemas. La gestión de la identidad digital personal ha sido abordada por la doctrina científica y puede definirse "como la habilidad de gestionar con éxito la propia visibilidad, reputación y privacidad en la red como un componente inseparable y fundamental del conjunto de habilidades informacionales y digitales, las cuales se han convertido en fundamentales para vivir en la sociedad informacional"[482].

Pero, una cuestión clave es si la identidad digital on-line de una persona se define de forma autónoma por ella misma o "se la definen" como indica Piñar Mañas "heterónomamente"[483].

Dado que el tema de la seguridad en un mundo digital es una constante preocupación, el Instituto Nacional de Ciberseguridad (INCIBE), a través de INCIBE-CERT, y como entidad de referencia para el desarrollo de la ciberseguridad y de confianza digital, tiene entre sus cometidos fomentar la cultura de seguridad entre los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos. Para alcanzar estos fines se imponen como tarea la creación de guías y estudios sobre temas relacionados con la ciberseguridad[484].

---

[482] GIONES-VALLS, A., SERRAT-BRUSTENGA, M., *La gestión de la identidad digital: una nueva habilidad informacional y digital*, disponible en: http://bid.ub.edu/24/giones2.htm [Fecha de consulta: 10/11/2018].
[483] PIÑAR MAÑAS, J.L. *Derecho e innovación tecnológica. Retos de presente y futuro*, Madrid, CEU Ediciones, 2018, p. 14.
[484] Instituto Nacional de ciberseguridad de España, disponible en: https://www.incibe.es/CERT/guias_estudios/guias/Guia_Identidad_Reputacion_usuarios [Fecha de consulta: 25/01/2019].

En cuanto a los riesgos existentes en la suplantación de la identidad de otra persona, los mismos han sido descritos con anterioridad. Desde el punto de vista legal, el problema reside en la falta de tipificación penal de esta conducta, que inevitablemente se reconduce al delito de usurpación del estado civil del art. 401 del Código Penal: el que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años.

El Tribunal Supremo ha precisado los requisitos para que se cometa este delito: (…) para usurpar no basta con usar un nombre y apellidos de otra persona, sino que es necesario hacer algo que solo puede hacer esa persona por las facultades, derechos u obligaciones que a ella solo corresponden; como puede ser el obrar como si uno fuera otro para cobrar un dinero que es de este, o actuar en una reclamación judicial haciéndose pasar por otra persona, o simular ser la viuda de alguien para ejercitar un derecho en tal condición, o por aproximarnos al caso presente, hacerse pasar por un determinado periodista para publicar algún artículo o intervenir en un medio de comunicación (FJ segundo de la STS núm. 635/2009 de 15 junio, de la Sala de lo Penal, Sección 1ª).

La carencia de una regulación penal adecuada se manifiesta con mayor intensidad en los actos derivados de la suplantación. De ahí que la doctrina penal considere aplicar distintos tipos de delito, como la estafa ordinaria (art. 248.1 CP); la estafa informática (art. 248.2 CP), los delitos contra la intimidad (art. 197 CP); o los delitos contra la propiedad intelectual e industrial y las falsedades documentales (arts. 270, 274 y 390 CP).

La AEPD ha abierto una vía útil para conseguir que los proveedores de servicios en Internet retiren la información y colaboren en la identificación de los suplantadores. Así, en el Procedimiento Sancionador PS/ 00137/201115 15 Procedimiento disponible en: en el que una persona suplantó la identidad de otra en una red social, y habiendo identificado al suplantador mediante la información facilitada sobre la IP del ordenador desde la que ésta se produjo, la AEPD consideró que existía un tratamiento de datos

personales y se vulneraba el principio del consentimiento del (entonces) artículo 6.1 LOPD"[485].

3.1. El DNI electrónico biométrico.

El Real Decreto 1553/2005, de 23 de diciembre, regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, modificado por el Real Decreto 1586/2009, de 16 de octubre y por el Real Decreto 869/2013, de 8 de noviembre. 2. El artículo 1.2 del Real Decreto 1553/2005 atribuye a dicho Documento "el suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo"[486]. Por su parte, el artículo 5.3. entre los requisitos para su expedición señala: "En el momento de la solicitud, al interesado se le recogerán las impresiones dactilares de los dedos índices de ambas manos. Si no fuere posible obtener la impresión dactilar de alguno de los dedos o de ambos, se sustituirá, en relación con la mano que corresponda, por otro dedo según el siguiente orden de prelación: medio, anular o pulgar; consignándose, en el lugar del soporte destinado a tal fin, el dedo utilizado, o la imposibilidad de obtener alguno de ellos". Es indudable que el almacenamiento de la impresión dactilar es un almacenamiento de datos biométricos que ha de verse amparado por el derecho a la autodeterminación informativa y sobre los que cada titular debe poder ejercitar su derecho de control sobre las finalidades de su uso posterior. Y si el solicitante del DNI se niega a facilitar estos datos sobre la base de una falta de garantías en la no utilización posterior de los datos biométricos para otros fines, es evidente que se plantea un problema. A este respecto, merece ser citada la sentencia de 16 de abril de 2015 del Tribunal de Justicia de la Unión Europea (TJUE) que interpreta los artículos 1, apartado 3 y artículo 4 apartado 3 del Reglamento (CE) nº 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros (DO L 385, p. 1), en su versión modificada por el Reglamento (CE) nº 444/2009 del Parlamento

[485] Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2011/common/pdfs/PS-00137-2011_Resolucion-de-fecha-27-07-2011_Art-ii-culo-6.1-LOPD.PDF [Fecha de consulta: 10/09/2018].

[486] BOE 307/2005, de 24 de diciembre de 2005 Ref Boletín: 05/21163.

Europeo y del Consejo, de 6 de mayo de 2009 (DO l 142, p.1, con corrección de errores en el DO L 188, p. 127). En esta sentencia se resuelve una petición, en concreto la del holandés Sr. *Kooistra*, quien presentó en su país una solicitud de expedición de un documento de identidad neerlandés, pero negándose a facilitar sus impresiones dactilares y una foto, lo que le acarreó la denegación de su solicitud. La cuestión que se plantea al Tribunal es la aplicabilidad del Reglamento citado en lo que respecta a sus normas de incorporación de datos biométricos a un documento de identidad a un documento, en este caso, holandés. Pues bien, como ha puesto de relive Cancio Fernández, el TJUE "considera que el legislador de la Unión ha decidido expresamente excluir del ámbito de aplicación de dicho Reglamento los documentos de identidad expedidos por los Estados miembros a sus nacionales […]"[487]. De este modo, el requisito del artículo 5.3. del Real Decreto 1553/2005, que más arriba hemos citado, no se ampara en el Reglamento 2252/2004. Se planteada así una cuestión, en absoluto baladí, cómo es la de armonizar la recogida, almacenamiento y tratamiento de datos biométricos de alta criticidad como el dactilograma de individuos con alteraciones dactilares a nivel europeo si el Reglamento, al que de forma natural nos habríamos de remitir todos, no resulta de aplicación. En definitiva, la Sentencia resuelve que el Reglamento 2252/2004 es inaplicable a los documentos de identidad expedidos por los Estados miembros a sus nacionales, ya sean temporales o no, u sea cual sea su periodo de validez.

Deseamos recordar aquí, la ya mencionada comparecencia del entonces Director de la AEPD, Don José Luís Piñar Mañas, en el Congreso de los Diputados el 28 de septiembre de 2005 a fin de informar sobre la memoria de la Agencia correspondiente al año 2004. En esta intervención Piñar Mañas llama la atención sobre las nuevas técnicas biométricas y su creciente utilización en los documentos hasta ahora conocidos de identificación de las personas, a saber, pasaporte, documentos de viaje y DNIs. Lo cierto es que estos datos biométricos pueden llegar a ser recabados incluso sin conocimiento de su titular lo que supone un evidente riesgo para sus derechos. Riesgo de pérdida del control sobre los datos recogidos, pudiendo ser uilizados en el futuro con fines espúreos, en definitiva, indeterminados.

[487] CANCIO FERNÁNDEZ, R., *Datos biométricos, seguridad, protección de la vida privada y DNI* Cátedra Paz, Seguridad y Defensa, Observatorio PSyD, septiembre, 2015, disponible en: http://catedrapsyd.unizar.es/observatorio-psyd/opina/datos-biometricos-seguridad-proteccion-de-la-vida-privada-y-dni.html [Fecha de consulta: 02/08/2018].

No podemos dejar de mencionar la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana; en concreto, nos interesa el artículo 8 de la misma, que hace referencia a la acreditación de la identidad de los ciudadanos españoles el que merece nuestra atención al establecer que:

> "1. Los españoles tienen derecho a que se les expida el Documento Nacional de Identidad.
>
> El Documento Nacional de Identidad es un documento público y oficial y tendrá la protección que a éstos otorgan las leyes, así como suficiente valor por sí solo para la acreditación de la identidad y los datos personales de su titular.
>
> 2. En el Documento Nacional de Identidad figurarán la fotografía y la firma de su titular, así como los datos personales que se determinen reglamentariamente, que respetarán el derecho a la intimidad de la persona, sin que, en ningún caso, puedan ser relativos a la raza, etnia, religión, creencias, opinión, ideología, discapacidad, orientación o identidad sexual, o afiliación política o sindical. La tarjeta soporte del Documento Nacional de Identidad incorporará las medidas de seguridad necesarias para la consecución de condiciones de calidad e inalterabilidad y máximas garantías para impedir su falsificación.
>
> 3. El Documento Nacional de Identidad permite a los españoles mayores de edad que gocen de plena capacidad de obrar y a los menores emancipados la identificación electrónica de su titular, así como la firma electrónica de documentos, en los términos previstos en la legislación específica. Las personas con capacidad modificada judicialmente podrán ejercer esas facultades cuando expresamente lo solicite el interesado y no precise, atendiendo a la resolución judicial que complemente su capacidad, de la representación o asistencia de una institución de protección y apoyo para obligarse o contratar.
>
> El prestador de servicios de certificación procederá a revocar el certificado de firma electrónica a instancia del Ministerio del Interior, tras recibir éste la comunicación del Encargado del Registro Civil de la inscripción de la resolución judicial que determine la necesidad del complemento de la

capacidad para obligarse o contratar, del fallecimiento o de la declaración de ausencia o fallecimiento de una persona."

Es importante hacer constar que, hoy, tras la aprobación de la LO 3/2018, en la identificación de los ciudadanos en los actos administrativos, la ley impide el uso conjunto de apellidos, nombre y número completo de Documento de identificación oficial de los ciudadanos en aquellos actos administrativos que vayan a ser objeto de publicación o notificación por medio de anuncios.

3.2. Datos biométricos en pasaportes y documentos de viaje

En nuestro país, el Real Decreto 896/2003, de 11 de julio, por el que se regula la expedición del pasaporte ordinario y se determinan sus características, recogía en su versión primigenia en su artículo 10.5 en relación con el contenido: "Igualmente se podrán incluir datos biométricos que sean necesarios para una más completa identificación del titular, insertándose bien en la página de datos personales, referida en el apartado 2 de este artículo, o bien en la que se determine por el Ministerio del Interior". Esta versión fue modificada por el RD 411/2014 de 6 junio 2014 y desde el 26 de junio de 2014 la versión actualmente vigente es: "5. El pasaporte llevará incorporado un chip electrónico que contendrá la siguiente información referida a su titular: datos de filiación, imagen digitalizada de la fotografía, impresiones dactilares de los dedos índices de ambas manos, o los que en su defecto correspondan conforme al siguiente orden de prelación: medio, anular o pulgar". Por su parte la Ley Orgánica 4/2015, ya mencionada, de protección de la seguridad ciudadana recoge en su artículo 11, que lleva por título "Pasaportes de ciudadanos españoles", en su punto 1. que:

"El pasaporte español es un documento público, personal, individual e intransferible que, salvo prueba en contrario, acredita la identidad y nacionalidad de los ciudadanos españoles fuera de España, y dentro del territorio nacional, las mismas circunstancias de los españoles no residentes".

El pasaporte es, por tanto, una prueba *iuris tantum* de la identidad del ciudadano español fuera y dentro del territorio nacional. En el mismo sentido, de acreditación de la identidad por el ciudadano extranjero, se pronuncia el artículo 13.1 de la LO 4/2015:

> "Los extranjeros que se encuentren en territorio español tienen el derecho y la obligación de conservar y portar consigo la documentación que acredite su identidad expedida por las autoridades competentes del país de origen o de procedencia, así como la que acredite su situación regular en España".

Tras los trágicos acontecimientos del 11 de septiembre de 2001, los Estados miembros invitaron a la Comisión a adoptar urgentemente medidas destinadas a reforzar la seguridad de los documentos. El Consejo decidió así introducir elementos biométricos en los pasaportes europeos. Estos identificadores se concretaron en una fotografía digitalizada e impresiones dactilares, a fin de luchar más eficazmente contra el fraude y la falsificación. Así en este ámbito se adoptó Reglamento (CE) nº 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros[488].

Resulta de gran interés, en relación con los datos biométricos en pasaportes y documentos de viaje, la Sentencia del TJUE (Sala Cuarta) de 17 de octubre de 2013[489]. El asunto se tramitó ante el Tribunal como una petición prejudicial planteada con arreglo al artículo 267 TFUE, por el *Verwaltungsgericht Gelsenkirchen* (Alemania). Vamos a exponer primero los antecedentes de hecho y a continuación los fundamentos jurídicos o marco jurídico aplicable.

En relación con los antecedentes de hecho la petición de decisión prejudicial versa sobre la validez del artículo 1, apartado 2, del Reglamento (CE) no 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados

[488] Siendo un acto modificativo de este Reglamento la Decisión de la Comisión de 28 de junio de 2006 por la que se establecen las especificaciones técnicas sobre las normas de las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros [C(2006) 2909 final – No publicado en el Diario Oficial].
[489] Sentencia de 17.10.2013 – Asunto C-291/12 SCHWARZ. ECLI:EU:C:2013:670.

miembros, en su versión resultante del Reglamento (CE) nº 444/2009 del Parlamento Europeo y del Consejo, de 6 de mayo de 2009. Esta petición se presentó dentro de un procedimiento judicial entre el Sr. *Schwarz* y la ciudad de *Bochum*. En este litigio se dirimía la negativa de la ciudad a expedir un pasaporte al Sr. *Schwarz* si no tomaba simultáneamente sus impresiones dactilares para ser almacenadas en el pasaporte. Una cuestión con similitudes con la del holandés Sr. *Kooistra*, que hemos comentados más arriba, y que fue resuelta por Sentencia de 16 de abril de 2015 del TJUE.

Entrando ya en la fundamentación jurídica, se tiene primero en cuenta la Directiva 95/46/CE. El Tribunal de Justicia parte de la definición que de datos personales y de tratamiento de datos personales recoge la, ya derogada, Directiva 95/46/CE en su artículo 2 apartados a) y b); y de la legitimación de los Estados miembros para el tratamiento, recogida en el artículo 7 e), que no es otra que la necesidad de dicho tratamiento para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos.

También son tenidos en cuenta los considerandos 2, 3, y 8 del Reglamento nº 2252/2004; en concreto, el considerando 2 expresamente reconoce que la integración de identificadores biométricos en los pasaportes o documentos de viaje establece un vínculo fiable entre el documento y su titular real evitando así falsificaciones. En todo caso toda incorporación de datos al pasaporte ha de respetar el principio recogido en la Directiva 95/46/CE de que no han de ser excesivos, y en el mismo sentido el RGPD.

El considerando 5 del Reglamento nº 444/2009, advierte de la legitimidad del almacenamiento en pasaporte y documentos de viaje de datos biométricos con el objeto de expedir dichos documentos. Ahora bien, lo que no tiene amparo en el Reglamento es el establecimiento o mantenimiento de bases de datos con la finalidad única de almacenamiento de dichas informaciones por los Estados miembros. Estas bases de datos, de existir, tendrán amparo en la legislación estatal.

Asimismo, podemos destacar la Sentencia del TJUE, Sala 4ª de 16 de abril de 2015, nº C-446/2012. Esta Sentencia interpreta los artículos 1.3 y 4.3 del Reglamento 2252/2004

resolviendo así unas cuestiones prejudiciales planteadas en unos litigios entre varios ciudadanos holandeses contra sus respectivos alcaldes ante la negativa de éstos a expedir a aquéllos un pasaporte o un documento de identidad sin captar previamente sus datos biométricos. Así el Tribunal declara que:

> "[…]
> 1) El artículo 1, apartado 3, del Reglamento (CE) nº 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaporte y documentos de viaje expedidos por los Estados miembros, en su versión modificad por el Reglamento (CE) nº 444/2009 del Parlamento Europeo y del Consejo, de 6 de mayo de 2009, debe interpretarse en el sentido de que dicho Reglamento no es aplicable a los documentos de identidad expedidos por un Estado miembro a sus nacionales, tales como los documentos de identidad neerlandeses, con independencia de su período de validez y de las posibilidades de utilizarlos en viajes efectuados fuera de dicho Estado.
> 2) El artículo 4, apartado 3, del Reglamento nº 2252/2004, en su versión modificada por el Reglamento nº 444/2009, debe interpretarse en el sentido de que no obliga a los Estados miembros a garantiza, en su legislación, que los datos biométricos recogidos y almacenados de conformidad con el referido Reglamento no serán recogidos, tratados ni utilizados con fines distintos de la expedición de pasaporte o del documento de viaje, pues este aspecto no está comprendido en el ámbito de aplicación del citado Reglamento."

Es decir, las normas recogidas en el citado artículo 1 relativas a que los pasaportes y documentos de viaje incluirán un soporte de almacenamiento, que garantizando la integridad, la autenticidad y la confidencialidad de los datos, contenga una imagen facial y dos impresiones dactilares, quedando exentos de la obligación de facilitar las impresiones dactilares los menores de 12 años y las personas a las que sea físicamente imposible tomar las impresiones dactilares, son normas inaplicables a los documentos de identidad expedidos por un Estado miembro a sus nacionales. Y así mismo el artículo

4.3 del Reglamento que dispone que los datos biométricos se recogerán y conservarán en el medio de almacenamiento de pasaportes y documentos de viaje con objeto de expedir dichos documentos y que las medidas de seguridad con datos biométricos del pasaporte o documento de viaje se utilizarán únicamente para verificar la autenticidad del pasaporte o del documento de viaje y la identidad del titular mediante características comparables accesibles directamente, no obliga a los Estados a garantizar que los datos recogidos conforme al Reglamento no sean utilizados con fines distintos. Lo dispuesto en este artículo 4.3 en relación a la comprobación de las medidas de seguridad complementarias se llevará a cabo sin perjuicio de lo dispuesto en el artículo 7, apartado 2, del Reglamento (CE) no 562/2006 del Parlamento Europeo y el Consejo, de 15 de marzo de 2006, por el que se establece un Código comunitario de normas para el cruce de personas por las fronteras (Código de fronteras Schengen)[490] .

Es destacable la previsión del Reglamento en relación a la imposibilidad temporal de tomar las impresiones dactilares de los dos dedos. En esos casos, los Estados miembros permitirán que se tomen las impresiones dactilares de los otros dedos. Cuando también resulte temporalmente imposible tomar las impresiones dactilares de cualquiera de los otros dedos, expedirán un pasaporte temporal de validez igual o inferior a 12 meses. Lo consideramos de interés toda vez que pone de manifiesto la posibilidad de que la huella dactilar se vea alterada por distintas circunstancias siendo una de ellas, como ya hemos apuntado en el capítulo anterior, el padecimiento de una enfermedad.

No podemos concluir el epígrafe relativo a la identidad digital sin mencionar los documentos de identidad de "la gente del mar". El conocido como C108 (Convenio sobre los documentos de identidad de la gente de mar, 1958 (núm. 108)[491], determina los requisitos que deben reunir estos documentos: estará confeccionado con materia resistente, contendrá, entre otros datos, las características físicas y la firma, o la impresión del pulgar cuando el titular no sepa firmar (art. 4 Convenio); este último inciso, pensado para aquéllos que no sabían firmar, fue eliminado tras una revisión del Convenio (C185 - Convenio sobre los documentos de identidad de la gente de mar

[490] DO L 105 de 13.4.2006, p. 1.
[491]Disponible en: http://www.ilo.org/dyn/normlex/es/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C108 04/02/2017.

(revisado), 2003 (núm. 185)[492], contemplado en un nuevo artículo 3; asimismo, se añade algo muy relevante para el tema que nos ocupa: "(…) se exigirá, además, que al documento de identidad de la gente de mar se incorpore una plantilla u otra representación biométrica del titular, (…) siempre que se cumplan los requisitos siguientes:

(a) que los datos biométricos puedan obtenerse sin que ello implique injerencia en la privacidad del titular, molestia, riesgo para su salud, o lesión de su dignidad;

(b) que los datos biométricos sean visibles en el documento, y no puedan reconstituirse a partir de la plantilla o de otras representaciones;

(c) que el material necesario para proveer y verificar los datos biométricos sea fácil de utilizar y, en general, asequible para los gobiernos a bajo costo;

(d) que el material necesario para verificar los datos biométricos pueda utilizarse con comodidad y fiabilidad en los puertos y en otros lugares, incluso a bordo de los buques, donde las autoridades competentes suelen proceder a las verificaciones de identidad, y

(e) que el sistema en el que se hayan de utilizar los datos biométricos (con inclusión del material, las tecnologías y los procedimientos de utilización) permita obtener unos resultados uniformes y fiables en materia de autentificación de la identidad" (art 3.8 C-185). Además, "su contenido y forma se conformarán a las normas internacionales pertinentes (…)" (art. 3.10 C-185).

En definitiva, con todos estos ejemplos, hemos pretendido recordar la existencia de la identidad digital en un mundo virtual que, desde luego, puede acarrear ciertos riesgos.

Como ya nos advierte GIONES-VALLS[493], actualmente, "Internet ofrece numerosas soluciones telemáticas, como facturación electrónica, visado digital, voto electrónico, firma electrónica, carné de identidad digital, formularios telemáticos, certificado digital, receta electrónica, etc., todas ellas opciones basadas en la encriptación de datos y en la utilización de dispositivos inteligentes como claves, tarjetas y generadores de contraseñas, que permiten la autenticación"; en este contexto, y a pesar de las medidas contempladas a nivel informático y jurídico, la usurpación de la identidad y el uso

[492] C185- Convenio sobre los documentos de identidad de la gente de mar (revisado) (Entrada en vigor: 09 febrero 2005). Adopción: Ginebra, 91ª reunión CIT (19 junio 2003). Disponible en: https://www.ilo.org/dyn/normlex/es/f?p=NORMLEXPUB:12100:0::NO::P12100_INSTRUMENT_ID:312330 [Fecha de consulta: 09/10/2018].

[493] GIONES-VALLS, A., SERRAT-BRUSTENGA, M., op. cit.

fraudulento son problemas comunes en un mundo virtual. Por ello, “la construcción de una identidad digital en la red implica un aprendizaje y una actitud colaborativa y participativa en la cultura digital”, siendo de vital importancia la correcta y eficaz gestión de aquélla.

Sin lugar a dudas, y reiterando lo dicho al comienzo de este capítulo III, diversas cuestiones planteadas en el mismo serán objeto de una nueva y atractiva investigación que, es nuestro deseo llevar a cabo en un futuro.

CONCLUSIONES

Primera. El ámbito de este estudio se ha detenido en datos biométricos biológicos con base en la anatomía del individuo y, dentro de esta categoría, han sido los datos biométricos biológicos obtenidos de la huella dactilar el objeto de atención.

Resulta evidente la afección a derechos fundamentales del individuo proveniente de la utilización de sistemas biométricos; una persona puede ver afectados alguno o algunos, o todos, sus derechos fundamentales en la recogida, almacenamiento, tratamiento o cesión posterior de sus datos biométricos dactiloscópicos. La información sobre aspectos físicos de los individuos puede afectar a ámbitos tan críticos como su intimidad y tener un alto potencial discriminatorio, comprometiendo así al principio de igualdad. Sin duda, de entre estos derechos, el de autodeterminación informativa es el que se verá más afectado.

En efecto, con los sistemas biométricos se hace posible obtener un grupo discriminado del conjunto de la población en base únicamente a que dichos individuos presenten determinadas características físicas diferenetes o especiales. El sistema es capaz de revelar una información espúrea, pero de alto alcance para los derechos del individuo, no siendo esta la finalidad del tratamiento. No se puede perder nunca la condición de "persona" del individuo. Las técnicas de identificación de personas no deberían derivar en una identificación de pacientes, alumnos, trabajadores, viajeros, etc… que no dejan de ser en ningún momento personas por mucho que en un determinado momento su condición de pacientes o alumnos sea la que prevalezca, o bien, sea con la que el responsable del tratamiento se haya encontrado. Los empleados o trabajadores conla nueva LO ven garantizado su derecho a la intimidad en su lugar de trabajo de forma explícita, ya que ahora este derecho a la intimidad se defiende frente al uso de dispositivos de videovigilancia, de grabación de sonidos, de dispositivos digitales y sistemas de geolocalización. Si estos sistemas se utilizan, el trabajador deberá ser informado de manera expresa, clara e inequívoca. Entendemos incluidos los sistemas de identificación biométrica, puesto que la grabación de sonidos es uno de esos sistemas, desde el momento en que recoge la voz del individuo-trabajador, que, sin duda, es un dato biométrico.

La identificación biométrica utilizada al margen de las normas de protección de datos de carácter personal puede convertir a las personas en elementos identificados susceptibles de tomar decisiones sobre ellos en los ámbitos más variopintos de la vida.

Segunda. El dato biométrico puede considerarse dato identificativo y ésta es una característica que lo distingue, por ejemplo, del dato de salud. No obstante, hay puntos de confluencia entre dato biométrico y de salud; es el caso de que aquél revele una enfermedad. En este supuesto entra en juego la normativa y doctrina de datos personales relativos a la salud, bien entendido que no podemos considerar como sinónimos uno y otro dato.

Tercera. La fractura o desequilibrio en la base de la estructura de la sociedad de la información como organización social puede producirse si el individuo desconoce que sus datos de huella dactilar han sido captados y son objeto de tratamiento. La simetría entre dato y tratamiento debe ser perfecta para permitir al individuo el ejercicio de su derecho fundamental a la autodeterminación informativa. Si la vía de conexión, en el sentido de conocimiento, entre dato y tratamiento del dato está quebrada, el ejercicio del derecho de autodeterminación se hace inviable y el efecto reequilibrador de poderes se rompe, produciendo una asimetría de poder en favor del responsable de ese tratamiento. Al ser un tratamiento desconocido para el titular, éste no puede neutralizar jurídicamente, con el ejercicio del derecho de autodeterminación, la asimetría de poder que dicho tratamiento produce. La pérdida de conocimiento conduce a una pérdida de control y la pérdida de control a una pérdida de libertad para el individuo. Los ciudadanos tienen derecho, con arreglo a la nueva LO 3/2018, a conocer el registro de actividades de tratamiento (RAT) de sus datos personales por los organismos públicos. Este derecho se concreta en tres grupos de información: 1. Quién trata sus datos personales. 2. Con qué finalidad y 3. Qué base jurídica legitima este tratamiento.

Cuarta. La plantilla es la medida biométrica registrada de un individuo. Por tanto, el rasgo biométrico permanece en la persona y solo cuando el sistema lo extrae, para elaborar la plantilla, hay tratamiento porque hay estructura y registro y posibilidad de almacenamiento. De este modo, el dato biométrico dactiloscópico será dato personal si, una vez extraído de la persona en su versión digital, en forma de plantilla, utilizando un

conjunto de medios razonables, es posible atribuirlo a una persona identificada o identificable.

Quinta. El elemento material del dato biométrico dactiloscópico encuentra su ámbito jurídico de protección en los derechos de la personalidad y fundamentales de intimidad, propia imagen e integridad física y el elemento inmaterial, en el sentido de la información extraída, en el derecho de autodeterminación informativa.

Sexta. Si realmente el dato biométrico no contiene ninguna información adicional del individuo efectivamente, sin negarle su carácter de dato personal, su análisis podría quedar circunscrito al cumplimiento del principio de calidad de los datos, recogido, con anterioridad en el artículo 4.1 LOPD -y, actualmente, recogido, en cierto modo, como principio de exactitud en el LO 3/2018-, en el sentido de que solo podrá ser recogido para su tratamiento cuando sea adecuado, pertinente y no excesivo en relación con el ámbito y las finalidades para las que se haya obtenido. Pero, a nuestro entender, esta es una visión parcial del tema porque el dato biométrico, o algunos datos biométricos y, entre ellos, la huella dactilar, puede contener información adicional y de tan alta sensibilidad como la relativa a la salud de su titular. En este sentido, el nuevo RGPD es así como considera a los datos biométricos: como datos merecedores de especial protección; entendemos que lo regula de este modo, precisamente porque contienen datos adiconales de la persona.

Séptima. Las Nuevas Tecnologías de la Información y la Comunicación han alcanzado una virtualidad práctica, real, de recoger, tratar, almacenar y reproducir elementos intrínsecos al propio cuerpo humano. Estos elementos, ya no son sólo datos o informaciones sobre un individuo, sino que son “el individuo en sí mismo”, pudiendo quedar comprometidos o afectados los derechos del mismo a que hace referencia el art. 18.4 CE.

Octava. Es difícil considerar que se pueda producir una intromisión en la integridad moral del individuo en la recogida del dato, ya que en la captación no hay finalidad de humillarle o envilecerle de ninguna manera. Pero un caso especial lo representarían todos aquellos individuos que, por una malformación congénita, accidente, edad etc. presenten una alteración de sus dedos o de sus huellas o carezcan de ellas. El mero

hecho de no poder someterse al sistema de captación o presentar dificultades o imposibilidad mecánica para la captación, ya podría representar una humillación y, por ende, una intromisión en su "integridad moral".

Novena. La lectura/captación de huellas dactilares o imagen de la mano, por una parte, entraría en la primera categoría de inspección o registro que en absoluto supone una lesión corporal o menoscabo de la integridad física y, por otra, no afectaría al recato o pudor de la persona, no afectando así a su intimidad corporal. Ahora bien, igual que hemos llamado la atención sobre una posible afección a la integridad moral, si en la recogida de la huella se produce una humillación o envilecimiento de la persona, también puede verse afectada la "intimidad corporal" de la persona que sufriendo una alteración física de una parte de su cuerpo se ve obligada por el sistema de captación a su exposición pública. Puede plantearse una situación en la que la captación de la huella de un dedo o dedos o palma de una mano alteradas físicamente, afecte al pudor de la persona. Estamos planteando la posibilidad de que, en determinados casos, personas con alteraciones físicas o edad avanzada se vean humilladas o envilecidas o afectado su pudor, al tener que exponer en un dispositivo de captación del dato biométrico su mano o dedo distinto del resto. La humillación, envilecimiento de la persona está directamente relacionado con su integridad moral. Y el pudor con su intimidad corporal. Determinados colectivos, niños, ancianos, personas con discapacidad física… son grupos de riesgo al tener unos contornos del concepto de humillación y pudor distintos al conjunto general de la población.

Décima. El tratamiento de datos biométricos, y en concreto dactiloscópicos, por la parte del cuerpo a la que afectan, sobre la que no cabe apreciar un especial recato en su exhibición, no permite deducir una vulneración del derecho a la "integridad" corporal, ni a la "intimidad" corporal, con las salvedades apuntadas en relación con determinados grupos de riesgo, personas que por sus características físicas especiales, o bien, quedan por ello fuera del sistema, o el simple hecho de incorporarse al sistema afecta a su integridad moral y/o intimidad corporal.

Décimo primera. Es indudable que existe una estrecha relación entre la tecnología de la videovigilancia y la captación de datos biométricos, pero a la vez una clara diferencia, puesto que la captación de imágenes por sistemas de videovigilancia sirve de base a la

captación de datos biométricos, pero no necesariamente y en todos los casos. Asimismo, la fotografía de un individuo es dato de carácter personal biométrico y especialmente protegido, únicamente si permite la identificación de ese individuo, de esa persona física concreta. Asimismo, no cabe confundir los ámbitos de protección de la imagen y los datos biométricos dactiloscópicos, puesto que éstos no permiten la identificación directa de un individuo, cosa que sí permite la imagen. La normativa sobre videovigilancia no es aplicable a la protección de dato biométrico.

Décimo segunda. El principal debate jurídico que suscita el tratamiento de datos biométricos, y en particular el de los datos dactiloscópicos, es en relación con el derecho fundamental a la protección de datos. Es decir, la legitimidad de algunos tratamientos de datos biométricos se debe estudiar a la luz de principios como los de finalidad y proporcionalidad, puesto que sólo respetando estos principios cabe aceptar la limitación al derecho fundamental a la protección de datos que el tratamiento de datos biométricos puede suponer o entrañar. Para todo ello, deberemos analizar: 1º cómo el tratamiento de datos biométricos es un tratamiento de datos personales y supone una limitación al derecho fundamental aludido y, 2º la legitimidad del tratamiento depende de si la vulneración al derecho fundamental es ajustada a los principios y derechos de la protección de datos y, en especial, a los principios apuntados de finalidad y proporcionalidad.

Décimo tercera. En cuanto a los principios de protección de datos, no hacemos rigurosamente sinónimos los conceptos de exactitud y actualización, aunque estén íntimamente relacionados, ya que un dato no actualizado es imposible que sea un dato exacto. Ahora bien, no todos los datos actualizados por el mero hecho de estar actualizados, son exactos. Estos conceptos de exactitud y actualización llenaban de contenido al antiguo principio de calidad de los datos de la LOPD. Debemos precisar, por último, en relación con este principio de exactitud que, como dispone el RGPD, la inexactitud de los datos ha de ser suprimida o rectificada, no siendo imputable al responsable del tratamiento, siempre que éste haya adoptado todas las medidas razonables que estén a su alcance. El derecho de cancelación de los contenidos ilícitos se ha visto reforzado con la configuración del nuevo derecho al olvido. En definitiva, el RGPD utiliza otra terminología, pero hace referencia a los mismos conceptos.

Décimo cuarta. Entendemos que, teniendo en cuenta el "hermanamiento", al incluirse en la misma categoría de datos, según el artículo 9.1 del RGPD, los datos biométricos dirigidos a identificar de manera unívoca a una persona física y los datos relativos a la salud, las consideraciones relativas al consentimiento efectuadas respecto a las muestras biológicas son plenamente aplicables a los datos objeto de nuestro estudio.

Décimo quinta. En relación con el consentimiento del titular de los datos, que ha sido la piedra angular sobre la que se basaba el tratamiento de los mismos, hoy ha cambiado en parte esta situación, ya que el RGPD y la nueva LO 3/2018 establecen varias bases jurídicas legitimadoras del tratamiento, por parte de las organizaciones privadas. En concreto, una relación contractual previa o un interés legítimo que prevalezca sobre el derecho de las personas constituyen esta base a lo que nos referimos. Si no existe otra base legitimadora, evidentemente el consentimiento del afectado sigue siendo suficiente para el tratamiento, ahora bien, entendiéndolo como una declaración clara o una acción afirmativa, no admitiendo, por tanto, un consentimiento tácito o implícito. Todo ello, sin duda, aplicable al tratamiento de datos dactiloscópicos.

Décimo sexta. En relación con los datos de las personas fallecidas, hoy pueden ser conocidos, rectificados y/o suprimidos por sus herederos, familiares o personas vinculadas con el fallecido por vías de hecho. Con la nueva LO 3/2018 en la mano, no cabe que las empresas, entidades u organismos públicos o privados nieguen las solicitudes de borrado de datos, incluidos los dactiloscópicos, por el hecho de que su titular esté fallecido.

Decimo séptima. Si realmente el dato biométrico no contiene ninguna información adicional del individuo efectivamente, sin negarle su carácter de dato personal, su análisis podría quedar circunscrito al cumplimiento del principio de calidad de los datos que se recogía en el artículo 4.1 de la LOPD (no especificado en la nueva Ley como tal, sino a través del principio de exactitud), en el sentido de que solo podrá ser recogido para su tratamiento cuando sea adecuado, pertinente y no excesivo en relación con el ámbito y las finalidades para las que se haya obtenido. Pero a nuestro entender, esta es una visión parcial del tema porque el dato biométrico, o algunos datos biométricos y entre ellos la huella dactilar, puede contener información adicional y de tan alta sensibilidad como la relativa a la salud de su titular. El análisis del dato biométrico, y en

concreto el dato biométrico dactiloscópico, se ha abordado distinguiendo un elemento material y un elemento inmaterial. El elemento material, fuente del dato biométrico, bien sea el conjunto de surcos y valles de la huella, o las características del óvalo facial, o del iris de un individuo es distinto de la información contenida en ese conjunto de surcos y valles que incluso puede revelar información sobre los hábitos ocupacionales o profesionales de la persona si se aprecian corrosiones o desgastes anormales o, incluso proporcionar información sobre la salud, o revelar deformidades congénitas. Por consiguiente, entendemos que el elemento inmaterial, la información inmanente en el soporte material-físico propiamente dicho, sí puede revelar nuevas características referentes a la intimidad y privacidad del individuo; asimismo, puede contener aspectos concretos de su personalidad, no limitándose su funcionalidad a identificar a un sujeto.
Por lo demás, consideramos que la huella digital puede contener aspectos concretos de la personalidad del individuo incluso datos de salud que hacen que estos datos pasen a la categoría de datos sensibles.

Décimo octava. Actualmente las Administraciones públicas en España permiten la identificación de los administrados a través de medios digitales, reconociendo la identidad digital de aquéllos; en dicha identidad juegan un papel muy relevante, entre otros datos biométricos, los dactiloscópicos, ya que la conforman. Coincidiendo con un sector importante de la doctrina científica, la construcción de una identidad digital en la red exige una correcta y eficaz gestión de aquélla.

Décimo novena. Una vez más, se observa que la tecnología va por delante del Derecho y, en este sentido, la UE está haciendo frente al reto de la identificación digital del individuo partiendo de un documento transcendetal como es el RGPD, cuya entrada en vigor ha obligado a incorporar en todas las legislaciones internas de los países miembros la nueva normativa europea. Nuestra LOPD no ha sufrido grandes cambios, como así ha puesto de manifiesto la doctrina científica, si bien, se echan en falta en el nuevo Reglamento y, por ende, en la LO 3/2018, ciertas concreciones o especificaciones que contemplaba la LOPD, dejando ahora un margen para la interpretación, lo que siempre puede ser delicado. Por último, fuera del ámbito europeo la regulación recogida en la LOPD y el RLOPD podrá, por el momento, sevir de referente para los obligados a aplicar la normativa de protección de datos; pero con la nueva Ley española (y el resto

de desarrollos legislativos en la UE) se facilitará la mejor convivencia entre las legislaciones nacionales y la europea.

FUENTES UTILIZADAS

I. ARTÍCULO 29 – GRUPO DE PROTECCIÓN DE DATOS.

I. *Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware*. 5093/98/EN/final WP 17. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp17en.pdf

II. Dictamen 6/2000 sobre la cuestión del genoma. Aprobado el 13 de julio de 2000. WP 34 5062/00/ES/FINAL. Dirección en Internet: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp34es.pdf

III. Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral. Aprobado el 13 de septiembre d 2001. WP 48 (5062/01). Dirección en Internet: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf

IV. Dictamen 9/2001 sobre la comunicación de la Comisión titulada "Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos". Adoptado el 5 de noviembre de 2001. WP 51 5074/01/ES/final. Dirección en Internet: www.europa.eu.int/comm/internal_market/en/dataprot/index/htm

V. Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo. Aprobado el 29 de mayo de 2002. WP 55 5401/01/ES/Final Dirección en Internet: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf

VI. Dictamen 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos. Aprobado el 24 de octubre de 2002 11647/02/ES/Final WP 66.

VII. Documento del Grupo de Trabajo del artículo 29 Directiva 95/46/CE. Documento de trabajo relativo al tratamiento de datos personales mediante vigilancia por videocámara. Adoptado el 25 de noviembre de 2002. WP 67 11750/02/ES. Sitio web: www.europa.eu.int/comm/privacy

VIII. Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los

datos personales en Internet por sitios web establecidos fuera de la UE, Aprobado el 30 de mayo de 2002, (5035/01/ES/Final WP 56).

IX. Documento de trabajo sobre biometría. Adoptado el 1 de agosto de 2003. WP 80 12168/02/ES. Sitio de Internet: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2003_en.htm

X. Documento de trabajo sobre datos genéticos. Adoptado el 17 de marzo de 2004. WP 91 12178/03/ES. Sitio de Internet: www.europa.eu.int/comm/privacy

XI. *Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas* (VIS). Adopted on 11 August 2004. WP 96 11224/04/EN. Website: http://europa.eu.int/comm/internal_market/privacy/index_en.htm

XII. *Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (Official Journal L 385 , 29/12/2004 p. 1 - 6)* Adopted on 30 September 2005. Dictamen 3/2005 sobre la aplicación del Reglamento (CE) nº 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros. Adoptado el 30 de septiembre de 2005. WP 112. 1710-01/05/ES-rev. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp112_en.pdf

XIII. Dictamen 4/2007 sobre el concepto de datos personales Adoptado el 20 de junio 01248/07/ES WP 136. Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

XIV. Dictamen nº 3/2007 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica la Instrucción consular común dirigida a las misiones diplomáticas y oficinas consulares de carrera en relación con la introducción de datos biométricos, y se incluyen disposiciones sobre la organización de la recepción y la tramitación de las

solicitudes de visado (COM (2006) 269 final). Sitio de Internet: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

XV. Documento de trabajo 1/08 sobre la protección de datos personales de los niños. (Directrices generales y el caso especial de los colegios). Adoptado el 18 de febrero de 2008. WP 147. Sitio web: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

XVI. Dictamen 3/2010 sobre el principio de responsabilidad. 00062/10/ES GT 173. Adoptado el 13 de julio de 2010. Sitio de Internet: http://ec.europa.eu/justice/policies/privacy/index_en.htm

XVII. Dictamen 02/2012 sobre reconocimiento facial en los servicios en línea y móviles. 00727/12/ES WP 192. Adoptado el 22 de marzo de 2012. Sitio de Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_es.pdf 09/02/2016.

XVIII. Dictamen 3/2012 sobre la evolución de las tecnologías biométricas. 00720/12/ES
WP193, adoptado el 27 de abril de 2012. Sitio de Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_es.pdf 09/02/2016.

XIX. Dictamen 8/2014 sobre la evolución reciente del Internet de los objetos. 1471/14/ES WP 223. Adoptado el 16 de septiembre de 2014. Sitio de Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf 09/02/2016.

XX. *Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting*. 14/EN WP 224. Adopted on 25 November 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf 09/02/2016.

I. CONSEJO DE EUROPA.

XXI. Consejo de Europa. Comité Consultivo de la Convención para la protección de las personas respecto al proceso automatizado de los datos de carácter personal (T-PD). Informe de Situación relativo a la aplicación de los Principios de la Convención 108 a la recogida y al proceso de los datos biométricos. Elaborado por el T-PD en su 21ª reunión (Estrasburgo, 2-4 de febrero de 2005). T-PD (2005) BIOM F. Sitio de Internet: http://www.agpd.es/portalwebAGPD/canaldocumentacion/textos_interes/common/pdfs/informe-principios-convencion-108.pdf

XXII. Convenio para la Protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina. Convenio relativo a los derechos humanos y la biomedicina. Hecho en Oviedo el 4 de abril de 1997. Instrumento de Ratificación del Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina). BOE núm. 251 miércoles, 20 octubre 1999.

II. OCDE

XXIII. *Organisation for Economic Co-operation and Development. Directorate for Science, Technology and Industry. Committee for Information, Computer and Communications Policy*. Working Party on Information Security and Privacy. Biometric-based technologies. DSTI/ICCP/REG(2003)2/FINAL Unclassified. 30 de junio de 2004. Website: https://doi.org/10.1787/232075642747

XXIV. OECD (2011), "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers", *OECD Digital Economy Papers*, No. 186, OECD Publishing. http://dx.doi.org/10.1787/5kg1zqsm3pns-en

XXV. Recomendación adoptada por el Consejo de la OCDE el 23 de septiembre de 1980, por la que se formulan directrices en relación con el flujo internacional de datos personales y la protección de la intimidad y las libertades fundamentales", en *Documentación Informática*, Serie Amarilla,

Tratados Internacionales nº 2. Presidencia del Gobierno, Madrid, Servicio Central de Publicaciones, Servicio Central de Informática, 1982.

III. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

XXVI. *European Data Protection Supervisor. Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the Eupean Parliament and the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications* (COM (2006) 269 final)-2006/0088 (COD). Official Journal of the European Union 29.12.2006 C321/38. EN.

IV. PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA

XXVII. Reglamento (CE) Nº 767/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS). Diario Oficial de la Unión Europea L 218/60 de 13 de agosto de 2008. ES.

XXVIII. Reglamento (CE) Nº 810/2009 del Parlamento Europeo y del Consejo, de 13 de julio de 2009, por el que se establece un Código comunitario sobre visados (Código de visados). Diario Oficial de la Unión Europea L 243/1 de 15 de septiembre de 2009. ES.

XXIX. Reglamento (CE) 444/2009, de 6 de mayo - LCEur\2009\789 Modifica el Reglamento (CE) núm. 2252/2004 (LCEur 2004\3679), sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros. DOL 6 junio 2009, núm. 142, [pág. 1]; rect. DOL 18 julio 2009, núm. 188, [pág. 127].

XXX. Reglamento (CE) 2252/2004, de 13 de diciembre del Consejo de la Unión Europea. LCEur\2004\3679 Normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros DOL 29 diciembre 2004, núm. 385, [pág. 1, Núm. Págs. 6].

XXXI. Reglamento (CE) 390/2009, de 23 de abril, del Parlamento Europeo Y Consejo LCEur\2009\736 Modifica Instrucción consular común, de 22-12-2005 (LCEur 2005\3109), dirigida a las misiones diplomáticas y oficinas consulares de carrera en relación con la introducción de identificadores biométricos e incluye disposiciones sobre la organización de la recepción y la tramitación de las solicitudes de visado. DOL 28 mayo 2009, núm. 131, [pág. 1]; rect. DOL 22 octubre 2009, núm. 277, [pág. 54]

XXXII. Reglamento (CE) núm. 45/2001, del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

XXXIII. Reglamento (UE) n. 603/2013 del Parlamento Europeo y del Consejo de 26 de junio de 2013 relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) no 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) no 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia (refundición)

V. CONSEJO DE LA UNIÓN EUROPEA

XXXIV. Decisión 2008/633/JAI del Consejo de 23 de junio de 2008, de 23 de junio de 2008 sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades designadas de los Estados miembros y por Europol, con los fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves. Diario Oficial de la Unión Europea L 218/129 de 13 de agosto de 2008. ES.

XXXV. Reglamento (CE) Nº 2725/2000 del Consejo de 11 de diciembre de 2000 relativo a la creación del sistema “Eurodac” para la comparación de las

impresiones dactilares para la aplicación efectiva del Convenio de Dublín. Diario Oficial de la Comunidades Europeas L 316/1 de 15 de diciembre de 2000. ES.

XXXVI. Decisión Marco 2008/977/JAI del Consejo de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. DOUE L 350/60 30.12.2008.

VI. COMISIÓN DE LAS COMUNIDADES EUROPEAS

XXXVII. Decisión de la Comisión de 30 de noviembre de 2009 por la que se adoptan medidas técnicas de aplicación para introducir los datos y las solicitudes vinculados entre sí, acceder a los datos, modificar, suprimir y suprimir anticipadamente datos, conservar registros de operaciones de tratamiento de datos y acceder a ellos en el Sistema de Información de Visados [notificada con el número C(2009) 9402]. Diario Oficial de la Unión Europea L 315/30 de 2 de diciembre de 2009. ES.

XXXVIII. Decisión de la Comisión de 9 de octubre de 2009 por la que se establecen especificaciones sobre la resolución y el uso de impresiones dactilares a efectos de la verificación e identificación biométricas en el Sistema de Información de Visados [notificada con el número C(2009) 7435]. Diario Oficial de la Unión Europea L 270/14 de 15 de octubre de 2009. ES.

XXXIX. Comisión Europea. COM(97) Versión 3. Libro verde sobre la convergencia de los sectores de telecomunicaciones, medios de comunicación y tecnologías de la información y sobre sus consecuencias para la reglamentación, en la perspectiva de la sociedad de la información. Bruselas, 3 de diciembre de 1997. Disponible en la página web: http://www.euskalnet.net/oig/archivo/lvmedia.pdf

XL. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y Social Europeo y al Comité de las Regiones. La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI. COM(2012) 9 final. Bruselas 25 de enero de 2012.

XLI. Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de

datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos). COM(2012) 11 final. Bruselas 25 enero de 2012.

VII. TRATADOS INTERNACIONALES

XLII. Tratado del Reino de Bélgica, la República Federal de Alemania, el Reino de España, la República Francesa, el gran Ducado de Luxemburgo, el Reino de los Países Bajos y la República de Austria, relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal. Instrumento de ratificación de España del Convenio relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, hecho en *Prüm* el 27 de mayo de 2005.

XLIII. Tratado de la Unión Europea. Diario Oficial de la Unión Europea (DOCE) 30.3.2010. C83/13-45. https://www.boe.es/doue/2010/083/Z00013-00046.pdf [Fecha de consulta: 12/03/2017].

VIII. CÓDIGO DE CONDUCTA

XLIV. *Biometrics Institute Australia. Privacy Code. Approval of the Biometrics Institute Privacy Code Section* 18BB(2) *of the Privacy Act* 1988 (Cth). 19 july 2006.

IX. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

XLV. Agencia Española de Protección de Datos. Gabinete Jurídico. *Informe0082/2010.* https://www.aepd.es/informes/historicos/2010-0082.pdf [Fecha de consulta: 20/11/2018].

XLVI. Agencia Española de Protección de Datos. Gabinete Jurídico. *Proporcionalidad del tratamiento de la huella dactilar de alumnos de un colegio. Informe 368/2006.* Disponible en https://www.aepd.es/informes/historicos/2006-0368.pdf [Fecha de consulta: 23/11/2018].

XLVII. Agencia Española de Protección de Datos. Gabinete Jurídico. *Informe 0065/2015*. Disponible en https://www.aepd.es/informes/historicos/2015-0065.pdf [Fecha de consulta: 23/11/2018].

XLVIII. Agencia Española de Protección de Datos. Gabinete Jurídico. *Informe 073667/2018*. https://www.aepd.es/media/informes/2018-0046-investigacion-biomedica.pdf [Fecha de consulta:05/10/2018].

XLIX. Agencia Española de Protección de Datos. Gabinete Jurídico. *Informe 0324/2009*. Disponible en https://www.aepd.es/informes/historicos/2009-0324.pdf [Fecha de acceso: 19/10/2018].

L. *Memoria de la Agencia Española de Protección de Datos 1999*. "3.2.1.3. Tratamiento de la huella digital de los trabajadores por el empresario". Disponible en: https://www.aepd.es/media/memorias/memoria-AEPD-1999.pdf [Fecha de consulta: 10/10/2018].

X. CORTES GENERALES

LI. Cortes Generales, Diario de Sesiones del Congreso de los Diputados. Comisiones. Año 2005 VIII Legislatura Núm. 353 Constitucional. Presidencia del Excmo. Sr. D. Alfonso Guerra González. Sesión núm. 10 celebrada el miércoles, 28 de septiembre de 2005.

BIBLIOGRAFÍA

ABAD AMORÓS, M. R., *El carácter sensible de los datos biométricos.* Datos Personales – Núm. 4, septiembre 2003. vLex. http://vlex.com/vid/caracter-sensible-datos-biometricos-204792. [Fecha de consulta: 06/07/2016].

AGENCIA de los Derechos Fundamentales de la Unión Europea (FRA), *Manual de legislación europea en materia de la protección de datos,* Secretaría del Tribunal Europeo de Derechos Humanos, Consejo de Europa, Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2014.

ALEXY, R., *Teoría de los Derechos Fundamentales*, (Título original *Theorie der grundrechte.* Suhrkamp-Verlag 1986), Versión castellana Ernesto Garzón Valdés, Madrid, Centro de Estudios Políticos y Constitucionales, 2002.

ALONSO-FERNÁNDEZ, F., (*et al*), "*A review of schemes for fingerprint image quality computation"* en *Biometrics on the Internet*, Proceedings of Third COST 275 Workshop, University of Hertfordshire, United Kingdom 27 and 28 October 2005, Luxembourg: Office for Official Publications of the European Communities, 2006.

ÁLVAREZ GARCÍA, F. J., *El acceso por parte de las fuerzas y cuerpos de seguridad del Estado a ficheros de datos personales. Protección de Datos y proceso penal*, Madrid, La Ley, 2010.

ÁLVAREZ RIGAUDIAS, C., "El poder del usuario digital*",* en *Hacia un nuevo derecho europeo de protección de datos,* Valencia, Tirant lo Blanch, 2015.

APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de datos de carácter personal*, Navarra, Aranzadi, 2009.

ARZOZ SANTISTEBAN, X., *Videovigilancia, seguridad ciudadana y derechos fundamentales*, Navarra, Civitas, Thomson Reuters, 2010.

AVANZINI BLANCO, E., "Tecnologías para una asistencia sanitaria global: la telemedicina" en *Tecnologías del espacio aplicadas a la industria y servicios de la defensa.* Documentos de Seguridad y Defensa nº 41, Centro Superior de Estudios de la Defensa Nacional, Ministerio de Defensa, mayo de 2011.

BELL, D., *The coming of post-industrial society; a venture in social forecasting*, - New York, Basic Books [1973], - xiii, 507 p. illus. 25 cm. [traducción: Advenimiento de La Sociedad Post-Industrial. - Alianza (January, 1992). Ttraducción: *Vers la société post industrielle*. - Robert Laffont, 1976.

BENTHAM, J., *El Panoptico*, https://iedimagen.files.wordpress.com/2012/02/bentham-jeremy-el-panoptico-1791.pdf [Fecha de consulta:21/03/2018].

BYK, C., *La patente de genes humanos. El Derecho ante el Proyecto Genoma Humano*, vol. II, Bilbao, Fundación BBV, 1994.

CAMPUZANO TOMÉ, H., *Vida privada y datos personales. Su protección jurídica frente a la sociedad de la información*, Madrid, Tecnos, 2000.

CANCIO FERNÁNDEZ, R., *Datos biométricos, seguridad, protección de la vida privada y DNI* Cátedra Paz, Seguridad y Defensa, Observatorio PSyD, septiembre, 2015, disponible en: http://catedrapsyd.unizar.es/observatorio-psyd/opina/datos-biometricos-seguridad-proteccion-de-la-vida-privada-y-dni.html [Fecha de consulta: 02/08/2018].

CASAR CORREDERA, J. R., *Transformaciones audaces de las Tecnologías de la Información: los espacios, el conocimiento, los otros*, Real Academia de Doctores de España. Discurso de toma de posesión como académico de número, Madrid, 2016.

CANOSA USERA, R., *El Derecho a la Integridad personal*, Valladolid, Lex Nova, 2006.

CASSESE, A., *Los derechos humanos en el mundo contemporáneo*, Barcelona, Ariel, 1993.

CASTÁN TOBEÑAS, J., *Derecho Civil Español, común y foral. (*Tomo Primero, Introducción y Parte General. Vol. II Teoría de la relación jurídica. La persona y los derechos de la personalidad. Las cosas. Los hechos jurídicos), Madrid, REUS, 1984.

CASTELLS, M., *L´etá dell´informazione economica societá cultura*, Milano, Universitá Bocconi, 2004.

CAVOUKIAN, A., STOIANOV, A., "Guía de cifrado biométrico. Comisionado de Protección de Datos de Notario (Canadá)", *Revista Española de Protección de Datos. 2*, enero-junio, 2007, Madrid, Civitas, 2007.

CNIL (Biometría). https://www.cnil.fr/fr/biometrie-dans-les-smartphones-loi-informatique-et-libertes-exemption-ou-autorisation [Fecha de consulta: 27/05/2018].

Comisión Europea. COM (97) Versión 3. *Libro verde sobre la convergencia de los sectores de telecomunicaciones, medios de comunicación y tecnologías de la información y sobre sus consecuencias para la reglamentación, en la perspectiva de la sociedad de la información*, Bruselas, 3 de diciembre de 1997. http://www.euskalnet.net/oig/archivo/lvmedia.pdf [Fecha de consulta: 03/12/2017].

Comisión Europea. *Un Sistema Europeo Común de Asilo*. Oficina de publicaciones de la Unión Europea 2014. http://ec.europa.eu/dgs/home-affairs/e-library/docs/ceas-fact-sheets/ceas_factsheet_es.pdf [Fecha de consulta: 11/05/2016].

CORREA, M. (et al) La construcción de estándares legales para la vigilancia en América latina. Parte II: Reglas comparadas a nivel global, América Latina, Derechos digitales, 2018. Disponible en: https://creativecommons.org/licenses/by/4.0/deed.e [Fecha de consulta: 25/04/2019].

CORTÉS VÉLEZ, J. J., "Privacidad y seguridad en el universo digital" en *El Derecho*, Lefebvre ELDERECHO.COM

http://tecnologia.elderecho.com/tecnologia/internet_y_tecnologia/Privacidad-seguridad-universo-digital_11_1265680001.html [Fecha de consulta:28/08/2018].

DAVARA RODRÍGUEZ, M.A., *Manual de Derecho Informático*, Pamplona, Aranzadi, 1997.

DAVARA RODRÍGUEZ, M.A., "El concepto de fichero en la normativa sobre protección de datos", en Troncoso Reigada, A. (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de carácter personal*, Cizur Menor, Civitas, 2010.

DE ANTÓN y BARBERÁ, F., *Iniciación a la Dactiloscopia y otras Técnicas Policiales*, Valencia, Tirant Lo Blanch, Colección Ciencia policial, 2004.

DE CASTRO y BRAVO, F., "Los llamados derechos de la personalidad*", Anuario de Derecho Civil* X-XII, 1959.

DE MIGUEL ASENSIO, P.A., *Derecho privado de Internet*, Madrid, Civitas, 2000.

DE NICOLÁS, E., "Cloud computing: qué es y para qué se usa*"* en *Cloud computing: la nueva frontera de servicios tecnológicos. GEOECONOMÍA*, invierno, 2010-2011, Instituto Choiseul España y Instituto de Postgrado CEU, Cátedra de Geoeconomía y Estrategia Internacional, Madrid, 2010.

DEL PESO NAVARRO, E., RAMOS GONZÁLEZ, M.A., *La Seguridad de los Datos de Carácter Personal*, Madrid, Díaz de Santos, 2002.

DEL PESO NAVARRO, E., RAMOS GONZÁLEZ, M.A., *Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socioeconómicas*, Madrid, Díaz de Santos, 1994.

DIETRICH PLAZA, C., *El Tratado de Prüm en el marco de la regulación de protección de datos personales en la Unión Europea.* https://www.ugr.es/~redce/REDCE7/articulos/03cristinadietrichplaza.htm [Fecha de consulta: 31/07/2018].

ELVIRA PERALES, A., "Sipnosis artículo 18", disponible en http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2 [Fecha de consulta: 10 de abril de 2018].

ESCOBAR, G., *Introducción a la teoría jurídica de los derechos humanos*, Madrid, Cicode-Trama, 2005.

FERNÁNDEZ ESTEBAN, M.L., *Nuevas tecnologías, Internet y Derechos Fundamentales*, Madrid, McGrawHill, Monografía Ciencias Jurídicas, 1998.

GARCÍA-CUEVAS ROQUE, E., "La transparencia en el nuevo Reglamento Europeo de Protección de Datos", *Anales de la Real Academia de Doctores*, Vol 3, 2018.

GIONES-VALLS, A., SERRAT-BRUSTENGA, M., *La gestión de la identidad digital: una nueva habilidad informacional y digital*, disponible en: http://bid.ub.edu/24/giones2.htm [Fecha de consulta: 10/11/2018].

GÓMEZ SÁNCHEZ, Y., "Datos de salud como datos especialmente protegidos" en TRONCOSO REIGADA, A. (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de carácter personal*, Cizur Menor, Civitas, 2010.

GUÍA *para gestionar los datos personales*, Alianza Formación Gestión, Edición en formato digital: julio 2015, Madrid, Álvaro López-Amo Editor, 2015. Disponible en www.alianzaformacion.com [Fecha de consulta: 28/03/2016].

HEREDERO HIGUERAS, M., *La Directiva Comunitaria de Protección de los Datos de Carácter Personal*, Pamplona, Aranzadi, 1997.

HERRERA BRAVO, R., "El Derecho en la sociedad de la información: Nociones generales sobre el Derecho de las tecnologías de la información y las comunicaciones", en *Observatorio Iberoamericano de Protección de Datos*. Disponible en: http://oiprodat.com/2014/08/11/el-derecho-frente-a-la-sociedad-de-la-informacion/ [Fecha de consulta: 26/01/2019].

HERRERO-TEJEDOR, F., *Honor, intimidad y propia imagen*, Madrid, COLEX, 1994.

Instituto Nacional de Tecnologías de la Comunicación (INTECO). *Guía sobre las tecnologías biométricas aplicadas a la seguridad.* Instituto Nacional de Tecnologías de la Comunicación (INTECO), Observatorio de la Seguridad de la Información, Ministerio de Industria, Turismo y Comercio, Gobierno de España, octubre 2011.

Instituto Nacional de ciberseguridad de España, *Guías y estudios*. Disponible en: https://www.incibe.es/CERT/guias_estudios/guias/Guia_Identidad_Reputacion_usuarios [Fecha de consulta: 25/01/2019].

JAIN, A.K., BOLLE, R.M., PANKANTI, S. (editors), *Biometrics: Personal Identification in a Networked Society*, Kluwer Academic Piblishers, 1999.

JIMÉNEZ CAMPO, J., "Artículo 10.1" en Rodríguez-Piñero, M. y Casas Baamonde, M. E. (Dir.), *Comentarios a la Constitución española*, Tomo I, Conmemoración del XL Aniversario de la Constitución, Madrid, Wolters Kluwer, BOE, TC y Ministerio de Justicia, 2018.

KELSEN, H., *Esencia y valor de la Democracia*, Barcelona, ediciones Guadarrama, Punto Omega. Sección: Historia social y política, Número 233, 1977.

LAGE, J., "El cloud computing no está en la nube" en *Cloud computing: la nueva frontera de servicios tecnológicos GEOECONOMÍA*, invierno, 2010-2011, Instituto Choiseul España e Instituto de Postgrado CEU Cátedra de Geoeconomía y Estrategia Internacional, Madrid, 2010.

LEZERTUA, M., "El derecho a la vida privada y familiar en la jurisprudencia del Tribunal Europeo de Derechos Humanos", en *Perfiles del derecho constitucional a la vida privada y familiar*, Cuadernos de Derecho Judicial, Madrid, Consejo General del Poder Judicial, 1996.

LÓPEZ AGUILAR, J. F., "La protección de datos personales en la más reciente jurisprudencia del TJUE: los Derechos de la CDFUE como parámetro de validez del Derecho europeo, y su impacto en la relación transatlántica EU-EEUU*"* en *Teoría y Realidad Constitucional* núm. 39, 1º semestre 2017.

LÓPEZ DÍAZ, E., *El Derecho al honor y El Derecho a la Intimidad: Jurisprudencia y Doctrina,* Madrid, Dykinson, 1996

LORENTE ACOSTA, J. A., *El ADN y la Identificación en la Investigación Criminal y en la Paternidad Biológica,* Granada, Comares, 1995.

LUCAS, A., *Le droit de l`ìnformatique,* París, PUF, Themis, 1987.

LUCAS MURILLO DE LA CUEVA, P., "El derecho fundamental a la protección de los datos relativos a la salud*"* en *Estudios de Protección de datos de carácter personal en el ámbito de la salud*. Madrid Barcelona, Marcial Pons-Agencia Catalana de Protección de datos, 2006.

LLÁCER MATACÁS, M. R., *Protección de datos personales en la sociedad de la información y la vigilancia,* La Ley, Madrid, 2011.

LLÁCER MATACÁS, M. R., "La autodeterminación informativa en la sociedad de la vigilancia: Ubiquitous Computing*"* en *Protección de Datos Personales en la Sociedad de la Información y la Vigilancia,* Madrid, LA LEY, 2011.

LLEIXÀ ALSINA, À., *La economía colaborativa y el nuevo Reglamento. ¿Qué ocurre con mis datos?* http://www.abogacia.es/2017/11/06/la-economia-colaborativa-y-el-nuevo-reglamento-que-ocurre-con-mis-datos/?lang=es [Fecha de consulta: 5/12/2017].

MALTONI, D., Maio, D., JAIN, A.K., PRABHAKAR, S., *Handbook of Fingerprint Recognition,* Springer -Verlag. 2003.

MARTÍNEZ FERRE, A., https://psnsercon.com/blog/index.php/la-firma-biometrica-y-la-ley-de-proteccion-de-datos. [Fecha de consulta: 8/09/2016].

MARTÍNEZ PÉREZ, F. y POZA CISNEROS, M., *El Principio de Disponibilidad: Antecedentes Penales y Convenio de Prüm,* Nota de Servicio interior, Consejo General del Poder Judicial. Escuela judicial, Red Europea de Formación Judicial (REFJ), 5ª edición, 2013, http://www5.poderjudicial.es/cvcp12-13/CVCP13-09-ES.pdf [Fecha de consulta: 01/08/2018].

NEHF, J. P., *Recognizing the societal value in Information privacy,* 78 Wash. L. Rev. 1 2003.

NICOLÁS JIMÉNEZ, P., "El concepto de dato médico y genético" en RIPOL CARULLA, S. (ed.), BACARIA MARTRUS, J. (coord.). *Estudios de protección de datos de carácter personal en el ámbito de la salud*, Barcelona-Madrid, Agencia Catalana de Protección de Datos y Marcial Pons, 2006.

NICOLÁS JIMÉNEZ, P., *La protección jurídica de los datos genéticos de carácter personal*, Granada, Cátedra de Derecho y Genoma Humano-Editorial Comares, 2006.

OCDE Organisation for Economic Co-operation and Development. Directorate for Science, Technology and Industry. Committee for Information, Computer and Communications Policy. *Working Party on Information Security and Privacy. Biometric-based technologies*. DSTI/ICCP/REG(2003)2/FINAL Unclassified. 30 de junio de 2004. www.oecd.org/sti/security-privacy [Fecha de consulta: 20/01/2016].

OECD, "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers", *OECD Digital Economy Papers*, No. 186, OECD Publishing, 2011. Disponible en http://dx.doi.org/10.1787/5kg1zqsm3pns-en, [Fecha de consulta: 09/07/2016].

ORTÍ VALLEJO, A., *Derecho a la intimidad e informática, (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*, Granada, Comares, 1994.

PARDO FALCÓN, J., "Artículo 18.4. La protección de datos", en Rodríguez-Piñero, M. y Casas Baamonde, M. E. (Dir.), *Comentarios a la Constitución española*, Tomo I, Conmemoración del XL Aniversario de la Constitución, Madrid, Wolters Kluwer, BOE, TC y Ministerio de Justicia, 2018.

PEDRAZ PENALVA, E., "La utilización en el proceso penal de datos personales recopilados sin indicios de comisión delictiva" en *Protección de datos y proceso penal*, Madrid, LA LEY, 2010.

PERA, C., *Pensar desde el cuerpo. Ensayo sobre la corporeidad humana*, Madrid, Triacastella, 2006.

PÉREZ GÓMEZ, J. M., "La protección de los datos de salud", en Rallo Lombarte, A. y García Mahamut, R., (editores), *Hacia un nuevo derecho europeo de protección de datos*, Valencia, Tirant lo blanch, 2015.

PÉREZ SAN JOSÉ, P, (*et al*), *Guía sobre las tecnologías biométricas aplicadas a la seguridad*, INTECO (Instituto Nacional de Tecnologías de la Comunicación), Observatorio de la seguridad de la Información. Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Ministerio de Industria y Comercio, octubre 2011, https://www.incibe.es/CERT/guias_estudios/Estudios//estudio_biometria [Fecha de consulta: 25/01/2016].

PIÑAR MAÑAS, J. L., (*et al*), "Cuadro comparativo del articulado del Reglamento (UE) 2016/679 y la Directiva 95/46/CE" en Piñar Mañas, J.L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus, 2016.

PIÑAR MAÑAS, J.L., "El derecho fundamental a la protección de datos personales. Contenido esencial y retos actuales. En torno al nuevo Reglamento de Protección de Datos*"* en *Legislación de Protección de Datos*, Madrid, Iustel, 2011.

PIÑAR MAÑAS, J.L., *El derecho al olvido y las hemerotecas digitales*, Newsletter RedAbogacía Nº 64 – Julio 2018, Sección Actualidad TIC. Disponible en https://www.abogacia.es/2018/07/23/el-derecho-al-olvido-y-las-hemerotecas-digitales/?lang=es [Fecha de consulta: 01/08/2018].

PIÑAR MAÑAS, J.L., "Concepto de dato de carácter personal*"* en Troncoso Reigada, A. (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de carácter personal*, Cizur Menor, Civitas, 2010.

PIÑAR MAÑAS, J. L., "Consideraciones introductorias sobre el derecho fundamental a la protección de datos de carácter personal", *Revista Jurídica General*, Boletín del Ilustre Colegio de Abogados de Madrid nº 35, 3ª época, febrero 2007.

PIÑAR MAÑAS, J.L. *Derecho e innovación tecnológica. Retos de presente y futuro*, Madrid, CEU Ediciones, 2018.

REBOLLO DELGADO, L., *Vida Privada y Protección de datos en la Unión Europea*, Madrid, Dykinson, 2008.

REBOLLO DELGADO, L., SERRANO PÉREZ, M., M., *Manual de Protección de Datos*, Madrid, Dykinson, 2019.

REBOLLO DELGADO, L., "El derecho a la propia imagen y la imagen como dato", *Revista española de Protección de Datos*, 5 Julio-Diciembre, Thomson, Civitas, 2008.

RICO PÉREZ, F., "La individualización de la persona humana en el Derecho Civil*"*, *Revista General de Legislación y Jurisprudencia*, enero 1975, Reus, Separata.

RICO PÉREZ, F., *Las homonimias, como problema. (En torno al artículo 109 del Código Civil),* Separata del Boletín del Ilustre Colegio de Abogados de Madrid, Nº 1/1983.

RODOTÁ, S., *Tecnología y derechos fundamentales.* Conferencia pronunciada en los actos de inauguración de la sede de la Agencia Catalana de Protección de Datos, Barcelona, 2004. Disponible en http://www.apdcat.net/media/188.pdf. [Fecha de consulta: 10/04/2017].

RODOTÁ, S., *La vida y las reglas. Entre el derecho y el no derecho*, Madrid, Editorial Trotta Fundación Alfonso Martín Escudero, 2010.

ROMEO CASABONA, C. M., *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información*, Madrid, Fundesco, Colección Impactos, 1987.

RUIZ-GIMÉNEZ, J., RUIZ-GIMÉNEZ, I., "Artículo 10 Derechos Fundamentales de la Persona" en *Comentarios a la Constitución Española de 1978*, Madrid, Cortes Generales-EDERSA, 1997.

SAN JOSÉ i AMAT, C., "Los principios del Reglamento (UE) General de Protección de Datos (1)", en *Factor GDA*, 7 de marzo de 2017, disponible en: https://esaged.wordpress.com/2017/03/07/los-principios-del-reglamento-ue- general-de-proteccion-de-datos-1/ [Fecha de consulta: 05/11/2017]

SÁNCHEZ GONZÁLEZ, S., "Los derechos fundamentales en la Constitución Española de 1978*"* en *Dogmática y Práctica de los Derechos Fundamentales,* Valencia, Tirant lo blanch, 2006.

SÁNCHEZ-CARO, J., ABELLÁN, F., *Datos sobre la salud y datos genéticos, Su protección en la Unión Europea*, Granada, Comares, 2004.

SANTOLAYA, P., "El derecho a la vida privada y familiar (un contenido notablemente ampliado del derecho a la intimidad)", en *La Europa de los Derechos: El Convenio Europeo de Derechos Humanos,* Madrid, Centro de Estudios Políticos y Constitucionales, 2014.

SEGURA RODRÍGUEZ, A., *Reglamento Europeo de Protección de Datos. Licitud de tratamiento sin consentimiento explícito.* Disponible en https://elderecho.com/reglamento-europeo-de-proteccion-de-datos-licitud-de-tratamiento-sin-consentimiento-explicito [Fecha de consulta: 23/04/2019].

SEMPERE RODRÍGUEZ, C., "Artículo 18 Derecho al honor, a la intimidad y a la propia imagen" en ALZAGA VILLAAMIL, O. (Dir.), *Comentarios a las leyes políticas. Constitución española de 1978.* Tomo II, Madrid, EDERSA, 1984.

SIMÓN ZORITA, D., *Reconocimiento automático de patrones biométricos de huella dactilar,* Universidad Politécnica de Madrid. Escuela Universitaria de Ingeniería Técnica de Telecomunicación, 2004.

SOLINAS, C., "Tutela de la persona y tratamiento de los datos personales. Derecho interno y jurisprudencia del Tribunal Europeo de los Derechos Humanos y de las Libertades Fundamentales", en *Protección de Datos Personales en la Sociedad de la Información y la Vigilancia*, Madrid, LA LEY, 2011.

TRONCOSO REIGADA, A., *La protección de datos personales en busca del equilibrio,* Valencia, Tirant lo blanch, 2010.

ULL PONT, E., *Derecho público de la informática (Protección de datos de carácter personal),* Madrid, UNED, 2000.

VIDAL, M., *Moral de Actitudes. Moral Social,* Tomo III, Madrid, Perpetuo Socorro, 1981.

VILLAFÁÑEZ GALLEGO, R., "Los medios electrónicos en la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones Públicas", en *ELDERECHO.COM*, Lefevure, 8 de junio de 2016, disponible en: https://elderecho.com/los-medios-electronicos-en-la-ley-392015-de-1-de-octubre-del-procedimiento-administrativo-comun-de-las-administraciones-publicas [Fecha de consulta: 10/03/2019].

VILLAVERDE MENENDEZ, I., "Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993", *Revista Española de Derecho Constitucional*, Año 14 nº 41, agosto 1994, Madrid, Centro de Estudios Constitucionales, 1994.

VIZCAÍNO CALDERÓN, M., *Comentarios a la Ley Orgánica de Protección de Datos de carácter personal,* Madrid, Civitas, 2001.

ANEXO. Legislación sobre biometría en EEUU

- ***BIOMETRIC INFORMATION PRIVACY ACT*. ILLINOIS**

(740 ILCS 14/1)

Sec. 1. Short title. This Act may be cited as the Biometric Information Privacy Act. (Source: P.A. 95-994, eff. 10-3-08).

(740 ILCS 14/5)

Sec. 5. Legislative findings; intent. The General Assembly finds all of the following:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.

(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.

(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.

(f) The full ramifications of biometric technology are not fully known.

(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.
(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/10)

Sec. 10. Definitions. In this Act:

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency.

Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

"Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

"Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/15)

Sec. 15. Retention; collection; disclosure; destruction.

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric

identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(e) A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/20)

Sec. 20. Right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:

(1) against a private entity that negligently violates a provision o this Act liquidated damages of $1,000 or actual damages, whichever is greater;

(2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;

(3) reasonable attorneys' fees and costs, including expert witness fees and expert witness fees and other litigation expenses; and

(4) other relief, including an injunction, as the State or federal court may deem appropriate.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/25)

Sec. 25. Construction.

(a) Nothing in this Act shall be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person.

(b) Nothing in this Act shall be construed to conflict with the X-Ray Retention Act, the federal Health Insurance Portability and Accountability Act of 1996 and the rules promulgated under either Act.

(c) Nothing in this Act shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.

(d) Nothing in this Act shall be construed to conflict with the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004 and the rules promulgated thereunder.

(e) Nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/30)

Sec. 30. (Repealed).

(Source: P.A. 95-994, eff. 10-3-08. Repealed internally, eff. 1-1-09.)

(740 ILCS 14/99)

Sec. 99. Effective date. This Act takes effect upon becoming law.

(Source: P.A. 95-994, eff. 10-3-08.)

- ***BIOMETRIC IDENTIFIER STATUTE*** (replicada en el art. 503.001 de su Código de Comercio). **TEXAS**

Texas Business and Commerce Code - BUS & COM § 503.001. Capture or Use of Biometric Identifier:

(a) In this section, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.
(b) A person may not capture a biometric identifier of an individual for a commercial purpose unless the person:

(1) informs the individual before capturing the biometric identifier; and

(2) receives the individual's consent to capture the biometric identifier.

(c) A person who possesses a biometric identifier of an individual that is captured for a commercial purpose:

(1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless:

(A) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death;

(B) the disclosure completes a financial transaction that the individual requested or authorized;

(C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code; or

(D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant;

(2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other confidential information the person possesses; and

(3) shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires, except as provided by Subsection (c-1).

(c-1) If a biometric identifier of an individual captured for a commercial purpose is used in connection with an instrument or document that is required by another law to be maintained for a period longer than the period prescribed by Subsection (c)(3), the person who possesses the biometric identifier shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the instrument or document is no longer required to be maintained by law.

(c-2) If a biometric identifier captured for a commercial purpose has been collected for security purposes by an employer, the purpose for collecting the identifier under Subsection (c)(3) is presumed to expire on termination of the employment relationship.

(d) A person who violates this section is subject to a civil penalty of not more than $25,000 for each violation. The attorney general may bring an action to recover the civil penalty.

(e) This section does not apply to voiceprint data retained by a financial institution or an affiliate of a financial institution, as those terms are defined by 15 U.S.C. Section 6809 .

- ***BIOMETRIC PRIVACY ACT*. WASHINGTON**

Chapter 19.375 RCW
BIOMETRIC IDENTIFIERS

Sections

RCW 19.375.010

Definitions.

The definitions in this section apply throughout this chapter , unless the context clearly requires otherwise.

(1) "Biometric identifier" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. "Biometric identifier" does not include a physical or digital photograph, video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996.

(2) "Biometric system" means an automated identification system capable of capturing, processing, and storing a biometric identifier, comparing the biometric identifier to one or more references, and matching the biometric identifier to a specific individual.

(3) "Capture" means the process of collecting a biometric identifier from an individual.

(4) "Commercial purpose" means a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier. "Commercial purpose" does not include a security or law enforcement purpose.

(5) "Enroll" means to capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual.

(6) "Law enforcement officer" means a law enforcement officer as defined in RCW **9.41.010** or a federal peace officer as defined in RCW **10.93.020**.

(7) "Person" means an individual, partnership, corporation, limited liability company, organization, association, or any other legal or commercial entity, but does not include a government agency.

(8) "Security purpose" means the purpose of preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value, including tangible and intangible goods, services, and other purposes in furtherance of protecting the security or integrity of software, accounts, applications, online services, or any person.

[**2017 c 299 § 3.**]

RCW 19.375.020

Enrollment, disclosure, and retention of biometric identifiers.

(1) A person may not enroll a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose.

(2) Notice is a disclosure, that is not considered affirmative consent, that is given through a procedure reasonably designed to be readily available to affected individuals. The exact notice and type of consent required to achieve compliance with subsection (1) of this section is context-dependent.

(3) Unless consent has been obtained from the individual, a person who has enrolled an individual's biometric identifier may not sell, lease, or otherwise disclose the biometric identifier to another person for a commercial purpose unless the disclosure:

(a) Is consistent with subsections (1), (2), and (4) of this section;

(b) Is necessary to provide a product or service subscribed to, requested, or expressly authorized by the individual;

(c) Is necessary to effect, administer, enforce, or complete a financial transaction that the individual requested, initiated, or authorized, and the third party to whom the biometric identifier is disclosed maintains confidentiality of the biometric identifier and does not further disclose the biometric identifier except as otherwise permitted under this subsection (3);

(d) Is required or expressly authorized by a federal or state statute, or court order;

(e) Is made to a third party who contractually promises that the biometric identifier will not be further disclosed and will not be enrolled in a database for a commercial purpose inconsistent with the notice and consent described in this subsection (3) and subsections (1) and (2) of this section; or

(f) Is made to prepare for litigation or to respond to or participate in judicial process.

(4) A person who knowingly possesses a biometric identifier of an individual that has been enrolled for a commercial purpose:

(a) Must take reasonable care to guard against unauthorized access to and acquisition of biometric identifiers that are in the possession or under the control of the person; and

(b) May retain the biometric identifier no longer than is reasonably necessary to:

(i) Comply with a court order, statute, or public records retention schedule specified under federal, state, or local law;

(ii) Protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability; and

(iii) Provide the services for which the biometric identifier was enrolled.

(5) A person who enrolls a biometric identifier of an individual for a commercial purpose or obtains a biometric identifier of an individual from a third party for a commercial purpose pursuant to this section may not use or disclose it in a manner that is materially inconsistent with the terms under which the biometric identifier was originally provided without obtaining consent for the new terms of use or disclosure.

(6) The limitations on disclosure and retention of biometric identifiers provided in this section do not apply to disclosure or retention of biometric identifiers that have been unenrolled.

(7) Nothing in this section requires an entity to provide notice and obtain consent to collect, capture, or enroll a biometric identifier and store it in a biometric system, or otherwise, in furtherance of a security purpose.

[**2017 c 299 § 2.**]

RCW 19.375.030

Application of consumer protection act.

(1) The legislature finds that the practices covered by this chapter are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter **19.86** RCW. A violation of this chapter is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter **19.86** RCW.

(2) This chapter may be enforced solely by the attorney general under the consumer protection act, chapter **19.86** RCW.

[**2017 c 299 § 4.**]

RCW 19.375.040

Exclusions.

(1) Nothing in this chapter applies in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley act of 1999 and the rules promulgated thereunder.

(2) Nothing in this chapter applies to activities subject to Title V of the federal health insurance privacy and portability act of 1996 and the rules promulgated thereunder.

(3) Nothing in this chapter expands or limits the authority of a law enforcement officer acting within the scope of his or her authority including, but not limited to, the authority of a state law enforcement officer in executing lawful searches and seizures.

[**2017 c 299 § 5.**]

RCW 19.375.900

Finding—Intent—2017 c 299.

The legislature finds that citizens of Washington are increasingly asked to disclose sensitive biological information that uniquely identifies them for commerce, security, and convenience. The collection and marketing of biometric information about individuals, without consent or knowledge of the individual whose data is collected, is of increasing concern. The legislature intends to require a business that collects and can

attribute biometric data to a specific uniquely identified individual to disclose how it uses that biometric data, and provide notice to and obtain consent from an individual before enrolling or changing the use of that individual's biometric identifiers in a database.

[**2017 c 299 § 1.**]