UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE DERECHO

TESIS DOCTORAL

Regulación y realidad de las bases de datos médicos desde las perspectivas de la protección de datos y la salud

MEMORIA PARA OPTAR AL GRADO DE DOCTOR

PRESENTADA POR

Marta Vidal Raso

Director

Manuel Sánchez de Diego Fernández de la Riva

Madrid, 2017

UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE CIENCIAS DE LA INFORMACIÓN

TESIS DOCTORAL

REGULACIÓN Y REALIDAD DE LAS BASES DE DATOS MÉDICOS DESDE LAS PERSPECTIVAS DE LA PROTECCIÓN DE DATOS Y LA SALUD

Marta Vidal Raso

DIRECTOR

Dr. Manuel Sánchez de Diego Fernández de la Riva

Madrid, Octubre 2015

AGRADECIMIENTOS.

Han sido muchos años de estudio y de trabajo, en los que me he cruzado y convivido con muchas personas, que positiva o negativamente me han hecho reflexionar sobre las cuestiones que se ven reflejadas hoy en esta tesis.

Desde sus primeras páginas hasta las conclusiones, el trabajo dedicado ha sido fruto de la colaboración de multitud de personas, que, incluso sin saberlo, han influido de alguna forma en el contenido de este estudio.

Una de las partes más importantes de este estudio es sin lugar a duda la que viene a continuación, los agradecimientos, ya que cada uno de los mencionados han sido determinantes para que este trabajo haya podido concluirse.

Empezando por el ámbito universitario, quería agradecer su amabilidad y compromiso a Dª. Cristina Marín Echeverría de la biblioteca de la Facultad de Medicina de la Universidad Complutense de Madrid, así como a Dª. Beatriz García García, ayudante de la biblioteca de la Facultad de Ciencias de la Información de la Universidad Complutense de Madrid y a Dª. Ana Rodríguez Romero, ayudante de biblioteca de la Facultad de Derecho de la Universidad Complutense de Madrid. También quería agradecer su ayuda a Dª. María Isabel Serrano Maíllo, Profesora titular Interina de Derecho Constitucional de la Sección Departamental de Derecho Constitucional de la Facultad den Ciencias de la Información de la Universidad Complutense de Madrid, por haberse acordado durante estos años de mi tesis y sobre todo de mí. Igualmente a todos los profesores que en su día me impartieron los cursos del doctorado; A D. José Ignacio Bell Mallen, director de comunicación de IESE Madrid, a D. Teodoro González Ballesteros, catedrático de derecho constitucional, a D. Manuel Sánchez de Diego Fernández de la Riva, profesor titular de la Universidad Complutense de Madrid, quien como director de esta tesis, será merecidamente referido más adelante y, por ser la primera en introducirme en el estudio de la

materia de protección de datos de carácter personal, a Dª. Rosa María Abad Amorós, profesora titular de Derecho de la Información en la Facultad de Ciencias de la Información de la Universidad Complutense de Madrid, aunque ya no se encuentre entre nosotros, al igual que D. Luís Ortega Álvarez, Magistrado del Tribunal Constitucional y vecino, quien me aconsejó y apoyó en la decisión sobre el objeto de mi tesis. Ya en el plano personal a Dª. Nuria Terribas i Sala, directora de l'Institut Borja de Bioètica de la Universitat Ramon Llull de Barcelona, por su intereés en este estudio. De una forma muy especial quería agradecer a quienes se ocuparon mucho de mi salud en mi infancia y hoy por la de mis hijos, a la Dra. Gloria Pérez Tejerizo, Jefe Asociado en el Servicio de Cirugía Pediátrica de la Fundación Jiménez Díaz, y al Dr. Enzo Mario Digiuni Avaliz cirujano pediátrico en consultorios de San Lucas y en Las clínicas Pasteur, San Lucas Neo y San Lucas de la ciudad de Neuquén, gracias especialmente por vigilarme aquella primera noche después del accidente. También al Dr. Eduardo Adrián Cubillo Rodríguez, ginecólogo y amigo, por su forma de ver la medicina y la vida, y por mantener siempre la esperanza. Como gran amigo y fisioterapeuta, por su ánimo cuando solo había desconsuelo y por cuidarnos siempre tanto, a D. Felipe Herranz Pérez. A dos familias muy queridas, los “Enciso” y los “Mediavilla”, por haber compartido tantas cosas desde la infancia, y también a Belén y a Pilar, por ser tan buenas vecinas. A mis padrinos, Rafa y Puri, por estar siempre pendientes de mí, y a mi prima Arancha por estar a nuestro lado en cualquier circunstancia, espero de corazón que consiga todo lo que desea. Desde luego a Manuel, por dirigirme en este estudio, por apoyarme siempre y enseñarme que las cosas tienen que hacerse sin prisa pero sin pausa, gracias por darme la tranquilidad de estar a mi lado durante todos estos años. Ante todo a mis padres, Jose y Justi, ellos me han inculcado los valores que me han hecho la persona que hoy soy, gracias por vuestra bondad y generosidad, por enseñarme que la familia es lo primero, por ayudarme siempre que

lo necesito, y educarme a ayudar a los demás, sin vosotros no hubiese podido escribir esta tesis, al igual que sin mi hermana Virginia, a la que cito con gran cariño, porque ella fue la principal motivación de este estudio y sobre todo, por no decirme nunca que no cuando me hace falta. Por supuesto a mi marido Alberto, por estar siempre a mi lado, y por quererme tanto. Y en último lugar, pero en primero, a mis hijos, Pablo y Javier, porque ellos son el verdadero motor de mi vida.

RESUMEN.

La protección de datos de carácter personal es un derecho fundamental y autónomo, relativamente reciente, que tiene su origen en Europa y que se ha ido asumiendo lentamente en nuestro país, llegando a todos los sectores de la sociedad. Lo cierto es que este es un tema que ha calado profundamente en la población, pues últimamente observamos en la población una mayor preocupación por la protección de los datos de carácter personal. El vertiginoso avance que ha sufrido la tecnología, ha sido sin duda una gran ayuda para el tratamiento de los datos, pero también uno de los factores que genera más incertidumbre, que pone en peligro la seguridad de la información y preocupa a los ciudadanos.

En el ámbito de la medicina, los datos personales debido a la importancia que tienen para el paciente y para la salud en general, precisan de un régimen jurídico especial, así se establece en los artículos 7.3, 8 y 11.2.f) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Esta Ley y su reglamento de desarrollo se completan en el ámbito de la salud con una gran cantidad de normas sanitarias que hace difícil el cumplimiento de todas ellas. Los derechos de los pacientes son ampliamente regulados por esa normativa dispersa. Sin embargo, la adaptación de los centros sanitarios públicos y privados a la legislación existente, todavía en la actualidad presenta muchas carencias.

En el sector sanitario, tan necesario es el conocimiento de los datos de los pacientes por el personal que trabaja en los centros que les atienden, como la confidencialidad de los mismos. Es necesario encontrar un equilibrio entre la protección de los datos personales relativos a la salud y un imprescindible flujo de información entre los profesionales encargados de realizar su labor sanitaria. Es necesario que la información fluya de forma segura, garantizando la normativa de protección de datos, y así reforzar la relación médico-paciente,

como uno de los elementos esenciales en los procesos asistenciales.

En este sentido, el personal sanitario, y no sanitario, que maneja la información médica, se encuentra obligado a respetar una serie de principios, para que los datos relativos a la salud de los pacientes no se vean desprotegidos, y puedan sentirse vulnerables cuando sean atendidos a los centros a los que acudan. Por esta razón es fundamental que el sistema sanitario integre en su operativa, de una forma constante, la formación al personal que maneja los datos de los pacientes, para lo que es necesario que conozcan exactamente cuáles son sus funciones y obligaciones al respecto. La otra exigencia es la protección de los archivos y sistemas informáticos.

Se trata en definitiva de una cuestión de concienciación y constancia, el que la protección de los datos de carácter personal se instaure definitivamente en la actividad global que se lleva a cabo en España en materia sanitaria. La continuidad en la aplicación de las normas existentes en materia de protección de datos, conseguirán que el sector de la medicina sea seguro para todos, sin menoscabo de la función asistencial que tiene encomendada.

ABSTRACT.

The protection of personal data is a fundamental and autonomous law, relatively recent, that has its origin in Europe and that has been slowly assumed in our country, reaching all sectors of society. The truth is that this is an issue that has deeply permeated the population, as we can recently note a greater concern for the protection of data of a personal nature. Undoubtfully, the rapid advance of technology, has been a great help for the treatment of the data, but has also been one of the factors that generates more uncertainty, which endangers the security of the information and concerns citizens.

In the field of medicine, due to the importance that personal data have for the patient and the health in general, they require a special legal regime, and so is established in the articles 7.3, 8 and 11.2. f) of the organic law 15/1999, of 13 December, of protection of data of a Personal nature. This law and its regulations are completed in the field of health with a lot of health standards, which makes it difficult to comply with all of them. The rights of patients are widely covered by that scattered regulations. However, the adaptation of public and private health centers to existing legislation, still today has many shortcomings.

In the health sector, so necessary is the knowledge of patient data by the staff working in the centers that cares for them, as well as the confidentiality thereof. It is necessary to find a balance between the protection of personal data concerning health and the essential flow of information among professionals carrying out the health work. It is also necessary the safely flow of information, guaranteeing data protection rules, and thus strengthen the doctor-patient relationship as one of the essential elements in the healthcare process.

In this sense, health and non-health personnel handling medical information, is obliged to respect a series of principles for data on the health of patients are not disadvantaged, and can be vulnerable

when they are attended on a medical center. For this reason it is essential that the health care system integrates into its operational, in a consistent manner, the training of the staff that handles the patient data, for which they need to know exactly what their roles and responsibilities in this regard are. The other requirement is the protection of files and computer systems.

This is ultimately a question of awareness and perseverance that the protection of personal data is finally put in place in the overall activity carried out in Spain in health care. The continuity on the implementation of the existing rules on data protection will get a medical sector safe for all, without prejudice to the care task that it has entrusted.

ÍNDICE.

I. INTRODUCCIÓN.

¿Por qué un médico se queda fuera de su horario de trabajo, vigilando el estado de una niña que entra en el servicio de urgencias de un hospital, con pronóstico muy grave, hasta ver algún síntoma de evolución favorable? La respuesta es la vocación. Quizás sea esto lo que me ha impulsado a investigar sobre el sector médico, en relación con la protección de datos personales.

Vinculada desde pequeña al mundo de la medicina como paciente, cobro conciencia a lo largo de muchos años de la vocación del personal sanitario. Más recientemente con el revés de salud de alguien muy cercano, que supone una nueva ligadura familiar al mundo de la medicina. Además mi profesión como abogada se ha orientado hacia la protección de datos personales, por lo que entiendo la gran importancia del manejo de datos personales relativos a la salud en el proceso de curación de los pacientes, pero también la necesidad de proteger los datos personales.

Cuando los problemas de salud irrumpen en el ámbito personal, supongo que a todos nos invade el ansia por buscar cuantas soluciones sean válidas para acelerar el proceso de bienestar y curación de los nuestros, por imposibles que parezcan. Quizás es aquí donde hay que ir un poco más allá y dejarse llevar por nuestro lado más instintivo, para a lo mejor descubrir cosas que por habernos parecido descabelladas en un principio, podrían suponer una gran ayuda en el mundo de la medicina.

Pese a que no tengo conocimientos en materia sanitaria, esta inquietud personal me ha llevado a querer conocer más sobre los protocolos existentes en este ámbito, respecto del tratamiento de los datos de carácter personal relativos a la salud.

Sin duda ha ayudado a comenzar este proceso de investigación mi dedicación plena, en el ámbito laboral, al área de la protección de los datos de carácter personal. La actividad y continuo aprendizaje

en este nuevo sector del Derecho, han potenciado mi interés por esta faceta de la protección de los datos de carácter personal en el sector de la medicina.

II. HIPÓTESIS.

La principal pregunta, e hipótesis de este estudio es si podría encontrarse el modo de poner a disposición de los profesionales médicos esa riqueza de diagnósticos, pruebas, síntomas, tratamientos, experimentos, reacciones y resultados contenidos en las historias clínicas de los pacientes, que a lo largo de los años han ido constituyendo una gran base de datos, que puestos en común, podrían suponer una gran riqueza para la medicina del presente y del futuro. Todo ello debería hacerse, sin duda, de forma disociada con el fin de preservar la intimidad de los pacientes y el derecho a la protección de sus datos personales, ya que son estos derechos distintos y autónomos, como se explicará más adelante.

Sería así posible que existiera una gran base de datos, quizás por comunidades, provincias, países o continentes, en la que de forma anónima, se expusiese el contenido de las historias clínicas, para que esto pudiera servir de ayuda a otros profesionales de la salud. Podrían quizás encontrarse con un caso parecido a otro que pudiese existir y del que no tuviese conocimiento, para "aprovecharse" de esa experiencia y, con ello, ayudar quizás a la curación de otros pacientes. La idea es rentabilizar al máximo todos los recursos existentes, aunque desconocidos por no estar compartidos.

Podría, por ejemplo, diseñarse un programa organizado por campos que pudiesen ser consultados de forma separada, solo los casos de una determinada enfermedad o sintomatología (si la enfermedad no está diagnosticada), en mujeres o varones de una misma raza o edad, por ubicación geográfica, hábitos alimenticios, peso, viajes realizados recientemente, etc., para poder observar y comparar las pruebas y el comportamiento de la evolución de un paciente ante determinados estímulos y, así tener en cuenta estas referencias a la hora de tratar al nuevo paciente coincidente en

síntomas, edad, sexo, ubicación geográfica, peso, viajes realizados, etc.

Se trataría de un acercamiento geográfico e institucional con un fin sanitario claro, del que a priori se me ocurren innumerables ventajas. ¿O es que acaso no existe la obligación para todas las empresas españolas de registrarse en ciertos organismos públicos e incluso de exhibir sus cuentas en aras de la transparencia? ¿No sería por tanto igual o más válido aún, poner en común del sector médico cierta información al servicio de la medicina, aún más a favor de la transparencia recientemente regulada?

Esta es la propuesta que más adelante analizaré en detalle, y que constituye el interrogante de mi tesis. Quizás sea solo una ilusión, pero ésta, la ilusión, es sin duda un gran aliciente, de hecho creo personalmente que es necesaria para el curso de la vida, llámese como se quiera llamar, ilusión, energía o motivación.

No obstante, a lo largo de los años de estudio que llevo dedicados al Derecho en general, a la protección de datos en particular, y especialmente en los invertidos en el doctorado, he comprobado complacida, que esta idea, mi hipótesis, ya ha sido barajada por otros, y que ya existen programas en el sector sanitario, que funcionan a nivel de comunidades autónomas, y en los que los profesionales de la medicina incluyen datos de los procesos asistenciales de los pacientes, para que estos puedan ser conocidos por otros profesionales, que puedan aprovechar esas experiencias. Este es el caso del programa Horus utilizado en algunos hospitales de la comunidad de Madrid. Sin embargo, son aplicaciones que no están todavía demasiado perfiladas, ya que no exigen una gran cantidad de campos obligatorios, dejando al entender del profesional que plasma los datos en ella, el contenido y los detalles que en mayor o menor medida hagan constar; esto sin duda puede dar mucha riqueza o por lo contrario pobreza a lo que se quiera compartir con el resto de profesionales, probablemente la mayoría

de las veces por la falta de tiempo que nos oprime en la sociedad en la que vivimos.

III. CONSIDERACIONES PREVIAS.

El derecho a la intimidad de las personas era considerado en sus orígenes como "*el derecho a estar solo*", pero en este derecho se han implicado otros factores que rompen ese inicial carácter individualista.

Con el ritmo que lleva la sociedad, muchas veces se nos olvida lo esencial, que son los derechos de las personas. En concreto el derecho a la protección de datos personales, que procede, como se verá más adelante, del derecho a la intimidad. A propósito de este último, y de otros que también serán nombrados, traigo a las primeras líneas de mi estudio una frase del Catedrático Teodoro González Ballesteros, en la que sostiene que: *"El derecho al honor comprende también el derecho a la intimidad personal y familiar y a la propia imagen (art.18.1 CE), porque en el fondo, su naturaleza esencial, que es la dignidad de la persona, representa el común denominador de los tres derechos fundamentales"*[1]. Y es que la protección de datos personales, como descendiente del derecho a la intimidad, participa también de esta afección, porque aunque sea el primero un derecho autónomo, es también derecho fundamental, y si se vulnera, daña sin duda la dignidad de la persona, al igual que en los otros derechos citados.

El concepto de intimidad ha sido estudiado y analizado por diversos métodos tanto etimológicos y semánticos, que parten del significado de lo íntimo como "*lo más interno*", así como históricos, que se basan en la aparición en todas las culturas de este término, desde el Derecho Romano hasta nuestros días.

En estos principios solo se entendía el valor negativo de la intimidad a no permitir que nadie entrase en esta faceta reservada de la vida de las personas, pero posteriormente se ha ido valorando

[1] GONZÁLEZ BALLESTEROS, Teodoro: *"El Honor en el contexto"*. Cuadernos de Periodistas · Diciembre de 2010. Pág 120.

también el sentido positivo del ser humano a poder defenderse de esos ataques.

Respecto al sentido positivo y negativo de la intimidad, se manifiesta una corriente doctrinal que afirma que: "*Dentro de la protección de la intimidad es posible diferenciar una dualidad de aspectos o facetas que si bien comparten el mismo fundamento explicativo de la tutela de aquel derecho resultan, sin embargo, nítidamente diferenciables. Se trata de sus vertientes negativa y positiva que de forma clásica reconoce la doctrina y la jurisprudencia. Con la primera de ellas que, como recordábamos más arriba es la que inspiró sus primeras formulaciones, se hace referencia a una pretensión de exclusión absoluta de conocimiento de los datos reservados frente a terceros*"[2].

Lo comparan entrando en el ámbito sanitario respecto del que establecen que "*así caracterizado, no debe pasarse por alto que el ámbito de la información relativa a la salud es, además, uno de los mejores exponentes de la singular vulnerabilidad de los datos personales en la sociedad actual y que, como ya advertíamos en las consideraciones introductorias, aparece condicionada, entre otros factores, por las posibilidades que proporciona el uso de la informática y, en general, las nuevas técnicas asociadas a la misma. Baste pensar que la gestión del sistema sanitario ha estado marcada de forma singular en los últimos años por la informatización en la prestación de los servicios, y puede augurarse sin temor a errores que en el futuro lo estará aún más. Sirvan como ejemplos la utilización de la historia clínica electrónica, la tarjeta sanitaria, la receta electrónica o incluso la posibilidad de utilizar la red como medio para proporcionar asistencia sanitaria personalizada*"[3]. Y

[2] GÓMEZ RIVERO, María del Carmen: *"La protección penal de los datos sanitarios. Especial referencia al secreto profesional médico".* Editorial Comares, S.L., Granada, 2007. Pág. 21.

[3] GÓMEZ RIVERO, María del Carmen: *"La protección penal de los datos sanitarios. Especial referencia al secreto profesional médico".* Editorial Comares, S.L., Granada, 2007. Pág. 35.

concretan que "*ya en el específico ámbito sanitario, esta comprensión funcional de la afectación a la intimidad, que en relación con los profesionales prescinde de la entidad del dato para poner el acento en el deber de sigilo, se confirma a través de un recorrido por la red normativa relacionada con los profesionales de la salud, una indagación que, dicho sea de paso, debido a la ausencia de una ley que de modo unitario contemplase la regulación del secreto médico, obliga a acudir a la dispersa normativa que hace referencia al secreto profesional*"[4].

De modo que "*el recorrido por la configuración actual del derecho a la intimidad quedaría incompleto si no se hiciera referencia a una de las vertientes del mismo que, por su actualidad y creciente importancia, ha dado paso incluso a la discusión más amplia en torno a si debe caracterizarse como un derecho autónomo. Me refiero al que se ha dado en llamar como derecho a la protección de los datos personales y, relacionado con él en cuanto una de sus más importantes facetas, la libertad informática, que afecta fundamentalmente a la vertiente positiva de la protección de la intimidad*"[5].

Esta preocupación por la dispersidad normativa que tenemos en la actualidad, y que provoca en muchas ocasiones duplicidad en las distintas regulaciones, es compartida por algunos que opinan que la solución está en una norma sanitaria global. Pero por otro lado, esta sería difícil del confeccionar y actualizar por su magnitud. No podemos olvidar que las leyes están en constante cambio.

Por otro lado, el gran avance tecnológico surgido en los últimos tiempos, reduce sin duda el espacio y el tiempo, ayudando al acercamiento de los recursos utilizados en el sector sanitario, lo cual juega en beneficio de las comunicaciones, necesarias hoy en día en casi todos los sectores de actividad, y por tanto también en el

[4] Ibídem. Pág. 38.

[5] Ibídem. Pág. 41.

sanitario. Sin embargo, la tecnología es, en este aspecto, un arma de doble filo, ya que a la vez que transmite información a cualquier parte del mundo en pocos segundos, también la hace más vulnerable durante su viaje y recepción, por las innumerables y constantes formas que aparecen continuamente para burlar los sistemas de seguridad informática. Los *hackers* informáticos están a la orden del día, lo vemos continuamente en las noticias e incluso en la vida diaria que nos rodea.

Muestra de la doble cara de la tecnología, es el caso que publica el diario El País: *"El desconocimiento tecnológico de algún empleado de una clínica ginecológica pudo llevarle a poner a disposición del programa eMule (el más popular de intercambio de archivos entre particulares), y por lo tanto al alcance de millones de personas, todos estos datos, contenidos en una carpeta del disco duro del ordenador. No se sabe con exactitud quien ha sido el culpable, ni las razones de la filtración, pero la Agencia Española de Protección de Datos (AEPD) acaba de sancionar a la clínica, el Centro Médico Lasaitasuna, en Bilbao, con 150.000 euros"*[6] .

Con el título "Sanidad <on line>: 17 autonomías, una sola red", publica Diario Médico que: "Petición de cita a través de internet, gestión de reclamaciones y quejas, consulta de información sanitaria, registro de voluntades anticipadas…Estos son los más comunes, pero solo unos pocos de los servicios interactivos que las regiones han ido implantando para relacionarse electrónicamente con sus ciudadanos"[7]. Lo cual nos hace ver la facilidad de gestión que ofrece la tecnología en una sociedad colapsada en la que se agradece cualquier tipo de avance.

Esta era de la informática en la que vivimos, pone al alcance de nuestra mano una gran variedad de productos cada vez más

[6] C.BELAZA, Mónica: "4.000 historias clínicas de abortos se filtran en la Red a través de eMule". El País, viernes 25 de abril de 2008, vida & artes, Madrid. Pág 34.

[7] SIERRA, Rosalía: "Sanidad <on line>: 17 autonomías, una sola red". Diario Médico, martes 17 de marzo de 2009. Pág 25-Especial Inforsalud 2009.

sofisticados, de los que se irán viendo algunos ejemplos a lo largo de este estudio, así como especialistas en la materia, por lo que hay que extremar la vigilancia para que su uso sea adecuado. Por ello, creo necesario aumentar el control informático de las entidades que almacenen información relativa a la salud de los individuos, ya que una fuga de la misma, podría causar graves daños a las personas, desde la perspectiva de la protección de datos. Podrían incluso, con el impulso de la tecnología, reducirse los plazos establecidos sobre la aplicación de las medidas en función del volumen de información o complejidad de los recursos que la tratan; y así intentar lograr con ello el máximo control en el menor tiempo posible, en beneficio de la seguridad de los datos. En este sentido, cada persona que maneja datos de salud, en sus distintos niveles y puestos de trabajo, deben estar involucrados al máximo en la seguridad de los datos, contribuyendo a formar una cadena de protección entre las distintas secciones para intentar conseguir un proceso completo. Para esto es fundamental una buena coordinación y formación del personal en lo que a protección de datos se refiere.

La información es en este sentido esencial dentro de nuestra sociedad, y también, por supuesto, en el sector sanitario. María Teresa Fernández Bajón lo expresa de forma muy clara cuando asegura que: *"La información se ha convertido en una variables estratégica de primer orden de la gestión de cualquier institución o empresa. Vivimos en la sociedad de la información"*[8].

Un sector de la doctrina manifiesta respecto al desarrollo de las nuevas tecnologías que "*nunca como ahora se ha podido acceder a contenidos académicos y científicos, políticos, económicos, culturales, etc., y a grandes bases de datos de manera inmediata. La información generada a través de los sistemas informáticos e internet se ha convertido en un valor sin precedentes al conseguir*

[8] FERNÁNDEZ BAJÓN, María Teresa: *"La profesión del documentalista: Apuntes para una reflexión"*. Boletín de la ANABAD, Tomo 48, Nº 2, 1998. Págs. 295-308.

una inimaginable capacidad de almacenamiento, acceso y operatividad en tiempo real. Es indudable que, en general, estas innovaciones científicas y tecnológicas han permitido incrementar la capacidad de progresar en todos los aspectos de la vida humana, convirtiéndose en herramientas casi esenciales tanto para la vida pública como privada. En general, las consecuencias inmediatas del desarrollo de la sociedad de la información han hecho que el mundo sea más pequeño y asequible, pero inabarcable por la cantidad de contenidos informacionales y la velocidad a la que éstos se generan"[9]. Pero por otro lado pone de manifiesto esta corriente que "*si los beneficios que han proporcionado el progreso tecnológico para las sociedades contemporáneas son incuestionables, estas ventajas vienen acompañadas de nuevos desafíos que hay que abordar ineludiblemente. El mal uso de la información, sobre todo de carácter personal, en la utilización de las nuevas tecnologías se pone de manifiesto en los casos de intrusión en la intimidad de las personas. Los actuales sistemas información y la comunicación se han convertido en la mayor amenaza a la intimidad porque cuentan con sofisticadas herramientas de vigilancia generalizada, bases de datos masivas y la capacidad de almacenar y distribuir la información en todo el mundo a tiempo real*"[10.] Además el progreso tecnológico avanza más rápido que la vida y así lo manifiestan estos mismos autores al asegurar que "*hablar a día de hoy, con propiedad de las modernas tecnologías de la información o la comunicación resulta casi imposible. La celeridad con la que evolucionan hace que tan pronto como centramos nuestra atención y nuestro tiempo en el estudio de las repercusiones jurídicas que el uso de alguna de sus últimas manifestaciones puede tener, ésta deje de ser considerada como moderna, para pasar a ser rápidamente abandonada, tras un*

9 ARRIBAS LEÓN, Mónica, CARRIZOSA PRIETO, Esther, CARRUSO FONTÁN, Viviana, GALAÁN MUÑOZ, Alfonso, HOLGADO GONZÁLEZ, María, LUCENA CID, Isabel Victoria, TOSCANO GIL, Francisco. *"La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación".* Tirant Lo Blanch, Valencia, 2014. Pág. 17.

10 Ibídem.

brevísimo periodo de reinado y fascinación, ante la imparable irrupción de otra más nueva, más atractiva y generalmente más eficaz, que convierte a la anterior en obsoleta y la condena a la desaparición o al ostracismo"[11].

Otra parte de la doctrina ha puesto de manifiesto que "*el riesgo de que se vulneren los datos informáticos, que como venimos insistiendo planea de forma general sobre cualquiera de ellos con independencia de su contenido, resulta singularmente acuciante cuando la información almacenada se refiere a aspectos especialmente sensibles y, entre ellos, los relativos a la salud. Al respecto ha influido sin lugar a dudas el uso generalizado de internet, ya que, como recuerda Pérez Luño, la circulación de datos relacionados con la salud en la red ha corrido paralela al creciente uso de aquél*"[12].

Respecto a la sensibilidad de los datos de salud que ocupan este estudio, el informe jurídico de la AEPD 0367/2009 establece que "*la especial protección conferida a los datos relacionados con la salud de las personas no es arbitraria, sino que resulta de lo dispuesto en las normas Internacionales y Comunitarias reguladoras del tratamiento automatizado de datos de carácter personal. En este contexto, tanto el artículo 8 de la Directiva 95/46/CE del Parlamento y del Consejo, así como el artículo 6 del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, ratificado por España en fecha 27 de enero de 1984, hacen referencia a los datos de salud como sujetos a un régimen especial de protección*".

Hoy en día, las llamadas Tecnologías de la Información y la Comunicación (TIC), están presentes en todos los ámbitos de la

11 Ibídem. Pág. 203.

12 GÓMEZ RIVERO, María del Carmen: *"La protección penal de los datos sanitarios. Especial referencia al secreto profesional médico".* Editorial Comares, S.L., Granada, 2007. Pág. 42

sociedad. Respecto a este tema Aberasturi Gorriño manifiesta que "*La Historia de la Humanidad está compuesta por distintas etapas que se unen por eslabones de cambio, espacios de tiempo en los que uno o varios factores hacen que distintos aspectos de la vida se vean inmersos en un proceso de transformación. Antes fueron la rueda, la máquina de vapor, la electricidad, la imprenta, y ahora son las TIC: el teléfono, el ordenador, internet, etc. Las que sitúan a la sociedad en uno de esos intervalos que dan paso a una nueva etapa*"[13]. Y es que este autor sostiene que "*Las TIC se han incorporado prácticamente a todos los ámbitos en los que se desarrolla la vida y los centros sanitarios no han constituido una excepción. En la práctica sanitaria la manipulación de datos constituye una actividad fundamental, si no la más importante. En el ejercicio de la medicina la práctica totalidad de funciones están relacionadas de alguna manera con la información y se puede afirmar que el sanitario es uno de los sectores en que la información adquiere mayor trascendencia*"[14]. Y ello debido, asegura, a que "*la cantidad de datos referidos a nuestras personas o a nuestras vidas que circulan por la red y que, en consecuencia, están almacenados no en uno, sino en cientos de ordenadores, no ha dejado de crecer, como tampoco lo ha hecho el número de los que se han convertido en instrumentos esenciales de nuestra vida personal o profesional*"[15].

Publica Diario Médico a este respecto que: *"Las tecnologías de la información y de la comunicación (TIC) son una parte de la gestión sanitaria, y la gestión sanitaria… es una parte de las TIC, o por lo*

[13] ABERASTURI GORRIÑO, Unai: *"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 25.

[14] Ibídem. Pág. 26.

[15] ARRIBAS LEÓN, Mónica, CARRIZOSA PRIETO, Esther, CARRUSO FONTÁN, Viviana, GALAÁN MUÑOZ, Alfonso, HOLGADO GONZÁLEZ, María, LUCENA CID, Isabel Victoria, TOSCANO GIL, Francisco: *"La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación"*. Tirant Lo Blanch, Valencia, 2014. Pág. 204.

menos debería serlo si quiere que este sector despegue"[16]. De lo que se desprende la necesidad de la tecnología en la actualidad en el sector sanitario.

En este mismo sentido, manifestaba unos días antes este mismo diario que: *"Ya queda poco para que las tecnologías de la información y de la comunicación empiecen a explotar su gran potencial en la sanidad".* Y que*: "La interconexión de los sistemas es una de las prioridades de unas TIC que optimizarán los recursos hospitalarios reduciendo costes y elevando la atención"*[17].

En cuanto al uso de las nuevas tecnologías, ha manifestado igualmente Aberasturi Gorriño que, respecto a su aplicación en el sector sanitario "*las distintas administraciones, conscientes de esa necesidad, han impulsado constantemente ese proceso de informatización. En el ámbito europeo el plan estratégico Europa 2020 incorpora diferentes elementos vinculados con esta materia atendiendo a lo marcado por el Plan de Acción a favor de un Espacio Europeo de la Salud Electrónica. Este plan señala una serie de objetivos a cumplir a largo plazo. Probablemente uno de los mayores retos que se plantea es el de la interoperabilidad de los sistemas de información, con el fin de que la información pueda fluir entre los diferentes estados. En el ámbito estatal, en el marco del Plan Avanza, se pretende propiciar una mejor asistencia y, sobre todo, una mayor movilidad de los pacientes por todo el territorio estatal. Los principales proyectos se centran sobre todo en crear la posibilidad de intercambiar información clínica entre CCAA a través del Nodo Central del Sistema Nacional de Salud. Así como de crear un sistema de intercambio de información asociada a las recetas electrónicas entre las CCAA a través del mismo Nodo, y promover los proyectos autonómicos de historias clínicas y recetas*

[16] RODRíGUEZ CRENAS; David: "Generando una red de conocimiento de las TIC". Diario Médico, lunes 19 de julio de 2010. Año XIX, Núm.4156. Pág 16.

[17] Ibídem. Pág 18.

electrónicas"[18]. Así concluye el autor que *"…uno de los principales retos que plantea la incorporación de las nuevas tecnologías en el ámbito sanitario es el aumento de las posibilidades de manipular la información relativa a la salud de las personas y el peligro que ello genera de que el derecho a la protección de datos de los usuarios se vea afectado negativamente*"[19].

Lucas Murillo de la Cueva expresa respecto a la utilización de la tecnología que *"…el uso informático incontrolado de los datos personales es lo que puede producir perjuicios en múltiples derechos de los individuos. Se trata, por consiguiente, de determinar si el derecho al honor y el derecho a la intimidad personal y familiar –o sea, las otras referencias del artículo 18.4 de la Constitución- son idóneos para suministrar el soporte material sobre el que descansa la técnica de la protección de datos*"[20].

Otra parte de la doctrina, manifiesta igualmente el doble filo de las nuevas tecnologías al asegurar que "*nadie va a poner en duda a estas alturas, las considerables ventajas que, en términos de eficacia y gestión de la información, ofrecen las nuevas tecnologías, en materias tales como acceso y transmisibilidad de la misma. Pero tampoco parece razonable olvidar que en idéntica proporción a las ventajas que suministra, las nuevas tecnologías suponen un potencial peligro para la intimidad de los pacientes cuya información es así almacenada, y dificultan notablemente la delimitación e incluso la exigibilidad del correlativo deber de sigilo*"[21].

---

[18] ABERASTURI GORRIÑO, Unai, "La protección de datos en la salud". Editorial Aranzadi, S.A., Navarra, 2013. Pág. 27.

[19] Ibídem. Pág 34.

[20] LUCAS MURILLO DE LA CUEVA, Pablo. "*Informática y Protección de Datos Personales"*, Centro de Estudios Constitucionales, Madrid 1993. Pág. 28.

[21] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso. *"La protección de datos personales en el ámbito sanitario"*, Editorial Aranzadi, Navarra 2002. Pág. 21.

En este mismo sentido, pero respecto al ámbito de la sanidad de forma más específica, Cristina Centeno Soriano mantiene por su parte que "*sin extendernos en los avances tecnológicos en el campo sanitario, si queremos, sin embargo, realizar una reflexión sobre los cambios que está experimentado el formato original de la historia clínica. En la historia clínica informatizada, la información se captura de forma mecanizada y ésta se organiza en sistemas masivos de almacenamiento de información. En este contexto, el médico no utilizará el papel y el bolígrafo para escribir, sino sistemas que permitan el registro de los datos directamente en estructura binaria*"[22]. Así, asegura esta autora, "*en la historia clínica digitalizada, los documentos se digitalizan, pero la captura de los datos se realiza de manera tradicional, sin exigencias de definición de elementos informáticos mínimos, ni de organización de una arquitectura especial. En las historias digitalizadas se utilizan sistemas masivos de almacenamiento como los CD-ROM*"[23]. Y "*aunque las perspectivas abiertas por las nuevas tecnologías de la información apuntan hacia una historia clínica sin papel, el momento actual continua regido por una historia clínica que integra un volumen importante de documentación escrita, de exploraciones en papel continuo, de registros gráficos, de placas radiólogas, etc., que deben almacenarse, de manera ordenada, en una carpeta para facilitar su manejo y consulta posterior*"[24].

También en relación a los avances en materia sanitaria, Noelia de Miguel ha manifestado que "*el sector sanitario no ha podido sustraerse a la irrupción de las nuevas tecnologías y ha visto remozadas muchas de sus estructuras tradicionales con las nuevas opciones traídas por la aplicación de técnicas de tratamiento de datos en sectores como la gestión y administración hospitalaria, a*

[22] CENTENO SORIANO, Cristina: "*Operaciones administrativas y documentación sanitaria*". Formación Alcalá, Jaén, 2007. Pág. 113.

[23] Ibídem.

[24] Ibídem.

través de la creación de bases de datos para almacenar la información hasta ahora recopilada en archivos de difícil acceso, o posibilitando proyectos como la historia clínica informatizada y la tarjeta sanitaria"[25]. Y se extiende la autora diciendo que "*esta situación es generadora de innumerables ventajas tanto en el ámbito asistencial como en el científico, al permitir el empleo de esos datos en el desarrollo de investigaciones cuyos resultados repercuten directamente sobre el conjunto de la sociedad. Pero junto a esos innegables beneficios, la utilización de las nuevas tecnologías en el sector de los datos sanitarios puede generar, si se separa de los criterios que lícitamente han de guiarla, atentados contra derechos fundamentales de la persona, significadamente su derecho a la intimidad y el control que esta puede ejercer sobre sus datos personales...*"[26].

Enlaza así De Miguel el tema de las nuevas tecnologías con el de autodeterminación informativa, que será tratado de forma más amplia a continuación, afirmando que "*en este contexto se plantea la polémica surgida en torno al reconocimiento de un nuevo derecho a la protección de datos personales, denominado en sus inicios derecho a la autodeterminación informativa, analizando su posible especificidad, debido al estrecho vínculo que presenta con el derecho a la intimidad (STC 73/1982,2dic, F.J. 5º)* "[27]. De este modo, "*la polémica sobre el reconocimiento de un derecho fundamental, independiente a la protección de datos personales, que surgió como derecho a la autodeterminación informativa, ha cobrado especial importancia en los últimos años*"[28]. Pero además "*la necesidad de reconocer la existencia de un derecho fundamental a la protección de datos personales, conocido en principio como autodeterminación*

[25] DE MIGUEL SÁNCHEZ, Noelia: "*Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público*". Tirant lo Blanch, Valencia, 2004. Pág. 17.

[26] Ibídem.

[27] Ibídem.

[28] DE MIGUEL SÁNCHEZ, Noelia: "*Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público*". Tirant lo Blanch, Valencia, 2004. Pág. 27.

informativa tendría su reflejo constitucional más próximo en el artículo 18.4, o la posibilidad de que las particularidades que la aplicación de la informática conlleva para los datos personales puedan hallar encaje en el derecho a la intimidad"[29]. Y reflexiona sobre este tema, al expresar que "*pese a ello tampoco entiendo que sea negativo el reconocimiento de un derecho específico a la protección de datos personales, porque aunque en nuestra constitución no exista una cláusula específica sobre el carácter abierto del catálogo de derechos por ella reconocidos, no parece que esto sea un inconveniente para ampliar el mismo, puesto que dicha ampliación es consecuencia lógica de la evolución social y de la creación de nuevas situaciones que no estaban en la mente del constituyente*"[30].

Disponemos además de cauces procesales que protegen la libertad de la persona, que por similitud al Hábeas Corpus abrevian los procedimientos para el ejercicio de derechos fundamentales de las personas, es el denominado Habeas Data de tratamiento jurisprudencial en nuestro país.

Así lo recoge un sector de la doctrina que sostiene que "*en todas las sentencias el Tribunal Constitucional deja claro que el derecho recogido en el apartado 4 del artículo 18 abarca la facultad de «controlar el uso de los datos insertos en un programa de ordenador».Es lo que se ha venido a denominar libertad informática o «habeas data»*"[31].

En este sentido, Karla Cantoral expresa también que *"… puede prevalecer la existencia de una nueva figura que puede encontrar su protección a través del habeas data, o de otras medidas protectoras*

[29] Ibídem. Pág. 29.

[30] Ibídem. Pág. 30.

[31] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso. *"La protección de datos personales en el ámbito sanitario"*, Editorial Aranzadi, Navarra 2002. Pág. 26.

y precautorias judiciales que no debe separarse en intimidad, imagen e identidad, sino que debe ser integrada y protegida a través de los datos personales"[32].

Esta misma autora ha manifestado igualmente que "*el derecho a la autodeterminación informativa constituye una nueva modalidad de libertad personal, tendiente a proteger jurídicamente la identidad personal, y como refiere Murillo de la Cueva, el bien jurídico subyacente es la autodeterminación informativa, que consiste en el control que a la persona le corresponde sobre su información personal para preservar «de este modo y en el último extremo, la propia identidad, nuestra dignidad y libertad»*"[33]. Y hace una mención al respecto sobre la doctrina española "*por su parte, en España la doctrina acepta dos posturas al respecto: la de aquellos que defienden la libertad informática como derecho fundamental autónomo y la de aquellos que consideran la autodeterminación informativa como una especificación o como una ampliación del derecho a la intimidad…*"[34]. Además sostiene que "*a diferencia del derecho a la intimidad, cuya razón de ser es la protección del círculo íntimo del sujeto que desea tener fuera del conocimiento de los demás, el derecho a la autodeterminación informativa protege a la persona frente a la recolección de datos de carácter personal, íntimos o no íntimos, que pueden convertir al individuo en un ser transparente*"[35].

El reconocimiento de derecho a la protección de datos personales como un derecho autónomo e independiente, es contemplado por otros sectores de la doctrina que afirma que "*la configuración del derecho fundamental a la protección de datos*

[32] CANTORAL DOMÍNGUEZ, Karla: "*Derecho de protección de datos personales en la salud*". Editorial Novum, MEXICO D.F., 2012. Pág. 57.

[33] Ibídem. Pág. 71.

[34] Ibídem. Pág. 70.

[35] CANTORAL DOMÍNGUEZ, Karla: "*Derecho de protección de datos personales en la salud*". Editorial Novum, MEXICO D.F., 2012. Pág. 71.

reclama de manera especial la estrategia del diálogo entre tribunales y no sólo en Europa. De algún modo podría trazarse un círculo que uniese puntos judiciales tan diferentes pero tan importantes en la «artesanía» judicial de nuestros días"[36]. Y sostienen que "*esta exigencia viene determinada, en primer lugar, por la novedad que supone la protección jurídica en un entorno tecnológico en vertiginoso cambio. Asimismo y, en segundo lugar, porque en este ámbito las nuevas tecnologías han laminado los viejos conceptos territoriales de soberanía. Y, en fin, porque, particularmente en Europa, se cuenta de facto y, en breve, de iure, con tres niveles jurisdiccionales: el nacional, el de la Unión Europea y el del Convenio Europeo de Derechos Humanos*"[37].

Noelia de Miguel por su parte nos recuerda que "*el Supremo, intérprete de la Constitución ha manifestado que «la intimidad es un ámbito o reducto en el que se veda que otros penetren y que no guarda por si solo relación directa con la libertad de relacionarse con otras personas o derecho a tener amistades»"[38]. Y sigue diciendo que "…«el tributo más importante de la intimidad, como núcleo central de la personalidad, es la facultad de exclusión de los demás, de abstenerse de injerencias por parte de otro, tanto en lo que se refiere a la toma de conocimientos intruista, como a la divulgación ilegítima de datos» (STC 142/1993,22 abril, F.J. 7º)*"[39]. Además reflexiona al respecto manifestando que, "De este pronunciamiento se desprende claramente una facultad esencial en la nueva configuración del derecho a la intimidad, la potestad que este implica para el particular de disposición sobre la información relativa a su persona, controlando el uso, difusión y manejo de la misma, lo que

[36] DIEZ-HOCHLEITNER, Javier, MARTÍNEZ CAPDEVILLA, Carmen, BLÁZQUEZ NAVARRO, Irene, FRUTOS MIRANDA, Javier: "*Últimas tendencias de la jurisprudencia del Tribunal de Justicia de la Unión Europea*". La Ley, Madrid, 2012. Pág. 160.

[37] Ibídem.

[38] DE MIGUEL SÁNCHEZ, Noelia: "*Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público*". Tirant lo Blanch, Valencia, 2004. Pág. 24.

[39] DE MIGUEL SÁNCHEZ, Noelia: "*Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público*". Tirant lo Blanch, Valencia, 2004. Pág. 24.

supone una auténtica autodeterminación informativa, que como pueden apreciarse no se ejerce únicamente frente al tratamiento de datos personales, sino ante cualquier empleo de la información personal, no necesariamente íntima: el propio concepto lo dice, el particular autodetermina su información".[40] Así pues asegura que "Corresponde pues a cada individuo reservar un espacio, más o menos amplio según su voluntad, que quede resguardado a la curiosidad ajena, sea cual sea el contenido de este espacio"[41].

De Miguel ha manifestado además a este respecto que "*la preocupación por la protección de datos surgió en los años sesenta, cuando se fue consciente que utilizando las entonces nuevas tecnologías era posible, no solo almacenar una ingente cantidad de información, sino, lo cual es más importante, someterla al tratamiento automatizado*"[42]. Y que por tanto "*esos tratamientos suponían un potencial riesgo para la intimidad, por lo que el legislador consideró necesario prever medios frente a las posibles injerencias de la tecnología en la intimidad personal*"[43]. Y es que "*recientemente el protagonismo ha sido asumido de forma clara por la consideración inequívoca de la protección de datos personales como derecho fundamental. Las sentencias Constitucionales 290 y 292 de 2000 son determinantes*"[44].

Otra parte de la doctrina secunda esta última reflexión afirmando que "*desde un punto de vista jurídico es necesaria una aproximación al contenido de la protección de datos como derecho fundamental, y los eventuales límites que se pueden establecer al*

[40] Ibídem. Pág. 25.

[41] Ibídem. Pág. 26.

[42] Ibídem. Pág. 13.

[43] Ibídem.

[44] DE MIGUEL SÁNCHEZ, Noelia: "*Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público*". Tirant lo Blanch, Valencia, 2004. Pág. 13.

mismo"[45]. Y asegura que "*nunca debemos olvidar que el reconocimiento de la dignidad humana y de los derechos tiene una larga historia, y a pesar de que solemos hablar de derechos en un sentido universal, no es menos cierto que el reconocimiento de los mismos está unido al propio desarrollo de los Estados nacionales, y que su universalidad o no ha dependido en gran medida del reconocimiento que han disfrutado en el ámbito internacional*"[46]. Afirmando que "*el fundamento de la tutela de los datos de carácter personal debemos buscarlo en la intimidad y la vida privada. El avance crecientemente progresivo de las nuevas tecnologías ha requerido de una respuesta de los ordenamientos jurídicos para tutelar precisamente la intimidad y la vida privada de las personas, de tal forma que se garantice la protección de los datos de carácter personal*"[47].

Y en cambio otro sector doctrinal mantiene a este respecto que "*no obstante, cada vez, ante la digitalización de la sociedad se hace más complicada la protección de datos de los historiales médicos, precisamente porque paulatinamente va desapareciendo lo material que está dando paso cada vez más a lo digital y los datos circulan por la red. Esto hace que las situaciones sean más complicadas. Antes se cerraba el cajón con una llave y se podía saber si se había accedido forzando, pero la digitalización hace que en ocasiones no podamos saber quién ha accedido a esos datos"*[48]. Manifestando que *"por tanto, la protección de estos datos es de suma importancia, no sólo porque su publicación y vulneración afecta a un derecho fundamental, sino porque su no protección puede traer dificultades*

[45] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores): *"La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural".* Tirant Lo Blanch, Valencia, 2014. Pág. 334.

[46] Ibídem.

[47] Ibídem.

[48] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores): *"La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural"*. Tirant Lo Blanch, Valencia, 2014. Pág. 333.

para las personas a las que se les ha vulnerado el derecho fundamental"[49].

Sosteniendo otros que "…*si bien es cierto que las tecnologías constituyen un instrumento de progreso con muchas cosas positivas, ya que ofrecen importantes ventajas y posibilidades, y que la información facilitada por las mismas es necesaria para el Estado en orden a cumplir sus fines, una utilización abusiva de dicha información, no controlada o poco cuidadosa puede afectar los derechos de las personas*"[50]. Y aseguran que "*por ello, la aparición y avance de las nuevas tecnologías han hecho necesaria una especialización, una singularización de la tutela de la intimidad y de la vida privada respecto a los datos de carácter personal, para garantizar una mayor protección del individuo. Por eso el derecho a la protección de datos «ha evolucionado de forma muy significativa, incluso podríamos decir que adquiere autonomía, se independiza del derecho originario, como ha ocurrido en la historia de los derechos humanos en muchas ocasiones»*"[51].

De modo que, según se ha apuntado hace unos renglones por parte de la doctrina, los derechos fundamentales han ido evolucionando a lo largo de la historia desde el siglo. XVIII donde se partía del carácter individualista de los mismos, pasando por los derechos de participación e igualdad, que surgen tras los movimientos revolucionarios, para continuar en el siglo XX con los derechos de naturaleza jurídica que protegen a la persona de la tecnología. En la actualidad todos ellos se insertan y participan unos de otros; la pretensión es legitimarlos para todos los ciudadanos y no para un colectivo concreto.

En este sentido una parte de la doctrina establece que "*es ya bien conocida la expresión «generaciones de derechos» y la triple*

[49] Ibídem.

[50] Ibídem. Pág. 334.

[51] Ibídem. Pág. 335.

gradación que en función de la misma se establece para poner de manifiesto la evolución que ha ido experimentando el reconocimiento de los derechos fundamentales con el correr de los tiempos"[52].

Otro sector doctrinal manifiesta en este sentido que *"las sociedades van cambiando e incluso en nuestro país, hasta no hace mucho, en cuanto a la acción médica daba supremacía a los principios de beneficencia y no maleficencia, base del juramento hipocrático: «doctor, haga lo que Ud. crea conveniente, Ud. es el que entiende y está preparado» Hoy predominan los principios «mayores» de la autonomía y la justicia, fruto de la evolución del conjunto de la sociedad y de la gran mayoría de los ciudadanos*"[53]. Así "*el artículo 3 del CDM expone en cuanto a determinadas leyes: «... e intentará que se cambien las disposiciones legales de cualquier orden que se opongan a ellas». Se refiere a determinadas normas del citado Código. Algunas disposiciones legales actuales o venideras sobre aspectos médicos, reflejo de un consenso o mayoría social o gubernamental, pueden ser menos exigentes que los principios éticos. Es un compromiso de la Organización Médica Colegial (OMC) procurar que la Ley se ajuste lo más posible a la realidad médico-social de cada momento*"[54].

También en relación al juramento de Hipócrates, otros argumentan la existencia de unos principios basados en que "*los médicos desde la tradición hipocrática, se impusieron a sí mismos*

[52] DE MIGUEL SÁNCHEZ, Noelia: "*Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público*". Tirant lo Blanch, Valencia, 2004. Pág. 21.

[53] BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: "*Manual de ética y deontología médica*". Organización Médica Colegial de España, 2012. Pág. 21.

[54] BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: *"Manual de ética y deontología médica".* Organización Médica Colegial de España, 2012. Pág. 21.

actuar conforme al «Principio de Beneficencia». Comprendieron que el enfermo (persona sin-firmeza por su enfermedad) mantenía respecto al médico una situación injusta, desigual, de dependencia, confiada y esperanzada; esto obligaba moralmente al médico a esforzarse para hacer por él lo que fuera más beneficioso y más favorable. También comprendieron la gravedad de actuaciones médicas que amparándose en esta desigual relación, se aprovechan en su beneficio"[55]. Además sostienen que "*cuando se acepta hoy en día que la persona tiene capacidad de comprender, razonar, enjuiciar y sobre todo libertad de elección, se reconoce que estas capacidades también deben aplicarse y ejercerse en la relación médico-enfermo. Conforme a su autonomía, el paciente puede y debe decidir, y para decidir, tiene derecho a conocer su situación y las circunstancias de su estado de salud. Conceptualmente empieza a dejar de ser «enfermo» para convertirse en «paciente», como persona que con paciencia debe sobrellevar la enfermedad, siendo sujeto activo del proceso*"[56]. Y sin olvidar "*un aspecto del «Principio de Justicia» es la distribución de los recursos que se destinan a la asistencia sanitaria. Desde una óptica utilitarista el fin es obtener el mejor bienestar para mayor número de personas, es aceptable, pero no puede ser el único objetivo, porque desde la perspectiva personalista, el ser humano es un fin en sí mismo, cada persona es sujeto de dignidad y no se pueden olvidar aquellos que, por ser minoría no pueden ejercer la misma presión social a la hora de reclamar sus necesidades (como ejemplo pacientes con enfermedades muy poco frecuentes); o incluso los que aún no pueden defenderse por sí mismos como sucede con los no nacidos*"[57].

[55] Ibídem. Pág. 54.

[56] Ibídem.

[57] BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO

Respecto a lo establecido concluye este sector que "*los tres principios citados (Beneficencia, Autonomía y Justicia) hay que aplicarlos en la relación médico-paciente cuando el paciente es mayor de edad y está capacitado para tomar sus propias decisiones, pero también cuando los pacientes son menores de 16 años en que son los padres los que deciden en virtud de la patria potestad o cuando el paciente está incapacitado de forma transitoria o permanente para comprender su situación y poder elegir lo que es más favorable para él. Todo ello va a ocasionar una gran variedad de situaciones y circunstancias que son un verdadero desafío para el médico, que tendrá siempre el deber deontológico de buscar el mejor resultado respetando y jerarquizando adecuadamente los principios éticos enunciados*"[58].

Retomando las opiniones de Noelia de Miguel en este tema, manifiesta esta autora al respecto que "*el derecho a la intimidad impone a los poderes públicos la obligación de adoptar cuantas medidas fuesen necesarias para hacer efectivo aquel poder de disposición (el del particular sobre su información personal), y preservar de potenciales agresiones en ese ámbito reservado de la vida personal y familiar, no accesible a los demás (STC 144/1999, 22 de julio, F.J.8º). La acción del particular será agente esencial de cara a su configuración, y que pone de relieve la posición de este como gestor de sus datos personales*"[59].

Respecto de los límites de la intimidad, Nuria Terribas recalca que "*como todo derecho, la intimidad puede tener ciertos límites y por ende, reconocerse excepciones en el deber de confidencialidad y secreto profesional. Habitualmente estas excepciones cuentan con una justificación, como es el bien de terceros o de la comunidad, y*

SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: *"Manual de ética y deontología médica".* Organización Médica Colegial de España, 2012. Pág. 55.

[58] Ibídem.

[59] DE MIGUEL SÁNCHEZ, Noelia: *"Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público"*. Tirant lo Blanch, Valencia, 2004. Pág. 27.

que en un ejercicio de ponderación de valores, cede el valor individual frente al valor colectivo"[60]. La autora resume estas situaciones en tres, la cesión de datos epidemiológicos, el peligro para terceros o para el propio profesional, y la colaboración con la justicia, haciendo hincapié en que en este último caso sería bueno advertir antes al paciente para que este no se sienta traicionado, aunque se encuentra amparada tal fuga de información tanto por la normativa de protección de datos como por la Ley del paciente.

En relación al concepto de vida privada, directamente relacionado con el concepto de intimidad analizado al principio de este apartado, hay que atender a lo que expone el profesor Sánchez de Diego cuando dice que "*en el Congreso de Juristas de Países Nórdicos sobre el derecho al respeto de la vida privada, se estableció un listado de conductas consideradas agresoras de la intimidad, entre las que se encontraba entre otras «la utilización del nombre, la intimidad o la imagen»*. En opinión de este autor, y en relación al artículo 18 de la Constitución Española, *"…nos encontramos con que existe una confusión de partida entre la intimidad, el honor y la propia imagen…*"[61]. Y sigue reflexionando sobre*"… que se hace preciso realizar un esfuerzo doctrinal que determine qué es el derecho de la intimidad, quienes determinan cual es el derecho de la intimidad y en último término cuales son los criterios de definición de lo público y lo privado*"[62]. A este respecto "*el tribunal Constitucional parece apuntar la idea que el derecho a la intimidad se extiende más allá de la esfera de la intimidad, abarcando la esfera de la vida privada*"[63].

[60] TERRIBAS SALA, Núria: *"Los avances del derecho ante los avances de la medicina. Confidencialidad de los datos sanitarios: de la norma a la práctica médica"*. In Salomé Adroher Biosca- Thomson Aranzadi, 2008. Pags 796-802.

[61] SANCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA, Manuel: *"Sobre la intimidad".* Fundación Universitaria San Pablo C.E.U., Valencia, 1.996. Pág. 218.

[62] SANCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA, Manuel: *"Sobre la intimidad".* Fundación Universitaria San Pablo C.E.U., Valencia, 1.996. 219.

[63] Ibídem.

También Karla Cantoral habla sobre la vida privada estableciendo que "*el concepto de vida privada, es muy amplio, genérico y engloba a todo que no es, o que no queremos que sea de general conocimiento. En ese concepto existe un núcleo que se protege con más celo, con mayor fuerza, y al que se denomina intimidad, porque lo entendemos como esencial en la configuración de nuestra persona*"[64].

Sobre estos términos hace Lucas Murillo de la Cueva una interesante reflexión "*mientras que el honor y la propia imagen son formas positivas de la personalidad, la intimidad tiene una dimensión negativa: se respeta en tanto no se desvela…*"[65].

Respecto a la intimidad y la vida privada se manifiesta también este autor, quien expone que "*la noción de intimidad o vida privada que se tutela constitucionalmente se circunscribe al ámbito más próximo de la persona*"[66].

Hay otra serie de autores que recuerdan en este sentido que "*la privacidad no es, como predican algunos, una reliquia del pasado. Y, en particular, la protección de datos personales es un signo jurídico de nuestro tiempo cuya interpretación última se confía a los tribunales. La protección de los datos personales se ha desarrollado como un derecho fundamental en Europa en los últimos 30 años tal y como lo han interpretado los Tribunales de Luxemburgo y de Estrasburgo. El Tribunal Europeo de Derechos Humanos ha adoptado su jurisprudencia a la vista del Convenio Europeo de Protección de Datos Personales (1981); y el Tribunal de Justicia ha resuelto sus casos más paradigmáticos a partir de la Directiva*

[64] CANTORAL DOMÍNGUEZ, Karla: *"Derecho de protección de datos personales en la salud"*. Editorial Novum, MEXICO D.F., 2012. Pág. 31.

[65] LUCAS MURILLO DE LA CUEVA, Pablo, *"La protección de los datos personales frente al uso de la informática"*. Editorial Tecnos, Madrid, 1990. Pág. 86.

[66] Ibídem. Pág. 96.

95/46/CE sobre protección y libre circulación de datos personales"[67]. Y aseguran que "*la Carta de Derechos Fundamentales de la Unión, como parte del Tratado de la Unión Europea, ha supuesto un avance considerable en la garantía de los derechos de privacidad y de protección de datos, y ejerce una importante influencia en el razonamiento del propio Tribunal de Justicia. En efecto, se puede observar una nueva forma de enjuiciar por parte del Tribunal de Justicia a partir de la vigencia indiscutible de la Carta de Derechos Fundamentales de la Unión*"[68]. Así sostienen que "*el derecho a la protección de datos personales depende, ciertamente, de los tribunales nacionales, pero cuenta con una dimensión global innegable. Por esa razón, se impone el diálogo entre los tribunales no solo en Europa sino también en un contexto cosmopolita. Con este fin será necesaria una delimitación permanente del alcance del enjuiciamiento de cada tribunal: lo que cotidianamente en los ámbitos nacionales es una verdadera lucha entre la instancia, la apelación o la casación, deberá perfilarse con más nitidez en los ámbitos supranacionales*"[69].

Vemos claramente después de lo examinado, que el sector médico ha girado de forma radical hacia el mundo de las nuevas tecnologías, lo cual requiere también prestar una especial atención a los sistemas de seguridad para la protección de la información de los pacientes.

Sin dudarlo pienso que la transmisión de información es esencial entre profesionales en el proceso de curación del paciente y, tiene que circular por todos los sectores del entramado sanitario para poder gestionar adecuadamente la atención del paciente. La puesta en contacto con el sector sanitario es un constante

[67] DIEZ-HOCHLEITNER, Javier, MARTÍNEZ CAPDEVILLA, Carmen, BLÁZQUEZ NAVARRO, Irene, FRUTOS MIRANDA, Javier*: "Últimas tendencias de la jurisprudencia del Tribunal de Justicia de la Unión Europea"*. La Ley, Madrid, 2012. Pág. 167.

[68] Ibídem.

[69] Ibídem. Pág. 168.

intercambio de información entre diversos departamentos (administración, laboratorio, especialistas, etc.), que van a parar a manos del médico, el cual los plasma junto a su juicio en la historia clínica en la que los transforma. Este constante ir y venir de información es absolutamente necesario en el proceso de atención al paciente, pero sin duda debe hacerse con las garantías necesarias que preserven el derecho a la protección de sus datos personales. Hay que encontrar el equilibrio entre necesidad de comunicación de los datos y la protección de los mismos, para que el tratamiento de sus datos se produzca sin vulnerar sus derechos fundamentales.

Creo que es importante plantear, como premisa, cuál debe ser la actitud de las personas que van a acceder a este tipo de información, a través de los distintos recursos que se pongan a su disposición, ya sean informáticos o manuales (sistemas de seguridad informática, armarios, documentación, etc.). Su comportamiento es sin duda clave en el tratamiento de los datos personales, ya que las personas, como humanas, pueden cometer errores. Es primordial en este sentido una buena concienciación en materia de protección de datos, ya que es el ser humano quien toma las medidas para la protección de los datos, pero también quien decide no aplicarlas y olvida hacerlo. Las consecuencias que pueden acarrear estas situaciones podrían vulnerar el derecho a la protección de los datos personales que todos tenemos. De nada serviría tomar todas las medidas si no se aplican en la realidad de forma periódica y concienzuda, empezado por algo tan sencillo como cerrar un cajón o una puerta con llave, o tirar a la basura los documentos destruidos, como ya he sugerido en otras ocasiones. “*¿Se han planteado alguna vez algo tan sencillo como dónde van a parar las copias de las recetas que se quedan en las farmacias cuando decimos que no las queremos? Muchas veces a la basura, con nuestros datos de identificación, nuestro número de la seguridad social y por supuesto, el tratamiento que nos han prescrito. Incluso puede revelar el estado de salud, sin que haga falta que lo interprete un profesional sanitario,*

simplemente porque se conozca que determinado medicamento está asociado a determinadas enfermedades. Y de ello somos responsables nosotros mismos al no destruir la copia de la receta"[70].

Por otra parte, hay un factor que juega un papel muy importante en este tema, "la confianza", que puede asociarse de forma directa a la confidencialidad exigida en materia de protección de datos y, que a menudo nos hace saltarnos las normas de conducta; pasa en la vida cotidiana y también en el ámbito profesional, por eso es también muy importante vigilar este aspecto.

Al hilo de lo anteriormente expuesto, las creación de bases de datos médicas, suponen sin dudas grandes ventajas en el sector sanitario, pero también un potencial riesgo desde que son creadas, si no se ponen en marcha las debidas medidas de seguridad.

Sin duda, la idea es averiguar hasta qué punto, el personal que maneja datos sanitarios conoce y cumple con la normativa en materia de protección de datos en sus distintas escalas, lo cual dependerá de una cadena de comunicaciones internas, que tendrán que partir de la cúspide de la organización. No obstante, muchas veces nos ayuda el sentido común, es decir, que aunque una persona no tenga ninguna noción sobre la normativa de protección de datos personales, si le pedimos algo que no le pertenece, probablemente nos diga que debe preguntar antes al propietario. Lo que ocurre también, es que muchas veces, la precipitación, la ignorancia, o incluso el no pensar las cosas dos veces, nos lleva a tomar decisiones equivocadas y, por ejemplo, tirar algo que tenemos de hace tiempo a la basura, sin antes preguntar a su dueño. Pues bien, si esto lo trasladamos al ámbito sanitario y comunicamos el dato de un paciente sin su consentimiento, o tiramos su expediente médico a la basura por considerar que ya no es útil, podrían

[70] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos"*. Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012.

causarse graves daños a las personas titulares de dichos datos. El daño no afectaría solo a la protección de los datos personales, ya que podría incidir además en la faceta de su derecho a la intimidad, siendo estos dos derechos diferentes, por iguales que parezcan, según se ha comentado.

Estos son simples aspectos del tratamiento de datos cotidiano, contados a modo ejemplificativo, que hacen pensar en lo cuidadosa que tiene que ser la formación de las personas que van a manejar los datos personales relativos a la salud, para darse cuenta de la gran importancia de esta tarea, que se irá complementando y complicando, conforme mayor sea el entramado de la organización y más amplia la diversificación de sus servicios. Pero esto será sin duda posible, por compleja que sea la entidad, si se acotan dichas medidas desde el principio, lo cual facilitará la concienciación y puesta en marcha de las mismas, reduciendo en gran medida los fallos que puedan cometerse durante el tratamiento de los datos de carácter personal.

Tiene mucho esto que ver esto con el ya conocido secreto profesional, que también la normativa de protección de datos contempla de forma parecida, como el deber de guardar secreto sobre los datos personales. Pero existen además muchos otros requisitos en otros ámbitos para la protección de los datos personales, como la calidad de esos datos, la inscripción de los ficheros, la información a los titulares de los datos y la atención de los derechos de los ciudadanos, como principales obligaciones a cumplir en materia de protección de datos que serán detenidamente examinados, y puestos en común para dar una visión general de los que es la protección de datos de carácter personal en el ámbito sanitario.

Elena Urso mantiene en este sentido que “*no sólo son relevantes el derecho a la vida y a la salud, sino también el derecho a la vida familiar, a la privacidad, a la libertad personal y a la libre*

manifestación del pensamiento y de la fe religiosa, así como el respeto a la dignidad humana, sin olvidar el derecho a la audiencia del interesado, cuando tenga capacidad de «discernimiento», y con ellos el deber de tener en cuenta su voluntad, si está en condiciones de comprender y tomar las decisiones"[71].

Enlazando con el tema de la intimidad a propósito del uso de la tecnología, y en relación con el sentido más estricto de la primera, hay un sector doctrinal que manifiesta al respecto que "…*un tema delicado de la relación médico-paciente es la exploración física; éste es un acto médico imprescindible para el diagnóstico*"[72]. Sosteniendo que "*por ello, hay que aceptar que con estas maniobras el médico está actuando como tal y no van en contra de la intimidad del paciente cuando se realizan en el ámbito y condiciones adecuadas y con la necesaria delicadeza y profesionalidad; estas maniobras se integran en una actitud de respeto y de normalidad y constituyen parte de los medios de que el médico dispone para llegar al diagnóstico*"[73].

Y en relación con la intimidad y los datos sensibles, que ocupan este estudio, hay un sector doctrinal que manifiesta que *"…los medios técnicos capaces de obtener, acumular, procesar y transmitir información sensible relativa a las personas, especialmente datos de carácter personal, suponen una evidente amenaza para la intimidad*

[71] Urso, Elena, traducción Torre, E: *"Infancia, adolescencia y derecho a la salud en el hospital: el papel clave de los derechos fundamentales"*. Revista europea de derechos fundamentales. ISSN 1699-1524. Núm. 14/2ºsemestre 2009. Páginas 183-229.

[72] BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: *"Manual de ética y deontología médica".* Organización Médica Colegial de España, 2012. Pág. 58.

[73] BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: *"Manual de ética y deontología médica".* Organización Médica Colegial de España, 2012. Pág. 58.

de las personas, por su enorme potencial vulnerador de la misma…"[74]. Si consideramos los datos médicos como información sensible, que desde luego lo es, podremos aplicar esta opinión a la protección de datos personales relativos a la salud que ocupan este estudio.

Hay en cambio otra parte de la doctrina que se refiere a una parte muy concreta de la intimidad en relación con los datos sensibles y así lo manifiesta, "…*definir lo que debemos entender por derecho a la intimidad genética es una labor que no está exenta de dificultades, ya que se hace necesario previamente llegar a un consenso sobre cuestiones tales como qué es lo que debemos entender por información genética y si ésta realmente es merecedora por su propia naturaleza de una protección reforzada, pues debemos tener en cuenta que hay información de carácter genético que puede no considerarse privada por ser visible a cualquier persona que tenga un contacto bastante superficial con el afectado; éste es el caso por ejemplo de la estatura o del color de piel*"[75]. Y se extiende sobre este tema estableciendo que "*lo cierto es que el derecho a la intimidad genética encuentra su fundamento tanto en documentos nacionales como internacionales, especialmente en estos últimos, en los que ya se recoge este derecho de forma expresa, como ocurre con el art. 7 de la Declaración Universal sobre el Genoma Humano o el art. 10 del Convenio de Oviedo. Por lo que se refiere a los textos jurídicos de carácter nacional, en la actualidad el derecho a la intimidad genética encuentra una base implícita en el art. 18 de la Constitución española, que reconoce el derecho a la intimidad personal y familiar: así sería factible definir este derecho*

[74] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso. "La protección de datos personales en el ámbito sanitario", Editorial Aranzadi, Navarra 2002. Pág. 113.

[75] SUÁREZ DEL ESPINO, María Lidia, "El derecho a la intimidad genética". Marcial Pons Ediciones Jurídicas y Sociales, S.A., Madrid, 2008. Pág. 88.

como aquel que confiere a su titular la facultad de determinar las condiciones en que se podrá acceder a la información contenida en sus genes. Es por ello, al igual que ocurre con la intimidad informática y la autodeterminación informativa, que se puede concluir que el derecho a la intimidad genética desborda el concepto de intimidad en su sentido más clásico, tal y como se recoge en el art. 18 CE, pues no es un simple derecho de defensa frente a injerencias externas no deseadas, sino más bien un derecho más activo que otorga a su titular un haz de facultades que requieren de él una actitud activa, como los derechos de acceso, rectificación, cancelación, etc"[76].

Y como reflexión a lo anteriormente dicho, explica que "*la última argumentación nos resulta útil para llevarnos a la conclusión de que se trata de un derecho que presenta dos facetas. Una de derecho de libertad, que faculta al individuo para defenderse de intromisiones indeseadas, tanto por parte de los poderes públicos como por parte de los particulares, pero también es un derecho prestacional que hace posible exigir de los poderes públicos la toma de medidas efectivas para garantizar y proteger este derecho de una manera eficaz, por ejemplo exigiendo una intervención judicial motivada y precisa cuando se realice cualquier análisis no consentido del genoma de una persona, o articulando procedimientos encaminados a rectificar de una manera ágil y sencilla informaciones genéticas erróneas o imprecisas o creando incluso un organismo público independiente, parecido a la Agencia de Protección de Datos Personales, que vele por la utilización no abusiva de esta información tan sensible*"[77].

Pensemos, por ejemplo, que alguien puede mantener o no en privado su homosexualidad. Cuando esta condición se hace pública, no por ello deja este de ser un dato personal, ni tampoco deja de ser

[76] Ibídem. Pág. 89.

[77] SUÁREZ DEL ESPINO, María Lidia*: "El derecho a la intimidad genética"*. Marcial Pons Ediciones Jurídicas y Sociales, S.A., Madrid, 2008. Pág. 90.

un dato íntimo, simplemente pasa a ser conocido, de forma que determinado tipo de dato referente a una faceta tan reservada de la persona, como lo es su sexualidad, puede ser a la vez un dato personal, ya que se desprende de una persona, íntimo, ya que denota una característica extremadamente interior del sujeto, y a la vez conocido por un grupo más o menos amplio de personas, ¿o es que a caso esta característica deja de ser un dato íntimo en su esencia cuando es conocido por determinadas personas? No hay que olvidar que determinados datos, conocidos o no, jamás dejan de pertenecer a la faceta más reservada del individuo, aquella que se encuentra dentro de nuestra vida privada y que se protege con mayor intensidad.

Respecto de los términos íntimo y privado, Herranz Ortiz manifiesta que "*ha representado una constante en el estudio de la protección de datos personales el enfrentamiento entre ambos términos, privacidad e intimidad se han presentado como dos realidades irreconciliables e incompatibles*"[78].

Y sobre estos dos términos, en relación con el tratamiento de los datos personales, se expresa también Manuel Sánchez de Diego *"…el hecho es que el tratamiento automatizado de esos datos personales, privados aunque no íntimos, permite el conocimiento de la intimidad de la persona*"[79].

De acuerdo a lo visto, quizás existan dos visiones de la intimidad, lo que para cada uno mismo es íntimo, y lo que a ojos de los demás puede considerarse íntimo, pero para uno mismo no lo sea tanto o viceversa.

Hay otro sector doctrinal que se atreve en este sentido con la definición del término «intimidad» manifestando que *"…aunque no es*

[78] HERRÁN ORTIZ, Ana Isabel: *"La violación de la intimidad en la protección de datos personales"*. Dykinson, Madrid 1.999. Pág. 94.

[79] SANCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA, Manuel: *"Sobre la intimidad".* Fundación Universitaria San Pablo C.E.U., Valencia, 1.996. Pág. 220.

fácil de definir, podemos aproximarnos al concepto de intimidad afirmando que se trata de la esfera o ámbito más interior y reservado de una persona o grupo. Un espacio, físico y espiritual, que no pertenece de forma exclusiva y nos es enteramente propio…"[80]. Pero por otro lado también opinan que "…*la intimidad es también necesaria para que cada uno pueda establecer relaciones humanas significativas con otras personas, pues sólo desde la existencia de esa intimidad es posible definir y decidir qué partes de uno mismo y de la propia existencia se quieren compartir con los demás, y cuáles se quieren mantener reservadas y ajenas al conocimiento de otros…*"[81]. Y mantiene además que "*…según el objeto protegido variará el alcance del derecho a la intimidad como derecho humano y fundamental, según se trate de personas famosas, figuras públicas o ciudadanos de vida normal en las que las circunstancias de su actividad profesional no deben "motivar" a los medios de comunicación, y mucho menos sus actividades familiares o personales"*[82]*.* Concluyendo a este respecto que "*las legislaciones comparadas pueden ordenarse en tres grupos: en el primero se encuentran las que otorgan un reconocimiento constitucional pleno al derecho a la intimidad; en el segundo se hayan las constituciones que acogen las manifestaciones del derecho y realizan referencias globales respecto a la proporción de la intimidad como un ámbito personal; por último, en el tercer grupo se sitúan las normas constitucionales que no recogen ni el derecho ni sus diversas manifestaciones*"[83].

Lucas Murillo de la Cueva sostiene en este sentido que "*la libertad de los antiguos consistía en la participación activa*

[80] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso*: "La protección de datos personales en el ámbito sanitario"*. Editorial Aranzadi, Navarra 2002. Pág. 111.

[81] Ibídem. Pág. 112.

[82] CANTORAL DOMÍNGUEZ, Karla: *"Derecho de protección de datos personales en la salud"*. Editorial Novum, MEXICO D.F., 2012. Pág. 35.

[83] Ibídem. Pág. 36.

continuada en el poder colectivo". Así ha expresado que "*en la sociedad moderna las condiciones sociales exigen más autonomía individual y menos participación*"[84]. Manifiesta el autor que se trata de *"…dos nociones de libertad: la positiva y la negativa. La primera se refiere a la capacidad del individuo para desarrollar sus potenciales, la segunda alude a la garantía de un ámbito exento de injerencias ajenas, reservado para la persona"*[85]. Y en relación con la protección de datos argumenta que "*…algunos afirman que el derecho a la intimidad supone el control por parte del individuo de la información de carácter personal*"[86].

Todo este examen de opiniones en torno a la intimidad, se ve influenciado por la participación pública ante la que la gente se siente invadida y aumenta en torno a ella la esfera de lo privado.

Recordemos en este sentido que "*el antiguo «the right to privacy» formulado por Warrens y Brandeis como derecho individual de exclusión ha sido sustituido por un nuevo derecho que ha adquirido un significado cautelar fundado en la idea de riesgo social que permite configurarlo como un derecho subjetivo autónomo llamado a tutelar la «privacy» o vida privada*"[87]. "*Mediante el concepto de privacidad se hace referencia a aquellas facetas del ser humano que si bien no integran la esencia de su personalidad aisladamente consideradas, pudieran llegar a perjudicar al individuo si se relacionasen oportunamente entre sí, porque revelarían aspectos de la persona que la comprometen o que impiden un ejercicio satisfactorio de sus derechos*"[88].

Otros autores han manifestado al respecto que "*los cambios en la historia más reciente de la humanidad han venido siempre*

[84] LUCAS MURILLO DE LA CUEVA, Pablo: *"La protección de los datos personales frente al uso de la informática"*. Editorial Tecnos, Madrid, 1990. Pág. 46.

[85] Ibídem. Pág. 49.

[86] Ibídem. Pág. 65.

[87] HERRÁN ORTIZ, Ana Isabel: *"La violación de la intimidad en la protección de datos personales"*. Dykinson, Madrid 1.999. Pág. 97.

[88] Ibídem. Pág. 102.

acompañados de la necesidad de una respuesta por parte de las sociedades y los sistemas que los gobiernan. También el derecho y los conceptos jurídicos en los que se sustentan deben estar en continua revisión para cumplir con su sentido y función social. Eso es lo que Warren y Brandeis sugerían en el inicio de su opúsculo cuando decían que "es un principio tan viejo como el «common law» que el individuo debe gozar de total protección en su persona y en sus bienes, sin embargo, resulta necesario, de vez en cuando, redefinir con precisión la naturaleza y la extensión de esta protección. Los cambios políticos, sociales y económicos imponen el reconocimiento de nuevos derechos, y el «common law», en su eterna juventud, evoluciona para dar cabida a las demandas de la sociedad. En la época en la que estos autores publicaron su artículo "The Right to Privacy" ((Harvard Law Review, 1890), los medios tecnológicos de incursión en ,la vida privada que denunciaban eran la captura, de imagen a distancia y sin permiso a través de fotografías y la distribución de las mismas en la prensa (una práctica que perdura en nuestros días), Después de más de un siglo, las denuncias se realizan contra "otras familias tecnológicas": almacenamiento y tratamiento de datos personales, transferencias y difusión de datos a través de tecnologías digitales electrónicas, Internet, redes sociales, video vigilancia de ciudadanos, etc, Estos nuevos sistemas socio-técnico-informáticos no solo han puesto de manifiesto el poder de la innovación informática y los beneficios que aportan, también han revelado nuevas amenazas y desafíos en materia de protección a la intimidad"[89].

La autora Karla Cantoral afirma en este sentido que "*en la actualidad, con acelerado desarrollo de las nuevas tecnologías, los intentos de democratización y la globalización, las preocupaciones*

[89] ARRIBAS LEÓN, Mónica, CARRIZOSA PRIETO, Esther, CARRUSO FONTÁN, Viviana, GALAÁN MUÑOZ, Alfonso, HOLGADO GONZÁLEZ, María, LUCENA CID, Isabel Victoria, TOSCANO GIL, Francisco: *"La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación"*. Tirant Lo Blanch, Valencia, 2014. Pág. 15.

de Warren y Brandeis no han dejado de tener sentido, pero la protección constitucional se ha ampliado hacia otros horizontes, debido en parte a las exigencias que se han derivado de los desarrollos tecnológicos, que permite a particulares tener acceso a una gran cantidad de información sobre nuestra vida"[90].

Y en cambio, otra parte de la doctrina se refiere también al término «*privacy*», en relación a las posibilidades que ofrece el uso de la informática *"…esta dimensión más amplia de la intimidad entronca directamente con lo que en el ámbito anglosajón se ha denominado «privacy». Así, la llamada privacidad es un concepto relativamente reciente en el Ordenamiento Jurídico español y que fue originalmente acotado y definido por la exposición de motivos de la ya derogada LORTAD, en la que se venía a expresar que la privacidad constituye un conjunto –más amplio y global que la intimidad- 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…"*[91]. Así vemos que *"…el derecho a la intimidad puede ser configurado como un derecho fundamental con una doble dimensión: una negativa, propia de los derechos subjetivos, que constituye la facultad de exclusión del conocimiento ajeno de aquello que se refiere a la propia persona. Y una dimensión positiva, que constituye la facultad de control y vigilancia por el interesado de la información que le afecta…"*[92].

En este sentido, *"…una de las perspectivas jurisprudenciales más avanzadas del concepto la encontramos en el Tribunal*

[90] CANTORAL DOMÍNGUEZ, Karla: *"Derecho de protección de datos personales en la salud"*. Editorial Novum, MEXICO D.F., 2012. Pág. 56.

[91] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso: *"La protección de datos personales en el ámbito sanitario"*. Editorial Aranzadi, Navarra 2002. Pág.115.

[92] Ibídem. Pág. 116.

Constitucional alemán que, ya en su célebre y significativa Sentencia de 15 de diciembre 1983, apuntó la idea de la autodeterminación informativa, al establecer y reconocer «la facultad del individuo, derivada de la idea de autodeterminación, de decidor básicamente por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a su propia vida»…"[93] Y *"…consecuentemente, el derecho a la intimidad comprende no sólo el reconocimiento de esa reserva, sino también la facultad de control sobre la implicación de terceros en la misma, debiendo resaltar que incluimos no sólo el conocimiento sino también el desenvolvimiento en sí mismo, lo cual amplía notablemente su ámbito…*"[94].

Noelia de Miguel sostiene al respecto que "*hoy la privacy se concibe como la libertad positiva de ejercer un control sobre los datos referidos a la propia persona, que han superado el ámbito de la intimidad para formar parte de un archivo electrónico*"[95]. Y comenta al igual que "*el derecho a la autodeterminación informativa halla su base en la sentencia del Tribunal Constitucional Federal Alemán de 15 de diciembre de 1983*"[96].

Herrán Ortiz ha manifestado por su parte que "*hoy, frente a una sociedad que avanza y reduce en gran manera la esfera íntima del ser humano, se contempla una obligada respuesta del individuo ante dicha expansión de la vida pública, buscando instrumentos que faciliten el aislamiento y la autodeterminación de cada persona en su vida y en las relaciones que desarrolla*"[97.]

Respecto de lo público y lo privado realiza varias reflexiones el profesor Sánchez de Diego, quien nos dice que "*podemos distinguir*

[93] Ibídem. Pág. 117.

[94] Ibídem.

[95] DE MIGUEL SÁNCHEZ, Noelia*: "Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público"*. Tirant lo Blanch, Valencia, 2004. Pág. 21.

[96] DE MIGUEL SÁNCHEZ, Noelia*: "Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público"*. Tirant lo Blanch, Valencia, 2004. Pág. 30.

[97] HERRÁN ORTIZ, Ana Isabel: *"La violación de la intimidad en la protección de datos personales"*. Dykinson, Madrid 1.999. Pág.29.

distintos criterios: el grado de divulgación de la información, el detentador de los datos, el origen de la noticia y la propia naturaleza de la información. Pese a que los criterios expuestos nos aproximan a los conceptos de lo público y lo privado, ninguno de ellos puede determinar por si solo que es información pública y que es información privada"[98].

El referido profesor recuerda, "*ya he manifestado en otra ocasión que el hecho es que el tratamiento automatizado de esos* datos personales, privados aunque no íntimos, permite el conocimiento de la intimidad de la persona"[99].

Según expresa otra parte de la doctrina, más encaminada a los datos de salud en concreto, "*el ejercicio de la medicina y de las profesiones sanitarias, tanto en el marco de la medicina socializada e institucionalizada, como en la medicina privada, está basada en la relación médico-paciente de la que derivan derechos y deberes recíprocos*"[100]. Opinando igualmente que *"…la salud de la colectividad está por encima del interés individual de cada paciente, en ocasiones de confrontación de derechos del paciente, como el derecho a la vida y a la libertad…"*[101]. Así mismo considera esta corriente que "*los problemas médico-legales y éticos que se manifiestan y derivan de la historia clínica, fundamentalmente afectan a: la propiedad de la misma, al consentimiento informado, al secreto profesional, su conservación y custodia, la informatización de la misma y la responsabilidad médico-legal que deriva de su tratamiento*"[102]. No en vano sostienen que *"…el grupo de expertos sobre información e historia clínica, subrayó la necesidad de una Ley*

[98] SANCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA, Manuel: *"Sobre la intimidad"*. Fundación Universitaria San Pablo C.E.U., Valencia, 1.996.Pág. 222.

[99] Ibídem. Pág. 220.

[100] CRIADO DEL RÍO, María Teresa y SEOANE PRADO, Javier: "*Aspectos médico-legales de la historia clínica"*. Colex, Madrid, 1999.Pág. 13.

[101] Ibídem.

[102] Ibídem. Pág.14.

sobre la historia clínica, teniendo en cuenta la LORTAD y las recomendaciones y convenios de la UE a tales efectos"[103].

En este punto, habría que preguntarse ¿dónde se encuentra el límite entre lo que uno considera privado y lo que consideran los demás? ¿En qué momento cada cual siente invadida la esfera que le rodea como el campo íntimo que protege? Es probable, ya que en la vida diaria ocurre, que ante distintos estados de ánimo, nos tomamos una información de forma distinta, cuanto más si se trata de datos referentes a nuestra salud. Nosotros decidimos a qué grupo de personas le queremos comunicar la información y a cual no. Considero que el tema de la publicidad es muy relativo, pues yo puedo hacer público un hecho entre mis amigos, lo cual no les da derecho a difundirlo entre otras personas. Cabría pensar también que un mismo dato, tradicionalmente considerado íntimo para una persona, para otra no lo es. Podría visualizarse la publicidad de nuestros datos personales como grandes globos, comunicados selectivamente a determinados sectores o personas, que explotarían en el momento en que esta información entrase en contacto con el público de forma masiva, momento en el cual se formaría una única burbuja de información conocida públicamente. Esta representación es la llamada teoría de las esferas que es comentada por varios autores.

Noelia de Miguel mantiene que "*la polémica actual de este derecho ha superado los debates tradicionales sobre la dimensión y alcance de la intimidad y privacidad o la teoría de las tres esferas, para situarse, en la dialéctica de su adaptabilidad a la situación creada por la aplicación de las nuevas tecnologías al tratamiento de datos personales, o frente a la polémica sobre la necesidad de*

[103] Ibídem.

defender la existencia de un nuevo derecho a la protección de datos personales, que abarcando el ámbito de la intimidad lo supera"[104].

Herran Ortiz lo hace, por su parte, de la siguiente forma: "*Piénsese en un conjunto de círculos concéntricos que representan las esferas de actuación e intimidad del individuo. Así el círculo de mayor amplitud estaría integrado por la vida de relación en sociedad, en una esfera más reducida que la anterior las relaciones familiares, y caso de profundizar un poco más se toparía con el aspecto privado de la persona y finalmente el núcleo íntimo o estrictamente personal en el que se encuentra la esencia de la persona*"[105].

Esta misma autora ha manifestado además que: *"Una situación privada se desarrolla lejos de las miradas ajenas de terceros, pero esa misma realidad será pública si se efectúa en una plaza pública o a voz en grito en un centro comercial. Así la naturaleza privada de las realidades humanas tiene un carácter relativo, depende de la decisión de la persona que en cada momento realice la actividad privada de que se trate"*[106].

Y Karla Cantoral también utiliza estos términos cuando recoge que "*la teoría de las esferas fue superada por la jurisprudencia del Tribunal Federal Alemán-el lugar donde nació tal teoría- a partir de la sentencia de 15 de diciembre de 1983, sobre el Censo de Población, que da origen a configurar un nuevo derecho denominado "autodeterminación informativa" basado en la posibilidad de cada individuo de determinar quién, qué, y con qué finalidad puede conocer o utilizar un tercero datos que lo afectan*"[107]. Afirmando esta autora que "*esta teoría es una configuración doctrinal muy reciente,*

[104] DE MIGUEL SÁNCHEZ, Noelia: *"Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público"*. Tirant lo Blanch, Valencia, 2004. Pág. 20.

[105] HERRÁN ORTIZ, Ana Isabel*: "La violación de la intimidad en la protección de datos personales"*. Dykinson, Madrid 1.999. Pág. 141.

[106] HERRÁN ORTIZ, Ana Isabel: "*La violación de la intimidad en la protección de datos personales*". Dykinson, Madrid 1.999. Pág. 16.

[107] CANTORAL DOMÍNGUEZ, Karla: *"Derecho de protección de datos personales en la salud".* Editorial Novum, MEXICO D.F., 2012. Pág. 33.

que surge como explicación de la necesidad de protección a la intimidad del individuo frente a la amenaza que produce de forma genérica internet y la sociedad de la información. Madrid Conesa explica esta teoría basándose en que hoy lo conceptos de lo público y lo privado son relativos…"[108].

Obviamente se tuvo en cuenta en ese momento la normativa entonces actual de protección de datos. Hoy en día habría que trasladarlo en la misma línea a la normativa existente en la materia; me refiero a la LO de protección de datos y a su reglamento de desarrollo.

Enlazando la existencia de esta normativa, con un tema e gran actualidad en el sector sanitario, y según he manifestado ya en alguna ocasión a propósito de la instauración en nuestro país del sistema de copago sanitario en función de la renta, los profesionales que manejasen tal información, conocerían dos grupos de datos a los que la citada normativa confiere el nivel alto de protección: los de salud y los de la renta, resultando peligrosa tal combinación. "*Recordemos que la LO sobre protección del honor, intimidad e imagen, establece que las personas ponen el límite a su intimidad con sus propias acciones y, en este caso, las acciones no serían propias, sino ajenas, del Estado, y no del ciudadano*"[109]. Y por asimilación podría decirse que el hecho de bajar el umbral del límite que cada uno ponemos a nuestra intimidad, corresponde también al propio individuo, que con sus acciones deberá hacer ver que ciertas cosas que antes no le importaba que se conociesen, ahora si le importa, o es que ¿no existe derecho al olvido en este sentido? Me refiero a que si por el hecho de haber dejado a una persona conocer determinados aspectos de su vida en determinada situación o periodo de tiempo, no pudiera ya retractarse nunca es este sentido y,

[108] Ibídem. Pág. 34.

[109] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

para siempre, esa determinada cosa pudiese ya ser conocida por todo público. No cabe duda que en materia de protección de datos, la persona debe consentir en cada caso concreto para el tratamiento de sus datos personales, pudiendo retractarse en cualquier momento de esa decisión, a través del oportuno ejercicio de sus derechos.

Sin duda *"el cobro o copago por los servicios sanitarios podría evitar en parte el mal uso de los recursos sanitarios públicos. No obstante este problema no es nuevo, pues ya se afronta en la Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios, en la Ley 28/2009, de 30 de diciembre, de modificación de la anterior, así como en el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación, que se dicta en desarrollo de la primera. El citado reglamento, establece en sus disposiciones generales que, "profundiza en la mejora racional del uso de los medicamentos", al tiempo que proclama que se "refuercen las garantías de los ciudadanos". La recaudación económica de los servicios sanitarios, el copago, podría hacer vulnerables a los ciudadanos a los que se transfiere una competencia que en realidad corresponde al personal sanitario. Son estos los que deben valorar la salud de sus pacientes, si no fuera así se pueden llegar a generar complicaciones médicas graves por "miedo al pago", o "miedo a la transparencia"*[110].

Respecto al tema del copago sanitario, la Carta Europea de los Derechos de los Pacientes (CEDP- Carta de los Derechos de los Pacientes), firmada en Roma en el año 2002, recoge en su preámbulo a propósito de la manipulación de la sanidad que "*a pesar de sus diferencias, los sistemas nacionales de salud de los países de la Unión Europea tienen en común el poner en peligro los derechos de los pacientes, consumidores, usuarios, familiares,*

[110] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

poblaciones desfavorecidas y ciudadanos de a pie de sus países. A pesar de las solemnes declaraciones sobre el "Modelo Social Europeo" (el derecho al acceso universal a los cuidados médicos), diversas restricciones ponen en tela de juicio la realidad de este derecho. Como ciudadanos europeos, no podemos aceptar que estos derechos puedan ser formulados en teoría, para más tarde ser denegados en la práctica debido a restricciones financieras. Estas restricciones, aunque puedan estar justificadas, no pueden negar ni comprometer los derechos de los pacientes. No aceptamos que estos derechos puedan ser establecidos por ley, para no ser respetados posteriormente, que puedan formar parte de los programas electorales pero sean olvidados más tarde tras la llegada de un nuevo gobierno".

Analizada y contrastadas protección de datos e intimidad, podríamos pensar que dos derechos tan cercanos, aunque distintos, como son estos, pudieran tener un tratamiento parecido.

III.1. HISTÓRICAS:

Los inicios de la legislación sanitaria se remontan a 1822 con el proyecto del primer Código Sanitario. Más de cien años después, la Constitución Española del 78 reconoce el derecho de las personas a la protección de su salud en sus artículos 43 y 49. Y hoy en día existe una especial preocupación por la sanidad, contaminada en parte por el aprovechamiento de recursos provocado por la actual crisis que sufrimos. Uno de los principios básicos de esta norma es la proximidad que deben sentir los usuarios a los servicios sanitarios.

Según manifiesta un sector de la doctrina *"…resulta que es precisamente la Constitución, a través del bloque de la constitucionalidad al que se incorpora la Ley de Protección de Datos, la que establece un sistema de protección de la intimidad de los pacientes, médicos y de cualquier otro ciudadano, que exige que se*

respeten determinadas normas por aquellos que manejan sus datos personales, sean o no médicos de profesión y se dediquen o no a tal actividad…"[111].

III.1.a. Normativa general y de protección de datos:

En la Carta de las Naciones Unidas (CNU), firmada en San Francisco el 26 de junio de 1945, todos los pueblos de las Naciones Unidas reafirman la fe en los derechos fundamentales del hombre; según consta en el segundo punto de su preámbulo: *"nosotros los pueblos de las Naciones Unidas Resueltos a reafirmar la fe en los derechos fundamentales del hombre…"*, y tiene entre sus propósitos dentro de la cooperación internacional, fomentar el respeto a los derechos humanos y a las libertades fundamentales, sirviendo como centro de apoyo para ello, según indica su artículo 1.3 y 1.4: *"Realizar la cooperación internacional en la solución de problemas internacionales de carácter económico, social, cultural o humanitario, y en el desarrollo y estímulo del respeto a los derechos humanos y a las libertades fundamentales de todos, sin hacer distinción por motivos de raza, sexo, idioma o religión; y servir de centro que armonice los esfuerzos de las naciones por alcanzar estos propósitos comunes".*

Igualmente, la Declaración Universal de Derechos Humanos de la Unesco (DUDH), aprobada por resolución de la Asamblea General el 10 de diciembre de 1948, ya cita en su preámbulo "*de los derechos y libertades fundamentales del hombre*", la dignidad y el valor de la persona humana. Dicha declaración, adoptada y proclamada por la Resolución de la Asamblea General el 10 de diciembre de 1948, considera que los derechos humanos deben ser

[111] ATELA BILBAO, Alfonso, BENAC URROZ, Mariano, CODÓN HERRERA, Alfonso, GARAY ISASI, Josu, GONZÁLEZ SALINAS, Pedro, HERNÁNDEZ-MARTÍNEZ CAMPELLO, Carlos, LIZARRAGA BONELLI, Emilio, MARTÍ MONTESINOS, Cristina, PELLEJERO GARCÍA, Carlos, PIDEVAL BORRELL, Ignasi, VILLAR ABAD, Gloria, GONZÁLEZ PÉREZ, Jesús: *"Autonomía del paciente, información e historia clínica"*. Editorial Aranzadi, Madrid 2004. Pág. 177.

protegidos, con el compromiso de los Estados Miembros a respetar los derechos y libertades fundamentales del hombre y a cooperar con las Naciones Unidas. Establece igualmente la protección de la vida privada, concretamente en su artículo 12 donde prohíbe las injerencias en la vida privada, la familia, el domicilio y la correspondencia, protegiendo de los ataques contra la honra o reputación. Esta protección de la vida privada y la honra podríamos equipararla a la intimidad y el honor protegidos en la Constitución Española, y del mismo modo al resto de derechos aludidos en las demás normas citadas, para concluir, que esta materia no es una preocupación actual, sino que importa y se va renovando con el cambio de los tiempos; así dice literalmente este artículo *"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".* Y también el derecho a la salud y a la asistencia médica es recogido en el artículo 25.1*"toda persona tiene derecho a un nivel de vida adecuado que le asegure, así como a su familia, la salud y el bienestar, y en especial la alimentación, el vestido, la vivienda, la asistencia médica y los servicios sociales necesarios; tiene asimismo derecho a los seguros en caso de desempleo, enfermedad, invalidez, viudez, vejez u otros casos de pérdida de sus medios de subsistencia por circunstancias independientes de su voluntad"*, haciendo una referencia expresa en el 25.2 a los menores *"la maternidad y la infancia tienen derecho a cuidados y asistencia especiales. Todos los niños, nacidos de matrimonio o fuera de matrimonio, tienen derecho a igual protección social".*

También el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950 y firmado por España el 24 de noviembre de 1977 (CEDHLF- Convenio sobre Derechos Humanos y Libertades Fundamentales), garantiza en su artículo 8 el derecho de

las personas al respeto de su vida privada, familiar, domicilio y correspondencia, y en el 19 recoge dos instituciones: la Comisión Europea de Derechos Humanos y el Tribunal Europeo de Derechos Humanos, como órganos que garanticen el respeto a los compromisos establecidos en el presente convenio. Y así lo recoge literalmente este precepto, "*con el fin de asegurar el respeto de los compromisos que resultan para las Altas Partes Contratantes del presente Convenio, se instituyen: a) una Comisión Europea de Derechos Humanos, denominada en adelante «la Comisión»; b) un Tribunal Europeo de Derechos Humanos, denominado en adelante «el Tribunal»".*

Así mismo establece este texto en sus considerados que *"la finalidad del Consejo de Europa es realizar una unión más estrecha entre sus miembros, y que uno de los medios para alcanzar esta finalidad es la protección y el desarrollo de los derechos humanos y de las libertades fundamentales"*. Y recoge más adelante respecto el Derecho al respeto de la vida privada y familiar en su artículo 8.1 que: *"Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia"*, y en el punto segundo de este mismo precepto, se apunta además que, *"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".*

En el artículo 60 de dicho convenio, respecto de la protección de los derechos humanos, se reconoce además que *"ninguna de las disposiciones del presente Convenio será interpretada en el sentido de limitar o perjudicar aquellos derechos humanos y libertades fundamentales que podrían ser reconocidos conforme a las leyes de*

cualquier Alta Parte Contratante o en cualquier otro Convenio en el que ésta sea parte".

El Pacto internacional de derechos civiles y políticos (PDCP-Pacto de Derechos Civiles y Políticos), hecho en Nueva York el 16 de diciembre de 1966, firmado por España el 28 de septiembre de 1976, tiene en principal consideración la Carta de las Naciones Unidas, así como la Declaración Universal de Derechos Humanos, y conforme a ello, considera que no cabe el desprecio a los derechos fundamentales, actualmente reconocidos en los Estados, de acuerdo a sus leyes, convenciones, reglamentos o costumbres, según establece su artículo 5.2, *"no podrá admitirse restricción o menoscabo de ninguno de los derechos humanos fundamentales reconocidos o vigentes en un Estado Parte en virtud de leyes, convenciones, reglamentos o costumbres, salvo pretexto de que el presente Pacto no los reconoce o los reconoce en menor grado".* Igualmente se reconoce el derecho a la protección de la vida privada en el artículo 17.1, el cual recoge que *"nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Se establece un Comité de Derechos Humanos, según su artículo 28.1 Se establecerá un Comité de Derechos Humanos (en adelante denominado el Comité)…".* Que será provisto de personal y servicios a través del Secretario general de las Naciones Unidas; así, según marca el artículo 36, *"el Secretario general de las Naciones Unidas proporcionará el personal y los servicios necesarios para el desempeño eficaz de las funciones del Comité en virtud del presente Pacto"*. Este a su vez, trasladará al Comité, para su estudio, los informes que cada Estado deberá presentar, sobre las disposiciones adoptadas; de acuerdo al artículo 40.3, *"el Secretario general de las Naciones Unidas, después de celebrar consultas con el Comité, podrá transmitir a los organismos especializados interesados copias de las partes de los informes que caigan dentro de sus esferas de competencia".* Así mismo, el Comité

dará traslado a la Asamblea General de las Naciones Unidas, de un informe anual de sus actividades, ya que, como marca el artículo 45, *"el Comité presentará a la Asamblea General de las Naciones Unidas, por conducto del Consejo Económico y Social, un informe anual sobre sus actividades".*

Es importante recordar las resoluciones que el Consejo de Europa lleva emitiendo en este tema desde hace casi medio siglo, sobre la problemática que se ha ido planteando a lo largo de los años sobre la intromisión de la tecnología en la vida de las personas. Entre ellas se encuentra el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981 (C108- Convenio 108 del Consejo de Europa), como punto de partida para la regulación de la protección de datos de carácter personal.

Este convenio exalta la unión de sus miembros bajo la tutela de los derechos y libertades de las personas, con la plena libertad de información. Esto sin duda es un ideal que las legislaciones de cada uno de los países deben modular internamente para su buen funcionamiento, así dice su preámbulo que *"los Estados miembros del Consejo de Europa, signatarios del presente Convenio. Considerando que el fin del Consejo de Europa es llevar a cabo una unión más íntima entre sus miembros, basada en el respeto particularmente de la preeminencia del derecho así como de los derechos humanos y de las libertades fundamentales; considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados; reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras; reconociendo la*

necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos,…". Aquí habla de datos automatizados, porque los no automatizados no estaban regulados, pero en la actualidad se con templan ambos.

Y así mismo ratifica en su artículo primero esta norma, que establece como fin del convenio la garantía del respeto a los derechos y libertades fundamentales, en concreto a su vida privada con respecto a tratamiento de los datos de cualquier persona, con cualquier nacionalidad o residencia, en el territorio de cada parte. Dice este artículo literalmente que *"el fin del presente Convenio es garantizar, en el territorio de cada parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de 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 ("protección de datos")".*

No olvidemos que, según se ha expuesto anteriormente, la vida privada de las personas es aquella faceta dentro de la cual existe un núcleo que protegemos con mayor fuerza, que es precisamente nuestra intimidad. Ésta última consiste en la facultad de organización que tenemos sobre la primera. Estos dos derechos son diferentes pero complementarios y ambos inherentes al ser humano.

Define igualmente el citado Convenio 108 en su artículo segundo los conceptos de "*datos de carácter personal*", "*fichero automatizado*", "*tratamiento automatizado*" y *"autoridad controladora del fichero*". Podríamos decir que en este texto se encuentra uno de los orígenes de la protección de datos personales, que hace referencia también en su artículo tercero a que dichas normas se aplicarán tanto en el sector público como en el privado. Concretamente establece este artículo como definiciones *"a los efectos del presente convenio: a) "datos de carácter personal"*

significa cualquier información relativa a una persona física identificada o identificable ("persona concernida"); b) "fichero automatizado" significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado; c) por "tratamiento automatizado" se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión; d) autoridad "controladora del fichero" significa la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuales categorías de datos de carácter personal deberán registrarse y cuales operaciones se les aplicaran".

Su capítulo II está dedicado en pleno a los principios básicos para la protección de datos, regulando conceptos que hoy han sido desarrollados más ampliamente en la normativa actual como, el compromiso entre las partes, la calidad de los datos, sus categorías y seguridad, la de garantías complementarias referidas al deber de información y el ejercicio de derechos, las excepciones y restricciones, las sanciones y recursos o la protección más amplia.

Y tampoco se olvidó ya hace más de una treintena de años el flujo trasfronterizo de datos regulado en el capítulo III, y referido en el apartado correspondiente.

En definitiva, el convenio, dedicado a la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, compromete a los países firmantes, a desarrollar en su normativa interna, una regulación específica para la protección de los datos de carácter personal. España entró a formar parte del convenio el 31 de enero de 1984.

La LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, la intimidad personal y familiar y la propia imagen (LOPHII-

Ley Orgánica sobre protección del honor, intimidad e imagen), establece en el párrafo primero que: *"Conforme al artículo dieciocho, uno, de la Constitución, los derechos al honor, a la intimidad personal y familiar y a la propia imagen tienen el rango de fundamentales, y hasta tal punto aparecen realzados en el texto constitucional que el artículo veinte, cuatro, dispone que el respeto de tales derechos constituya un límite al ejercicio de las libertades de expresión que el propio precepto reconoce y protege con el mismo carácter de fundamentales".* Puntualizando el segundo párrafo que: *"El desarrollo mediante la correspondiente Ley Orgánica, a tenor del artículo ochenta y uno, uno, de la Constitución, del principio general de garantía de tales derechos contenidos en el citado artículo dieciocho, uno, de la misma constituye la finalidad de la presente ley".* Así mismo, el párrafo quinto nombra los llamados derechos de la personalidad y dice que: *"Los derechos garantizados por la ley han sido encuadrados por la doctrina jurídica más autorizada entre los derechos de la personalidad, calificación de la que obviamente se desprende el carácter de irrenunciable irrenunciabilidad referida con carácter genérico a la protección civil que la ley establece".*

En referencia directa a esta Ley, Karla Cantoral reconoce que *"es notable que en el Distrito Federal, con plena influencia de la Ley española de protección del derecho al honor, intimidad e imagen, se haya aprobado la Ley de Responsabilidad Civil para la Protección de Derecho a la Vida Privada, el Honor y la Propia Imagen…."*[112]. Además a nivel internacional, según ha manifestado esta autora *"La Red Iberoamericana de Protección de Datos (RIPD) surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de datos celebrado en Antigua, Guatemala, del 1º al 6 de*

[112]CANTORAL DOMÍNGUEZ, Karla: *"Derecho de protección de datos personales en la salud"*. Editorial Novum, MEXICO D.F., 2012. Pág. 37.

junio de 2003, con la asistencia de representantes de 14 países iberoamericanos"[113].

Esta misma autora respecto de los derechos de la personalidad manifiesta que *"…precisamente porque hay que salvaguardar la existencia física y la integridad moral y espiritual del individuo-del sujeto de derecho-, ha sido imprescindible la construcción de los denominados derechos de la personalidad…"*[114] Y especifica que *"…en el derecho español, por ejemplo, el tema ha quedado solucionado a favor de la posición pluralista de tales derechos"*[115].

A propósito de los derechos de la personalidad, Ana Isabel Herran Ortiz recoge, por su parte que *"las diversas definiciones consultadas respecto a los derechos de la personalidad coinciden en afirmar que se trata de bienes que garantizan el disfrute por cada persona de sus propias facultades físicas, morales e intelectuales, sin los cuales el ser humano se vería desprovisto de sus principales garantías para asegurar el pleno desarrollo de su persona. Entre los derechos de la personalidad destaca el derecho a la intimidad"*[116]. Y nos recuerda que *"no ha de olvidarse la significación de esta norma que estableció la protección en el ámbito civil de los derechos de la personalidad que hasta entonces descansaba del art. 1902 CC que impone la obligación de responder civilmente a la realización de un comportamiento dañoso"*[117]. Ya que, según sostiene *"el artículo 18 de la CE se ha visto desarrollado legislativamente por la LO 1/1982 de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen"*[118].

[113] Ibídem. Pág. 81.

[114] Ibídem. Pág. 9.

[115] Ibídem. Pág. 10.

[116] HERRÁN ORTIZ, Ana Isabel: *"La violación de la intimidad en la protección de datos personales"*. Dykinson, Madrid 1.999. Pág. **34.**

[117] Ibídem. Pág.49.

[118] Ibídem. Pág.49.

Retomando la Ley del derecho al honor, su artículo 1 establece en su punto primero que: *"El derecho fundamental al honor, a la intimidad personal y familiar y a la propia imagen, garantizado en el artículo dieciocho de la Constitución, será protegido civilmente frente a todo género de intromisiones ilegítimas, de acuerdo con lo establecido en la presente Ley Orgánica*". Y en su punto tercero que: "*El derecho al honor, a la intimidad personal y familiar y a la propia imagen es irrenunciable, inalienable e imprescriptible. La renuncia a la protección prevista en esta ley será nula, sin perjuicio de los supuestos de autorización o consentimiento a que se refiere el artículo segundo de esta ley*".

Con el cometido de desarrollar el párrafo 4º del artículo 18 de la Constitución, se aprueba en España la antes citada Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), cuya, a mi parecer, brillante exposición de motivos, realiza un cercano examen de la situación reciente respecto a esta materia. Vale la pena quedarse con estas afortunadas valoraciones, ya que la norma posterior que la deroga carece de ellas. Me refiero a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personal (LOPD), que no cuenta en su redacción con una exposición de motivos como su antecesora, pero que incluye cambios importantísimos respecto de esta; probablemente uno de los más significativos sea la ampliación del objeto de la misma al tratamiento de los datos personales en general, y no solo a los que se traten de forma automatizada. Ya lo dice su art.2, *"…se aplicará a los datos de carácter personal almacenados en soporte físico que los haga susceptibles de tratamiento".* Pero esta cuestión será analizada más adelante en su lugar correspondiente.

Según he manifestado en otras ocasiones *"España ha desarrollado desde 1992 una completa normativa sobre Protección de Datos Personales, desarrollo normativo viene motivado por un*

compromiso con Europa. En la actualidad, las normas esenciales que desarrollan el derecho fundamental a la protección de datos son la Ley Orgánica 15/1999, de Protección de Datos Personales (LOPD) y su correspondiente reglamento de desarrollo, el RLOPD (RD 1720/2007, de 21 de diciembre)"[119]*.* Pero *"pese a la normativa, surgen a diario problemas en todos los sectores, incluido el sanitario. No es fácil proteger de forma íntegra los datos de los pacientes en la vida cotidiana de un centro sanitario, en el que entran y salen datos constantemente, ni mucho menos controlar que se apliquen todas las medidas necesarias. Quizás la labor debería comenzar por concienciar al personal que maneja los datos, de la importancia de la protección de los datos y, de que es un derecho constitucional de los ciudadanos que hay que respetar a través del cumplimiento de la normativa"*[120]*.*

El nacimiento en Luxemburgo de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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 (D95/46- Directiva sobre protección en el tratamiento de datos), marca un antes y un después en la protección de los datos personales en nuestro país. Comienza refiriéndose este texto a la actual situación de tránsito de datos entre los Estados, y establece así las normas para la regulación de la materia. A través de ella se establecen para los estados miembros de la Comunidad Europea, los principios básicos en materia de protección de datos que deben regir en el ordenamiento interno de cada uno de ellos, con el objeto de garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas y, en particular, del derecho a

[119] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

[120] VIDAL RASO, Marta:*"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

la intimidad, en lo que respecta al tratamiento de sus datos personales. De este modo, queda ampliada la protección de los datos personales contenidos en cualquier tipo de soporte.

Con esta ampliación, se refiere la actual Ley de Protección de datos a los ficheros y tratamientos no automatizados, en su disposición adicional primera, estableciendo el plazo de 12 años a contar desde el 24 de octubre de 1995, para la adecuación a la presente Ley Orgánica, así como la comunicación a la Agencia de Protección de Datos –organismo creado por la LORTAD para desarrollar y proteger el derecho a la protección de datos personales- de los ficheros que hayan sido generados.

Entre la larga lista de considerandos que integran esta normativa, hay que resaltar los siguientes puntos que ha tenido en cuenta en su redacción. En primer lugar los sistemas de tratamiento de datos que se encuentran a disposición del hombre y que deben respetar los derechos y libertades fundamentales, en concreto la intimidad, sin dejar de contribuir al desarrollo económico y social y al desarrollo y bienestar de la sociedad, así lo dice literalmente el segundo considerando: *"Considerando que 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…".*

Además regula esta norma el aumento de intercambio de información a través de las nuevas tecnologías y su incesante avance, según establece el cuarto considerando *"Considerando que se recurre cada vez más en la Comunidad al tratamiento de datos personales en los diferentes sectores de actividad económica y social; que el avance de las tecnologías de la información facilita considerablemente el tratamiento y el intercambio de dichos datos".*

Y la inserción en este aspecto del sector empresarial dentro de la Unión Europea, según establece el quinto considerando: *"Considerando que la integración económica y social resultante del establecimiento y funcionamiento del mercado interior, definido en el artículo 7 A del Tratado, va a implicar necesariamente un aumento notable de los flujos transfronterizos de datos personales entre todos los agentes de la vida económica y social de los Estados miembros, ya se trate de agentes públicos o privados; que el intercambio de datos personales entre empresas establecidas en los diferentes Estados miembros experimentará un desarrollo; que las administraciones nacionales de los diferentes Estados miembros, en aplicación del Derecho comunitario, están destinadas a colaborar y a intercambiar datos personales a fin de cumplir su cometido o ejercer funciones por cuenta de las administraciones de otros Estados miembros, en el marco del espacio sin fronteras que constituye el mercado interior".*

Las garantías legales que establecen las normas nacionales de los derechos y libertades fundamentales en general y del respeto a la vida privada en particular, ya reconocido en el Convenio Europeo de Derechos Humanos y Libertades Fundamentales, las establece el décimo considerando: *"Considerando que las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del citado Convenio, así como en los principios generales del Derecho comunitario; que, por lo tanto, la aproximación de dichas legislaciones no debe conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la Comunidad".*

Esta directiva pretende ampliar lo ya establecido en este sentido por el Convenio 108 del Consejo de Europa, que será

analizado a continuación, según el cual dice el onceavo considerando: *"Considerando que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales".*

No se puede olvidar tampoco, que en la actual sociedad de la información la imagen y el sonido forman un papel cada vez más importante, debiendo regularse debidamente el tratamiento de este tipo de datos, según dice el catorceavo considerando: *"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…".*

Todos los principios de protección deberán aplicarse a toda información relativa a personas identificadas o identificables, según dice el vigésimo sexto considerando: *"Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; 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; que los códigos de conducta con arreglo al artículo 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado".*

Tanto si el tratamiento de sus datos es automatizado como manual, según dice el vigésimo séptimo considerando, *"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 la contrario daría lugar a riesgos graves de alusión; 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…".*

Respecto de la licitud, consentimiento y pertinencia de los datos dice el vigésimo octavo considerando de la citada Directiva: *"Considerando que todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados…".*

No pudiendo ser incompatibles tratamientos posteriores con el originalmente establecido, considerándose incompatibles como tal

aquellos destinados a fines históricos, estadísticos o científicos, según dice el vigésimo noveno considerando: *"Considerando que el tratamiento ulterior de datos personales, con fines históricos, estadísticos o científicos no debe por lo general considerarse incompatible con los objetivos para los que se recogieron los datos, siempre y cuando los Estados miembros establezcan las garantías adecuadas; que dichas garantías deberán impedir que dichos datos sean utilizados para tomar medidas o decisiones contra cualquier persona…".*

Estos dos últimos párrafos están directamente relacionados con el principio de calidad que se examinará en posteriores apartados.

Contempla también dicha directiva la comunicación por parte de los Estados miembros a terceros con fines de prospección comercial permitiendo siempre oponerse a los interesados sin gastos ni explicaciones, según dice el trigésimo considerando: *"Considerando que para ser lícito el tratamiento de datos personales debe basarse además en el consentimiento del interesado o ser necesario con vistas a la celebración o ejecución de un contrato que obligue al interesado, o para la observancia de una obligación legal o para el cumplimiento de una misión de interés público o para el ejercicio de la autoridad pública o incluso para la realización de un interés legítimo de una persona, siempre que no prevalezcan los intereses o los derechos y libertades del interesado; que, en particular, para asegurar el equilibrio de los intereses en juego, garantizando a la vez una competencia efectiva, los Estados miembros pueden precisar las condiciones en las que se podrán utilizar y comunicar a terceros datos de carácter personal, en el desempeño de actividades legítimas de gestión ordinaria de empresas y otras entidades; que los Estados miembros pueden asimismo establecer previamente las condiciones en que pueden efectuarse comunicaciones de datos personales a terceros con fines de prospección comercial o de prospección realizada por una institución benéfica u otras*

asociaciones o fundaciones, por ejemplo de carácter político, dentro del respeto de las disposiciones que permiten a los interesados oponerse, sin alegar los motivos y sin gastos, al tratamiento de los datos que les conciernan".

En relación a los datos de salud, o cualesquiera otros que por su naturaleza puedan comprometer la intimidad o las libertades fundamentales, no se tratarán salvo con el consentimiento explícito del interesado, regulándose igualmente las excepciones por necesidades específicas a esta prohibición, según dice el trigésimo tercero considerando: *"Considerando, por lo demás , que los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo en caso de que el interesado haya dado su consentimiento explícito; que deberán constar de forma explícita las excepciones a esta prohibición para necesidades específicas, en particular cuando el tratamiento de dichos datos se realice con fines relacionados con la salud, por parte de personas físicas sometidas a una obligación legal de secreto profesional, o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales…".*

Igualmente se establecerán excepciones a la prohibición del tratamiento de datos sensibles por motivos importantes de interés público, según dice el trigésimo cuarto considerando: *"Considerando que también se deberá autorizar a los Estados miembros, cuando esté justificado por razones de interés público importante, a hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro enfermedad, la investigación científica y las estadísticas*

públicas; que a ellos corresponde, no obstante, prever las garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida privada de las personas…".

Cuando los datos no provengan del interesado debe informarse al interesado, en última instancia, cuando los datos se comuniquen a un tercero, salvo que ya esté informado, esté previsto por ley o exija esfuerzos desproporcionados, según establece el trigésimo noveno considerando: *"Considerando que determinados tratamientos se refieren a datos que el responsable no ha recogido directamente del interesado; que, por otra parte, pueden comunicarse legítimamente datos a un tercero aún cuando dicha comunicación no estuviera prevista en el momento de la recogida de los datos del propio interesado; que, en todos estos supuestos, debe informarse al interesado en el momento del registro de los datos o, a más tardar, al comunicarse los datos por primera vez a un tercero…".*

A este respecto, y en relación con el sector sanitario, hay un sector doctrinal que comenta que *"…la LOPD se plantea además la posibilidad de que los datos no sean obtenidos de los propios interesados sino de un tercero, supuesto muy frecuente en las urgencias médicas. En este caso siempre que no haya existido una información previa al titular de los datos, el responsable del fichero, deberá informar, dentro de los tres meses siguientes al momento del registro…"*[121] Este plazo es en clara referencia al 5.4 de la LOPD que será comentado a continuación en el apartado correspondiente. Y como este mismo sector de la doctrina expresa *"…el consentimiento está íntimamente relacionado con el deber de información, aunque, bien es cierto, que existen supuestos excepcionales en los que*

[121] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso: *"La protección de datos personales en el ámbito sanitario".* Editorial Aranzadi, Navarra 2002. Pág. 94.

información y consentimiento no tienen que ir necesariamente unidos…"[122]*.*

Se reconoce además plenamente el derecho de acceso a los datos exactos y a la licitud de su tratamiento, que podrá ser limitado, al igual que el de información, en el caso de los datos médicos, para la protección del interesado o de terceros, de modo que estos sean proporcionados por un facultativo en medicina; según establece el cuatrigésimo considerando del referido Tratado de la Unión Europea: *"Considerando, no obstante, que no es necesario imponer esta obligación si el interesado ya está informado, si el registro o la comunicación están expresamente previstos por la ley o si resulta imposible informarle, o ello implica esfuerzos desproporcionados, como puede ser el caso para tratamientos con fines históricos, estadísticos o científicos; que a este respecto pueden tomarse en consideración el número de interesados, la antigüedad de los datos, y las posibles medidas compensatorias".*

Exigiendo la adopción de medidas técnicas y organizativas apropiadas, y el seguimiento de que los Estados miembros cumplan esas medidas y garanticen un nivel de seguridad apropiado, establecido en el cuatrigésimo primero considerando: *"Considerando que cualquier persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento, para cerciorarse, en particular, de su exactitud y de la licitud de su tratamiento; que por las mismas razones cualquier persona debe tener además el derecho de conocer la lógica que subyace al tratamiento automatizado de los datos que la conciernan, al menos en el caso de las decisiones automatizados a que se refiere el apartado 1 del artículo 15; que este derecho no debe menoscabar el secreto de los negocios ni la propiedad intelectual y en particular el derecho de autor que proteja el programa informática; que no*

[122] Ibídem. Pág.97.

obstante esto no debe suponer que se deniegue cualquier información al interesado".

Cuando se ofrezcan servicios a través de telecomunicaciones, el responsable del tratamiento será de quien proceda en mensaje y no el ofertante del servicio de transmisión, según establece el cuatrigésimo segundo considerando: *"Considerando que, en interés del interesado de que se trate y para proteger los derechos y libertades de terceros, los Estados miembros podrán limitar los derechos de acceso y de información; que podrán, por ejemplo, precisar que el acceso a los datos de carácter médico únicamente pueda obtenerse a través de un profesional de la medicina…*

Siempre las transferencias de datos a terceros países será aceptando las disposiciones establecidas por los estados miembros, según establece el cuatrigésimo sexto considerando: *"Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado; que corresponde a los Estados miembros velar por que los responsables del tratamiento respeten dichas medidas; que esas medidas deberán garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse…".*

A este propósito establece también el cuatrigésimo séptimo considerando que: *"Considerando que cuando un mensaje con datos personales sea transmitido a través de un servicio de telecomunicaciones o de correo electrónico cuyo único objetivo sea transmitir mensajes de ese tipo, será considerada normalmente responsable del tratamiento de los datos personales presentes en el*

mensaje aquella persona de quien proceda el mensaje y no la que ofrezca el servicio de transmisión; que, no obstante, las personas que ofrezcan estos servicios normalmente serán consideradas responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio…".

Igualmente establece el quincuagésimo quinto considerando que: *"Considerando que las legislaciones nacionales deben prever un recurso judicial para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados; que los daños que pueden sufrir las personas a raíz de un tratamiento ilícito han de ser reparados por el responsable del tratamiento de datos, el cual sólo podrá ser eximido de responsabilidad si demuestra que no le es imputable el hecho perjudicial, principalmente si demuestra la responsabilidad del interesado o un caso de fuerza mayor; que deben imponerse sanciones a toda persona, tanto de derecho privado como de derecho público, que no respete las disposiciones nacionales adoptadas en aplicación de la presente Directiva".* Y en último lugar respecto de este tema establece el sexagésimo considerando que: *"Considerando que, en cualquier caso, las transferencias hacia países terceros sólo podrán efectuarse si se respetan plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la presente Directiva, y en particular, de su artículo 8…".*

Los estados miembros y la Comisión deben propiciar la creación de códigos de conducta sectoriales en aplicación de esta directiva y de sus legislaciones específicas, según dice el sexagésimo primero considerando: *"Considerando que los Estados miembros y la Comisión, dentro de sus respectivas competencias, deben alentar a los sectores profesionales para que elaboren códigos de conducta a fin de facilitar, habida cuenta del carácter específico del tratamiento de datos efectuado en determinados*

sectores, la aplicación de la presente Directiva respetando las disposiciones nacionales adoptadas para su aplicación…".

Tras la lectura de esta larga lista de considerandos, podemos apreciar las similitudes con las cuestiones que posteriormente son desarrolladas por la normativa nacional en materia de protección de datos de carácter personal.

Entrando de lleno en el articulado de la Directiva, encontramos que su artículo 1.1, establece que como objetivo de la misma la garantía que deben dar los estados miembros sobre la protección de los derechos y libertades fundamentales, en especial la intimidad en relación al tratamiento de datos personales. Así establece que, *"los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de 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."* Y matiza en el punto segundo de este artículo que *"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".*

Del mismo modo, el novedoso tema del soporte en el que se recojan los datos personales, que pueden ser automatizados o no, lo contempla el artículo 3.1 de esta norma, que considera respecto del ámbito de aplicación tanto el tratamiento total como parcialmente automatizado, así como el tratamiento no automatizado de datos que vayan a pasar a formar parte de fichero, recogiendo que *"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".* Y el artículo 3.2, se refiere a aquello a lo que no alcanza esta directiva, el cual establece que *"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 sustitución de la LORTAD por otra norma nueva, encuentra su razón en la Directiva 95/46 que se acaba de analizar. Pero hay que resaltar, que anterior a la nueva LOPD, es aprobado por RD 994/1999, de 11 de junio, el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (en adelante RMS). Su derogación por el actual Reglamento de Protección de Datos, aprobado por el RLOPD, nos hace encontrarnos en un momento óptimo, en el que gozamos de una ley y su correspondiente reglamento de desarrollo. Recordemos que esta última ha convivido con un reglamento de desarrollo que no le correspondía durante muchos años, en cuyo periodo, ha existido un desajuste por la diferencia de materias reguladas, mucho más extensa en la LOPD.

Cabe resaltar, como importante diferencia entre LORTAD y LOPD que, de forma paralela a como se ha expuesto hace unas líneas en relación al artículo 3 de la Directiva 95/46, el artículo 2.1 de la LOPD establece respecto al ámbito de aplicación que: *"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. Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal: a) Cuando el tratamiento sea efectuado en territorio español en el marco de las*

actividades de un establecimiento del responsable del tratamiento. b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público. c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito".

E igualmente, el punto segundo del artículo 2 de la LOPD, establece las exclusiones de este ámbito de aplicación, recogiendo que: *"El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación: a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas. 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 de Protección de Datos".* Además el punto tercero de este mismo artículo, complementa a lo anterior estableciendo que: *"Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales: a) Los ficheros regulados por la legislación de régimen electoral. b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública. c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas. d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes. 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".

Y en directa referencia a lo anteriormente recogido en el artículo 2 de la LOPD, el RLOPD en el tercer párrafo del punto tercero de su introducción establece que: *"El título I contempla el objeto y ámbito de aplicación del reglamento. A lo largo de la vigencia de la Ley Orgánica 15/1999, se ha advertido la conveniencia de desarrollar el apartado 2 de su artículo 2 para aclarar qué se entiende por ficheros y tratamientos relacionados con actividades personales o domésticas, aspecto muy relevante dado que están excluidos de la normativa sobre protección de datos de carácter personal".* No obstante, también esta norma regula en su artículo cuarto respecto de los ficheros excluidos que: *"El régimen de protección de los datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos: a) A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares. b) A los sometidos a la normativa sobre protección de materias clasificadas. c) A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos".*

El Tratado de la Unión Europea, hecho en Maastricht, el 7 de febrero de 1992 (TUE- Tratado de la UE), dice en los primeros cuatro párrafos de su texto que: *"RESUELTOS a salvar una nueva etapa en el proceso de integración europea emprendido con la constitución de las Comunidades Europeas, INSPIRÁNDOSE en la herencia cultural, religiosa y humanista de Europa, a partir de la cual se han*

desarrollado los valores universales de los derechos inviolables e inalienables de la persona, así como la libertad, la democracia, la igualdad y el Estado de Derecho, RECORDANDO la importancia histórica de que la división del continente europeo haya tocado a su fin y la necesidad de sentar unas bases firmes para la construcción de la futura Europa, …" estableciendo a continuación en su artículo primero que, *"por el presente Tratado, las ALTAS PARTES CONTRATANTES constituyen entre sí una UNIÓN EUROPEA, en lo sucesivo denominada "Unión", a la que los Estados miembros atribuyen competencias para alcanzar sus objetivos comunes. El presente Tratado constituye una nueva etapa en el proceso creador de una unión cada vez más estrecha entre los pueblos de Europa, en la cual las decisiones serán tomadas de la forma más abierta y próxima a los ciudadanos que sea posible. La Unión se fundamenta en el presente Tratado y en el Tratado de Funcionamiento de la Unión Europea (en lo sucesivo denominados <<los Tratados>>). Ambos Tratados tienen el mismo valor jurídico. La Unión sustituirá y sucederá a la Comunidad Europea".*

Así mismo, su artículo segundo continúa diciendo que *"la Unión se fundamenta en los valores de respeto de la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías. Estos valores son comunes a los Estados miembros en una sociedad caracterizada por el pluralismo, la no discriminación, la tolerancia, la justicia, la solidaridad y la igualdad entre mujeres y hombres".*

Igualmente contamos con el Tratado de funcionamiento de Unión Europea (TFUE), que según establece su artículo 1.1 *"…organiza el funcionamiento de la Unión y determina los ámbitos, la delimitación y las condiciones de ejercicio de sus competencias" Y aclara el punto segundo que "El presente Tratado y el Tratado de la Unión Europea constituyen los Tratados sobre los que se*

fundamenta la Unión. Estos dos Tratados, que tienen el mismo valor jurídico, se designarán con la expresión <<los Tratados>>".

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI- Ley del comercio electrónico) tiene como objeto incorporar al ordenamiento español una directiva europea en esta materia, a propósito del gran desarrollo de las telecomunicaciones, en especial de internet como vía de comunicación de la información. Y así lo especifica literalmente su exposición de motivos en el primer párrafo de su punto primero: *"La presente Ley tiene como objeto la incorporación al ordenamiento jurídico español de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior…".* Y sigue diciendo en el siguiente párrafo: *"Lo que la Directiva 2000/31/CE denomina "sociedad de la información" 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…".* El concepto del título de la Ley "*servicios de la sociedad de la información*", se define acogiendo de forma amplia a las acciones realizadas en el comercio por vía electrónica, siempre que haya actividad económica para quien explote un sitio en internet. De hecho, el primer párrafo del segundo punto de esta exposición de motivos, lo recoge de forma muy detallada: *"Se acoge, en la Ley, un concepto amplio de "servicios de la sociedad de la información", que engloba, además de la contratación de bienes y servicios por vía electrónica, el suministro de información por dicho medio (como el que efectúan los periódicos o revistas que pueden encontrarse en la red), las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los*

propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...), siempre que represente una actividad económica para el prestador. Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico".

Incluso la accesibilidad para los discapacitados por este medio, en especial a la información proporcionada por las administraciones públicas, según se comprometió en su resolución sobre accesibilidad de los sitios web públicos y de su contenido el Consejo de la Unión Europea de 25 de marzo de 2002. El penúltimo párrafo del punto cuarto de esta exposición de motivos así lo recoge: *"Asimismo, se contempla en la Ley una serie de previsiones orientadas a hacer efectiva la accesibilidad de las personas con discapacidad a la información proporcionada por medios electrónicos, y muy especialmente a la información suministrada por las Administraciones públicas, compromiso al que se refiere la resolución del Consejo de la Unión Europea de 25 de marzo de 2002, sobre accesibilidad de los sitios web públicos y de su contenido".*

Hay unas materias que por su interés para este estudio resaltaré de la normativa que nos ocupa. Por un lado, el objeto de la misma, regulado en su artículo 1.2, el cual establece que *"las disposiciones contenidas en esta Ley se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas ajenas al ámbito normativo coordinado, o que tengan como finalidad la protección de la salud y seguridad pública, incluida la salvaguarda de*

la defensa nacional, los intereses del consumidor, el régimen tributario aplicable a los servicios de la sociedad de la información, la protección de datos personales y la normativa reguladora de defensa de la competencia".

Por otro lado, respecto del deber de colaboración de los prestadores de servicios de intermediación, establece el artículo 11.3 que *"…en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados".* Y en cuanto a las obligaciones de información sobre seguridad, dice el 12.1 bis, que regula las obligaciones de información sobre seguridad, a propósito de los proveedores de servicios de intermediación establecidos en España, y que aquellos *"…que realicen actividades consistentes en la prestación de servicios de acceso a Internet, estarán obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados".* Puntualizando en su apartado segundo que *"los proveedores de servicios de acceso a Internet y los prestadores de servicios de correo electrónico o de servicios similares deberán informar a sus clientes de forma permanente, fácil, directa y gratuita sobre las medidas de seguridad que apliquen en la provisión de los mencionados servicios".*

En cuanto al régimen jurídico, el 19.2 establece que: "*En todo caso, será de aplicación la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo, en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales".* Y

aunque en el sector sanitario no sea muy ortodoxo, por experiencia de que estas acciones se producen, sobre todo en la sanidad privada, pero también en la pública, a través de la filtración de datos que de otra forma, por no tenerlos nadie más en su poder, no pudieran haber llegado a manos de quienes ofrecen servicios y productos sanitarios, es necesario citar que el artículo 21.1, exige el previo consentimiento del interesado para el envío de publicidad por medios electrónicos recogiendo que *"queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas".*

Esto adquiere una mayor importancia si lo analizamos en el sector sanitario, ya que si, por ejemplo, nos llaman de un centro privado para darnos cita en la consulta de cardiología, por haber mucha espera en el sector público, habiendo previo acuerdo de colaboración entre ambos centros, público y privado, podría estar vulnerándose este precepto, si previamente no nos han pedido consentimiento para pasar nuestros datos del centro público en el que nos atienden, al centro privado con el que existe el concierto de colaboración. Se trata de un caso real, en que se ha querido privatizar claramente la sanidad, habiendo comprobado de forma posterior que no existía tal lista de espera para el citado servicio en el sector público; en aras de atención temprana, esta es una tendencia muy habitual en la actualidad, que afortunadamente se está frenando por los propios pacientes, así como por el propio personal sanitario que no cede a estas gestiones o fugas no consentidas de información; pensemos que lo que se está dando son datos sobre nuestra salud. No obstante se verá más adelante que este traspaso de información se encuentra amparado por la normativa.

Y por último, la disposición adicional segunda se refiere en concreto a los medicamentos y productos sanitarios en cuanto a la prestación de servicios de sociedad de la información, que debe regirse por su normativa específica, diciendo literalmente que *"la prestación de servicios de la sociedad de la información relacionados con los medicamentos y los productos sanitarios se regirá por lo dispuesto en su legislación específica." En este sentido, el Real Decreto 1907/1996, de 2 de agosto, sobre publicidad y promoción comercial de productos, actividades o servicios con pretendida finalidad sanitaria (RDPS- Real Decreto sobre Publicidad Sanitaria), establece en sus párrafos iniciales que la Ley General de Sanidad "… ordena que las Administraciones públicas, en el ámbito de sus competencias, realicen «un control de la publicidad y propaganda comerciales para que se ajusten a criterios de veracidad en lo que atañe a la salud y para limitar todo aquello que puede constituir un perjuicio para la misma» (artículo 27). Asimismo prevé la inspección y control de la promoción y publicidad de los centros y establecimientos sanitarios (artículo 30.1), la autorización previa de la publicidad de los medicamentos y productos sanitarios (artículo 102)…".*

El artículo 27 establece por su parte que: *"Las Administraciones públicas, en el ámbito de sus competencias, realizarán un control de la publicidad y propaganda comerciales para que se ajusten a criterios de veracidad en lo que atañe a la salud y para limitar todo aquello que pueda constituir un perjuicio para la misma, con especial atención a la protección de la salud de la población más vulnerable".* Y el artículo 30.1, dice literalmente: *"Todos los Centros y establecimientos sanitarios, así como las actividades de promoción y publicidad, estarán sometidos a la inspección y control por las Administraciones Sanitarias competentes".* En efecto, este ejemplo podría ser una manera de promocionar un centro privado, ya que se produciría una contraprestación por el servicio delegado; pero se me ocurren más ejemplos, también reales, en los que un rehabilitador te

da los datos de un centro privado para que te hagas unas plantillas que le irán muy bien a tu dolencia; en este caso no transfiere los datos a nadie, pero claramente está publicitando sus servicios. El 102 así mismo recoge en su punto primero que *"la información y promoción de los medicamentos y los productos sanitarios dirigida a los profesionales se ajustará a las condiciones técnicas y científicas autorizadas del producto y cumplirá con las exigencias y controles previstos en el artículo 76 de la Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios"*, especificando en su punto segundo que *"la publicidad de productos sanitarios dirigida al público requerirá la autorización previa de los mensajes por la autoridad sanitaria. Se procederá a revisar el régimen de control de la publicidad de los productos sanitarios atendiendo a su posible simplificación sin menoscabo de las garantías de protección de la salud pública que ofrece el régimen actual".*

La LOPD derogó, como ya se ha apuntado, a la LORTAD y es hasta hoy, la norma fundamental en materia de protección de datos con la que contamos, apoyada por su reglamento de desarrollo, el RLOPD.

Pero aunque la fundamental, no es la única norma que existe en nuestro país en materia de protección de datos, a nivel provincial contamos además con la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la agencia vasca de protección de datos, que comienza su exposición de motivos apostando por el avance tecnológico *"los avances de la técnica se han acelerado en los últimos tiempos. Actualmente, el uso de la informática permite tratar gran cantidad de datos relativos a las personas físicas, pudiendo llegar a conocer aspectos relacionados con las mismas que suponen una intromisión en su intimidad. Los ordenamientos jurídicos no pueden permanecer insensibles ante la eventualidad de usos perversos de las*

posibilidades tecnológicas, en detrimento de espacios que deben quedar reservados a la intimidad personal". Y que en su artículo segundo donde recoge el ámbito de aplicación el ámbito de aplicación, el cuarto apartado establece en relación al ámbito sanitario que: *"Las instituciones y centros sanitarios de carácter público y los profesionales a su servicio 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 tratadas en los mismos, de acuerdo con lo dispuesto en la legislación sectorial sobre sanidad, sin perjuicio de la aplicación de lo dispuesto en esta ley en todo lo que no sea incompatible con aquella legislación".*

También contamos, a nivel autonómico, con la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, la cual establece en el tercer párrafo de su preámbulo que: *"La Agencia Catalana de Protección de Datos, autoridad independiente creada por la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, ha velado por la garantía del derecho a la protección de datos en el ámbito de las administraciones públicas de Cataluña mediante el asesoramiento, la difusión del derecho y el cumplimiento de las funciones de control establecidas por el ordenamiento jurídico".*

La Carta de los Derechos Fundamentales de la Unión Europea de marzo de 2010 (CDFUE), teniendo en cuenta los derechos provenientes de las tradiciones constitucionales, así como de las obligaciones internacionales establecidas entre los estados miembros que firmaron el Convenio Europeo para la protección de los Derechos Humanos y las Libertades Fundamentales, y las Cartas Sociales adoptadas por el Consejo de Europa y la Unión Europea, el tribunal de justicia de este último organismo y el Tribunal Europeo de Derechos Humanos. Así establece en su preámbulo que *"la presente Carta reafirma, dentro del respeto de las competencias y misiones de la Unión, así como del principio de subsidiariedad, los derechos*

que emanan, en particular, de las tradiciones constitucionales y las obligaciones internacionales comunes a los Estados miembros, del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, las Cartas Sociales adoptadas por la Unión y por el Consejo de Europa, así como de la jurisprudencia del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos…".

Reconoce este texto el derecho a la integridad de la persona, en concreto en el marco de la medicina y la biología, donde deberá respetarse el consentimiento libre e informado de acuerdo a lo establecido en el artículo 3.2 a) de este texto, que dice literalmente: *"En el marco de la medicina y la biología se respetarán en particular: a) el consentimiento libre e informado de la persona de que se trate, de acuerdo con las modalidades establecidas por la ley".* Recoge también el respeto a la vida privada y familiar en su artículo 7, al establecer que *"toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones"*. Así como el derecho a la protección de los datos de carácter personal, que serán tratados de forma leal, concreta y consentida, con el derecho de acceso a los datos del individuo y a su rectificación en el artículo 8, según el cual *"toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. El respeto de estas normas estará sujeto al control de una autoridad independiente."* Igualmente se reconoce el derecho a la salud preventiva y asistencial de acuerdo a lo establecido en la ley, con el fin de conseguir un nivel de protección elevado.

Respecto al derecho a la salud, Karla Cantoral ha manifestado que *"el derecho a la salud está expresamente reconocido en la*

Declaración Universal de los Derechos Humanos de 1948, donde se estatuye que toda persona tiene derecho a un nivel de vida que le asegure, así como a su familia, la salud y el bienestar, y en especial la alimentación, el vestido, la vivienda, la asistencia médica y los servicios sociales necesarios…"[123]*.* Y estima que *"en el ámbito del derecho a la salud, es preciso analizar el concepto de expediente clínico para que dentro de la relación médico-paciente se determine la posición que ocupa cada una de las personas que intervienen en la actividad médica…"*[124]*.*

Herrero de la Fuente por su parte, opina sobre el derecho a la protección de datos personales que *"el estudio del derecho a la protección de datos personales, recogido en el art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea, a nuestro juicio, ofrece un doble interés. Por un lado, nos permite conocer la configuración del «derecho subjetivo» considerado. Pero además, en segundo lugar, nos pone de relieve, de forma agudísima y como muy pocos de los demás derechos de la CDF lo hacen (quizás los derechos de propiedad, igualdad, sufragio, libertad de circulación), una serie de problemas normativos que se derivan de la discutible conformación de los derechos que resulta de la Carta"*[125]*.* No en vano asegura que, *"la Carta de los Derechos Fundamentales nace en cumplimiento del mandato de la cumbre de Colonia de junio de 1999. En dicha cumbre se acordó, en primer lugar, que «en el presente estado de la Unión Europea, los derechos fundamentales aplicables en el nivel comunitario deberían consolidarse en una Carta para hacerse más evidentes» (n.º44). Además, en segundo*

[123] CANTORAL DOMÍNGUEZ, Karla: *"Derecho de protección de datos personales en la salud"*. Editorial Novum, MEXICO D.F., 2012. Pág. 104.

[124] Ibídem. Pág. 117.

[125] HERRERO DE LA FUENTE, Alberto A (Editor): *"La carta de los Derechos Fundamentales de la Unión Europea. Una perspectiva multidisciplinar"*. Cuadernos del Instituto Rei Alfonso Henriques de Cooperación Transfronteriza n.º2, Fundación Rei Alfonso Henriques, Zamora, 2003. Pág. 173.

lugar, se acordó que el citado documento debiera recoger los derechos de los «ciudadanos europeos»"[126].

Tras este largo recorrido, podemos hacernos una idea de la importancia que se ha dado, tanto a nivel nacional, como internacional, a la protección de datos en los últimos tiempos.

III.1.b. Normativa sanitaria:

Entrando más de lleno en materia sanitaria, la Ley 14/1986, de 25 de abril, General de Sanidad (LGS- Ley General de Sanidad), por su parte, establece en su artículo 10.1 que *"todos tienen los siguientes derechos con respecto a las distintas administraciones públicas sanitarias: Al respeto a su personalidad, dignidad humana e intimidad, sin que pueda ser discriminado por su origen racial o étnico, por razón de género y orientación sexual, de discapacidad o de cualquier otra circunstancia personal o social".* De modo que la Ley sanitaria también se refiere al punto de partida de este estudio, lo que sumo como otra razón para reiterar la aplicación de la normativa existente en materia de protección de datos al ámbito sanitario. No obstante, el objetivo principal de esta ley, queda establecido en su artículo 1.1: *"La presente Ley tiene por objeto la regulación general de todas las acciones que permitan hacer efectivo el derecho a la protección de la salud reconocido en el artículo 43 y concordantes de la Constitución".* Y así mismo establece en su punto 3.1 *"los medios y actuaciones del sistema sanitario estarán orientados prioritariamente a la promoción de la salud y a la prevención de las enfermedades".* Diciendo su artículo sexto en el punto primero que *"las actuaciones de las Administraciones Públicas Sanitarias estarán orientadas: 1. A la promoción de la salud. 2. A promover el interés individual, familiar y social por la salud mediante la adecuada educación sanitaria de la población. 3. A garantizar que cuantas acciones sanitarias se desarrollen estén dirigidas a la prevención de las enfermedades y no sólo a la curación de las*

[126] Ibídem.

mismas. 4. A garantizar la asistencia sanitaria en todos los casos de pérdida de la salud. 5. A promover las acciones necesarias para la rehabilitación funcional y reinserción social del paciente".

Del mismo modo se ocupa esta norma de los derechos y deberes de los pacientes, recogiendo en su artículo noveno que *"los poderes públicos deberán informar a los usuarios de los servicios del sistema sanitario público, o vinculados a él, de sus derechos y deberes"*, matizando en el 10.2 los derechos sobre los servicios a disposición de los pacientes que *"a la información sobre los servicios sanitarios a que puede acceder y sobre los requisitos necesarios para su uso. La información deberá efectuarse en formatos adecuados, siguiendo las reglas marcadas por el principio de diseño para todos, de manera que resulten accesibles y comprensibles a las personas con discapacidad".* De la asignación de un profesional que le atienda, se ocupa el 10.7 al establecer que: *"A que se le asigne un médico, cuyo nombre se le dará a conocer, que será su interlocutor principal con el equipo asistencial. En caso de ausencia, otro facultativo del equipo asumirá tal responsabilidad".* La elección de médico marca el 10.13 recogiendo que: *"A elegir el médico y los demás sanitarios titulados de acuerdo con las condiciones contempladas, en esta Ley, en las disposiciones que se dicten para su desarrollo y en las que regulen el trabajo sanitario en los Centros de Salud".* Y el abastecimiento de la medicación necesaria, lo regula el 10.14 *avocando "a obtener los medicamentos y productos sanitarios que se consideren necesarios para promover, conservar o restablecer su salud, en los términos que reglamentariamente se establezcan por la Administración del Estado".* Pero además, podrán disfrutar en acciones beneficiosas para su salud, según marca el 10.10 *"a participar, a través de las instituciones comunitarias, en las actividades sanitarias, en los términos establecidos en esta Ley y en las disposiciones que la desarrollen"*, así como reclamar, si lo creen necesario, según marca el 10.11 *"a utilizar las vías de reclamación y de propuesta de sugerencias en los plazos previstos. En uno u otro*

caso deberá recibir respuesta por escrito en los plazos que reglamentariamente se establezcan".

Podemos aplicar también a los derechos fundamentales lo que dice el art. 67.4 de de la Ley General de Sanidad, al establecer que *"serán causas de denuncia del Convenio por parte de la Administración Sanitaria competente las siguientes: lesionar los derechos establecidos en los artículos 16,18, 20 y 22 de la Constitución cuando así se determine por sentencia"*. Recordemos que todos estos artículos se encuentran ubicados en el capítulo segundo, sección primera, bajo la rúbrica "*De los derechos fundamentales y de las libertades públicas*", y se refieren a las libertades ideológicas, religiosas y de culto, al honor, a la intimidad personal y familiar y a la propia imagen, así como a la libertad de expresión y de asociación.

Entre las dos leyes que han existido en nuestro país en materia de protección de datos, ya expuestas, la LORTAD y la LOPD, encontramos que en el año 1994 se realiza en Amsterdam la Consulta Europea sobre los Derechos de los Pacientes que da lugar a la Declaración para la de los derechos de los pacientes en Europa, surgida en Amsterdam en 1994 (DPPE- Declaración sobre derechos de los pacientes). Con motivo de promover los derechos de los pacientes en Europa en atención al cambio global sanitario, dando un enfoque común a las diversidades establecidas por los factores económicos, sociales, culturales y étnicos, estableciendo derechos y deberes para pacientes, profesionales e instituciones sanitarias, así como códigos profesionales, apoyo interrelaciones y encuentros que acerquen a médico y paciente, fomentar la información, concienciación, sensibilizando al público sobre la promoción de la investigación, así como la cooperación entre los organismos internacionales. Así comienza esta declaración "*La consulta europea de la OMS sobre los Derechos de los Pacientes, celebrada en Amsterdam del 28 al 30 de marzo de 1994, suscribió el documento*

anexo (Principios de los Derechos de los Pacientes en Europa: un marco común) como un grupo de principios para la promoción y aplicación de los derechos de los pacientes en los Estados europeos miembros de la OMS".

En los antecedentes de su introducción se establece que *" El desarrollo de los sistemas de salud, su creciente complejidad, el hecho de que la práctica médica se haya vuelto más arriesgada y en muchos casos más impersonal y deshumanizada, a menudo implicando burocracia, y sin olvidar el progreso realizado en la ciencia médica y de salud en la tecnología han llevado a colocar un renovado énfasis en la importancia de reconocer el derecho del individuo a la autodeterminación y a menudo en la necesidad de reformular garantías para otros derechos de los pacientes"*. Se distingue entre derechos sociales e individuales, unos se defienden para la colectividad y otros para un paciente concreto. Así establece este texto entre sus principios receptores que *"En el tratamiento de los derechos de los pacientes, debería hacerse una distinción entre los derechos sociales y los derechos individuales. Los derechos sociales en la atención sanitaria hacen referencia a la obligación social del gobierno y otras entidades públicas o privadas de proveer una atención sanitaria razonable en el sector de la salud pública para toda la población. Lo que se considera razonable en términos de volumen y oferta de servicios disponibles y el grado de sofisticación, tecnología y especialización dependerá de factores políticos, sociales, culturales y económicos. Los derechos sociales también suponen un acceso igual a la atención sanitaria para todos aquellos que vivan en un país u otras áreas geopolíticas y la eliminación de barreras discriminatorias injustificadas, ya sean económicas, geográficas, culturales, sociales o psicológicas. Los derechos sociales son disfrutados colectivamente y hacen referencia al nivel de desarrollo de la sociedad en particular. En cierta medida, están sujetos al juicio político referente a prioridades para el desarrollo de una sociedad concreta. Por el contrario, los derechos individuales en*

materia de atención al paciente se expresan con mayor facilidad en términos absolutos y cuando se transforman en algo operativo pueden ser defendidos en nombre de un paciente concreto. Estos derechos cubren áreas como la integridad de la persona, su privacidad y convicciones religiosas…".

Insta esta norma a los países a promover la mejora de los derechos de los pacientes en cooperación conjunta con las organizaciones que los integran, así, cuando se refiere el documento a la implementación de mismo, establece que *"cada país debe decidir el futuro uso de un documento como éste, al revisar sus actuales políticas respecto a la ejecución de y apoyo legislativo a, los derechos de los pacientes. Aunque con el objetivo de presentarlo de forma clara, algunas propuestas se han realizado de forma simple y concisa, el texto está formado por una serie de directrices que pueden ser utilizadas en debates políticos dentro de cada país así como en la formulación o reformulación, según cada caso, de políticas nacionales, leyes o declaraciones oficiales sobre alguno o todos los temas que se tratan. Sin embargo, esperamos que este documento tenga un valor directo para todas las partes, incluyendo a organizaciones de pacientes y consumidores implicados en la atención sanitaria, asociaciones profesionales médicas y de otros profesionales de la salud, y asociaciones de hospitales y otros establecimientos sanitarios".*

Con el objetivo de reforzar los derechos fundamentales humanizando la asistencia sanitaria, potenciando unos principios que refuercen los derechos de los pacientes, promoviendo a la vez que se haga uso de los sistemas públicos de salud, no olvida atender en cualquier ámbito territorial las necesidades concretas de los pacientes, llamado a la cooperación entre los distintos organismos tanto sanitarios como sociales. Así recoge su punto segundo al establecer los objetivos del presente texto que *"teniendo en cuenta estos antecedentes, los Principios de los Derechos de los Pacientes*

en Europa pueden ser vistos, en términos de contenido, como un documento que busca: Reafirmar los derechos fundamentales humanos en el apartado de la atención sanitaria, y en particular proteger la dignidad e integridad de la persona, así como promover el respeto del paciente como persona; Ofrecer a la consideración de los Estados Miembros un grupo de principios básicos que subrayen los derechos de los pacientes, que puedan ser utilizados al enmarcar o revisar las políticas de atención a los pacientes; Ayudar a los pacientes a obtener el beneficio completo derivado del uso de los servicios del sistema público de salud, y mitigar los efectos de cualquier problema que puedan experimentar con ese sistema; Promover y mantener relaciones beneficiosas entre los pacientes y los profesionales de la salud, y en particular alentar la participación activa del paciente; Reforzar oportunidades existentes y proporcionar nuevas oportunidades para el diálogo entre las organizaciones de los pacientes, los profesionales de la salud, las administraciones sanitarias y otros agentes sociales; Enfocar la atención nacional, regional e internacional sobre las necesidades cambiantes en los derechos de los pacientes y fomentar una cooperación internacional más estrecha en este campo; Asegurar la protección de los derechos humanos fundamentales y humanizar la asistencia que se presta a todos los pacientes, incluyendo a los más vulnerables, como los niños, pacientes psiquiátricos, los ancianos o los enfermos graves".

Se concretan además en este documento los derechos de los pacientes en unos derechos humanos que deben poder ejercer y disfrutar los pacientes basados en el respeto, la autodeterminación, la integridad y la privacidad, en unos valores sociales, culturales y morales, así como en la protección de su salud. Recoge entre los derechos humanos y valores en la atención sanitaria que *"todo el mundo tiene derecho a ser respetado como ser humano. Todo el mundo tiene derecho a la autodeterminación. Todo el mundo tiene derecho a la integridad física y mental y a la seguridad de su persona. Todo el mundo tiene derecho a que se respete su*

privacidad/intimidad. Todo el mundo tiene derecho a que se respeten sus valores morales y culturales así como sus convicciones religiosas y filosóficas. Todo el mundo tiene derecho a la protección de la salud mediante medidas apropiadas que prevengan enfermedades y garanticen la atención sanitaria y la oportunidad de lograr el más alto nivel de salud posible".

En el derecho a la atención sanitaria y tratamiento se encuentra en el apartado dedicado a los derechos de los pacientes, que tienen a recibir una atención sanitaria técnica, digna, humanizada, no discriminatoria y sin sufrimiento, que sea de calidad de forma continuada y a cambiar de médico si lo desean, y debiendo tener representación en todos los servicios sanitarios a nivel de planificación de los mismos incluidos los domiciliarios y comunitarios, así como el derecho a contar con la compañía se sus seres queridos. Concretamente establece este texto en su punto 5.1 que *"todo el mundo tiene derecho de recibir atención sanitaria adecuada a las necesidades de su salud, incluyendo cuidados preventivos y actividades dirigidas a promover la salud. Los servicios deberían estar continuamente disponibles y accesibles a todos de forma equitativa, sin discriminación y de acuerdo a los recursos financieros, humanos y materiales disponibles en una sociedad dada".* El punto 5.2 establece así mismo que *"los pacientes tienen el derecho colectivo a alguna forma de representación en cada nivel del sistema de salud en materias pertinentes a la planificación y evaluación de los servicios, incluyendo la oferta, calidad y funcionamiento de los servicios proporcionados".*

El punto tercero apunta que *"los pacientes tienen derecho a la calidad de la atención que se caracteriza a la vez por unos niveles técnicos altos y por una relación humana entre el paciente y los profesionales de la salud".*

El punto cuarto recuerda que *"los pacientes tienen derecho a la continuidad en la atención, incluyendo la cooperación entre todos los*

profesionales de la salud y/o los centros que pueden estar implicados en su diagnóstico, tratamiento y cuidado".

El punto quinto recuerda que *"dada la circunstancia en la que los profesionales de la salud deban elegir entre pacientes potenciales para recibir un tratamiento particular cuya disponibilidad es limitada, todos esos pacientes deben beneficiarse de un proceso de selección justo para dicho tratamiento. La elección debe estar basada en criterios médicos y debe realizarse sin discriminación".*

El punto sexto recoge que *"los pacientes tienen derecho a elegir y cambiar de médico u otro profesional de la salud y centro sanitario, mientras sea compatible con el funcionamiento del sistema sanitario".*

El punto séptimo establece que *"los pacientes para los que no haya motivos médicos para una estancia continuada en un centro sanitario tienen derecho a una explicación completa antes de ser trasladados a otro centro o enviados a sus casas. El traslado sólo podrá tener lugar cuando otro centro sanitario haya acordado aceptar al paciente. Cuando el paciente reciba el alta para trasladarse a su domicilio y cuando su condición lo requiera, deberían estar a su disposición servicios comunitarios y domiciliarios".*

El punto octavo recoge que *"los pacientes tienen derecho a ser tratados con dignidad en relación con su diagnóstico, tratamiento y cuidados, que deben ser proporcionados con respeto a su cultura y valores".*

El punto noveno apunta a que *"los pacientes tienen derecho a disfrutar del apoyo de sus familias, parientes y amigos durante el curso de los cuidados y tratamiento y a recibir apoyo espiritual y orientación en todo momento".*

El punto décimo que *"los pacientes tienen derecho al alivio de su sufrimiento de acuerdo al actual estado de conocimientos".* Y el

punto undécimo de este apartado quinto que *"los pacientes en fase terminal tienen derecho a una atención sanitaria humana y a morir con dignidad".*

Al ver esta larga lista de derechos se hace necesario, para comprobar la magnitud de la importancia de esta norma en relación con los datos personales y como abarca cuestiones fundamentales del ámbito médico.

Por otro lado, y a lo largo de los años, la atención sanitaria se ha venido prestando tradicionalmente de forma presencial, pero la entrada de este sector en el ámbito de las nuevas tecnologías, ha hecho que cambie esta situación, ya se ha comentado al inicio de este estudio. Una parte de la doctrina manifiesta a este respecto que *"para abordar el objetivo de evaluar la efectividad de un nuevo servicio de telemedicina se requiere establecer una comparación, centrada sobre algún tipo de medida preseleccionada, con la alternativa asistencial habitual aceptada tanto por la comunidad profesional y científica, como por la sociedad. La atención sanitaria, tanto si es suministrada de forma tradicional (presencialmente) o por medio de las tecnologías de la Información y comunicación (telemedicina), puede describirse como un proceso de convergencia y acomodación entre la demanda de los pacientes y la oferta de servicios por parte del sistema sanitario (toma de decisiones sobre diagnóstico o tratamiento) para alcanzar un objetivo final de mejora de la salud"*[127]*.*

Respecto a la prestación de la asistencia sanitaria a través de la telemedicina, Unai aberasturi Gorriño ha puesto de manifiesto que *"la incorporación de las nuevas tecnologías en el ámbito sanitario, impulsado en gran parte por los señalados proyectos, ha llevado a*

[127] Ministerio de Sanidad y Consumo Servicio Canario de la salud Consejería de Sanidad del Gobierno de Canarias: "Guía de diseño, evaluación e implantación de servicios de la salud basados en la telemedicina". Informes de Evaluación de Tecnologías Sanitarias SESCS Núm. 2006/27. Pág. 66.

que se cree una nueva forma de llevar a cabo la actividad sanitaria. Se está hablando de la telemedicina. El concepto de «telemedicina» se ha entendido de muy distintas formas. En un sentido estricto, eminentemente literal, se ha interpretado que la «telemedicina» es la práctica de la medicina a distancia. Se trata de la definición admitida por la mayoría. Esta acepción encuentra fundamento en los antecedentes históricos que se han vinculado a la telemedicina, pues las distintas experiencias que se relacionan con la telemedicina moderna, que emplea la telegrafía, telefonía, radio, TV y medios inalámbricos corno satélites y teléfonos móviles para llevar a cabo la transmisión de informaciones, se refieren a la práctica de la medicina a distancia. Esta línea interpretativa parece haber tenido eco también en las definiciones que, tanto la Organización Mundial de la Salud (OMS), como la Asociación Médica Mundial (AMM) han dado de este concepto, y ha sido aceptada también por otras instituciones. Estas definiciones pueden interpretarse, sin embargo, de otra manera. Se puede vislumbrar un concepto más amplio, donde lo relevante no es que el paciente se encuentre lejos, sino el hecho de que se empleen las TIC para la práctica de la medicina. Se entendería la telemedicina, como una nueva forma de realizar la actividad sanitaria en la que lo característico es la aplicación de las TIC en todas las áreas de la actuación sanitaria: asistencial, de gestión, de investigación, de formación, entre otras"[128].

En este sentido, y según sigue manifestando este autor, *"la evolución de la telemedicina ha sido constante. Este desarrollo ha venido de la mano de la incorporación y desarrollo de nuevas herramientas específicas dirigidas a manipular la información sanitaria de manera más eficiente. Probablemente, las más significativas sean la Historia de Salud Electrónica, la Tarjeta Sanitaria Electrónica y la Receta Electrónica. En relación al primer*

[128] ABERASTURI GORRIÑO, Unai: *"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 28.

instrumento, es sabido que la historia clínica es una de las herramientas más importantes para la prestación del servicio sanitario. Primero, constituye un documento indispensable a la hora de otorgar asistencia sanitaria. Segundo, se trata de una base de datos cuyo empleo resulta necesario para la consecución de fines de investigación de realización de estadísticas, de docencia, de gestión económica y administrativa, etc. La necesidad de que los distintos profesionales sanitarios puedan disponer de esta herramienta de una forma sencilla y rápida para llevar a cabo sus funciones es incuestionable. Para ello resulta indispensable que la información contenida en las historias clínicas fluya de manera segura, sencilla y rápida. En este sentido, la informatización de la historia resulta un paso necesario en la creación de ese flujo. La historia de salud electrónica constituiría un último estadio de desarrollo de la historia clínica, caracterizado por ser la infraestructura para introducir, procesar y almacenar la información, porque la información se adapta a las posibilidades del ordenador integrándose con aplicaciones y bases de datos interrelacionadas, sin mantener la estructura del formato de papel, porque el almacenaje deja de ser pasivo, permitiendo ayudas interactivas, por la interoperabilidad entre los sistemas de información de los centros sanitarios y sus bases de datos, tanto a nivel nacional como internacional, y, en última instancia, porque añade a estas características el que al historial se incluya cualquier información relativa a la salud de un individuo, no sólo la generada en la interacción con el sistema sanitario, a saber: información de tipo, social, hábitos de salud, empleo de medicinas y terapias, etc., y que el propio individuo coopera en su historial. La creación de este sistema de información sanitaria ha planteado también el debate sobre la necesidad o no de centralizar las bases de datos sanitarios, y sobre la necesidad de integrar la información sanitaria y crear la historia clínica única, no tanto a nivel de centro, sino a nivel de todo un sistema sanitario. La apuesta en la actualidad por un sistema avanzado de gestión de

historias clínicas es clara. En primer lugar se tiende a la integración de la información. Las propias leyes recogen el compromiso por la historia clínica única. En segundo lugar, la apuesta por la historia clínica electrónica parece también indudable. Ya se ha comentado que para hacer efectiva la integración de la información, resulta necesaria la aplicación de la telemática a la gestión de las historias clínicas. La relación entre ambos procesos se reconoce también en las leyes"[129]*.*

El Convenio relativo a los derechos humanos y la biomedicina, hecho en Oviedo el 4 de abril de 1997, también tuvo en cuenta el gran avance de la medicina y la biología, así como el peligro que supondría a la dignidad humana una mala praxis de las mismas, recogiendo en su preámbulo que *"los Estados miembros del Consejo de Europa, los demás Estados y la Comunidad Europea, signatarios del presente Convenio…"*, y en concreto en su punto noveno recoge que *"conscientes de los rápidos avances de la biología y la medicina";* y en su punto onceavo *"conscientes de las acciones que podrían poner en peligro la dignidad humana mediante una práctica inadecuada de la biología y la medicina".*

Igualmente, las partes del presente convenio establecen como objetivo, proteger la dignidad, integridad e identidad de las personas y el resto de sus derechos fundamentales sin discriminación en la aplicación de estas ciencias, para que, teniendo en cuenta la prevalencia del ser humano, tengamos todos el mismo acceso a los beneficios que la sanidad proporciona. Así lo marca el artículo primero en su objetivo y finalidad, al establecer que *"las Partes en el presente Convenio protegerán al ser humano en su dignidad y su identidad y garantizarán a toda persona, sin discriminación alguna, el respeto a su integridad y a sus demás derechos y libertades fundamentales con respecto a las aplicaciones de la biología y la*

[129] ABERASTURI GORRIÑO, Unai: *"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 29.

medicina. Cada Parte adoptará en su legislación interna las medidas necesarias para dar aplicación a lo dispuesto en el presente Convenio". Por su parte el artículo 2, regula la primacía del ser humano, recogiendo que *"el interés y el bienestar del ser humano deberán prevalecer sobre el interés exclusivo de la sociedad o de la ciencia".* Y el artículo tercero sobre el acceso equitativo a los beneficios de la sanidad, mantiene, por su parte, que *"las Partes, teniendo en cuenta las necesidades de la sanidad y los recursos disponibles, adoptarán las medidas adecuadas con el fin de garantizar, dentro de su ámbito jurisdiccional, un acceso equitativo a una atención sanitaria de calidad apropiada".*

Aunque se han citado ya normas importantes relativas al ámbito sanitario, como el primer código sanitario, la Declaración para los Derechos de los Pacientes en Europa, la Ley General de Sanidad, y el Convenio de Derechos Humanos y Biomedicina, es con el cambio de milenio, cuando surge la mayoría de normativa aplicable al sector médico, lo que no quita que se citen otras que no tengan que ver con él pero sean igualmente interesantes respecto a la protección de datos personales.

También recoge el derecho a la intimidad el artículo 7 de la Ley 41/2002 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 (LAP- Ley del paciente), donde se promulga la confidencialidad de los datos referentes a la salud. Pero la exposición de motivos de la ley del paciente reflexiona sobre la situación de la regulación sanitaria, comienza diciendo que *"la importancia que tienen los derechos de los pacientes como eje básico de las relaciones clínico-asistenciales se pone de manifiesto al constatar el interés que han demostrado por los mismos casi todas las organizaciones internacionales con competencia en la materia".*

Y continúa haciendo esta norma un recorrido por las organizaciones que, desde Las Naciones Unidas pasando por la

UNESCO, la OMS, la Unión Europea y el Consejo de Europa, se han preocupado a lo largo del tiempo por los derechos de los pacientes. Pasando igualmente por la normativa que pudiera afectar en materia sanitaria existente hasta el momento, como la Declaración Universal de Derechos Humanos de 1948, la Declaración sobre la promoción de los derechos de los pacientes en Europa del año 1994, el convenio sobre los derechos del hombre y la biomedicina del 4 de abril de 1997, la regulación del derecho a la salud por el artículo 43 de la Constitución Española, la Ley General de Sanidad, el dictamen de 26 de noviembre de 1997 suscrito por el grupo de expertos encargado de elaborar unas directrices que han sido tenidas en cuenta para la redacción de esta norma, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la Directiva sobre protección en el tratamiento de datos.

Y así, acaba la exposición de motivos de esta norma, diciendo que *"todas estas circunstancias aconsejan una adaptación de la Ley General de Sanidad con el objetivo de aclarar la situación jurídica y los derechos y obligaciones de los profesionales sanitarios, de los ciudadanos y de las instituciones sanitarias. Se trata de ofrecer en el terreno de la información y la documentación clínicas las mismas garantías a todos los ciudadanos del Estado, fortaleciendo con ello el derecho a la protección de la salud que reconoce la Constitución".*

La Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Sanitario (LCS- Ley de calidad sanitaria), tiene una extensa exposición de motivos, que se inicia con la mención a los artículos 41 y 43 de la CE referidos al régimen público de la Seguridad Social y a la protección de la salud. La protección de la salud, su calidad, equidad y la cooperación de la sociedad en el sistema nacional de salud son los pilares de esta norma, que viene a garantizar la colaboración entre las Administraciones Públicas Sanitarias.

Regula igualmente esta norma el catálogo de prestaciones, dentro del cual se incluyen servicios y productos que complementan

con las prestaciones contempladas en el Real Decreto 63/1995, de 20 de enero, de ordenación de prestaciones sanitarias del Sistema Nacional de Salud, dirigidos todos ellos a la preservación, promoción y protección de la salud, y abarcando desde la prevención y el diagnósticos, a las diversas atenciones en los distintos servicios que integran el Sistema Nacional de Salud, así como los productos o servicios que pudieran ser necesarios en el domicilio de los pacientes.

En concreto, el artículo 7.1, establece que: *"El catálogo de prestaciones del Sistema Nacional de Salud tiene por objeto garantizar las condiciones básicas y comunes para una atención integral, continuada y en el nivel adecuado de atención. Se consideran prestaciones de atención sanitaria del Sistema Nacional de Salud los servicios o conjunto de servicios preventivos, diagnósticos, terapéuticos, rehabilitadores y de promoción y mantenimiento de la salud dirigidos a los ciudadanos. El catálogo comprenderá las prestaciones correspondientes a salud pública, atención primaria, atención especializada, atención sociosanitaria, atención de urgencias, la prestación farmacéutica, la ortoprotésica, de productos dietéticos y de transporte sanitario."* Y también el artículo 11 de esta norma define las prestaciones de salud pública como *"…el conjunto de iniciativas organizadas por las Administraciones públicas para preservar, proteger y promover la salud de la población. Es una combinación de ciencias, habilidades y actitudes dirigidas al mantenimiento y mejora de la salud de todas las personas a través de acciones colectivas o sociales".* De modo que se definen dos conceptos, el de atención sanitaria del Sistema Nacional de Salud, y el de salud pública, el primero más específico y el segundo más genérico, uno habla de servicios destinados a velar por la salud de los ciudadanos y otro de métodos tendentes a lograrla, lo cual, viene a significar lo mismo en el primer supuesto para casos concreto y en el segundo para la generalidad.

Esta Ley de calidad sanitaria contiene además una importante referencia a la formación continuada de los profesionales de la sanidad, tanto en la exposición de motivos como en el artículo 38 de su articulado, en garantía de la calidad de la gestión de la información, a través de la creación de una comisión de recursos humanos, con competencia estatal y autonómica, la cual debería contemplar obligatoriamente, formación relativa a la utilización de los datos de los pacientes. Así el párrafo segundo del apartado quinto de la exposición de motivos, establece que: *"La ley contiene básicamente principios referidos a la planificación y formación de los profesionales de la sanidad, así como al desarrollo y a la carrera profesional y a la movilidad dentro del Sistema Nacional de Salud. Especial interés tiene la creación de una comisión de recursos humanos, en cuya composición participarán las Administraciones estatal y autonómicas y las correspondientes comisiones nacionales de las distintas especialidades sanitarias, que tendrá el cometido general de contribuir a la planificación y diseño de los programas de formación de los profesionales de la sanidad, en colaboración y sin menoscabo de las competencias de los órganos e instituciones responsables en cada caso de la formación pregraduada y postgraduada, así como de la continuada, y en la oferta de plazas dentro del sistema público".* Dentro de este punto, debería estar sin duda la formación de los profesionales en materia de protección de datos. Por su parte el artículo 38, establece lo siguiente al regular la formación continuada *"las Administraciones públicas establecerán criterios comunes para ordenar las actividades de formación continuada, con la finalidad de garantizar la calidad en el conjunto del Sistema Nacional de Salud. Los criterios comunes serán adoptados en el seno del Consejo Interterritorial del Sistema Nacional de Salud. Sin perjuicio de lo anterior, el Ministerio de Sanidad y Consumo y los órganos competentes de las comunidades autónomas podrán delegar las funciones de gestión y acreditación de la formación continuada en otras corporaciones o instituciones de*

derecho público, de conformidad con la ley". Lo aquí dispuesto está relacionado directamente con el apartado de formación al personal que será analizado más adelante.

Por otro lado, la gestión de la tarjeta sanitaria individual, incorpora a los sistemas de información sanitaria los datos de identificación de su titular, las prestaciones a las que tiene derecho, así como los órganos que prestan dicha asistencia, debiendo garantizarse la inclusión de dichos datos para su buen funcionamiento, al igual que la protección de los mismos, para que se mantenga íntegro el derecho a la protección de datos. Y así se recoge en el segundo párrafo del apartado séptimo de su exposición de motivos *"…para facilitar el acceso de los ciudadanos a las prestaciones de la atención sanitaria del Sistema Nacional de Salud, se regula la tarjeta sanitaria individual, que, sin perjuicio de su gestión en su ámbito territorial por las comunidades autónomas, incluirá, de manera normalizada, los datos básicos de identificación del titular, su derecho a las prestaciones y la entidad responsable de la asistencia sanitaria. La ley establece que deberá garantizarse que los dispositivos que las tarjetas incorporen para almacenar la información básica y las aplicaciones que la traten permitan la lectura y comprobación de datos en todo el territorio nacional".*

Respecto a este documento, la tarjeta sanitaria, Aberasturi Gorriño manifiesta que *"en relación a las Tarjetas Sanitarias, parece evidente que identificar a cada ciudadano es algo fundamental en los sistemas sanitarios, mucho más en la actualidad, si se pretende que esta información fluya por las «autopistas de la información» de todo el mundo de forma rápida y constante. Tanto es así que el ordenamiento estatal dispone que el acceso a las prestaciones sanitarias se facilitará a través de las tarjetas sanitarias, en la medida en que se trata del documento que refleja la identidad de los*

sujetos que tienen acreditado el derecho a recibir asistencia sanitaria pública"[130]*.*

Entrando en el articulado de esta Ley de calidad sanitaria que nos ocupa, su objeto, establecido en el artículo 1.1, llama a la reducción de las desigualdades en materia de sanidad, que dice literalmente *"el objeto de esta ley es establecer el marco legal para las acciones de coordinación y cooperación de las Administraciones públicas sanitarias, en el ejercicio de sus respectivas competencias, de modo que se garantice la equidad, la calidad y la participación social en el Sistema Nacional de Salud, así como la colaboración activa de éste en la reducción de las desigualdades en salud".* Estas acciones comprenden, según el artículo 5, las prestaciones sanitarias, la farmacia, los profesionales, la investigación, los sistemas de información, la calidad del sistema sanitario, los planes integrales, la salud pública y la participación de ciudadanos y profesionales, siendo vigiladas por el Consejo Interterritorial y la Alta Inspección. En cambio, la equidad, interpretada como igualdad, no estaría muy conseguida, ya se aplican unos varemos de renta muy amplios que nada reducen las desigualdades.

No obstante, sigue avocando el artículo 2 de esta norma a la igualdad y la calidad del sistema, que con los citados niveles de renta seguiría sin cumplirse, ya que la calidad se reduce en tanto los servicios sanitarios se basen en la renta de los ciudadanos. Establece este artículo entre los principios generales y en primer lugar que *"la prestación de los servicios a los usuarios del Sistema Nacional de Salud en condiciones de igualdad efectiva y calidad, evitando especialmente toda discriminación entre mujeres y hombres en las actuaciones sanitarias".*

[130] ABERASTURI GORRIÑO, Unai: *"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 31.

Respecto de la igualdad efectiva de todos los ciudadanos sobre el acceso a los servicios sanitarios, ya he comentado anteriormente que *"lo cierto es que las normas sanitarias, en general, hablan de igualdad efectiva para el acceso y prestaciones sanitarias y, el sistema de copago podría no cumplirlo, ya que el acceso no es igual para todos los pacientes en el plano económico, porque unos pagarían más que otros. Incluso la propia Constitución Española, es muy clara en su artículo 43.1, donde "Se reconoce el derecho a la protección de la salud" y, ese precepto hay que ponerlo en relación con el artículo 9.2 de esta misma norma, el cual establece que "corresponde a los poderes públicos promover las condiciones para que la libertad e igualdad del individuo y de los grupos en que se integra sean reales y efectiva. Posiblemente sería constitucionalmente admisible la discriminación en función de la renta, siempre para favorecer a los menos favorecidos económicamente; en todo caso debería establecerse que es lo que prima, si la salud –y por tanto los datos sanitarios- o la economía –y los correspondientes datos de renta"*[131].

El artículo 3, por su parte, establece las mismas garantías a todos los asegurados del Sistema Nacional de Salud en su punto primero asentando que *"la asistencia sanitaria en España, con cargo a fondos públicos, a través del Sistema Nacional de Salud, se garantizará a aquellas personas que ostenten la condición de asegurado."* Recogiendo en su punto segundo quienes ostentan tal condición: *"A estos efectos, tendrán la condición de asegurado aquellas personas que se encuentren en alguno de los siguientes supuestos: a) Ser trabajador por cuenta ajena o por cuenta propia, afiliado a la Seguridad Social y en situación de alta o asimilada a la de alta. b) Ostentar la condición de pensionista del sistema de la*

[131] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

Seguridad Social. c) Ser perceptor de cualquier otra prestación periódica de la Seguridad Social, incluidas la prestación y el subsidio por desempleo. d) Haber agotado la prestación o el subsidio por desempleo u otras prestaciones de similar naturaleza, encontrarse en situación de desempleo, no acreditar la condición de asegurado por cualquier otro título y residir en España".

Y no se quedan desamparados los menos favorecidos económicamente, ya que el punto tercero matiza que *"en aquellos casos en que no se cumpla ninguno de los supuestos anteriormente establecidos, las personas de nacionalidad española o de algún Estado miembro de la Unión Europea, del Espacio Económico Europeo o de Suiza que residan en España y los extranjeros titulares de una autorización para residir en territorio español, podrán ostentar la condición de asegurado siempre que acrediten que no superan el límite de ingresos determinado reglamentariamente."* También tiene cabida dentro de dicha condición de asegurado los beneficiarios, así lo establece el punto cuarto de este artículo, según el cual *"…tendrán la condición de beneficiarios de un asegurado, siempre que residan en España, el cónyuge o persona con análoga relación de afectividad, que deberá acreditar la inscripción oficial correspondiente, el ex cónyuge a cargo del asegurado, así como los descendientes y personas asimiladas a cargo del mismo que sean menores de 26 años o que tengan una discapacidad en grado igual o superior al 65%".*

Los que no quepan en ninguno de estos apartados, también podrán optar a la sanidad pública, siempre que se hagan cargo de los costes, según establece el punto quinto de este artículo, ya que *"aquellas personas que no tengan la condición de asegurado o de beneficiario del mismo podrán obtener la prestación de asistencia sanitaria mediante el pago de la correspondiente contraprestación o cuota derivada de la suscripción de un convenio especial".*

Esta ley habla de "*igualdad efectiva*" de acceso a las prestaciones como garantía de accesibilidad y establece el artículo 23 que: *"Todos los usuarios del Sistema Nacional de Salud tendrán acceso a las prestaciones sanitarias reconocidas en esta ley en condiciones de igualdad efectiva".* En la situación actual de España, hay muchas personas con dificultades efectivas económicas, a las que se aplican unos baremos de injustos por su amplitud. En cambio se aplican unos varemos de renta muy amplios que nada reducen las desigualdades. En la situación actual de nuestro país, hay muchas personas con dificultades efectivas económicas, a las que se aplican unos baremos de injustos por su amplitud.

Respecto al tema de las farmacias que tanta polémica ha suscitado a propósito de la cesión de información relativa a la renta de los pacientes a las mismas, está también regulado en esta norma, que empieza estableciendo acciones de concienciación para el uso racional de los medicamentos, para que los profesionales puedan hacer llegar esta máxima a los pacientes. Así lo expresa el artículo 31.4 de la misma: *"El Ministerio de Sanidad y Consumo, junto con las comunidades autónomas, acometerá acciones encaminadas al uso racional del medicamento que comprenderán entre otras: a) Programas de educación sanitaria dirigidos a la población general para la prevención de la automedicación, el buen uso de los medicamentos y la concienciación social e individual sobre su coste. b) Programas de formación continua de los profesionales, que les permita una constante incorporación de conocimientos sobre nuevos medicamentos y la actualización sobre la eficacia y efectividad de éstos".*

Y el artículo 33.1 establece, por su parte, el sistema de colaboración de las oficinas de farmacia: *"Las oficinas de farmacia colaborarán con el Sistema Nacional de Salud en el desempeño de la prestación farmacéutica a fin de garantizar el uso racional del medicamento. Para ello los farmacéuticos actuarán coordinadamente*

con los médicos y otros profesionales sanitarios". Puntualizándose en el punto dos que se hará bajo lo establecido en la ley del medicamento *"en el marco de la Ley 25/1990, de 20 de diciembre, del Medicamento, el Ministerio de Sanidad y Consumo, previo acuerdo del Consejo Interterritorial del Sistema Nacional de Salud, establecerá los criterios generales y comunes para el desarrollo de la colaboración de las oficinas de farmacia, por medio de conciertos que garanticen a los ciudadanos la dispensación en condiciones de igualdad efectiva en todo el territorio nacional, independientemente de su comunidad autónoma de residencia. Se tenderá a la dispensación individualizada de medicamentos y a la implantación de la receta electrónica, en cuyo desarrollo participarán las organizaciones colegiales médica y farmacéutica".* Y añadiéndose en el punto tercer de este artículo que la gestión de la información a través de las oficinas de farmacia, respetará siempre lo dispuesto en la normativa de protección de datos, recogiendo que: *"Entre los criterios del apartado anterior se definirán los datos básicos de farmacia, para la gestión por medios informáticos de la información necesaria para el desempeño de las actividades anteriormente mencionadas y para la colaboración con las estructuras asistenciales del Sistema Nacional de Salud. Se ajustarán a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y a las especificaciones establecidas por los servicios de salud de las comunidades autónomas".* De modo que, según lo establecido por la normativa de calidad sanitaria, debe hacerse con el respeto y armonización de las normas citadas.

El artículo 59.2 a), referido a la infraestructura de la calidad, marca como elementos de la misma en el Sistema Nacional de Salud normas de calidad y seguridad, que deben seguir los centros sanitarios para garantizar la seguridad de las prestaciones *"que contendrán los requerimientos que deben guiar los centros y servicios sanitarios para poder realizar una actividad sanitaria de forma segura".* Estableciendo también la letra c) de este artículo

guías de práctica clínica y, que contienen los procedimientos para el diagnóstico, tratamiento y cuidado de la salud *"que son descripciones de los procesos por los cuales se diagnostica, trata o cuida un problema de salud."* Además las letras d) y e) de este mismo artículo, incluyen en el armazón de la calidad del sistema sanitario tanto el registro de buenas prácticas *"que recogerá información sobre aquellas prácticas que ofrezcan una innovación o una forma de prestar un servicio mejor a la actual".* Así como el de acontecimientos adversos en relación a la mejoría o empeoramiento del paciente *"que recogerá información sobre aquellas prácticas que hayan resultado un problema potencial de seguridad para el paciente".*

El artículo 60.1 establece además para vigilar y mantener la calidad en todo el entramado del sistema sanitario la creación de *"…la Agencia de Calidad del Sistema Nacional de Salud órgano dependiente del Ministerio de Sanidad y Consumo al que corresponderá la elaboración y el mantenimiento de los elementos de la infraestructura de la calidad".* Dicho organismo, dependiente del Ministerio de Sanidad y Consumo, está encargado de vigilar y mantener la calidad en todo el entramado del sistema sanitario. El punto segundo de este artículo sienta las funciones de este órgano, estableciendo que *"la Agencia elaborará o adoptará los elementos de la infraestructura con el asesoramiento de sociedades científicas y expertos del sector, a partir de la experiencia nacional e internacional. También podrá promover convenios con instituciones científicas para elaborar o gestionar los elementos de la infraestructura. Asimismo difundirá los elementos de la infraestructura para su conocimiento y utilización por parte de las comunidades autónomas y los centros y servicios del Sistema Nacional de Salud".*

Las redes de conocimiento establecidas en el artículo 68 se crean como un puente para la puesta en común de información entre

los profesionales del Sistema nacional de salud, estableciéndose en su punto primero que *"las Administraciones sanitarias podrán crear redes que generen y transmitan conocimiento científico y favorezcan la participación social en las materias de su competencia. Estas redes se constituyen para servir como plataforma de difusión de la información, intercambio de experiencias y como apoyo a la toma de decisiones a todos los niveles del Sistema Nacional de Salud".* El punto 2 de este artículo afina un poco más recogiendo que *"el Ministerio de Sanidad y Consumo creará una infraestructura de comunicaciones que permita el intercambio de información y promueva la complementariedad de actuaciones en las siguientes materias, entre otras: a) Información, promoción y educación para la salud. b) Cooperación internacional. c) Evaluación de tecnologías sanitarias. d) Formación en salud pública y gestión sanitaria";* de modo que el intercambio de información podría suponer una gran riqueza para individualidades. Y puntualiza el punto tercero que *"las Administraciones públicas sanitarias apoyarán la participación en estas redes de organismos internacionales, nacionales, autonómicos, locales o del tercer sector".* Lo cual encaja perfectamente en la hipótesis planteada al principio de este estudio.

Y respecto a esta normativa establece la disposición transitoria única que *"en tanto no se apruebe el real decreto por el que se desarrolle la cartera de servicios, mantendrá su vigencia el Real Decreto 63/1995, de 20 de enero, de ordenación de prestaciones sanitarias del Sistema Nacional de Salud".*

En la Declaración Universal sobre Bioética y Derechos Humanos de 19 de octubre de 2005 (DBDH- Declaración sobre bioética y derechos humanos), se reconocen los problemas éticos que suscita el avance de la ciencia y la tecnología, y viendo la necesidad de unos fundamentos universales a estas controversias, sin olvidar que la salud no depende solo de esto factores, sino también de los psicosociales y culturales. Así se recoge en la

introducción que hace este texto: *"Reconociendo que los problemas éticos suscitados por los rápidos adelantos de la ciencia y de sus aplicaciones tecnológicas deben examinarse teniendo en cuenta no sólo el respeto debido a la dignidad de la persona humana, sino también el respeto universal y la observancia de los derechos humanos y las libertades fundamentales; Resolviendo que es necesario y conveniente que la comunidad internacional establezca principios universales que sirvan de fundamento para una respuesta de la humanidad a los dilemas y controversias cada vez numerosos que la ciencia y la tecnología plantean a la especie humana y al medio ambiente;… Reconociendo que la salud no depende únicamente de los progresos de la investigación científica y tecnológica sino también de factores psicosociales y culturales,…".*

Potencia a la vez que los logros científicos beneficien al máximo a los pacientes, respetando su dignidad e igualdad, la privacidad y confidencialidad de la información que les atañe, la autonomía de las personas a la hora de tomar decisiones con previo consentimiento libre e informado, así como su revocación, incluso en las personas carentes de su capacidad para darlo, en el mayor grado posible, respetando la vulnerabilidad de los grupos más desprotegidos.

Así el artículo 1.1 de esta norma establece respecto a su alcance que: *"Declaración trata de las cuestiones éticas relacionadas con la medicina, las ciencias de la vida y las tecnologías conexas aplicadas a los seres humanos, teniendo en cuenta sus dimensiones sociales, jurídicas y ambientales"*. Incluso su punto segundo concreta que *"la Declaración va dirigida a los Estados. Imparte también orientación, cuando procede, para las decisiones o prácticas de individuos, grupos, comunidades, instituciones y empresas, públicas y privadas".*

E igualmente el artículo 2 fija entre sus objetivos: *"a) proporcionar un marco universal de principios y procedimientos que*

sirvan de guía a los Estados en la formulación de legislaciones, políticas u otros instrumentos en el ámbito de la bioética; b) orientar la acción de individuos, grupos, comunidades, instituciones y empresas, públicas y privadas; c) promover el respeto de la dignidad humana y proteger los derechos humanos, velando por el respeto de la vida de los seres humanos y las libertades fundamentales, de conformidad con el derecho internacional relativo a los derechos humanos…".

Los principios de este texto comienzan recogiendo en su artículo 3.1, sobre la dignidad y derechos humanos, que *"se habrán de respetar plenamente la dignidad humana, los derechos humanos y las libertades fundamentales"*, puntualizando en el segundo punto que *"los intereses y el bienestar de la persona deberían tener prioridad con respecto al interés exclusivo de la ciencia o la sociedad".* El artículo cuarto, por su parte, establece sobre los beneficios y efectos nocivos para el paciente, *que "al aplicar y fomentar el conocimiento científico, la práctica médica y las tecnologías conexas, se deberían potenciar al máximo los beneficios directos e indirectos para los pacientes, los participantes en las actividades de investigación y otras personas concernidas, y se deberían reducir al máximo los posibles efectos nocivos para dichas personas"*.

Y el artículo 5 por su parte que *"se habrá de respetar la autonomía de la persona en lo que se refiere a la facultad de adoptar decisiones, asumiendo la responsabilidad de éstas y respetando la autonomía de los demás. Para las personas que carecen de la capacidad de ejercer su autonomía, se habrán de tomar medidas especiales para proteger sus derechos e intereses".* En cuanto la responsabilidad y autonomía de cada uno. Y como artículo envolvente a los anteriores, el artículo 10 establece que *"se habrá de respetar la igualdad fundamental de todos los seres humanos en*

dignidad y derechos, de tal modo que sean tratados con justicia y equidad".

Esta declaración trata de estas cuestiones para orientar a las personas hacia el respeto a la dignidad, los derechos humanos y las libertades fundamentales.

Respecto al término «*bioética*» hace referencia Karla Cantoral a sus orígenes de la siguiente forma *"el bioquímico estadounidense Van Rensselaer Potter introdujo en 1970 el neologismo bioética; en la explicación que Potter dio a su propio hallazgo, dijo que usó la raíz griega bios para significar los progresos de las ciencias biológicas y ethos para hacer referencia a los valores puesto en juego por esos adelantos. Uniendo ambos términos creó una palabra a la que agregó como símbolo un puente que metafóricamente alude a un "puente hacia el futuro", pero también advirtió lo siguiente: si los descubrimientos técnicos y la reflexión ética no caminan al unísono, el resultado podría resultar desastroso."*[132] Y asegura que *"para que la bioética cumpla eficazmente su función es necesario articular un método basado en principios que deben aplicarse a la hora de justificar las elecciones que se realicen en el ámbito biosanitario. Es así como surgen los cuatro principios de la bioética enunciados por primera vez en 1978 en el ya emblemático Informe Belmont, y que posteriormente adquirirían plena carta de aceptación con las modificaciones propuestas por Beauchamp y Childress. A partir de dichas modificaciones estos principios se constituyeron en marco de referencia para la resolución de los conflictos éticos que recurrentemente se plantean en la aplicación de la medicina. Estos cuatro principios son los siguientes: autonomía de la persona, beneficencia, no maleficencia y justicia"*[133]*.*

[132] CANTORAL DOMÍNGUEZ, Karla: "*Derecho de protección de datos personales en la salud*". Editorial Novum, MEXICO D.F., 2012. Pág. 135.

[133] CANTORAL DOMÍNGUEZ, Karla: "*Derecho de protección de datos personales en la salud*". Editorial Novum, MEXICO D.F., 2012. Pág. 139.

Según asegura Diario Médico: *"El conocimiento y manejo de la bioética por parte del médico, una disciplina que cada vez tiene más importancia, continúa siendo un gran desafío para el profesional sanitario, y de hecho si su capacitación fuera mayor en este apartado sus decisiones <<serían más seguras y el facultativo vería cómo disminuye la sensación de incertidumbre que siempre genera la decisión de actuar correctamente o no sobre el paciente oncológico en fase terminal>>"*[134].

La actual Ley 29/2006, de 26 de julio (LGUM- Ley sobre el uso de los medicamentos), de garantías y uso racional de los medicamentos y productos sanitarios, también hace una referencia a la protección de los derechos fundamentales, al establecer en su título III, bajo la rúbrica "*de las garantías de la investigación de los medicamentos de uso humano*", los ensayos clínicos con medicamentos" que "*se mantiene el régimen de autorización administrativa previa, respetando los derechos fundamentales de la persona y los postulados éticos que afectan a la investigación biomédica"*.

Pero ya la derogada Ley 25/1990, del medicamento, ya establecía estos puntos, sobre la concienciación en la utilización los medicamentos, que ante el avance de la tecnología ha hecho que la gestión de la información necesite matices en pro de la transparencia y control de los recursos, que desarrolla la nueva Ley sobre el uso de los medicamentos que será comentada a continuación. La exposición de motivos de esta nueva norma, comienza precisamente así su texto: *"La Ley 25/1990, de 20 de diciembre, del Medicamento pretendía, según se señala en su exposición de motivos, dotar a la sociedad española de un instrumento institucional que le permitiera esperar confiadamente que los problemas relativos a los medicamentos fueran abordados por cuantos agentes sociales se*

[134]REGO, Santiago: "*Un buen manejo de la bioética reduciría las dudas del médico*". Diario Médico, miércoles 21 de julio de 2010. Año XIX, Núm.4158, Pág 9.

vieran involucrados en su manejo, (industria farmacéutica, profesionales sanitarios, poderes públicos y los propios ciudadanos), en la perspectiva del perfeccionamiento de la atención a la salud. Los quince años transcurridos desde la aprobación de la citada Ley permiten afirmar que se ha alcanzado en gran parte el objetivo pretendido consagrándose la prestación farmacéutica como una prestación universal". Y concluye este punto primero de la exposición de motivos estableciendo que su objetivo es mantener la calidad en el Sistema Nacional de Salud, para normalizar el uso de los medicamentos de una forma coherente, donde y cuando lo necesiten; así lo recoge literalmente: *"El desafío actual es asegurar la calidad de la prestación en todo el Sistema Nacional de Salud en un marco descentralizado capaz de impulsar el uso racional de los medicamentos y en el que el objetivo central sea que todos los ciudadanos sigan teniendo acceso al medicamento que necesiten, cuando y donde lo necesiten, en condiciones de efectividad y seguridad".*

Así, por ejemplo, al regularse en esta normativa el Sistema Español de farmacovigilancia, la Agencia Española de Medicamentos y Productos Sanitarios se encarga de que la información de reacciones adversas registradas en España, pase a las redes europeas e internacionales de farmacovigilancia, con respeto siempre a la normativa existente en materia de protección de datos, según establece su artículo 54.2, según el cual *"la Agencia Española de Medicamentos y Productos Sanitarios evaluará la información recibida del Sistema Español de farmacovigilancia así como de otras fuentes de información. Los datos de reacciones adversas detectadas en España se integrarán en las redes europeas e internacionales de farmacovigilancia, de las que España forme parte, con la garantía de protección de los datos de carácter personal exigida por la normativa vigente".* Puntualizando el punto tercero de este mismo artículo que "*en el Sistema Español de farmacovigilancia están obligados a colaborar todos los*

profesionales sanitarios", de modo que establece de una obligación general de cumplimiento de la normativa de protección de datos, de lo cual deberían estar informados dichos profesionales; tema que será abordado en el apartado correspondiente.

La también derogada Ley 35/1988, de 22 de noviembre, sobre técnicas de reproducción asistida fue pionera en esta materia en los países con afinidad geográfica y cultural al nuestro. Así consta en el segundo párrafo del primer punto de la exposición de motivos *"en España esta necesidad se materializó tempranamente mediante la aprobación de la Ley 35/1988, de 22 de noviembre, sobre técnicas de reproducción asistida. La Ley española fue una de las primeras en promulgarse entre las legislaciones sobre esta materia desarrolladas en países de nuestro entorno cultural y geográfico".* Esta legislación fue posteriormente modificada por la Ley 45/2003, de 21 de noviembre para responder parcialmente al desarrollo en las nuevas técnicas de reproducción, pero finalmente ambas han sido derogadas por la actual Ley 14/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida (LRA- Ley de reproducción asistida), prestando una especial atención a la protección de datos personales.

La Ley 14/2007, de 3 de julio, de Investigación biomédica recoge en el tercer párrafo del segundo apartado del preámbulo dice que *"en particular, la Ley se construye sobre los principios de la integridad de las personas y la protección de la dignidad e identidad del ser humano en cualquier investigación biomédica que implique intervenciones sobre seres humanos, así como en la realización de análisis genéticos, el tratamiento de datos genéticos de carácter personal y de las muestras biológicas de origen humano que se utilicen en investigación. En este sentido, la Ley establece que la libre autonomía de la persona es el fundamento del que se derivan los derechos específicos a otorgar el consentimiento y a obtener la información previa. Asimismo, se establece el derecho a no ser*

discriminado, el deber de confidencialidad por parte de cualquier persona que en el ejercicio de sus funciones acceda a información de carácter personal, el principio de gratuidad de las donaciones de material biológico, y fija los estándares de calidad y seguridad, que incluyen la trazabilidad de las células y tejidos humanos y la estricta observancia del principio de precaución en las distintas actividades que regula. En la regulación de todas estas materias se ha tenido en cuenta lo previsto en la Ley 41/2002, de 14 noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, a las que se reconoce su condición supletoria en aquellas cuestiones no reguladas por esta Ley".

El párrafo cuarto del punto cuarto establece que *"respecto al sistema de garantías, se recoge una relación precisa que pone los límites del principio de libertad de la investigación en la defensa de la dignidad e identidad del ser humano y en la protección de su salud, y se regulan de manera específica el consentimiento informado y el derecho a la información, la protección de datos personales y el deber de confidencialidad, la no discriminación por motivos genéticos o por renuncia a la práctica de un análisis genético o a la participación en una investigación, la gratuidad en la donación y utilización de muestras biológicas, la garantía de la trazabilidad y la seguridad en el uso de las células, tejidos y cualquier material biológico de origen humano y, por último se establecen los límites que deben respetarse en los análisis genéticos".* Y por su parte el decimocuarto párrafo del punto cuarto dice lo siguiente *"…la Ley, a la vez que prescribe un conjunto de garantías en relación con los análisis genéticos y las muestras biológicas dentro del ámbito de la protección de los datos de carácter personal, configura un conjunto de normas con el fin de dar confianza y seguridad a los investigadores y a las instituciones públicas y privadas en sus actuaciones en el sector, despejando las incertidumbres legales*

actuales. Además de otros principios normativos ya mencionados, se marcan como principios rectores los de accesibilidad, equidad y calidad en el tratamiento de los datos, se exige el consentimiento previo y se prevé la situación de las muestras biológicas anonimizadas…".

Y en su articulado, recoge esta norma en el 1.2 que *"asimismo y exclusivamente dentro del ámbito sanitario, esta Ley regula la realización de análisis genéticos y el tratamiento de datos genéticos de carácter personal".*

Estableciendo el 9.1, los límites de los análisis genéticos, según los que *"se asegurará la protección de los derechos de las personas en la realización de análisis genéticos y del tratamiento de datos genéticos de carácter personal en el ámbito sanitario".*

El artículo 12 regula por su parte los comités de ética de la investigación y en su punto 2 d) establece que: *"El Comité de Ética de la Investigación correspondiente al centro ejercerá las siguientes funciones: d) Velar por el cumplimiento de procedimientos que permitan asegurar la trazabilidad de las muestras de origen humano, sin perjuicio de lo dispuesto en la legislación de protección de datos de carácter personal".*

Y el artículo 25.5 establece que: *"El Comité de Ética de la Investigación procederá al seguimiento del cumplimiento de lo establecido en el apartado anterior, debiendo dar cuenta de las incidencias que observe a la autoridad competente que dio la autorización para dicha investigación, con el fin de que ésta pueda adoptar las medidas que correspondan, de acuerdo con el artículo 17 de esta Ley y con pleno respeto a lo establecido en la normativa vigente en materia de protección de datos de carácter personal".*

Hay que retroceder en este punto al 25.4 para ver que establece que "*cualquier información relevante sobre la participación en la investigación será comunicada por escrito a los participantes o,*

en su caso, a sus representantes, a la mayor brevedad." Y aún hay que retroceder un poco más para ver que efectivamente, el artículo 17.2 establece que: *"Las autoridades sanitarias tendrán en todo momento facultades inspectoras sobre la investigación, pudiendo tener acceso a las historias clínicas individuales de los sujetos del estudio, para lo que deberán guardar en todo caso su carácter confidencial".* Y matiza el punto tercero que *"la autoridad autonómica procederá, por iniciativa propia o a instancias del Comité de Ética de la Investigación, a la suspensión cautelar de la investigación autorizada en los casos en los que no se hayan observado los requisitos que establece esta Ley y sea necesaria para proteger los derechos de los ciudadanos".*

Y de forma general, la Disposición final segunda recoge una aplicación supletoria *"en lo no previsto en esta Ley serán de aplicación la Ley 41/2002, de 14 noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, siempre que no sea incompatible con los principios de esta Ley, y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal".*

Por su parte también la Ley 28/2009, de 30 de diciembre, de modificación de la Ley 29/2006 incorpora a los podólogos y odontólogos como profesionales sanitarios facultados para recetar; además el avance de las nuevas tecnologías, con la introducción de la receta médica electrónica, hace necesario respetar los principios de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y disposiciones legales de aplicación, para facilitar una red de intercomunicación entre los sistemas de información de las Administraciones Públicas, para fomentar el intercambio de información.

Y así comienza literalmente este Real Decreto en su primer párrafo: "*La última regulación de la receta médica en España es la*

del Real Decreto 1910/1984, de 26 de septiembre, y desde entonces se ha producido una importante evolución de la asistencia sanitaria y del marco jurídico español y europeo en materia farmacéutica. En particular, la promulgación de la Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios, incorpora nuevas e importantes disposiciones en el ámbito de los medicamentos y de los productos sanitarios ligadas a sus garantías y uso racional que es preciso desarrollar reglamentariamente".

Para seguir diciendo a continuación que "*más recientemente, la Ley 28/2009, de 30 de diciembre, de modificación de la Ley sobre el uso de los medicamentos introduce en nuestro ordenamiento jurídico dos novedades de máxima relevancia: incorpora a los podólogos, junto a los médicos y odontólogos, como profesionales sanitarios facultados para recetar, en el ámbito de sus competencias, medicamentos sujetos a prescripción médica. Al mismo tiempo, contempla la participación de los enfermeros, por medio de la orden de dispensación, en el uso, indicación y autorización de dispensación de determinados medicamentos y productos sanitarios*".

Y enlaza el siguiente párrafo con la introducción de la tecnología en sistema sanitario para la dispensación de recetas diciendo que "*por otra parte, la progresiva utilización de las nuevas tecnologías en el ámbito de la prescripción y dispensación de medicamentos y productos sanitarios, en particular mediante la introducción de la receta médica electrónica, determina la necesidad de que la normativa sobre esta materia deba ser conforme con los principios y criterios emanados de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y disposiciones legales de aplicación, al objeto de posibilitar la creación de una red de comunicaciones que interconecte los sistemas de información de las Administraciones públicas españolas*

y permita el intercambio de información y servicios entre las mismas".

Este panorama hace necesario establecer este nuevo marco jurídico renovado para las recetas médicas y órdenes de dispensación, como documentos normalizados, necesarios para el intercambio de información entre profesionales sanitarios, que suponga una garantía para el paciente, haciendo hincapié en el uso racional de los medicamentos, en desarrollo de los artículos 19.6 y 77.6 y 8 de Ley sobre el uso de los medicamentos, y al amparo de los establecido en el artículo 149.1.16ª de la Constitución que confiere competencias exclusivas en materia de legislación sobre productos farmacéuticos. Así lo establece el cuarto párrafo del Real decreto que nos ocupa: "*Por todo ello, se hace necesario establecer un nuevo marco jurídico para la receta médica y la orden de dispensación que posibilite profundizar en la mejora del uso racional de los medicamentos, en los ámbitos público y privado y que, al tiempo que contribuya a la simplificación de la tarea de los profesionales sanitarios, refuerce las garantías de los ciudadanos*".

El Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación (RDRM- Real Decreto sobre Receta Médica), comienza haciendo en sus disposiciones generales un recorrido por la legislación que ha regulado la receta médica desde sus orígenes hasta la introducción de la receta médica electrónica, lo cual facilita la habilitación de una red de comunicación entre los sistemas de información de las Administraciones Públicas, a la vez que confiere a los ciudadanos a través de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y disposiciones legales de aplicación, la facultad de acceder electrónicamente a los servicios públicos. La regulación más reciente de la receta médica es de 1984, y desde entonces se han promulgado leyes importantes como la Ley sobre el uso de los medicamentos.

El actual Código de Deontología Médica (CDM) es del año 2011, y establece en el artículo 4 de sus principios generales que *"la profesión médica está al servicio del hombre y de la sociedad. En consecuencia, respeta la vida humana, la dignidad de la persona y el cuidado de la salud del individuo y de la comunidad, son deberes primordiales del médico".* Asimismo su artículo 8.2 exalta el respeto con delicadeza a la intimidad.

La Ley 33/2011, de 4 de octubre, General de Salud Pública, según dice en uno de sus últimos párrafos de su preámbulo, antes de articulado, *"…el capítulo IX regula un Sistema de información en salud pública, que posibilita el intercambio de la información necesaria para el mejor desarrollo de las actuaciones en materia de salud pública, con respeto a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*". El artículo séptimo, referido a el derecho a la intimidad, confidencialidad y respeto de la dignidad, en su punto segundo establece que "*la información personal que se emplee en las actuaciones de salud pública se regirá por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en 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*".

El título del Real Decreto- Ley 16/2012, de 20 de abril, de medidas urgentes para garantizar la sostenibilidad del Sistema Nacional de Salud y mejorar la calidad y seguridad de sus prestaciones (RDLS- Real Decreto Ley sobre sostenibilidad), parece poco apropiado para el contenido que desarrolla de esta norma, dedicado en gran parte a establecer recortes sanitarios, lo cual en sí, no mejora en nada la calidad de las prestaciones.

No hay mayor verdad que la que dice el primer párrafo de esta norma "*la creación del Sistema Nacional de Salud ha sido uno de los grandes logros de nuestro Estado del bienestar, dada su calidad, su*

vocación universal, la amplitud de sus prestaciones, su sustentación en el esquema progresivo de los impuestos y la solidaridad con los menos favorecidos, lo que le ha situado en la vanguardia sanitaria como un modelo de referencia mundial".

Tras este primer párrafo, empieza una interminable lista de razones sobre el envejecimiento de la población, la asistencia sanitaria duplicada, el coste del avance de la tecnología y los impactos medioambientales, entre otros, que llevan a destruir ese Estado de bienestar tan laureado. Todo ello según dice el quinto párrafo del punto segundo de esta norma "*el Gobierno ha expresado su deseo de abordar éstas y cuantas otras reformas sean necesarias o convenientes, no sólo mediante normas, sino también impulsando buenas prácticas y poniendo en común experiencias, siempre con base en el diálogo y contando con la colaboración de las comunidades autónomas, de los grupos políticos y de cuantas asociaciones y entidades actúan en este ámbito, velando así por la mejor atención a los pacientes, que son el verdadero centro del sistema*". Y continúa diciendo el párrafo siguiente que "*será de esta manera como realmente se podrá garantizar a los ciudadanos una asistencia sanitaria pública, gratuita y universal*".

Parece tras la lectura de estas líneas, que esta introducción del Real Decreto, hubiesen sido escritas por diferentes personas, con diferentes formas de pensar, unas a favor del paciente, y otras plenamente en su contra. Pues ya ni la sanidad es realmente pública, ya que se tiende vertiginosamente a su privatización, ni es gratuita, debido a la gran modificación en sus costes, ni tampoco universal, por todos los recortes en las prestaciones que se están introduciendo y cada vez van a más.

Respecto de la privatización de la sanidad y a propósito de la inauguración del Hospital Puerta de Hierro Majadahonda, el diario ADN bajo el título *"El sector privado dirigirá el futuro de la sanidad pública"*, publica respecto a la privatización de la sanidad: *"La*

Comunidad vende oportunidades de negocio en su Plan de Infraestructuras Sanitarias 2007-2011"[135].

Real Decreto Ley sobre sostenibilidad viene a modificar en ciertos aspectos la ley de calidad sanitaria, así como la de uso racional de los medicamentos, para intentar paliar este desgaste en la economía sanitaria. En primer lugar se modifica la ley de calidad en cuanto a la condición de asegurado, limitándola a aquellas personas trabajadoras que se encuentren dadas de alta y cotizando, los receptores de prestaciones del Sistema de la Seguridad Social, los demandantes de empleo debidamente inscritos que no estén ya asegurados. Así, modificaría el artículo 1 de este Real Decreto el artículo 3 de la ley de calidad sanitaria, que en su punto primero establecería que "*la asistencia sanitaria en España, con cargo a fondos públicos, a través del Sistema Nacional de Salud, se garantizará a aquellas personas que ostenten la condición de asegurado*". Estableciéndose en el punto segundo quienes ostentan tal condición "*a estos efectos, tendrán la condición de asegurado aquellas personas que se encuentren en alguno de los siguientes supuestos: a) Ser trabajador por cuenta ajena o por cuenta propia, afiliado a la Seguridad Social y en situación de alta o asimilada a la de alta. b) Ostentar la condición de pensionista del sistema de la Seguridad Social. c) Ser perceptor de cualquier otra prestación periódica de la Seguridad Social, incluidas la prestación y el subsidio por desempleo. d) Haber agotado la prestación o el subsidio por desempleo y figurar inscrito en la oficina correspondiente como demandante de empleo, no acreditando la condición de asegurado por cualquier otro título*".

No obstante, a esta clasificación, se amplían las coberturas para residentes y extranjeros no incluidos en los requisitos anteriores que no rebasen los ingresos establecidos reglamentariamente. Así,

[135] REJÓN, Raúl*: "El sector privado dirigirá el futuro de la sanidad pública"*. ADN, martes 23 de septiembre de 2008. Año 3, Núm. 561, Pág.5.

establece el punto tercero que "*en aquellos casos en que no se cumpla ninguno de los supuestos anteriormente establecidos, las personas de nacionalidad española o de algún Estado miembro de la Unión Europea, del Espacio Económico Europeo o de Suiza que residan en España y los extranjeros titulares de una autorización para residir en territorio español, podrán ostentar la condición de asegurado siempre que acrediten que no superan el límite de ingresos determinado reglamentariamente*".

E igualmente se incluye a los beneficiarios del asegurado, siendo estos los descendientes menores de 26 años o con un grado de discapacidad igual o superior al 65%, así como el cónyuge o ex cónyuge residentes a cargo del asegurado. Dando el punto cuarto amplias las coberturas "*a los efectos de lo establecido en el presente artículo, tendrán la condición de beneficiarios de un asegurado, siempre que residan en España, el cónyuge o persona con análoga relación de afectividad, que deberá acreditar la inscripción oficial correspondiente, el ex cónyuge a cargo del asegurado, así como los descendientes y personas asimiladas a cargo del mismo que sean menores de 26 años o que tengan una discapacidad en grado igual o superior al 65%".* Incluso el punto quinto amplia la cobertura a los no asegurados con una serie de condiciones "*aquellas personas que no tengan la condición de asegurado o de beneficiario del mismo podrán obtener la prestación de asistencia sanitaria mediante el pago de la correspondiente contraprestación o cuota derivada de la suscripción de un convenio especial*".

Se regulan además las situaciones especiales referidas a los extranjeros no registrados ni autorizados como residentes en España, que serán atendidos igual que los españoles si son menores de 18 años, así como en el embarazo, parto y postparto, y hasta el alta médica en casos de urgencia por enfermedad o accidente grave. Así lo establece el nuevo artículo 3 ter "*los extranjeros no registrados ni autorizados como residentes en*

España, recibirán asistencia sanitaria en las siguientes modalidades: a) De urgencia por enfermedad grave o accidente, cualquiera que sea su causa, hasta la situación de alta médica. b) De asistencia al embarazo, parto y postparto. En todo caso, los extranjeros menores de dieciocho años recibirán asistencia sanitaria en las mismas condiciones que los españoles".

La ley de calidad sanitaria también es modificada por este Real Decreto Ley sobre sostenibilidad, estableciendo que la cartera común de servicios del Sistema Nacional de Salud son aquellos procedimientos basados en la experiencia, que hacen efectivas las prestaciones sanitarias. Así, el artículo 2.1 del comentado Real Decreto modifica al octavo de la Ley de calidad sanitaria, que queda redactado en su punto primero de la siguiente forma "*la cartera común de servicios del Sistema Nacional de Salud es el conjunto de técnicas, tecnologías o procedimientos, entendiendo por tales cada uno de los métodos, actividades y recursos basados en el conocimiento y experimentación científica, mediante los que se hacen efectivas las prestaciones sanitarias*". Y el punto segundo de este artículo clasifica esta cartera común y la divide en básica, suplementaria y de servicios accesorios. "*la cartera común de servicios del Sistema Nacional de Salud se articulará en torno a las siguientes modalidades: a) Cartera común básica de servicios asistenciales del Sistema Nacional de Salud a la que se refiere el artículo 8 bis. b) Cartera común suplementaria del Sistema Nacional de Salud a la que se refiere el artículo 8 ter. c) Cartera común de servicios accesorios del Sistema Nacional de Salud a la que se refiere el artículo 8 quáter*".

La básica comprende la asistencia preventiva, diagnóstica, de tratamiento y rehabilitación, así como el transporte urgente financiados públicamente al cien por cien. Así lo establece el artículo 2.2 del RD que añade un nuevo artículo 8 bis, el cual en su punto primero establece que "*la cartera común básica de servicios*

asistenciales del Sistema Nacional de Salud comprende todas las actividades asistenciales de prevención, diagnóstico, tratamiento y rehabilitación que se realicen en centros sanitarios o sociosanitarios, así como el transporte sanitario urgente, cubiertos de forma completa por financiación pública". Especificando a continuación el punto segundo que "*la prestación de estos servicios se hará de forma que se garantice la continuidad asistencial, bajo un enfoque multidisciplinar, centrado en el paciente, garantizando la máxima calidad y seguridad en su prestación, así como las condiciones de accesibilidad y equidad para toda la población cubierta*". Lo cual choca un poco con el sistema de copago establecido en España.

La suplementaria contempla las prestaciones de dispensación ambulatoria, en las que el usuario tiene que hacer una aportación, Incluyendo prestaciones farmacéuticas, ortoprotésicas y productos dietéticos, así como el transporte sanitario no urgente prescrito por un facultativo, con una aportación similar a la de la prestación farmacéutica, que se regirá por su propia normativa, existiendo para el resto un catálogo de prestaciones, importes máximos y coeficientes correctores que los proveedores deberán aplicar en la facturación a los servicios autonómicos de salud; los porcentajes de aportación de los usuarios seguirán las mismas normas que la prestación farmacéutica basándose en el precio final del producto sin límite de cuantía a la aportación (no hay límite). El artículo 2.3 del RD da redacción al nuevo artículo 8 ter establece en su punto primero que "*la cartera común suplementaria del Sistema Nacional de Salud incluye todas aquellas prestaciones cuya provisión se realiza mediante dispensación ambulatoria y están sujetas a aportación del usuario*". El punto segundo clasifica las prestaciones de la siguiente forma "*esta cartera común suplementaria del Sistema Nacional de Salud incluirá las siguientes prestaciones: a) Prestación farmacéutica. b) Prestación ortoprotésica. c) Prestación con productos dietéticos*". Y el punto tercero regula el tema del transporte de enfermos "*también gozará de esta consideración el transporte*

sanitario no urgente, sujeto a prescripción facultativa, por razones clínicas y con un nivel de aportación del usuario acorde al determinado para la prestación farmacéutica".

Y por último la de servicios accesorios, que incluye los servicios no esenciales y que no tienen carácter de prestación, y están sujetas a aportación y/o reembolso del usuario. Esta se encuentra regulada en el nuevo artículo 8 cuáter, establecido en el artículo 2.4 del Real Decreto Ley sobre sostenibilidad, que tiene la siguiente redacción en su punto primero "*la cartera común de servicios accesorios del Sistema Nacional de Salud incluye todas aquellas actividades, servicios o técnicas, sin carácter de prestación, que no se consideran esenciales y/o que son coadyuvantes o de apoyo para la mejora de una patología de carácter crónico, estando sujetas a aportación y/o reembolso por parte del usuario*". Existe una referencia respecto de este último punto a la Comunidades Autónomas, que podrán aprobar sus propias carteras comunes de servicios, de acuerdo a lo establecido en el artículo 2.5 de este mismo Real Decreto que da nueva redacción al 8 quinquies que en su punto primero establece que "*las comunidades autónomas, en el ámbito de sus competencias, podrán aprobar sus respectivas carteras de servicios que incluirán, cuando menos, la cartera común de servicios del Sistema Nacional de Salud en sus modalidades básica de servicios asistenciales, suplementaria y de servicios accesorios, garantizándose a todos los usuarios del mismo*".

Así mismo se faculta a las comunidades autónomas a la inclusión de nuevas tecnologías estableciéndose para ello recursos adicionales, al igual que para prestar servicios complementarios, asumiendo con cargo a sus presupuestos los costes que se generen y garantizando la financiación de dicha cartera. Así lo establece el punto segundo de este último artículo comentado "*las comunidades autónomas podrán incorporar en sus carteras de servicios una técnica, tecnología o procedimiento no contemplado en la cartera*

común de servicios del Sistema Nacional de Salud, para lo cual establecerán los recursos adicionales necesarios".

La elaboración de esta cartera común de servicios, deberá tener en cuenta factores sociales, económicos, de efectividad, beneficios y organización, para valorar su utilidad y otras alternativas, participando en ello la Red Española de Agencias de Evaluación de Tecnologías Sanitarias y Prestaciones del Sistema Nacional de Salud. El artículo 2.6 del Real Decreto Ley sobre sostenibilidad, que se viene comentando, modifica el artículo 20 del al ley de calidad sanitaria que queda redactado de la siguiente forma "*el contenido de la cartera común de servicios del Sistema Nacional de Salud se determinará por acuerdo del Consejo Interterritorial del Sistema Nacional de Salud, a propuesta de la Comisión de prestaciones, aseguramiento y financiación. En la elaboración de dicho contenido se tendrá en cuenta la eficacia, eficiencia, efectividad, seguridad y utilidad terapéuticas, así como las ventajas y alternativas asistenciales, el cuidado de grupos menos protegidos o de riesgo y las necesidades sociales, así como su impacto económico y organizativo. En la evaluación de lo dispuesto en el párrafo anterior participará la Red Española de Agencias de Evaluación de Tecnologías Sanitarias y Prestaciones del Sistema Nacional de Salud*".

Y duro fin para el artículo, que parece dejar fuera un gran número de prestaciones sanitarias, ya que establece la no inclusión de aquellos métodos no suficientemente probados, aún refiriéndose ya no a la curación de enfermedades, sino a la mejora de vida de los pacientes o a la reducción de su dolor y el sufrimiento; resulta escalofriante leer del tirón este artículo, pero esta premisa se puede convertir en callejón sin salida muy perjudicial para los enfermos, ya que si la técnica no está probada no se aplica, pero si se desestima y no se sigue experimentando, nunca podrá probarse. Parece primar aquí la economía y no la salud, sensación que persiste a lo largo de

esta norma. El 20.2 quedaría redactado de la siguiente forma "*en cualquier caso, no se incluirán en la cartera común de servicios aquellas técnicas, tecnologías y procedimientos cuya contribución eficaz a la prevención, diagnóstico, tratamiento, rehabilitación y curación de las enfermedades, conservación o mejora de la esperanza de vida, autonomía y eliminación o disminución del dolor y el sufrimiento no esté suficientemente probada".* Lo cual tira por tierra parte de lo anteriormente dicho, ya que parece que la salud no es lo primero.

En cuanto a la prestación farmacéutica, se modifica también la Ley sobre el uso de los medicamentos en cuanto a los sistemas de información para su prescripción electrónica, que recogerán los datos relativos a los precios, para que el médico pueda valorar la repercusión económica de lo que está recetando. Una vez más se podrían estar transfiriendo responsabilidades, ya que son médicos, no contables.

A propósito de la instauración del copago en España, el periódico El País, publica un artículo titulado *"Médico, enfermero y contable"*, cuyo título es muy oportuno citar en este punto, a propósito del pluriempleo que se les garantiza a los médicos con este sistema, y el cual establece que: *"El pago de los fármacos según la renta afecta a la privacidad de los datos fiscales y es técnicamente muy complejo. Ningún país de nuestro entorno utiliza este modelo. Se trata de combinar dos de las informaciones más protegidas por la legislación española: la sanitaria y la fiscal. Un modelo cuya complejidad reconocen fuentes del ejecutivo, y que no existe en ningún otro país de los que tienen sistemas sanitarios parecidos. En todos hay copago de medicamentos (como ya había en España), pero ninguno en función de la Renta"*[136].

[136] DE BENITO, Emilio: *"Médico, enfermero y contable".* El País, sábado 21 de abril de 2012, vida & artes. Pág 36.

El artículo 4 del Real Decreto Ley sobre sostenibilidad modifica el 85 de la Ley sobre el uso de los medicamentos, que queda con la siguiente redacción en su punto primero "*la prescripción de medicamentos y productos sanitarios en el Sistema Nacional de Salud se efectuará en la forma más apropiada para el beneficio de los pacientes, a la vez que se protege la sostenibilidad del sistema*". Estableciéndose en el segundo una clasificación de las prioridades "*en el Sistema Nacional de Salud, las prescripciones de medicamentos incluidos en el sistema de precios de referencia o de agrupaciones homogéneas no incluidas en el mismo se efectuarán de acuerdo con el siguiente esquema: a) Para procesos agudos, la prescripción se hará, de forma general, por principio activo. b) Para los procesos crónicos, la primera prescripción, correspondiente a la instauración del primer tratamiento, se hará, de forma general, por principio activo. c) Para los procesos crónicos cuya prescripción se corresponda con la continuidad de tratamiento, podrá realizarse por denominación comercial, siempre y cuando ésta se encuentre incluida en el sistema de precios de referencia o sea la de menor precio dentro de su agrupación homogénea*".

En lo relativo a la aportación de los beneficiarios en la prestación farmacéutica ambulatoria, en la que se dispensa al paciente a través de las farmacias, estará sujeta a la aportación del usuario, que tendrá lugar en el momento de la dispensación del medicamento. Y es en el punto cuarto de este artículo, donde se establece que "*la aportación del usuario será proporcional al nivel de renta, que se actualizará, como máximo, anualmente*". Pero si seguimos leyendo el siguiente punto, nos daremos cuenta que no es tan equitativo como parece, ya que la renta tiene en cuenta para el cálculo de sus porcentajes infinidad de datos que influyen en el pago de la misma. En cambio aquí, se hacen cuatro grandes grupos; en uno de ellos, pagan el mismo porcentaje, el 50%, personas que tengan una renta de entre 18.000 € y 100.000 €.

A la vista salta que este baremo no es equitativo en absoluto. Es más, a personas cuya renta supere los 100.000 €, solo se les aplicará el 10% más en el pago de los medicamentos o productos sanitarios. Para el resto de asegurados no incluidos en los límites comentados, tan solo un 10% menos, es decir, el 40%. En cambio los pensionistas, pagarán solo un 10%, límite que parece mucho más razonable, excepto si su renta supera los 100.000 €, en cuyo caso pagarán como si no lo fueran. En cambio, el punto sexto de este artículo establece que para garantizar la continuidad de tratamientos crónicos y garantizar los tratamientos de los pensionistas de larga duración, se podrán aplicar porcentajes con topes máximos de aportación, pero siguiendo siempre los niveles de renta ya comentados.

Dentro de este artículo 4 del Real Decreto Ley sobre sostenibilidad, comentado, su apartado trece añade un nuevo artículo 94 bis, referido a la aportación de los beneficiarios en la prestación farmacéutica ambulatoria, y que define así en su punto primero "*se entiende por prestación farmacéutica ambulatoria la que se dispensa al paciente, a través de receta médica, en oficina o servicio de farmacia." Aclarando en el punto segundo que "La prestación farmacéutica ambulatoria estará sujeta a aportación del usuario*". Especificando en el punto tercero que "*la aportación del usuario se efectuará en el momento de la dispensación del medicamento o producto sanitario*". Y puntualizando en el cuarto punto que "*la aportación del usuario será proporcional al nivel de renta que se actualizará, como máximo, anualmente*".

Así las cosas, el punto quinto vierte el jarro de agua fría para marcar la desigualdad, estableciendo que "*con carácter general, el porcentaje de aportación del usuario seguirá el siguiente esquema: a) Un 60 % del PVP para los usuarios y sus beneficiarios cuya renta sea igual o superior a 100.000 euros consignada en la casilla de base liquidable general y del ahorro de la declaración del Impuesto*

sobre la Renta de las Personas Físicas. b) Un 50 % del PVP para las personas que ostenten la condición de asegurado activo y sus beneficiarios cuya renta sea igual o superior a 18.000 euros e inferior a 100.000 euros consignada en la casilla de base liquidable general y del ahorro de la declaración del Impuesto sobre la Renta de las Personas Físicas. c) Un 40 % del PVP para las personas que ostenten la condición de asegurado activo y sus beneficiarios y no se encuentren incluidos en los apartados a) o b) anteriores. d) Un 10 % del PVP para las personas que ostenten la condición de asegurado como pensionistas de la Seguridad Social y sus beneficiarios, con excepción de las personas incluidas en el apartado a)".

Todo ello, eso sí, con unos topes máximos en algunos supuestos, que regula el punto sexto de este artículo establece que "*con el fin de garantizar la continuidad de los tratamientos de carácter crónico y asegurar un alto nivel de equidad a los pacientes pensionistas con tratamientos de larga duración, los porcentajes generales estarán sujetos a topes máximos de aportación…*" en determinados supuestos, pero siguiendo siempre los niveles de renta ya comentados.

Si es interesante saber que en determinados casos hay exenciones razonables, dado lo irrazonable de los criterios económicos en los que se basa esta norma; el punto octavo de este 94 bis establece que: "*Estarán exentos de aportación los usuarios y sus beneficiarios que pertenezcan a una de las siguientes categorías: a) Afectados de síndrome tóxico y personas con discapacidad en los supuestos contemplados en su normativa específica. b) Personas perceptoras de rentas de integración social. c) Personas perceptoras de pensiones no contributivas. d) Parados que han perdido el derecho a percibir el subsidio de desempleo en tanto subsista su situación. e) Personas con tratamientos derivados de accidente de trabajo y enfermedad profesional*".

Salta a la vista que la clasificación en cuatro grandes grupos no es equitativa en absoluto, ya que en uno de ellos, pagan el mismo porcentaje, el 50%, personas que tengan una renta de 18.000 € y las que la tengan de 100.000 €. Es más, a personas cuya renta supere los 100.000 €, solo se les aplicará el 10% más en el pago de los medicamentos o productos sanitarios. Para el resto de asegurados no incluidos en los límites comentados, tan solo un 10% menos, es decir, el 40%. En cambio los pensionistas, pagarán solo un 10%, límite que parece mucho más razonable, excepto si su renta supera los 100.000 €, en cuyo caso pagarán como si no fueran.

En líneas generales, y a simple vista, llama la atención la proximidad de los porcentajes a pagar, salvo para los pensionistas, con la amplia gama de 0 a 100 que se podía haber aplicado. Este ha sido un reparto poco equitativo, ya que la diferencia entre los porcentajes que pagan personas con rentas muy altas y los que pagan aquellas que la tienen muy baja son iguales o muy similares. Parece que se hubiese cogido la calculadora, haciendo un estudio previo de la población, para sanear las arcas sanitarias. El caso es que esta situación puede afectar a los datos personales de los pacientes.

Pero además, este Real Decreto Ley sobre sostenibilidad, introdujo una disposición adicional décima en la Ley 16/2003, de 28 de mayo, creando el Registro Estatal de Profesionales Sanitarios, que se ve regulado por el Real Decreto 640/2014, de 25 de julio, por el que se regula el Registro Estatal de Profesionales Sanitarios, que ha sido sometido entre otros organismos al informe de la AEPD. Y según recoge el artículo 2 "*el registro tiene naturaleza administrativa y estará integrado en el sistema de información sanitaria del Sistema Nacional de Salud previsto en el artículo 53 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, y tendrá por finalidad: a) Facilitar la adecuada planificación de las necesidades de profesionales sanitarios del Estado. b) Coordinar las*

políticas de recursos humanos en el ámbito del Sistema Nacional de Salud". Conteniendo este registro los siguientes datos "*a) Número de incorporación al registro. b) Nombre y apellidos. c) Número del Documento Nacional de Identidad (DNI) o Tarjeta de Identidad del Extranjero (TIE). d) Fecha de nacimiento. e) Sexo. f) Nacionalidad. g) Medio preferente o lugar a efectos de comunicaciones. h) Titulación. i) Especialidad en Ciencias de la Salud. j) Diploma en Áreas de Capacitación Específica. k) Diploma de Acreditación y Diploma de Acreditación Avanzada. l) Situación profesional. m) Ejercicio profesional. n) Lugar de ejercicio. o) Categoría profesional. p) Función. q) Desarrollo profesional. r) Colegiación profesional. s) Cobertura de responsabilidad civil en cada uno de los ámbitos de ejercicio profesional. t) Suspensión o inhabilitación para el ejercicio profesional*". Su objetivo principal es la comunicación de estos datos en caso necesario, por lo que este tema se encuentra específicamente referido en el artículo 12.1. Y cuenta además esta norma con un artículo referido en concreto a la protección de datos personales, el 17, que establece en su punto primero que "*los datos que obran en el registro se utilizarán para los fines previstos en este real decreto*". Recogiendo en el punto segundo que "*el Ministerio de Sanidad, Servicios Sociales e Igualdad adoptará las medidas necesarias para garantizar su utilización para estos fines, además de los estadísticos, científicos, históricos y sanitarios, de acuerdo con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo*".

El Real Decreto 81/2014, de 7 de febrero, por el que se establecen normas para garantizar la asistencia sanitaria transfronteriza (RDAST- RD Asistencia Sanitaria Transfronteriza), y por el que se modifica el Real Decreto sobre Receta Médica, surge con el fin de favorecer la continuidad en la atención sanitaria. Así lo establece el quinceavo párrafo del texto de esta norma: "*Al Estado español, como Estado miembro de tratamiento, le corresponde ser responsable e impulsor de unos determinados niveles de calidad y*

seguridad en la atención sanitaria, así como garantizar la existencia de mecanismos de reclamación y reparación de los posibles daños derivados de la asistencia sanitaria recibida, y facilitar el intercambio de la información que garantice la continuidad asistencial tanto para sus ciudadanos como para los ciudadanos comunitarios en general". Garantizando los siguientes extremos: copia de los informes, pruebas y procedimientos realizados al paciente, así como el intercambio de información que sea necesario para garantizar la continuidad en la atención al paciente, respetando siempre la protección del derecho a la intimidad en el tratamiento de los datos, de acuerdo lo establecido en la LOPD y Ley del Paciente. Así, el artículo quinto de esta norma, respecto de la asistencia sanitaria que deban prestar otros estados miembros a pacientes afiliados en España, establece en su punto tercero que: "*En aras de favorecer la continuidad de la atención sanitaria, se garantizará al paciente que reciba atención sanitaria en otro Estado miembro: a) La disponibilidad de una copia, en el soporte adecuado, de los informes clínicos, y de los resultados de pruebas diagnósticas y/o procedimientos terapéuticos, difundiéndose el procedimiento para su acceso. Desde las administraciones públicas se promoverá el acceso electrónico a la documentación clínica por medio de los sistemas de información dispuestos a tal efecto por el ordenamiento jurídico. b) El seguimiento sanitario en España tras recibir la atención sanitaria, de igual forma que si la asistencia recibida en otro Estado miembro se hubiera prestado en España. c) La cooperación con otros Estados miembros en el intercambio de la información oportuna que garantice la continuidad asistencial. En este sentido, se tendrá en cuenta el artículo 23 en materia de sanidad electrónica. En el citado intercambio de información, España aplicará los estándares nacionales, europeos e internacionales de comunicación de la Historia Clínica Electrónica o de sus componentes. d) Las garantías de seguridad en el tratamiento de datos establecidas en la*

legislación española en materia de protección de datos de carácter personal".

Con el objeto de hacer más fluido el intercambio de información con otros Estados Miembros en este sentido, España estará incluida en la red europea de sanidad electrónica, que se regirá por la Decisión 2011/890/UE de la Comisión, de 22 de diciembre de 2011, por la que se establecen las normas de establecimiento, gestión y funcionamiento de la red de autoridades nacionales responsables en materia de salud electrónica. Así mismo, el Ministerio de Sanidad, Servicios Sociales e Igualdad, formará parte la Red europea de evaluación de tecnologías sanitarias, como canal por el que la Unión Europea gestiona el intercambio de información científica entre los Estados miembros.

De igual modo, los proveedores de asistencia sanitaria españoles, deberán garantizar a los pacientes de otros estados miembros, que necesiten asistencia sanitaria transfronteriza, una copia de su historia clínica para garantizar la citada continuidad en la prestación. Así lo establece el tercer punto del artículo sexto de esta norma "*se garantizará, en aras de favorecer la continuidad de la atención sanitaria: a) La disponibilidad de una copia, en el soporte adecuado, de los informes clínicos, y de los resultados de pruebas diagnósticas y/o procedimientos terapéuticos al paciente, difundiéndose el procedimiento para su acceso. Desde las administraciones públicas se promoverá el acceso electrónico a la documentación clínica por medio de los sistemas de información dispuestos a tal efecto por el ordenamiento jurídico. b) La cooperación con otros Estados miembros en el intercambio de la información oportuna que garantice la continuidad asistencial. En este sentido, se tendrá en cuenta el artículo 23 en materia de Sanidad electrónica. En el citado intercambio de información, España aplicará los estándares nacionales, europeos e internacionales de comunicación de la Historia Clínica Electrónica o*

de sus componentes. c) La protección del derecho a la intimidad con respecto al tratamiento de los datos personales y de salud, de conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y 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".

A propósito de lo establecido en el varias veces citado artículo 23, dice su punto primero que "*con el objeto de favorecer la cooperación y el intercambio de información con otros Estados miembros, España formará parte de la red europea de sanidad electrónica, regulada en la Decisión 2011/890/UE de la Comisión, de 22 de diciembre de 2011, por la que se establecen las normas de establecimiento, gestión y funcionamiento de la red de autoridades nacionales responsables en materia de salud electrónica*". Y respecto de la Red europea de evaluación de las tecnologías sanitarias, establece el artículo 24.1 que "*el Ministerio de Sanidad, Servicios Sociales e Igualdad participará en la Red europea de evaluación de tecnologías sanitarias, a través de la cual la Unión Europea facilitará la cooperación, la comunicación y el intercambio de información científica entre los Estados miembros*". Habría que ver si en estos casos la información científica pudiese llevar aparejada información personal y si esta está o no disociada de los daos de los pacientes.

La disposición adicional segunda en relación con otras disposiciones establece que este Real Decreto se aplicará sin perjuicio de lo establecido, entre otras disposiciones, en la LOPD. Así lo contempla literalmente: "*Este real decreto se aplicará sin perjuicio de lo establecido en las disposiciones siguientes: d) Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*".

Con el cometido de aprobar la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Sanidad, Servicios Sociales e Igualdad, surge la Orden SSI/321/2014, de 26 de febrero, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Sanidad, Servicios Sociales e Igualdad (OSI- Orden sobre seguridad de la información), según establece el cuarto párrafo de su texto, avocando al cumplimiento de la normativa en materia de protección de datos "*la Política de Seguridad de la Información del Ministerio de Sanidad, Servicios Sociales e Igualdad, de conformidad con lo dispuesto en el artículo 11 del Real Decreto 3/2010, de 8 de enero, da soporte a todas las exigencias del Esquema Nacional de Seguridad, así como a los requisitos derivados de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de desarrollo, aprobado mediante el Real Decreto 1720/2007, de 21 de diciembre*".

El citado Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, nació para garantizar la fiabilidad de estos servicios y proteger la información de accesos no autorizados, respetando el Esquema Nacional de Seguridad establecido por el Ministerio de Sanidad, con igual respeto a la normativa de protección de datos, según establece el párrafo tercero de esta norma "*el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas*".

Por otro lado, la administración electrónica hace necesario el tratamiento informático a través de redes de comunicaciones de una enorme cantidad de información, que puede exponerse a grandes riesgos, por lo que las redes por las que circulen los datos, así como los servicios que estas ofrezcan, deben estar preparadas ante las amenazas que pongan en peligro la información a través de ellas gestionada. Así lo establece el segundo párrafo de este texto "*en el contexto de la Administración Electrónica, se entiende por seguridad de la información la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes y acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de los datos almacenados o transmitidos y de los servicios que dichas redes o sistemas ofrecen, o a través de los cuales se realiza el acceso*". Y según concluye la introducción de este texto, bajo la supervisión de la Agencia Española de Protección de Datos "*esta norma ha sido sometida a informe previo de la Agencia Española de Protección de Datos*".

Entrando en el articulado de la citada orden que nos ocupa, surge más específicamente con el objeto de aprobar la Política de Seguridad de la Información (PSI), dentro de la administración electrónica del Ministerio de Sanidad, Servicios Sociales e igualdad, aplicable a todos sus sistemas de información, siendo aplicable también a los órganos dependientes y por todo su personal. Así lo establece su artículo 1.1 "*el objeto de esta orden es la aprobación de la Política de Seguridad de la Información (en adelante, PSI) en el ámbito de la Administración Electrónica del Ministerio de Sanidad, Servicios Sociales e Igualdad, así como el establecimiento del marco organizativo y tecnológico de la misma*". Aún cuando no estuvieran destinados en los mismos, siempre que tengan acceso a sus sistemas de información, les será de aplicación dicho sistema, según marca el segundo punto de este primer artículo "*la PSI se aplicará a todos los sistemas de información utilizados por todos los órganos y*

unidades centrales y territoriales del Ministerio de Sanidad, Servicios Sociales e Igualdad y por los organismos públicos que dependan del mismo. La PSI deberá ser observada, igualmente, por todo el personal destinado en dichos órganos y unidades, así como por aquellas personas que, aunque no estén destinadas en los mismos, tengan acceso a sus sistemas de información".

El marco normativo, según establece el artículo 3.1f) y g) de esta norma, comprende legislación sectorial y específica, entre la que se encuentra la LOPD y el RLOPD "*el marco normativo en que se desarrollan las actividades del Ministerio de Sanidad, Servicios Sociales e Igualdad comprende la legislación sectorial reguladora de la actuación de los órganos superiores y directivos del Departamento y de los organismos públicos dependientes del mismo, así como la legislación específica en vigor sobre la administración electrónica que se detalla a continuación: f) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. g) Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre*".

El artículo cuarto, regula la estructura organizativa de la PSI, detallando sus agentes "*la estructura organizativa de la gestión de la seguridad de la información en el ámbito de la administración electrónica del Ministerio de Sanidad, Servicios Sociales e Igualdad está compuesta por los siguientes agentes: a) El Comité de Seguridad de la Información. b) Los Responsables de Seguridad de la Información. c) Los Responsables de la Información. d) Los Responsables de los Servicios*." El comité se encuentra regulado en artículo 5.1 y se crea como *"…grupo de trabajo en el seno de la Comisión Ministerial de Informática del Departamento.", y como dice el punto tercero de este artículo "…coordinará todas las actividades relacionadas con la seguridad de los sistemas de información…*". El Responsable de seguridad de la información coordina la seguridad

de los sistemas de información, vela por esta en las infraestructuras de comunicaciones, recursos físicos y lógicos y personas que los manejan, siendo todo ello denominado "*dominio de seguridad*", que es gestionado de forma conjunta. Así lo establece el artículo 6.1: "*El Responsable de Seguridad de la Información (RSI) determina, en cada dominio de seguridad en el que resulta competente, las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios*", definiéndose tal dominio de seguridad en el segundo párrafo de este artículo como "*el conjunto de infraestructuras de comunicaciones, equipamientos físicos y lógicos y personas que sobre ellos operan, interrelacionados de tal modo que resulte más eficiente gestionar la seguridad de la información manejada por los mismos de forma conjunta*".

Por su parte un equipo de seguridad de la información apoyará al anterior, según establece el artículo 7.1: "*El Equipo de Seguridad de la Información se constituye como grupo de apoyo del RSI correspondiente para el cumplimiento de sus funciones*"., con el cometido de llevar a cabo auditorías preventivas de seguridad, así como la supervisión de la seguridad del sistema, la resolución de incidentes y la realización de los llamados "*planes de continuidad de los sistemas de información*", según establece el 7.2: "*A estos efectos, el Equipo de Seguridad de la Información realizará las auditorías periódicas de seguridad (prevención), el seguimiento y control del estado de seguridad del sistema (detección), la respuesta eficaz a los incidentes de seguridad desde su notificación hasta su resolución (respuesta) y el desarrollo de los planes de continuidad de los sistemas de información (recuperación)*".

Además según el artículo 11, el RSI se encargará del control en la realización de los análisis, detectando los problemas para comunicárselos a los Responsables de la Información y del Servicio, según marca el 11.2: "*El RSI es el encargado de que el análisis se realice en tiempo y forma, así como de identificar carencias y*

debilidades y ponerlas en conocimiento de los Responsables de la Información y del Servicio". Las funciones de estas figuras vienen reguladas en los artículos 8 y 9 de esta norma. El responsable de la información gestiona los procedimientos administrativos, según el 8.1: "*El Responsable de la Información es el titular del órgano o unidad que gestione cada procedimiento administrativo*", con sometimiento a la normativa de protección de datos, de acuerdo a lo establecido en el segundo párrafo de este artículo "*en los casos en que un sistema trate datos de carácter personal, el Responsable de la Información será además el responsable del fichero. Sus funciones vendrán determinadas por la legislación aplicable sobre protección de datos de carácter personal*". Y el responsable del servicio, determinará los diferentes niveles de seguridad, de acuerdo a lo establecido en el 9.2: "*El Responsable del Servicio tiene encomendada la función de determinar los niveles de seguridad del servicio dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero*".

Volviendo al cita artículo 11, habrá que proponer medidas de seguridad adecuadas a los riesgos, que deberán ser aprobadas en un Plan de Acción anual por el Responsable de Seguridad de la Información, según establece su punto tercero "*la gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionadas a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por el Responsable de Seguridad de la Información correspondiente al dominio de seguridad, recogiéndose en un Plan de Acción anual*".

Si existiera conflicto entre los distintos responsables, resolverá el superior jerárquico, y en última instancia el Comité, según establece el 10.1, "*en caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En su defecto, será el Comité quien resuelva*".

prevaleciendo las exigencias establecidas en la normativa de protección de datos, según establece el 10.2: "*En la resolución de estos conflictos, prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal*".

El artículo 12 por su parte, establece que el cuerpo normativo se organizará en cinco niveles: estos niveles son la política de seguridad de la información (PSI), las normas de seguridad, los procedimientos generales, los procedimientos específicos y los informes, registros, evidencias electrónicas y plantillas, todos ellos documentos técnicos. Así lo establece el punto primero de este artículo "*el cuerpo normativo sobre seguridad de la información se desarrollará en cinco niveles con diferente ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, pero de manera que cada elemento normativo se fundamente en las normas de nivel superior*", que además llama al cumplimiento de la normativa en materia de protección de datos en su segundo párrafo "*todos estos niveles prestarán especial atención a las exigencias derivadas del Esquema Nacional de Seguridad, así como a la normativa aplicable en materia de protección de datos de carácter personal*".

Y en relación directa al documento de medidas de seguridad, establece el artículo 13.2 que: "*Los ficheros que contengan datos de carácter personal estarán referenciados en el correspondiente documento de seguridad previsto en el artículo 88 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre*", puntualizando el punto tercero de este mismo artículo que "*las medidas de seguridad requeridas por el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, estarán incluidas en los diferentes niveles de desarrollo normativo previstos en el artículo 12*".

Así mismo, es de especial interés el artículo 14, dedicado al desarrollo de actividades de formación para el personal del Ministerio de Sanidad, Servicios Sociales e Igualdad, incluyendo actividades

dentro de sus planes de formación así como a la difusión de la mencionada PSI. Dice en concreto este artículo en su párrafo primero que "*en el Ministerio de Sanidad, Servicios Sociales e Igualdad, se desarrollarán actividades específicas orientadas a la formación de su personal en materia de seguridad de la información, así como a la difusión de la PSI y su desarrollo normativo*". Y en su párrafo segundo matiza que "*a estos efectos, deberán incluirse actividades formativas en esta materia dentro de los Planes de Formación del Ministerio*".

Por último, cuenta esta norma con un anexo sobre Directrices generales para el establecimiento de un marco de control de la seguridad de la información y para la determinación de los objetivos de control de la seguridad necesarios, basados en el estándar internacional ISO/IEC 27002:2005, centrándose en los siguientes conceptos: gestión de los activos, seguridad física y del entorno, gestión de comunicaciones y operaciones, control de acceso, adquisición, desarrollo y mantenimiento de sistemas, gestión de incidencias de seguridad de la información, gestión de la continuidad del negocio y conformidad. Estos puntos se pueden cotejar con los requisitos establecidos en el RLOPD.

Por otro lado la Orden SSI/1687/2014, de 9 de septiembre, por la que se modifica la Orden de 21 de julio de 1994, por la que se regulan los ficheros con datos de carácter personal (OFDP- Orden sobre ficheros de datos personales), recoge en el primer párrafo de su texto que "*mediante la Orden de 21 de julio de 1994, por la que se regulan los ficheros con datos de carácter personal gestionados por el Ministerio de Sanidad y Consumo, se dio cumplimiento a lo establecido en la disposición adicional segunda, 2 de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal*" Especificando en el artículo segundo, dedicado a la gestión y organización del fichero que, "*la persona titular de la Delegación del Gobierno para la*

Violencia de Género adoptará, bajo la superior dirección de la persona titular del Ministerio de Sanidad, Servicios Sociales e Igualdad, las medidas de gestión y organización que sean necesarias, asegurando, en todo caso, la confidencialidad, seguridad e integridad de los datos, así como las conducentes a hacer efectivas las garantías, derechos y obligaciones reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y demás normas de desarrollo. Los datos de carácter personal registrados en los ficheros relacionados con el Anexo sólo serán utilizados para los fines expresamente previstos y por el personal debidamente autorizado".

La derogada Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones tenía sus objetivos, contenidos en el artículo 3, la defensa de los usuarios, haciendo hincapié en los derechos al honor, la intimidad y la protección de datos. La actual Ley 9/2014, de 9 de mayo, de Telecomunicaciones (LT-Ley de Telecomunicaciones), que la sustituye, contribuye al bienestar social y al avance de la tecnología, en especial al de las telecomunicaciones; así se establece en el primer párrafo del segundo punto del preámbulo de la citada norma *"las telecomunicaciones constituyen uno de los sectores más dinámicos de la economía y uno de los que más pueden contribuir al crecimiento, la productividad, el empleo, y por tanto, al desarrollo económico y al bienestar social, afectando directamente al círculo de protección de los intereses generales".*

Además, estos factores constituyen en el actual momento económico-financiero un modo de activar la competencia, siendo necesario que exista un marco que regule esta situación; y así lo recoge el tercer párrafo del comentado punto segundo del preámbulo

“la situación económica y financiera que afecta a una gran parte de los países desarrollados, la necesidad actual de fomentar la inversión e impulsar la competencia, son elementos esenciales a considerar en la revisión del marco regulador”.

La liberalización del sector persigue aumentar la seguridad jurídica en este aspecto reduciendo las cargas para los operadores, según establece el primer párrafo del punto tercero del preámbulo *“la presente Ley persigue, por tanto, garantizar el cumplimiento de los objetivos de la Agenda Digital para Europa, que requiere, en la actual situación de evolución tecnológica e incertidumbre económica, asegurar un marco regulatorio claro y estable que fomente la inversión, proporcione seguridad jurídica y elimine las barreras que han dificultado el despliegue de redes, y un mayor grado de competencia en el mercado”*, que se cierra estableciendo que *“en definitiva, los criterios de liberalización del sector, libre competencia, de recuperación de la unidad de mercado y de reducción de cargas que inspiran este texto legal pretenden aportar seguridad jurídica a los operadores y crear las condiciones necesarias para la existencia de una competencia efectiva, para la realización de inversiones en el despliegue de redes de nueva generación y para la prestación de nuevos servicios, de modo que el sector pueda contribuir al necesario crecimiento económico del país”.* El artículo 28.2b) por su parte, faculta al gobierno a imponer obligaciones de servicio público motivadas entre otras causas por la utilización de las tecnologías o nuevos servicios referidos, al sector sanitario, entre otros. Así habilita este precepto al gobierno para *“…imponer otras obligaciones de servicio público, previo informe de la Comisión Nacional de los Mercados y la Competencia, así como de la administración territorial competente, motivadas por: b) Razones de extensión del uso de nuevos servicios y tecnologías, en especial a la sanidad, a la educación, a la acción social y a la cultura”.*

En concreto, el párrafo cuarto del artículo 28 establece que *"en cualquier caso, la obligación de encaminar las llamadas a los servicios de emergencia sin derecho a contraprestación económica de ningún tipo debe ser asumida tanto por los operadores que presten servicios de comunicaciones electrónicas al público para efectuar llamadas nacionales a números de un plan nacional de numeración telefónica, como por los que exploten redes públicas de comunicaciones electrónicas. Esta obligación se impone a dichos operadores respecto de las llamadas dirigidas al número telefónico 112 de atención a emergencias y a otros que se determinen mediante real decreto, incluidas aquellas que se efectúen desde teléfonos públicos de pago, sin que sea necesario utilizar ninguna forma de pago en estos casos".* Esta llamada supondrá un posterior aporte de datos personales a los citados servicios, que deberán cumplir igualmente con la normativa de protección de datos personales.

El punto cuarto del preámbulo establece, por su parte, en su párrafo segundo que: *"El Título I, «Disposiciones generales», establece, entre otras cuestiones, el objeto de la Ley, que no se limita a la regulación de las «comunicaciones electrónicas», término que, de acuerdo con las Directivas comunitarias, engloba aspectos tales como la habilitación para actuar como operador, los derechos y obligaciones de operadores y usuarios, o el servicio universal, sino que aborda, de forma integral, el régimen de las «telecomunicaciones» al que se refiere el artículo 149.1.21.ª de la Constitución Española. Por ello, la presente Ley regula, asimismo, otras cuestiones como la instalación de equipos y sistemas, la interceptación legal de las telecomunicaciones, la conservación de datos, o la evaluación de conformidad de equipos y aparatos, temas que a nivel comunitario son objeto de normativa específica".*

Los operadores de comunicaciones electrónicas, ya sea porque estas están disponibles al público, o porque se explotan a través de

redes públicas, el Ministerio de Industria, Energía y Turismo, podrá exigirles que informen gratuitamente a los abonados sobre cuestiones de interés público, cubriendo los riesgos para la privacidad, seguridad personal y datos de carácter personal, según el artículo 54.4b), que literalmente dice: *"El Ministerio de Industria, Energía y Turismo podrá exigir a los operadores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público que difundan de forma gratuita, y en un determinado formato, información de interés público a los antiguos y nuevos abonados, cuando proceda, por las mismas vías utilizadas normalmente por éstos para comunicarse con los abonados, información que cubrirá los siguientes aspectos: Los medios de protección contra los riesgos para la seguridad personal, la privacidad, y los datos de carácter personal en el uso de los servicios de comunicaciones electrónicas".*

Regulando de igual modo el artículo 48 las comunicaciones no solicitadas, los datos de tráfico y localización y las guías de abonados. En esta materia corresponderá a la AEPD potestad sancionadora en determinadas infracciones de los derechos de los usuarios sobre protección de datos y privacidad reconocidos en esta ley. Así lo establece su punto primero: *"Respecto a la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas los usuarios finales de los servicios de comunicaciones electrónicas tendrán los siguientes derechos: a) A no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de comunicación comercial sin haber prestado su consentimiento previo e informado para ello. b) A oponerse a recibir llamadas no deseadas con fines de comunicación comercial que se efectúen mediante sistemas distintos de los establecidos en la letra anterior y a ser informado de este derecho".* Esto está en relación con lo dicho sobre la privatización de la sanidad, cuando nos reconducen al sector privado por un supuesto colapso en el servicio público de salud.

Posteriormente se ha promulgado también la Orden SSI/1885/2015, de 8 de septiembre, por la que se modifica la Orden de 21 de julio de 1994, por la que se regulan los ficheros con datos de carácter personal gestionados por el Ministerio de Sanidad y Consumo (OFMS- Orden sobre ficheros Ministerio de Sanidad y Consumo). Que proclama en su artículo cuarto que "*el titular del órgano responsable del fichero Registro de Actividad de Atención Sanitaria Especializada (RAE-CMBD) adoptará, bajo la superior dirección del titular del Ministerio de Sanidad, Servicios Sociales e Igualdad, las medidas de gestión y organización que sean necesarias, asegurando, en todo caso, la confidencialidad, seguridad e integridad de los datos, así como las conducentes a hacer efectivas las garantías, obligaciones y derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en su Reglamento de desarrollo aprobado por Real Decreto 1720/2007, de 21 de diciembre, y demás normas de desarrollo. Los datos de carácter personal registrados en el fichero que se crea mediante esta orden sólo serán utilizados para los fines expresamente previstos y por el personal debidamente autorizado*". Incidiendo también en el tema de la cesión de datos e su artículo quinto "*los datos contenidos en este fichero sólo podrán ser cedidos en los supuestos expresamente previstos por la ley*".

El Real Decreto 69/2015, de 6 de febrero, por el que se regula el Registro de Actividad de Atención Sanitaria Especializada (RDAE-Real Decreto de atención especializada), se encarga de esta materia, en un momento en el que el sector público está tendiendo a la privatización de la sanidad, cuyo objeto es, según marca su artículo primero, "*… regular el Registro de Actividad de Atención Sanitaria Especializada, en adelante registro, con base en el actual Conjunto Mínimo Básico de Datos (RAE-CMBD), así como establecer su estructura y contenido".*

El contenido de dicho registro lo marca el artículo 1: "*El registro contendrá los siguientes datos: 1. Tipo de código de Identificación Personal., 2. Código de Identificación Personal., 3. Número de historia clínica., 4. Fecha de nacimiento., 5. Sexo., 6. País de nacimiento., 7. Código postal del domicilio habitual del paciente., 8. Municipio del domicilio habitual del paciente., 9. Régimen de financiación., 10. Fecha y hora de inicio de la atención., 11. Fecha y hora de la orden de ingreso., 12. Tipo de contacto., 13. Tipo de visita., 14. Procedencia., 15. Circunstancias de la atención., 16. Servicio responsable de la atención., 17. Fecha y hora de finalización de la atención., 18. Tipo de alta., 19. Dispositivo de continuidad asistencial., 20. Fecha y hora de intervención., 21. Ingreso en Unidad de Cuidados Intensivos., 22. Días de estancia en Unidad de Cuidados Intensivos., 23. Diagnóstico principal., 24. Marcador POA1 del diagnóstico principal., 25. Diagnósticos secundarios., 26. Marcador POA2 de los diagnósticos secundarios., 27. Procedimientos realizados en el centro., 28. Procedimientos realizados en otros centros., 29. Códigos de morfología de las neoplasias., 30. Centro sanitario., 31. Comunidad autónoma del centro sanitario*". Contemplando además el segundo punto de este precepto que "*las comunidades autónomas, en el ámbito de sus competencias podrán establecer sus respectivos modelos de registro, incorporando, además, otros datos que consideren oportunos*". Y curiosamente, el punto tercero, excluye de su contenido al resto de datos especialmente protegidos en el artículo 7 de la LOPD, salvo el de afiliación sindical "*en el registro no podrá figurar ningún dato relativo a la ideología, creencia, religión, origen racial, ni orientación sexual del paciente*".

Del mismo modo, el artículo 3.1 de esta norma establece que, "*esta normativa afecta tanto a hospitales como a centros ambulatorios que prestan servicios de atención especializada, tanto públicos como privados*". El órgano competente será el Dirección General de Salud Pública, Calidad e Innovación del Ministerio de

Sanidad, Servicios Sociales e Igualdad, al que se adscribirá el registro, y que según el artículo 4.1 "*será el órgano encargado de su organización y gestión y el responsable de adoptar las medidas que garanticen la confidencialidad, seguridad e integridad de los datos contenidos en el registro*".

En medio de este continuo cambio nos encontramos en la actualidad, ante lo que todos debemos regirnos por unas mismas normas y principios, para que este aumento de volumen en el tratamiento de los datos personales, esté lo más controlado posible por aquellos a los que hacen referencia los datos, sus auténticos titulares. Aunque muchas veces pueda darnos la sensación de que determinadas personas o instituciones se apropien de ellos, pudiendo dar la sensación en algunos casos de que se está traficando con ellos.

No cabe duda tras este recorrido histórico, de que el derecho a la protección de datos personales, ya reconocido jurisprudencialmente, es un derecho nuevo y distinto a la intimidad, aunque el punto de partida jurisprudencial se encuentre en ella. A día de hoy, la intimidad está regulada en la Constitución Española en el art. 18.1 y la protección de datos de asimila a ella por contenidos a lo establecido en el 18.4, porque nuestra norma fundamental solo limita el uso de la informática como forma de irrupción en la intimidad, dejando fuera el resto de medios para vulnerarla.

Lucas Murillo de la Cueva sostiene que "*el derecho a la autodeterminación informativa se construye a partir del derecho a la intimidad…*"[137], siendo por tanto derechos distintos.

La profesora Serrano Maíllo, ha manifestado respecto al comentado precepto que: *"El artículo 18.4 CE dispone: "La Ley limitará el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el pleno uso de los*

[137] LUCAS MURILLO DE LA CUEVA, Pablo: *"La protección de los datos personales frente al uso de la informática"*. Editorial Tecnos, Madrid, 1990. Pág. 45.

derechos." A pesar de lo desafortunado de su redacción (por lo poco probable y, a la vez, poco deseable, que sería limitar el uso de la informática), se desprende de este artículo que nuestra Carta Magna introduce un mandato constitucional al legislador para que regule el tratamiento de los datos personales, con el fin de evitar posibles vulneraciones de los derechos al honor y a la intimidad. Pero además de una orden de regulación para el legislador, este precepto incluye, según la doctrina, un derecho fundamental: "la libertad frente a las potenciales agresiones a la dignidad y a la libertad provenientes del uso ilegítimo de datos mecanizados." Derecho del que solo son titulares las personas físicas, no jurídicas"[138].

Otros autores han manifestado sobre la existencia de un derecho independiente que *"…fue el propio Tribunal Constitucional el que reconoció, en su STC 254/1993, de 20 de julio, que, pese a que el art. 18.4 CE protege expresamente derechos como la intimidad o el honor, con lo que actúa como instituto de garantía de los mismos, lo hace otorgando a la persona un haz de facultades positivas de control sobre todos sus datos que trascienden a las que tradicionalmente definen a dichos derechos fundamentales, lo que demostraba, a su juicio, que tal precepto establecía un nuevo derecho o libertad fundamental autónomo, aunque conectado con aquellos, que podría quedar encuadrado bajo el nuevo y más amplio derecho a la privacidad…"*[139]. Entonces "*se convertía así al derecho a la privacidad, como derecho en cierta medida diferente pero conectado y garantizador de la intimidad, en el valor realmente tutelado por el arto 18.4 CE Y por toda la normativa que desarrollaba el mandato constitucional en él contenido; posición que dominó el desarrollo de las posteriores resoluciones jurisprudenciales relativas*

[138] SÁNCHEZ GONZÁLEZ, Santiago (coord.): *"Dogmática y práctica de los derechos fundamentales*". Tirant lo Blanch, Valencia 2015. Págs. 242-244.

[139] ARRIBAS LEÓN, Mónica, CARRIZOSA PRIETO, Esther, CARRUSO FONTÁN, Viviana, GALAÁN MUÑOZ, Alfonso, HOLGADO GONZÁLEZ, María, LUCENA CID, Isabel Victoria, TOSCANO GIL, Francisco: *"La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación"*. Tirant Lo Blanch, Valencia, 2014. Pág. 210.

a esta materia, hasta que se dictó la decisiva STC 292/2000, de 30 de noviembre"[140]. Y continúan estos autores diciendo que "*fue precisamente en esta Sentencia, donde nuestro Tribunal Constitucional señaló que, mientras la función de la intimidad era la de proteger al individuo frente a intromisiones no deseadas que pudiesen realizarse en su vida personal y familiar, lo que otorgaba a dicho derecho un contenido claramente negativo, la protección de datos le daba un poder de control sobre sus datos de carácter personal, tanto privados como públicos, que le convertía en titular de unas facultades positivas que imponían a terceros deberes jurídicos, (como los de informar, pedir el consentimiento, permitir el acceso, rectificar o cancelar los datos, etc.), que no solo trataban de proteger su intimidad, sino que también tutelaban a todos los bienes de la personalidad que pertenecían a su vida privada y estaban unidos a su dignidad personal, lo que convertiría a la protección de dichos datos en un derecho fundamental independiente y diferente de la intimidad y también de la privacidad, que, de hecho, reconocía a su titular unas facultades y unos poderes que trascendían con mucho a los que definían a estos dos últimos derechos*"[141].

A este respecto, Herranz Ortiz ha manifestado que "*se distinguen dos sectores enfrentados, uno de los cuales rechaza la consideración del derecho a la autodeterminación informativa como derecho fundamental argumentado que es suficiente para ofrecer garantías individuales…otro sostiene la idea insoslayable de admitir la existencia de un nuevo derecho fundamental, cuya construcción se asienta sobre el reconocimiento al individuo de unas facultades*

[140] Ibídem. Pág. 211.

[141] ARRIBAS LEÓN, Mónica, CARRIZOSA PRIETO, Esther, CARRUSO FONTÁN, Viviana, GALAÁN MUÑOZ, Alfonso, HOLGADO GONZÁLEZ, María, LUCENA CID, Isabel Victoria, TOSCANO GIL, Francisco: *"La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación"*. Tirant Lo Blanch, Valencia, 2014. Pág. 211.

de disposición y decisión respecto a sus propios datos personales"[142].

Pero no a todos los autores gusta el término de autodeterminación informativa, por lo que "*contribuirá a introducir la polémica sobre las diferentes acepciones que puede adoptar la técnica jurídica de protección de datos personales, recoger la reflexión que con acierto introduce Sánchez de Diego al rechazar la utilización del término «autodeterminación informativa» porque en opinión del citado autor, la expresión «derecho a la autodeterminación», tiene en la actualidad una significación muy precisa-referida a la capacidad de los pueblos a determinar su destino político-y totalmente diferente a la que se le quiere dar*"[143]. "*Cuando Sánchez de Diego se refiere a la protección de la intimidad frente a la utilización de la informática emplea el término derecho a la intimidad informática, aunque la expresión no permite duda sobre su ámbito, debe entenderse que no solo la intimidad-como esfera estrictamente interior y propia de la esencia de la personalidad-merece tutela frente al tratamiento informático de los datos personales*"[144].

Cualquiera de los dos términos, "*autodeterminación informativa o libertad informática*", han sido sustituidos por el de "*derecho a la protección de datos personales*", el cual garantiza a la persona el control y acceso sobre los datos que le conciernen.

Un sector doctrinal afirma a este respecto que "*la configuración de este nuevo derecho fundamental encontraría así su fundamento en el hecho de que lo que se trata de proteger no es ya tanto la intimidad sino el derecho de cada individuo a controlar el uso de sus datos contenidos en soportes electrónicos, proponiéndose por ello*

[142] HERRÁN ORTIZ, Ana Isabel: *"La violación de la intimidad en la protección de datos personales"*. Dykinson, Madrid 1.999. Pág. 77.

[143] HERRÁN ORTIZ, Ana Isabel: *"La violación de la intimidad en la protección de datos personales"*. Dykinson, Madrid 1.999. Pág. 78.

[144] Ibídem. Pág. 83.

que en relación con los que se guardan en soportes informáticos se empleen expresiones como «autodeterminación informativa» o libertad informática…"[145].

Lucas Murillo de la Cueva va más allá al sostener *"…la destrucción de la autodeterminación informativa a causa de un uso abusivo de la informática*"[146]. Así visto el riesgo *"…lo que se debe regular no es la informática en sí misma, ni en la multiplicidad de sus aplicaciones, sino la protección de la autodeterminación informativa, exigencia esta que, con la naturaleza de derecho fundamental, deriva directamente de la Constitución*"[147]. Y es que, como ya se ha dicho, la informática comporta importantes peligros, fundamentalmente para los titulares de los datos, en el caso que nos ocupa para los pacientes.

En otra de sus obras Lucas Murillo de la Cueva sostiene que *"…el bien jurídico subyacente es la libertad informática o –en fórmula menos estética pero más precisa- la autodeterminación informativa y consiste, sencillamente, en el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente sea íntima o no para preservar, de este modo y en último extremo, la propia identidad, nuestra dignidad y libertad. En su formulación como derecho implica necesariamente poderes que permitan a su titular definir los aspectos de su vida que no sean públicos que desea que se conozcan, así como facultades que le aseguren que los datos que de su persona manejan*

[145] GÓMEZ RIVERO, María del Carmen: *"La protección penal de los datos sanitarios. Especial referencia al secreto profesional médico".* Editorial Comares, S.L., Granada, 2007. Pág. 49.

[146] LUCAS MURILLO DE LA CUEVA, Pablo: *"La protección de los datos personales frente al uso de la informática"*. Editorial Tecnos, Madrid, 1990. Pág. 157.

[147] LUCAS MURILLO DE LA CUEVA, Pablo: *"La protección de los datos personales frente al uso de la informática"*. Editorial Tecnos, Madrid, 1990. Pág. 176.

informáticamente terceros son exactos, completos y actuales y que se han obtenido de modo leal y lícito"[148].

También Lucas Murillo expresa que *"…El artículo 10.2 de la Constitución que eleva a canon interpretativo de las normas relativas a derechos fundamentales los tratados y acuerdos internacionales sobre las mismas materias ratificados por España, refuerza los anteriores argumentos. En efecto, esta disposición obliga a interpretar el artículo 18.4 de la Constitución a la luz del Convenio 108 del Consejo de Europa que se propone, como sabemos, proteger a las personas con respecto al tratamiento automatizado de los datos de carácter personal. Opera, por tanto, en el campo de los derechos fundamentales…*"[149]. Por lo tanto *"…nada impide considerar que el derecho a la privacidad al que se refiere la LORTAD es un derecho fundamental aunque el legislador no le haya atribuido expresamente esta calificación, cosa, por otra parte, que no es indispensable «el carácter fundamental de un derecho nace de la Constitución, no de la ley», ni se hace en todos los casos*"[150].

Tras el exhaustivo examen de la normativa puede entenderse la complejidad de la aplicación de una norma en relación con el resto. No obstante, este panorama general, en cada apartado correspondiente se referirán los artículos de las citadas normativas que convengan.

III.2. ACTUALES: INTERÉS GENERAL DE LA MEDICINA BAJO LA PROTECCIÓN DE DATOS.

El sector médico, como cualquiera en el que se traten personales, se encuentra afectado por la normativa existente en

[148] LUCAS MURILLO DE LA CUEVA: Pablo. "*Informática y Protección de Datos Personales"*. Centro de Estudios Constitucionales, Madrid 1993. Pág. 32.

[149] LUCAS MURILLO DE LA CUEVA: Pablo. "*Informática y Protección de Datos Personales"*. Centro de Estudios Constitucionales, Madrid 1993. Pág. 36.

[150] Ibídem.

materia de protección de datos. Y aunque lo principal en este ámbito es preservar la salud de los pacientes, para llevar tal cometido a cabo, es necesario tratar los datos personales de los mismos. De modo que tal tratamiento debe llevarse a cabo bajo la protección de datos personales.

La primera referencia, tal y como argumentaremos a continuación sobre la protección de los datos médicos es que estos se encuentran desprotegidos en gran medida. A este respecto sostiene parte de la doctrina que *"… La LOPD es una norma claramente insuficiente para el sector sanitario que intenta abarcar todos los sectores pero no alcanza a profundizar en cada uno de ellos…"* [151].

Esta idea ya ha sido comentada anteriormente respecto a la gran cantidad de normativa existente en materia sanitaria y que refiere constantemente al cumplimiento de la normativa existente en materia de protección de datos personales. Se ha hablado también de la posibilidad de una norma única en el sector sanitario que regule todos los aspectos en este campo, pero que, según ya se apuntó, sería difícil de gestionar por el volumen de materias que tendría que regular. En mi opinión la LOPD se ve sobradamente complementada por la abundante regulación que existe en el ámbito de la salud, y a la que la legislación de protección de datos alude, al igual que lo hace en otros sectores, en los que exista normativa específica en la materia.

Además este mismo sector ha manifestado que *"… en el escenario actual, la mayoría de los centros sanitarios españoles aún no han tomado conciencia de la importancia de esta nueva cultura de la protección de datos, y presentan graves irregularidades en los*

[151] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso: *"La protección de datos personales en el ámbito sanitario"*. Editorial Aranzadi, Navarra 2002. Pág. 22.

sistemas de protección de datos de salud de sus pacientes. La APD lleva tiempo analizando el cumplimiento de la Ley en el sector sanitario y dando recomendaciones útiles sobre el tratamiento de los datos de los pacientes y los derechos y deberes de los facultativos en este campo" [152]*.*

Este tema de la concienciación será recordado en el apartado de la formación que debe recibir el personal que accede al fichero de datos, que es quien en mayor grado tiene en su mano el buen uso de la información.

En el año 1995, bajo el mandato de la derogada LORTAD, la AEPD, llevó a cabo el Plan de Inspección a hospitales públicos "*un plan de inspección de oficio en el sector hospitalario, que continuó en 1996, con el objetivo principal de conocer la situación actual hospitalaria respecto a la forma en la que son tratados los datos en cuanto a Seguridad, Privacidad y Confidencialidad, así como estudiar la medida en la que se garantizan los derechos de los afectados. En relación con el mencionado plan de inspección se realizaron inspecciones en varios hospitales dependientes del INSALUD*.. Producto de ello se generó un informe, cuyas conclusiones son la falta de mentalización sobre el problema de adaptación, no se guarda debidamente la confidencialidad, no te toman las precauciones necesarias en las cesiones dentro y fuera de las fronteras de nuestro país, no se informa correctamente a los afectados sobre el tratamiento de sus datos ni sobre el ejercicio de sus derechos, los ficheros no se encuentran correctamente declarados, no existen un plan de seguridad de forma generalizada.

Pero años más tarde, la AEPD lleva a cabo un Plan de Inspección a hospitales públicos, de acuerdo con el INSALUD, en el que se determina que "*como consecuencia de este informe, en septiembre de 1997, el INSALUD ha distribuido una Circular a los Servicios Centrales, Direcciones Provinciales, Gerencias y Centros*

[152] Ibídem. Pág. 23.

Asistenciales, en la que se indica que para dar cumplimiento a las recomendaciones de la Agencia, y adecuar de forma gradual y precisa los sistemas de información a las obligaciones que establece la Ley 5/1992, la Presidencia Ejecutiva, con el informe favorable de la Asesoría Jurídica, dicta instrucciones relativas a: Ámbito de aplicación, Controles en el acceso a la información, Administración de Seguridad, Utilización de la información, Controles en los soportes de datos, Seguridad en las comunicaciones, Controles de acceso a locales, Declaración de ficheros automatizados, Derecho de información del paciente, Cesión y transferencia internacional de datos, Relaciones con empresas externas, Desarrollo de un Plan de Seguridad". Medidas para intentar paliar las deficiencias detectadas.

Más recientemente, en 2010, la AEPD ha solicitado de nuevo informes para la verificación del cumplimiento de la normativa a un número importante de hospitales públicos y privados de todo el país. El análisis de dichos informes arroja unas garantías reforzadas en lo relativo al consentimiento, a la comisión de infracciones muy graves, así como a la implantación de las medidas de seguridad de nivel alto. Por otro lado los casos de vulneración más destacados, se refieren al intercambio de datos a través de redes, a la pérdida de historias clínicas mediante su automatización, al abandono de datos de salud en la vía pública y, al almacenamiento de documentación clínica en áreas no restringidas. Con esta numeración se podría decir que están al cincuenta por ciento de incumplimiento los datos informatizados y los manuales, ya que las dos primeras infracciones se podrían referir a estos últimos, y las dos siguientes a los primeros.

El estudio ha sido realizado en 605 centros hospitalarios del catálogo nacional de hospitales, 313 de ellos privados y, 292 públicos, de los que contestaron 562, es decir un 92% del total. A dichos centros les fue requerida la siguiente información; por un lado las medidas de seguridad que tenían implantadas así como las obligaciones que habían sido comunicadas al personal, el control y

registro de los accesos, los procesos de comunicación de datos, como también los de gestión de incidencias, gestión de soportes y documentos, copias de seguridad y documentación existente en soporte papel. Igualmente les fueron solicitadas las auditorías obligatorias de las medidas de seguridad, así como la acreditación sobre el deber de informar y la atención del ejercicio de derechos. Finalmente se les requirió información sobre la inscripción de los ficheros en el Registro General de Protección de Datos y sobre la contratación de servicios que implicasen el tratamiento de datos personales.

Del desgranado de los citados informes, se ve con claridad que, en general, cumplen más los centros privados que los públicos, quizás por la amenaza permanente de la sanción económica a la que pueden ser sometidos los centros privados y no los públicos; el artículo 46.1 de la LOPD establece estos privilegios *"…para que cesen o se corrijan los efectos de la infracción…"*, e incluso establece el punto 2 de este mismo artículo que *"el Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran…"*. Nada que ver con lo que establece el artículo 45 para el resto de responsables de ficheros que no sean administraciones públicas, llegando a alcanzar hasta los 600.000€ de multa. Podría entenderse la parte económica de que el estado no se sancione a sí mismo, pero lo que no tiene lógica es que tratándose de datos médicos tratados en centros públicos o privados, la presión de la multa pueda llevar a cumplir más las medidas en unos que en los otros, desde luego eso podría parecer al ver la diferencia de porcentajes en el cumplimiento de la normativa que superan con creces los centros privados respecto de los públicos.

Pero, debido al interés del estudio, merece la pena ir viendo uno por uno los porcentajes de cumplimiento de los centros públicos y privados sobre cada uno de los puntos analizados.

Respecto de los documentos de seguridad en las entidades sanitarias, los centros privados tiene un 98% de cumplimiento, frente al 83% de los centros públicos, encontrándose las mayores deficiencias en la implantación de las medidas para la custodia de la documentación, la información a los interesados y atención al ejercicio de derechos, frente al elevado cumplimiento del deber de inscripción de los ficheros en el RGPD. En porcentajes también muy elevados, tanto en el sector público como en el privado, se encuentran la inscripción de ficheros, con un 99% para el sector público y un 89% para el privado, así como el mantenimiento y actualización de los registros, con un 96% para el sector público y un 80% para el privado. También con un 96% en el sector privado se encuentran los procedimientos para atender efectivamente le ejercicio de derechos ARCO, frente al 84% de los públicos.

En valores algo menos altos para ambos sectores, estaría por un lado la información al personal de limpieza de garantizar la confidencialidad de la información a la que puedan acceder en el desarrollo de su trabajo, con un 94% de cumplimiento para el sector privado y un 74% para el público, por otro las medidas que eviten la sustracción, pérdida y acceso indebido a la información, que cumplen en un 85% los centros privados y en un 70% los públicos, y en tercer lugar la disposición de carteles informativos sobre el derecho a la protección de datos, en un 80% los centros privados y en un 64% los públicos. Habría otros valores igualmente aceptables para el sector privado, y no tanto para el público, relativos a los mecanismos de apertura de los dispositivos que custodian la información, en los que se encuentra el 65% de cumplimiento de los centros públicos, frente al 89,4% de los centros privados, al igual que la conservación de los registros de los accesos realizados en los datos que requieren esta medida, con un 79% para el sector privado y un 58% para el público; también se encontraría en este grupo la conservación de los registros de los accesos realizados a la información, con un 63,4% de cumplimiento para el sector público y

un 85,6% para el privado, al igual que ocurre con la conservación de esos registros de accesos realizados por un periodo mínimo de dos años, lo cual cumplen los centros públicos en un 58% y en un 79% los privados.

Y con valores mucho más dispares, pero más elevados igualmente en el sector privado, están por un lado la introducción de la cláusula informativa en los documentos de recogida de datos que cumplen el 45% de los centros públicos y el 94,5 % de los centros privados; por otro lado la realización de la auditoría bianual, la cumplen el 33% de los centro públicos y el 88% de los centros privados; y en último lugar, el control de la utilización de los datos de acuerdo a su finalidad, que cumplen el 65% de los centros públicos y el 25% de los privados. Curiosamente este último punto, clave en la protección de datos personales es el menos cumplido de todos en ambos sectores. De hecho, es uno de los principios relativos a la calidad de los datos, que marca la LOPD en su artículo 4.2, en el que establece que "Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos...", puntualizando posteriormente que "…no se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos". De este privilegio se hablará también más adelante respecto de la conservación disociada de los datos.

Se ha observado también en los últimos años, un aumento de solicitud de tutela por considerar que la historia clínica se proporcionaba de forma incompleta, así como por denegar el derecho de acceso a familiares de fallecidos. Así mismo, hay un porcentaje alto, del 86% de centros, tanto públicos como privados, que externalizan los servicios respetando el artículo12 LOPD; recordemos que el punto 2 de dicho precepto dice literalmente que: *"La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido,*

estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas…". Estableciendo igualmente que *"…en el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar".* Y dicho artículo 9.1 fija que tanto el responsable del fichero como el encargado del tratamiento *"…deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".* Es decir, que ambos, deben valorar las circunstancias que van a incidir sobre los datos, para tomar las medidas oportunas que mantengan a los datos a salvo; esto pasará por adaptar tanto recursos físicos como lógicos que reduzcan al mínimo la vulnerabilidad de los datos.

El mayor cumplimiento, por parte del sector privado, de todos los extremos examinados, puede deberse en gran parte a que este si paga multas cuando el público no lo hace. De todos modos, en este aspecto se ha tendido a aplicar en los últimos años un criterio reductor, tanto en las sanciones como en los criterios para aplicarlas, recurriéndose en primera instancia y en determinadas circunstancias al apercibimiento. Así se produce en este sentido un acercamiento entre ambos sectores, público y privado.

En el Año 2007 publica el periódico ABC, en relación a la utilización de historiales clínicos para verificar el uso del catalán a nivel autonómico, que: *"Con todo, desde la ACPD se precisó que expedientes no conllevarán ninguna <<sanción económica>> para*

los infractores, sino unas <<recomendaciones de obligado cumplimiento>> para que este hecho no vuelva a suceder. Y es que la Ley de Protección de Datos no contempla multas cuando el infractor es del sector público, para no perjudicar las arcas del públicas"[153].

Y del mismo modo lo adelantaba Europa Press un día antes asegurando que: *"Se trata de un plan piloto para auditar algunos hospitales y comprobar si la documentación que se ofrece en estos centros, entre los que se incluyen las historias clínicas, es en catalán y si el personal sanitario utiliza esta lengua"*[154].

Para evitar llegar a estas situaciones, habría que seguir una cadena en la protección de los datos personales, ya que no serviría de nada que el responsable de los ficheros cumpliera con la normativa y el encargado del tratamiento no, o viceversa, ya que en cualquiera de los casos la seguridad de los datos estaría en peligro, y mucho más, si el personal que accede a los datos personales no conociese las medidas al respecto. Esto ya lo he dicho anteriormente cuando he hablado de la importancia que tiene la formación del personal, medida a tomar tanto por responsables como por encargados de tratamiento, pero no viene mal repetirlo, porque se incumple constantemente, y si lo pensamos detenidamente son las personas las que toman la decisión de tirar un informe sin romper a la basura o revelar un secreto médico a un amigo, en cambio, los ordenadores no podrían autodestruir una clave de acceso por sí solos sin la ayuda del hombre. Desde este punto de vista parece que lo primero sería tomar medidas de formación del personal que va a manejar los datos, para que estos pongan en marcha y cumplan el resto de medidas necesarias para la seguridad de los datos. Todo

[153] GUIL, J: "Expedientan a varios hospitales por dar historiales para una encuesta sobre el catalán". ABC, viernes 19 de enero de 2007. España. Pág. 18.

[154] "Protección de datos expedienta a 9 hospitales catalanes por dar historiales para estudiar el uso del catalán". Europa Press, 18 de enero de 2007.

esto se abordará más detenidamente en el apartado de formación del personal correspondiente.

No quiero apartarme del artículo 12 de la LOPD sin citar su punto 3, el cual dice que *"una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".* Porque tan importante es mantener la seguridad de los datos durante, como una vez concluida la prestación del servicio; recordemos una vez más que hay que mantener esa permanencia en la seguridad de los datos, no me cansaré de decirlo, especialmente tratándose de datos médicos, porque esa información sobre la salud de los pacientes, dejará huella para siempre su el historial médico, en cambio otro tipo de datos, como pueda ser un domicilio o ciudad de residencia, cambian sin más sin que ello trascienda más allá de la mera rectificación. De modo que, en mi opinión, sí es muy importante el después para los datos relativos a la salud, en especial, ya que permanecerán ligados para siempre a su titular, no como otros de los que cada individuo puede desligarse voluntariamente.

Y como última observación en referencia al estudio sobre la verificación del cumplimiento de la normativa a un número importante de hospitales públicos y privados, elaborado por la AEPD, existe un bajo porcentaje de centros que disocian los datos en el caso de que exista un encargo de prestación de servicios, requisito recomendable, aunque no obligatorio, según la normativa de protección de datos, para el caso de que los datos sean tratados por cuenta de terceros.

Cabe reseñar aquí, que en el año 2009, el periódico El País, publicaba lo siguiente respecto a este mismo tema: *"El reputado sistema de trasplantes de órganos de la sanidad pública española- cuyos pilares son la igualdad, la gratuidad y la confidencialidad*

garantizada a donante y receptor- ha sufrido la mayor fuga de información en sus más de 20 años de historia. Un listado con datos personales de todos los enfermos que recibieron un corazón en el hospital Clinic de Barcelona entre 1998 (cuando comenzó a realizar estas operaciones) hasta marzo de 2007 fueron encontrados en la madrugada de ayer tirados en la acera de una calle, a unos 300 metros del hospital, según comprobó El País"[155].

Y poco antes también, un periódico local publicaba que: *"La Agencia de Protección de Datos ha iniciado un procedimiento de declaración de infracción al Hospital General de Segovia al considerar que podría haber vulnerado el deber de guardar secreto sobre los datos de sus pacientes. El ente ha investigado los sucesos hechos públicos por El Adelantado de Segovia en sus páginas los días 26 y 27 de octubre de 2006, que mostraban la presencia de documentos e informes de pacientes del hospital en un patio abierto del complejo sanitario, expuestos al aire y tirados junto a muebles viejos. En los documentos constaban datos identificativos de los pacientes, nombre y apellidos o edad, , así como fecha de ingreso, servicio o unidad que les ha atendido, medicación aplicada, pruebas o exploraciones realizadas…"*[156].

No obstante, podría pensarse que si lo que se persigue es que los datos de salud sean exclusivamente tratados por el personal especializado imprescindible, no se estaría cumpliendo esta máxima externalizando un servicio con el consecuente tratamiento por personal ajeno al centro sanitario; ya el artículo 9.3 de la LOPD fija que: *"Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo*

[155] GÜEL; Oriol: "*Hallados en la calle los datos de 173 trasplantados en un hospital catalán*". El País, martes 3 de noviembre de 2009, pág. 30, vida & artes, Barcelona

[156] BRAVO,P.: "*La Agencia de Protección de Datos abre proceso sancionador al Hospital General*". El Adelantado de Segovia, miércoles 22 de octubre de 2008, Segovia. Pág.9.

7 de esta Ley". De hecho, cuando el RLOPD habla de las medidas de nivel alto, establece en su artículo 113.1 que: *"El acceso a la documentación se limitará exclusivamente al personal autorizado…"* fijando en el punto segundo que *"se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios".* Y matizando finalmente en el punto tercero que *"el acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad".* De este modo, podría haber un descontrol en las personas que van a tratar los datos personales, ya que al externalizar un servicio, no sabemos quién accederá a la información en cada momento y, además, casi con total seguridad, no será personal sanitario. Lo centros médicos requieren de una gran inversión de trabajo y capital en llevar a cabo seccionamientos, permisos y limitaciones en el acceso a la información de los pacientes, así como en formar a su distinto personal en cuanto a tratamiento de datos personales en sus distintos departamentos, administrativo, de enfermería, médico, etc. De hecho, no accede a la misma información un médico que una secretaria o que una enfermera; toda esta inversión que se hace se estaría perdiendo al externalizar el servicio.

Pero el control de acceso a los datos opera para todos los niveles, no solo para los datos de nivel alto, ya que el artículo 91 RLOPD establece en su punto 1 que: *"Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones".* En su punto segundo recoge además que *"el responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos".* Además en el punto tercero establece que *"el responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados".* Obviamente estos procedimientos no

pueden ser realizados por cualquiera, ya que según establece este artículo en su cuarto punto: *"Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero".* De modo que el responsable del fichero, será quien reparta las funciones que corresponden a cada cual a través de personas directamente designadas por él, estableciendo en el documento de seguridad ese reparto de funciones y medidas, del que deberá dar traslado al encargado del tratamiento, dejando constancia de estas instrucciones en el contrato de prestación de servicios mencionado anteriormente. Además el RLOPD también contempla este caso, ya que regula en el punto 5 del artículo que nos ocupa *que "en caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio".* No obstante, todo esto se evitaría sin duda con la disociación de los datos.

Existe además de los dos Planes de Inspección de Oficio sobre el cumplimiento de la normativa de protección de datos en el sector hospitalario realizados en el del año 1997 y en el del año 2010, un Plan de Inspección de Oficio sobre tratamiento de datos personales en laboratorios hospitalarios del año 2004 que arroja conclusiones y recomendaciones en esta materia. Las conclusiones del análisis realizado versan sobre la seguridad de los datos (artículo 9 de la LOPD), el deber de secreto (Artículo 10 de la LOPD), el acceso a los datos por cuenta de terceros (Artículo 12 de la LOPD), los derechos de las personas: acceso, rectificación, cancelación y oposición (Artículos 15 y 16 de la LOPD) y sobre la creación, modificación o supresión de ficheros en relación a la notificación e inscripción registral (Artículos 20, 25 y 26 de la LOPD). Y sobre estas mismas materias versan las recomendaciones hechas por la AEPD los laboratorios hospitalarios inspeccionados que *"…tienen dependencia*

funcional y orgánica de la Gerencia del hospital al cual pertenecen, que, a su vez, como hospitales públicos que son, dependen de sus respectivas Consejerías de Salud". Y *"las conclusiones que se recogen en el presente documento se refieren fundamentalmente a aspectos relacionados con la seguridad de los datos tratados por los laboratorios, datos que se refieren a la salud de los afectados y que son considerados especialmente protegidos por la LOPD, por lo que deben gozar de un nivel mayor de seguridad tal y como especifica el Reglamento de Medidas de Seguridad. También se incluyen aspectos relativos a la confidencialidad de los datos tratados como son el deber de secreto y el acceso a los datos por cuenta de terceros. Finalmente se han incluido aspectos formales relativos a la inscripción de ficheros en el Registro General de Protección de Datos y el ejercicio de los derechos de los afectados".* Especificando el informe que *"dichas conclusiones se han obtenido a partir de las actuaciones realizadas en los laboratorios y entidades inspeccionadas. Sin embargo, debe tenerse en cuenta que los proveedores de estos servicios cuentan con cerca de 900 centros y dependencias sanitarias que utilizan uno o más de los aplicativos inspeccionados, por lo que pueden serles aplicables las presentes conclusiones y recomendaciones".*

Igualmente existen sendos planes de inspección del año 2002, del Hospital Psiquiátrico Penitenciario de Alicante, dependiente del Ministerio de Justicia, y del Hospital General Militar Gómez Hulla. En el caso del primero hay que tener en cuenta, además, que existe regulación específica en esta materia, así *"el RD 190/96, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario, regula el tratamiento de los datos de carácter personal tratados en los centros penitenciarios. Concretamente el artículo 7.1 especifica que "cuando los datos de carácter personal de los reclusos se recojan para el ejercicio de las funciones propias de la Administración Penitenciaria no será preciso el consentimiento del interno afectado, salvo en los relativos a su ideología, religión o creencias*". Se ha podido

comprobar que el Hospital Psiquiátrico Penitenciario no recoge datos relativos a ideología, religión o creencias, ”*las recomendaciones de este estudio se centran en el cumplimiento de los plazos para el ejercicio de derechos, en la observancia del consentimiento del artículo 7 de la LOPD respecto de los datos de salud, en el caso de que no medie incapacidad, en relación a la cesión internacional de datos a países con nivel de protección equiparable, a la obligatoriedad de inscribir todos los ficheros en el RGPD y sobre la adaptación en plazos de las medidas de seguridad exigidas*”.

Por su parte el plan de inspección del Hospital General Militar Gómez Hulla, concluyendo que dicha entidad que *“… dispone de los datos de identificación de todos los usuarios del Instituto Social de las Fuerzas Armadas (ISFAS).”* Que *“Posteriormente y con carácter mensual el ISFAS facilita al Hospital Gómez Hulla las variaciones habidas, mediante un disquete que incluye Tipo, Parentesco, DNI, Afiliación, nombre y apellidos”.* Que *“estos datos se obtienen a partir de la Tarjeta Sanitaria diseñada al efecto para cuya solicitud es necesaria la cumplimentación de un formulario. Los afectados no han sido informados de que sus datos se facilitan al mencionado Hospital”.* Y que *“el resto de los datos de los pacientes son facilitados al Hospital por ellos mismos o son obtenidos como consecuencia de la asistencia sanitaria prestada por dicho centro”.* Ante lo que se realizan recomendaciones relativas a el derecho de información en la recogida de los datos, el consentimiento para el tratamiento de los datos especialmente protegidos, el ejercicio de los derechos ARCO, la cesión de datos, la inscripción de los ficheros en el RGPD, de los contratos con terceras empresas y de la correcta aplicación de las medidas de seguridad correspondientes.

Respecto del acceso a los datos por el distinto tipo de personal y los problemas de unificación de la información que plantean, no es algo nuevo, una parte de la doctrina manifiesta en este sentido que: *“Los primeros intentos de normalización de la historia clínica*

surgieron, el siglo pasado, a comienzos de los años 60. Desde siempre ha existido una marcada tendencia al diseño particular y puntual, por parte de cada médico, de sus propias historias clínicas, elaborándolas como documentos particulares. En un sistema de trabajo en el que los usuarios son múltiples y utilizan un instrumento asistencial común como es la historia clínica, la falta de homogeneización dificultaba enormemente su manejo y la convertía a largo plazo en un elemento inútil. Era necesario, por lo tanto, facilitar el manejo asistencial de una documentación que se estaba complicando por la multiplicidad de usuarios"[157]*.* Pero advierten que *"esta estandarización será positiva, siempre y cuando consiga la premisa de facilitar la utilización de la historia clínica, sin llevar asociadas dificultades en la adopción de los cambios estructurales. Una historia perfectamente normalizada, pero que resulte difícil de manejar para los médicos no ha conseguido su objetivo. Para que esta normalización sea aplicable, ésta debe ser, por lo tanto, compartida y conocida por todos sus usuarios"*[158]*.*

Nuria Terribas insiste a este respecto *"…en la dificultad de acceso compartido a la información escrita de los pacientes, al igual que ocurría con la verbal, con los distintos servicios, siendo necesario, por otro lado, optimizar la gestión sanitaria, lo que sigue diciendo ha dado lugar a la "historia clínica electrónica compartida"*[159]*.*

En cambio, otros casos de comunicación de datos si contempla el tema de la disociación de los mismos, como se ha anunciado anteriormente; así el artículo 11. 6 de la LOPD refleja que *"si la comunicación se efectúa previo procedimiento de disociación, no*

[157] CENTENO SORIANO, Cristina: *"Operaciones administrativas y documentación sanitaria"*. Formación Alcalá, Jaén, 2007. Pág. 114.

[158] Ibídem.

[159] TERRIBAS SALA, Núria: *"Los avances del derecho ante los avances de la medicina. Confidencialidad de los datos sanitarios: de la norma a la práctica médica"*. In Salomé Adroher Biosca- Thomson Aranzadi, 2008. Pags 796-802.

será aplicable lo establecido en los apartados anteriores"; referidos naturalmente a este tema.

El concepto de procedimiento de disociación lo recogen tanto la Ley como el Reglamento de protección de datos, este en su artículo 5.1p) como *"todo tratamiento de datos personales que permita la obtención de datos disociados*", y aquella en el artículo 3f) como *"todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable"*. En cambio la definición de dato disociado solo la hace el RLOPD en el artículo 5.1d) como *"aquél que no permite la identificación de un afectado o interesado"*. Y desde luego parecería más que lógico, enlazando con lo anteriormente dicho sobre la acotación en el conocimiento de los datos de los pacientes y, con las definiciones recién mencionadas, que un dato médico no sea conocido por un tercero ajeno a la prestación de la asistencia sanitaria, aunque sea para la prestación de un servicio que el centro médico, por la razón que sea, ha externalizado en un tercero.

Y se hace necesario aquí definir este concepto de "*tercero*", que el RLOPD hace en su artículo 5.1r) como *"la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento".* Con la lectura de esta definición podríamos decir que un encargado del tratamiento o las personas por este autorizadas no serían terceros, en cambio, la rúbrica del tan comentado artículo 12 de la LOPD, es "*acceso a los datos por cuenta de terceros*", aunque si es cierto que matiza en su punto 1 que *"no se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al*

responsable del tratamiento". Esta cuestión será abordada de forma más exhaustiva en posteriores apartados.

Hay que reseñar aquí, volviendo al tema de la disociación, que el informe jurídico de la AEPD 0207/2008, estima que *"para entender que se efectúa una correcta disociación o anonimización es necesario que se efectúe el correspondiente procedimiento de disociación definido por el artículo 3 f) de la Ley Orgánica…".* Pero además el informe jurídico 0406/2008 de la AEPD que establece en este sentido que *"…para que un procedimiento de disociación pueda ser considerado suficiente a los efectos de la Ley Orgánica 15/1999, será necesario que de la aplicación de dicho procedimiento resulte imposible asociar un determinado dato con un sujeto determinado. En este sentido, las disposiciones internacionales reguladoras de la protección de datos de carácter personal vienen a considerar que el afectado no será determinable cuando su identificación exija un esfuerzo desproporcionado que sea suficiente para disuadir a quien accede al dato de la identificación de la persona a la que el mismo se refiere".*

Y según publica el periódico El País respecto de la disociación, a propósito del proyecto VISC+, que persigue la venta de datos del sistema sanitario catalán: *"La Generalitat encarga anonimizar la información personal de los pacientes", pero así mismo matiza que "El Observatorio de Bioética y Derecho de la Universidad de Barcelona advirtió en un informe a principios de 2015, de que las leyes de protección de datos que permiten su uso tras haber sido despersonalizados se han quedado "obsoletas" antes los avances tecnológicos: "Se reconoce hoy que la anonimización ya no garantiza la privacidad de los datos personales, pues técnicas informáticas permiten conocer datos anonimizados con el individuo al que pertenecen", sostenía el estudio"*[160].

[160] G, SEVILLANO, Elena: "*La ley no contempla el uso de datos con fines comerciales*". El País, jueves 2 de abril de 2015. Pág 34.

Existen también otros casos en los que la legislación contempla la disociación de datos, concretamente lo establece el 8.6 RLOPD para cuando haya concluido la finalidad con la que fueron recogidos y quieran conservarse por otros motivos, así *"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".* Y, respetando siempre la obligación de bloqueo establecida por la LOPD en el artículo 16.3 a propósito del ejercicio del derecho de cancelación, y matiza el reglamento también en este aspecto en el penúltimo párrafo del artículo arriba citado, que *"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".* Y recogiendo finalmente en el último párrafo de este mismo artículo que *"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".*

De modo que respecto de la conservación de los datos, ampara la ley a que se haga respetando unos principios que garanticen la calidad de los mismos y, en concreto, en referencia a su utilización con fines históricos, estadísticos o científicos, no considerándose estas finalidades incompatibles con aquellas para las que fueron recogidos, de acuerdo al artículo 4.2 de la LOPD, que establece que *"los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos".*

A este respecto, conviene apuntar aquí lo establecido por el artículo 28.2 del DCM, respecto de la disociación de los datos de los pacientes *“el médico procurará que en la presentación pública de documentación médica en cualquier formato, no figure ningún dato que facilite la identificación del paciente”.* Y en este mismo sentido el 28.3 recoge que *“está permitida la presentación de casos médicos que hayan sido fotografiados o filmados para fines docentes o de divulgación científica habiendo obtenido la autorización explícita para ello o conservando el anonimato”.*

Ahora ya, fuera de este ampliamente comentado estudio de la AEPD, y desde una perspectiva más general, con un simple vistazo al índice de la LOPD, nos damos cuenta de que los datos especialmente protegidos y, en especial los de salud, reciben un trato privilegiado en dicha norma; este tipo de datos se encuentran clasificados en el artículo 7 de la LOPD. Según el artículo 7.3 de la LOPD, *"los datos relativos a la salud de las personas, al igual que el origen racial o la vida sexual, solo podrán recogerse, tratarse y cederse con el consentimiento expreso del afectado o por disposición legal. Pero en cambio se exige además un requisito específico -que se haga por escrito -, para otro tipo de datos especialmente protegidos, como son los de ideología, afiliación sindical, religión y creencias; esto se debe sin duda al especial tratamiento que les da el artículo16.2 CE. En la realidad, cualquiera de los datos protegidos, tanto los que exigen el consentimiento escrito, como los que no, podrían figurar en un informe médico y, en cambio, se requieren diferentes formas para recabarlo, de modo que lo mejor sería unificar y tomar la más exigente, en forma expresa y por escrito para todos ellos. Además, si no es por escrito, está*

también el tema de la carga de la prueba, que recae en el responsable del fichero"[161].

Pero el privilegio que le quita la ley por un lado a los datos de salud, al no exigir el mismo tipo de consentimiento para ser recogidos, que para otro tipo de datos especialmente protegidos, según se acaba de exponer, se lo concede por otro lado, dedicándoles en primicia un artículo a los datos relativos a la salud, el artículo 8 que establece que *"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".*

En relación a la necesidad de consentimiento expreso del afectado para el tratamiento de los datos de salud, conviene aquí comentar que la sentencia de la Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 02-03-2006 referida al absentismo laboral, establece en sus fundamentos de derecho que *"la presente resolución impugnada razona que la parte recurrente, "ENTIDAD A", no ha acreditado la existencia del consentimiento expreso e informado de forma completa de los trabajadores de la Empresa "ENTIDAD B" (en adelante "ENTIDAD B") que son visitados por médicos de esa sociedad. Ciertamente, cuando actúan los médicos de la entidad demandante se identifican al paciente, les informa del objeto de su visita, que estribará en la corrección del diagnóstico, en efectuar, en su caso, diagnóstico alternativo, en valorar si es correcto o no el tratamiento, en valorar las exploraciones complementarias para agilizarlas y analizar la posible relación con su puesto de trabajo. Sin embargo, recalca la*

[161] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

resolución recurrida, no aparece en la documentación aportada por esa Sociedad que se informe al afectado de la segunda de las funciones que ha de prestar "ENTIDAD A" e incluidas en el contrato de prestación de servicio que ha suscrito con Transportes de Barcelona SA: servicio médico prestado por "ENTIDAD A" para habilitar la reconducción individual por "ENTIDAD B" mediante el ejercicio de la facultad de control del absentismo laboral que asiste a la Sociedad anónima respecto de sus trabajadores conforme al artículo 20 del Estatuto de los Trabajadores. En consecuencia, resalta el acto administrativo, que en la leyenda incluida "en el justificante de visita médica" que se presenta ante cada empleado en el momento de la visita, y sobre la que ha de basarse la información relativa a la finalidad del tratamiento que aquel consiente, no informa de modo expreso, preciso e inequívoco de que una de las finalidades del tratamiento está relacionada con el control del absentismo laboral que constituye, al menos, una parte del servicio que "ENTIDAD A" ha concertado con "ENTIDAD B", por lo que no ha podido obtener el consentimiento expreso para dicho tratamiento"[162]*.* Se comprueba una vez más, que en la práctica real, en muchas ocasiones se tratan datos médicos sin el consentimiento expreso del paciente.

Este es un tema que me interesa sobremanera, ya que, cuando vio la luz el RLOPD, era el momento de haber establecido el requisito de la escritura en el consentimiento para el tratamiento de los datos de salud, ya que la LOPD solo exige el consentimiento expreso y por escrito para los datos de ideología, afiliación, sindical, religión y creencias, y no así para los relativos al origen racial, salud o vida sexual de las personas, todos ellos clasificados como datos especialmente protegidos. Pero no se hizo esta corrección en reglamento de desarrollo de la LOPD, de modo que la brecha de discriminación entre unos datos y otros sigue abierta.

[162] Audiencia Nacional. Sentencia de 02-03-2006. Sala de lo Contencioso-Administrativo, sección primera. Tratamiento de datos de salud. Control del absentismo laboral.

En este punto es también interesante saber que *"…las leyes sanitarias establecen la información verbal como norma general, para el trámite de la recogida del consentimiento, requiriéndose solo por escrito en determinados casos, como en las intervenciones quirúrgicas. Una vez más podrían chocar ambas normas. En cambio, para el caso de la revocación del consentimiento se exige que se haga por escrito, lo cual no concuerda con la forma en que se obtuvo dicho consentimiento, en la mayoría de los casos"*[163].

Dicho esto, el artículo 7.6 de la LOPD establece, según se verá ampliamente en el apartado correspondiente, que los datos especialmente protegidos podrán tratarse cuando *"… 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 dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto".*

Resulta curioso que la propia LOPD requiera la condición de que el personal que maneja los datos de salud esté sujeto a guardar un secreto profesional o deber equivalente, cuando esta misma norma establece en su artículo 10, sean los datos especialmente protegidos o no, el deber de secreto para quienes intervengan en el tratamiento de los datos, incluso cuando este haya acabado. Tomémoslo como un plus debido a la sensibilidad de los datos, aunque establecido una vez el deber, establecido para siempre. Lo que ocurre es que la legislación de protección de datos tenía que establecer el requisito del deber de secreto por su parte, porque sí no, el resto de datos distintos de los de salud, para los que la legislación sanitaria ya establecía el deber de secreto, se quedarían sin él. Es justo que el deber de secreto se guarde de todos los datos,

[163] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs. 29 a 36.

y no solo de los de salud, porque estos gozan además de un tratamiento especial en la normativa de protección de datos debido a su sensibilidad. Y por otra parte es obvio que en un centro sanitario los datos no los maneja solamente personal médico, sino también administrativo, técnico, etc., como ya se ha referido anteriormente.

Es claro que el interés de la medicina se inclina por los datos, ya que estos son la herramienta imprescindible para poder llevarla a cabo; pero lo cierto es que hay que apostar también por su protección y, encontrar un equilibrio en la utilización de la información, que no haga que su mal uso se vuelva en contra del propio paciente. Pensemos que esa información que tan importante es en el proceso médico, está más aislada de sentimientos para el médico que para el paciente. Es decir, que cierta información sobre un paciente, puede no impresionarle a un profesional sanitario, pero sí afectar al paciente al que se refiere, si no es tratada con el debido respeto, de acuerdo a los deseos del paciente. Esta información no debe trascender más allá de lo que su titular autorice y, por supuesto, de lo que las leyes establezcan.

III.3. BASES DE DATOS MÉDICAS E HISTORIAL CLÍNICO.

III.3.a. Descripción de conceptos: dato médico e historia clínica:

Desde mi perspectiva personal y profesional, e intentando no contaminarme de lo establecido en otros textos y, anticipadamente al estudio de dichos conceptos, definir dato médico como la información relativa a la salud, obtenida a través de parámetros identificativos, físicos, de comportamiento o familiares, relativos a una persona. Y la historia clínica sería un conjunto de datos de distinta naturaleza, almacenados en cualquier soporte, referidos a una persona y, puestos en interconexión, con el fin de llegar a un diagnóstico para el tratamiento del paciente.

Podría decirse que la historia clínica no podría existir sin los datos médicos, y un dato médico aislado tampoco tendría demasiado valor si no se pone en interconexión con otros datos médicos, en un informe que pasará a formar parte de la historia clínica del paciente. De modo que ambos se necesitan mutuamente para poder albergar un valor.

Sobre las definiciones de estos conceptos, y de la incorporación de la información a la historia clínica de los pacientes, hablaré a continuación.

En primer lugar hay definiciones próximas a estos conceptos que es necesario analizar.

Respecto a la definición de dato médico, la LOPD no la contempla, exclusivamente se refiere en el artículo 3a) al dato de carácter personal como *"cualquier información concerniente a personas físicas, identificadas o identificables"*. Si regula, en cambio, los datos especialmente protegidos en su artículo 7 y dedica expresamente un artículo, el 8, a los datos relativos a la salud, en el que establece que *"…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".*

Este vacío en la definición de dato médico, viene a cubrirlo el reglamento de desarrollo de la citada ley, que define los datos de carácter personal relacionados con la salud en el artículo 5.1g), como *"las informaciones concernientes a la salud pasada, presente y futura, física o mental de un individuo…"*, y sigue considerando que *"…en particular se consideran datos relacionados con la salud de las personas, los referidos a su porcentaje de discapacidad y a su información genética".* Curiosa definición en varios aspectos; en primer lugar, habría que valorar la si la salud futura, se refiere a un

dato futuro de salud, lo cual cabría discutir, ya que el dato futuro no existe y por tanto, no sería dato; y en segundo lugar, la referencia concreta a los datos genéticos o de minusvalía. En estos últimos supuestos parece adivinarse una llamada de atención a falta de diligencia ante casos concretos en materia de protección de datos médicos, ya que se podrían haber enumerado otros datos igualmente importantes.

La ya citada Ley del paciente, define tanto documentación clínica, como historia clínica e información clínica, en el artículo 3 de su texto. La documentación clínica, consta como *"el soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial".* Pero no define lo que es un dato asistencial, lo que podríamos equiparar a dato médico. La información clínica es *"todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla".* Parece que esta definición quiere referirse al dato médico, pero difiere de la de dato de carácter personal relacionado con la salud del RLOPD, que recoge que *"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".* Y difieren en que esta última, no solo se refiere al estado físico, sino también al mental, pero si hace diferencia, entre el estado físico y la salud, que al parecer, son cosas distintas; quizás la redacción correcta sería "*estado físico y salud mental*". En cambio, parece que la definición de información clínica, si quiere preocuparse del cuidado de los datos, es decir, de proteger los datos personales.

Y por fin, define la historia clínica como *"el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un*

paciente a lo largo del proceso asistencial". Pero esta norma parece duplicar este concepto, y dedica además su artículo 14.1 exclusivamente a la definición de archivo de la historia clínica, en el que dice que *"la historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro".* Nos quedamos con la segunda por ser más completa. Y sigue diciendo el artículo 14.2, que *"cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información".* Este punto hace clara referencia al artículo 9.1 de la LOPD comentado anteriormente.

La propia AEPD en su informe jurídico 106/2008, establece que: *"Es conveniente, sin embargo, perfilar una definición válida, aunque no absoluta, de lo que deba entenderse por "historia clínica". Se entiende como tal el conjunto de datos sanitarios referentes a una determinada persona física, agrupados en un único expediente con vocación de uniformidad. En dicho "historial" podrán contenerse desde el cuadro médico o la sintomatología con la que acude una persona a un centro sanitario, hasta los episodios asistenciales a los que ha sido sometido, pasando por el tratamiento y diagnóstico del paciente".* No obstante, este informe establece como premisa que *"en primer lugar es preciso señalar que las cuestiones relativas al concepto de "historial clínico", su régimen de acceso, propiedad, contenido, conservación, custodia, y el deber de secreto en relación con el mismo, se encuentran recogidas, con carácter general, en la Ley 41/2002, de 14 noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica".*

Bien, parece a la vista de estas definiciones, que un dato, una valoración y una información son cosas distintas, mientras que la LOPD define en su artículo 3 a) como dato de carácter personal, *"cualquier información concerniente a personas físicas identificadas o identificables".* Aunque desde mi punto de vista bien podría ser un dato algo cierto, mientras que una valoración pudiera ser algo subjetivo, y una información una teoría o práctica asentada sobre un caso; por ejemplo, podría darse el dato de la fiebre, valorar que proviene de un dolor de muelas, y asociar la información de que mejorará con un analgésico. No obstante, según la LOPD, queda claro que un dato es cualquier tipo de información.

La RAE define información en primera instancia como "*Acción y efecto de informar*", de lo cual deducimos que se trata de un hecho, es decir, hay que hacerlo, no sobreentenderlo.

Un sector doctrinal, aporta su propia definición de historia clínica al afirma *"…que se entiende como historia clínica el relato escrito de la enfermedad del paciente, y por tanto, el documento en el que dicho relato queda recogido con el fin de ser guardado o conservado'. O en otras palabras, el instrumento donde se incorpora cronológicamente toda la información relativa a la práctica clínica y asistencial de un paciente"*[164]*.*

Por su parte, la Ley General de Sanidad no define ni dato médico, ni historia clínica.

Si nos vamos de nuevo al diccionario de la Real Academia Española a buscar estos conceptos, encontramos como definición de dato, el *"antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho"*, a lo que podría asimilarse, que el dato médico es necesario para llegar

[164] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores): *"La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural".* Tirant Lo Blanch, Valencia, 2014. Pág. 332.

a un diagnóstico o historia, de modo que, el dato sería el origen de la historia, que contendría muchos más, relacionados entre sí, para poder llegar a una deducción o juicio médico. También define el diccionario dato como "*documento, testimonio o fundamento*", encontrando aquí la contradicción, de que si un dato es un documento, en el estudio que viene al caso, el dato médico sería la historia clínica, si entendemos tal como un documento, pero en cambio son cosas distintas. Las definiciones de testimonio o fundamento tampoco se podrían acoplar, ya que el dato no es solo un testimonio, sino también una comprobación, y desde luego, nunca sería un fundamento por sí mismo, sino siempre asociado a un hecho o información. Y por último, define el diccionario como dato, la *"información dispuesta de manera adecuada para su tratamiento por un ordenador"*, lo cual está obsoleto, porque como bien dice la LOPD en su artículo 2.1 dice *"la presente LO será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento…"* y sigue diciendo el artículo 5.1t del RLOPD que, tratamiento de datos es *"cualquier operación o procedimiento técnico, sea o no automatizado…".* Por otra parte, esta definición de dato, también recuerda, que el artículo 3 de la LOPD define como fichero *"todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*". Parecen también estar de acuerdo ley y diccionario en este punto, ya que una manera adecuada de tratar los datos, parece que sea mediante conjuntos organizados.

A este respecto, una parte de la doctrina define como almacenamiento de la misma *"…la operación consistente en guardarla en las mejores condiciones de conservación y utilización"*[165]*.* Especificando a continuación que *"todo almacenamiento de la HC constituye un FONDO DOCUMENTAL*

[165] CURRIEL HERRERO, J y ESTÉVEZ LUCAS, J: "*Manual para la gestión sanitaria y de la historia clínica hospitalaria*", Editores Médicos, Madrid, 2000. Pág.84.

que permite realizar formación continuada, investigar en ciencias de la salud o servir como memoria histórica de los procesos asistenciales ocurridos a un paciente"[166]*.*

Otro sector doctrinal define en cambio historia clínica como "…el conjunto de datos sanitarios referentes a una determinada persona física, agrupados en un único expediente"[167].

Aberasturi Gorriño por su parte establece respecto al dato sanitario que *"el dato sanitario es antes de nada dato de carácter personal, por lo que resulta imprescindible realizar una aproximación al significado de esta expresión, Desde la UE, el Consejo de Europa, el Estado y las distintas Comunidades Autónomas que han regulado la protección del derecho a la autodeterminación informativa, se ha entendido que es dato de carácter personal «cualquier información relativa a una persona física identificada o identificable». Las normas han optado por dar una definición general del concepto, dejando a un lado la posibilidad de hacer la delimitación a través de un sistema casuístico. De una primera lectura de dicha definición se podría concluir que se trata de una delimitación acertada, ya que fija el contorno de la realidad «dato de carácter personal» de forma en principio reconocible. Sin embargo, en la práctica, a la hora de identificar esos datos en los supuestos concretos, surgen los problemas debido a la indeterminación de varios de los términos empleados en la definición. Es evidente que se trata de una definición excepcionalmente amplia. A pesar de que cierta amplitud en la misma puede ser positiva en cuanto posibilita su adecuación a nuevas circunstancias (más aún en el caso de las Nuevas Tecnologías en el que el avance es rápido y constante), la indeterminación resulta un problema en la práctica si no se*

[166] Ibídem.

[167] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso. "*La protección de datos personales en el ámbito sanitario*", Editorial Aranzadi, Navarra 2002. Pág. 66.

establecen criterios mínimamente estrictos y claros que posibiliten la identificación del concepto en los casos particulares"[168]*.*

Define también el diccionario como base de datos informáticos, *"el conjunto de datos organizado de tal modo que permita obtener con rapidez diversos tipos de información"*, lo que parece asimilarse también a la definición de fichero hecha anteriormente, aunque la AEPD no se refiere a bases de datos sino a ficheros.

Las definiciones de la Real Academia Española relativas al procesador de datos se encuentran asociadas a la informática y la tecnología, así se encuentran las siguientes definiciones: "*programa o aparato para el procesamiento de datos*", de lo cual deduzco que procesamiento puede asimilarse a tratamiento, y de lo que se desprende, que esta es otra definición obsoleta de acuerdo a la actual normativa en materia de protección de datos, ya que el tratamiento puede hacerse de forma manual como automatizada. En cambio, la definición de procesamiento de datos, es decir, la acción de procesar los datos, deja una puerta abierta en este sentido, ya que se define como la "*aplicación sistemática de una serie de operaciones sobre un conjunto de datos, generalmente por medio de máquinas, para explotar la información que estos representan*". Según esta última definición, generalmente el procesamiento de datos e hace por medio de máquinas, pero pensemos en el gran número de profesionales que manejan esas máquinas y dan sentido a la información que almacenan.

Así mismo, se encuentra en el diccionario de la RAE la definición de protección de datos, como el *"sistema legal que garantiza la confidencialidad de los datos personales en poder de las administraciones públicas u otras organizaciones"*; nombrando a continuación a la AEPD. Es decir, que ateniéndonos a esta

[168] ABERASTURI GORRIÑO, Unai, *"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 49.

definición, los centros sanitarios, tanto públicos, como privados, tendrían que garantizar la confidencialidad de la información que obre en su poder. Es una buena base, pero habría que matizar muchos más conceptos además de la confidencialidad, ya que esta se referiría solo a uno de los artículos de la LOPD. Este es uno de los objetos de este estudio, revisar las medidas que habría que tomar en los centros sanitarios, y analizar las posibles carencias que puedan producirse, en materia de protección de datos, habida cuenta de la situación real en nuestro país.

Una parte de la doctrina ha manifestado que *"del concepto médico de la historia clínica obtenemos su finalidad. La historia Clínica tiene como único objetivo recoger datos del estado de salud del paciente y con el relacionados (familiares, sociales, laborales, hábitos y costumbres…) con el objeto de facilitar la asistencia sanitaria del paciente"*[169]*.* Y especifica esta parte de la doctrina citando a otro autor que *"en el momento que la historia clínica se constituye como derecho del paciente, se convierte automáticamente en el deber del médico de realizarla de forma obligada (De Lorenzo,J., y cols.,1997)"*[170]. Y continúa diciendo este sector doctrinal *"además debe ser considerada como un derecho del médico, así como lo señala el art.15.1 del Código Deontológico: el acto médico quedará registrado en la correspondiente historia clínica, el médico tiene el deber y también el derecho de redactarla"*[171]*.*

En la Recomendación nº R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre Protección de Datos Médicos (R97- Recomendación sobre protección de datos médicos), *"la expresión "datos médicos" se refiere a todos los datos personales relativos a la salud de un*

[169] CRIADO DEL RÍO, María Teresa y SEOANE PRADO, Javier: *"Aspectos médico-legales de la historia clínica"*. Colex, Madrid, 1999. Pág.25.

[170] Ibídem.Pág. 31.

[171] Ibídem.

individuo. Se refiere también a los datos que tengan una clara y estrecha relación con la salud y los datos genéticos", definida en el punto primero de su apéndice, donde además de esta abierta definición, encontramos a continuación, en referencia a los datos genéticos, que según acabamos de ver contiene también la definición de datos de carácter personal relacionado con la salud del RLOPD, que *"la expresión "datos genéticos" se refiere a todos los datos, cualquiera que sea su clase, relativos a las características hereditarias de un individuo o al patrón hereditario de tales características dentro de un grupo de individuos emparentados. También se refiere a todos los datos sobre cualquier información genética que el individuo porte (genes) y a los datos de la línea genética relativos a cualquier aspecto de la salud o la enfermedad, ya se presente con características identificables o no. La línea genética es la línea constituida por similaridades genéticas resultantes de la procreación y compartidas por dos o más individuos".*

También, respecto de la recogida y tratamiento de datos, el apartado cuarto del apéndice de la recomendación R97 regula en puntos aparte los datos genéticos; el punto 4.7, establece que *"los datos genéticos recogidos y procesados para el tratamiento preventivo, el diagnóstico o el tratamiento del afectado o para investigación científica sólo deben emplearse con esos fines o para permitir al afectado tomar una decisión libre e informada en estas materias".* El punto 4.8 que *"el procesamiento de datos genéticos con fines judiciales o de investigación criminal debe ser objeto de una ley específica que ofrezca medidas de salvaguardia adecuadas. Los datos sólo deben emplearse para establecer si hay un eslabón genético en el conjunto de pruebas aportadas, para prevenir un peligro real o para reprimir un delito específico. En ningún caso deben emplearse para determinar otras características que pueden ser establecidas genéticamente".* Y el punto 4.9 que *"la recogida y procesamiento de datos genéticos con cualquier otro fin distinto de*

los previstos en los Principios 4.7 y 4.8 sólo debe permitirse, en principio, por razones de salud y en particular para evitar un serio perjuicio a la salud del afectado o de terceros. Sin embargo, puede permitirse la recogida y procesamiento de datos genéticos en orden a predecir enfermedades en casos en que exista un interés superior y bajo la sujección a las medidas de salvaguardia definidas por la ley". De modo que a la generalidad restrictiva, siempre existe la especialidad permisiva.

La Ley de Investigación Biomédica, respecto de los datos genéticos, contempla dos definiciones que es necesario introducir en este punto, en relación con lo anteriormente expuesto, la recogida en el artículo 3j) y que define como «*Dato genético de carácter personal*» la *"información sobre las características hereditarias de una persona, identificada o identificable obtenida por análisis de ácidos nucleicos u otros análisis científicos".* Igualmente el artículo 3w) define como «*Tratamiento de datos genéticos de carácter personal o de muestras biológicas*» las *"operaciones y procedimientos que permitan la obtención, conservación, utilización y cesión de datos genéticos de carácter personal o muestras biológicas".*

Respecto de los datos genéticos, Noelia de Miguel sostiene que *"por lo que se refiere a la información genética, se revela sin ambages el fuerte potencial de la misma, debido a la gran cantidad de datos que aporta, lo que crea un hombre transparente y, por ello especialmente vulnerable; pues cuanto mayor es el grado de información del que se dispone sobre nosotros, mayor es nuestra vulnerabilidad"*[172]*.*

Otro sector doctrinal se ha manifestado también a propósito de la información genética, sosteniendo que *"La utilización de una definición amplia de dato relativo a la salud, entendido como*

[172] DE MIGUEL SÁNCHEZ, Noelia*: "Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público"*. Tirant lo Blanch, Valencia, 2004. Pág. 18.

cualquier información concerniente a la salud pasada, presente y futura, física o mental del individuo permitiría estirar tal concepto hasta abarcar la inclusión de los datos relativos de cuestiones genéticas. La definición de dato genético como dato relativo a la salud o estrechamente relacionado con la misma está amparada por el criterio de la Agencia Española de Protección de Datos. Ésta considera los datos genéticos como datos relativos a la salud de las personas, tanto si provienen éstos del ADN codificante como si son resultado del ADN no codificante, señalando que "si bien es posible que del resultado del análisis de ADN no codificante no se deriven directamente datos de salud, dichos resultados vienen a conformar la huella genética de una persona, y por tanto, se encuentran íntimamente relacionados con la salud"[173]*.* Respecto a esto afirma que *"la identificación o relación entre la persona y la información genética se establece en unos términos distintos a lo que sucede con los datos relativos a la salud*. *Los datos genéticos son datos relativos a la salud de las personas cuando revelan el estado de salud físico o psíquico pasado, presente y futuro de un individuo. Pero en algunos supuestos, los datos genéticos revelan otro tipo de informaciones, como la relación del individuo con terceras personas o el origen étnico del titular de los mismos, cuya inclusión dentro del concepto de dato médico o dato relativo a la salud resulta dudosa"*[174]*.*

Además, esta misma autora habla de la sensibilidad de los datos genéticos *"los datos genéticos poseen una especial naturaleza. Por una parte, se trata de información vinculada con la salud de la persona; por otra, si no revelan datos relativos a la salud, proporcionan una serie de características físicas, de tal forma que la identificación de la huella genética del ser humano adquiere gran*

[173] PÉREZ FUENTES, Gisela María (coordinadora): *"Temas selectos de derecho a la información, derecho a la intimidad, transparencia y datos personales".* Editorial Sista, S.A. Tabasco, México, 2010. Pág. 117

[174] Ibídem. Pág. 119.

relevancia, debido a que los datos genéticos que se obtengan, pueden revelar información sobre un grupo de personas, es decir, revelan el carácter único de la persona en cuestión. En definitiva, son datos que tienen que ver con cuestiones íntimamente vinculadas al núcleo de la personalidad y de la dignidad humana, lo que conlleva a la posibilidad de que se generen acciones de discriminación en base a éstos. Son datos que constituyen información científica, que puede ser médica o no, dado que algunos datos genéticos, como los que determinan el color de ojos o de pelo, no pueden considerarse estrictamente datos relativos a la salud. De ahí que debemos preguntarnos si es viable clasificar como dato sensible a los datos genéticos"[175]*.* Este tema ya ha sido mencionado en la introducción de este estudio a propósito de la mención del término "intimidad genética", del cual se desprendía que algunos de los datos que revela la genética, no tienen porqué ser sensibles, tales como la altura o color del pelo, al igual que se ha expresado ahora. En base a este argumento, el sector doctrinal que venía comentando sostiene que *"los datos genéticos que proporcionan información vinculada con la salud, se consideran datos sensibles"*[176]*.*

Karla Cantoral, por su parte, ha manifestado al respecto que *"los datos genéticos que proporcionan información vinculada con la salud se consideran datos sensibles…"*[177]*.* Aunque, manifiesta que, *"…en ocasiones resulta difícil distinguir un dato genético de un dato relativo a la salud…"*[178]*.*

Puede sacarse en claro de este examen de conceptos, que pese a la gran cantidad de normativa sanitaria existente, dos

[175] PÉREZ FUENTES, Gisela María (coordinadora): *"Temas selectos de derecho a la información, derecho a la intimidad, transparencia y datos personales"*. Editorial Sista, S.A. Tabasco, México, 2010. Pág. 122.

[176] Ibídem. Pág. 123.

[177] CANTORAL DOMÍNGUEZ, Karla: *"Derecho de protección de datos personales en la salud"*. Editorial Novum, MEXICO D.F., 2012. Pág. 148.

[178] Ibídem. Pág. 149.

conceptos fundamentales como son en el ámbito de la salud “dato médico” e “historial clínico”, no se encuentran definidos de forma generalizada; en cambio si se produce una diversidad de definiciones de conceptos más o menos afines, que producen confusión en este sentido y dificultad al intentar aplicar estas normas de forma interrelacionada.

III.3.b. Incorporación de la información:

La incorporación de los datos médicos a la historia clínica del paciente debe hacerse con suma delicadeza; desde los auxiliares, enfermeros y, por supuesto médicos. El entramado de personas que intervienen en el proceso de creación de la historia clínica, a través de la recopilación de los distintos datos, hacen que esta maniobra tenga que ser lo más cuidadosa posible. La historia clínica nace, crece y se nutre de los datos del paciente y, quien la crea es el distinto personal que trabaja en los centros sanitarios, cada uno de ellos de acuerdo a sus funciones.

El Real Decreto de atención especializada, establece en su artículo 8.1 que: *“De conformidad con lo dispuesto en los artículos 53 y 55 de la Ley 16/2003, de 28 de mayo, las comunidades autónomas y, en su caso, los centros sanitarios, estarán obligados a suministrar los datos al órgano responsable del registro”.* Especificando en el punto tercero que: *“Según lo dispuesto en el artículo 53.5 de la Ley 16/2003, de 28 de mayo, cada comunidad autónoma tendrá acceso a los datos del registro correspondientes a la atención recibida en otras comunidades autónomas por los ciudadanos que residan en su ámbito territorial. Asimismo, las mutualidades administrativas de los regímenes especiales de la Seguridad Social de funcionarios (MUFACE, MUGEJU e ISFAS), tendrán acceso a los datos del registro correspondiente a su respectivo colectivo protegido”.*

Cristina Centeno Soriano ha manifestado al respecto que *“en la mayoría de hospitales, la conservación de la historia clínica es res-*

ponsabilidad del departamento de documentación médica, que se ocupa de su custodia, de dictar normas sobre el contenido y de la forma de realizar la historia, así como de establecer las normas para el acceso de los profesionales sanitarios a dicha información"[179]*.* Y así mismo mantiene que *"este servicio de archivo de historias clínicas es único y centralizado para todo el hospital. Abarca, así mismo, la totalidad de la documentación clínica que se genera durante la asistencia del paciente, independientemente de la naturaleza de su soporte"*[180]*.* No obstante argumenta que *"el archivo, para su funcionamiento, cuenta con la colaboración de la Comisión de Historias Clínicas, que trata un amplio abanico de asuntos relativos a la historia clínica: su cumplimentación, custodia, requisitos de privacidad, funciones, y circuito de funcionamiento"*[181].

Un sector de la doctrina argumenta en este sentido que *"la historia clínica se construye en gran parte con la información que proporciona el paciente, pero el médico corresponde explicándole la interpretación que se hace de la misma y de los resultados de la exploración y las pruebas complementarias"*[182]*.*

Respecto a la variedad del personal que accede hoy en día a las historias clínicas, es interesante referir aquí una reflexión doctrinal, *"actualmente encontramos cada vez con mayor frecuencia, sistemas que han automatizado la gestión de pacientes, sin embargo, son los especialistas sanitarios documentales y de gestión*

[179] CENTENO SORIANO, Cristina: *"Operaciones administrativas y documentación sanitaria"*. Formación Alcalá, Jaén, 2007. Pág. 162.

[180] CENTENO SORIANO, Cristina: *"Operaciones administrativas y documentación sanitaria"*. Formación Alcalá, Jaén, 2007. Pág. 162.

[181] Ibídem.

[182] BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: *"Manual de ética y deontología médica".* Organización Médica Colegial de España, 2012. Pág. 60.

(médicos/enfermeras), los que deben concebir, mantener, alimentar con información y utilizar los sistemas informáticos"[183]*.*

En cualquier caso, y según comparte otro sector doctrinal, *"…la asistencia a los pacientes, hospitalizados y ambulatorios, genera un volumen significativo de información médica y administrativa sobre los mismos. Dicha información se registra en varios documentos, siendo el conjunto de estos documentos lo que constituye la historia clínica"*[184]*.* Afirmado esta autora que *"en esta misma línea, la historia clínica debe ser única, integrada y acumulativa para cada paciente en el hospital, debiendo existir un sistema eficaz de recuperación de la informática clínica"*[185]*.* Así, *"En el contexto descrito, la historia clínica única por paciente es un documento sanitario único y permanentemente abierto, que va integrando, progresivamente, la nueva información generada a lo largo de las sucesivas y diferentes asistencias que ha recibido el paciente…"*[186] . De modo que *"si la historia es única para cada paciente en un hospital y su gestión está centralizada desde un archivo único, se garantiza que todos los sucesivos episodios de ese enfermo queden conservados juntos"*[187]*.*

El que una historia clínica sea más o menos completa, dependerá de la diligencia de quienes deban trasladar la información a la misma, ya sean auxiliares, enfermeras, médicos u otro tipo de personal que intervenga en tal proceso. No es algo sencillo, pensemos en la cantidad de informes que se pueden generar en un centro hospitalario en un solo día. Habrá operaciones programadas, urgencias, consultas, partos, etc.; y por ejemplo, en el caso de los últimos, puede darse el caso de que un mismo profesional asista varios de ellos en un corto espacio de tiempo, o incluso a la vez,

[183] CURRIEL HERRERO, J y ESTÉVEZ LUCAS, J: *"Manual para la gestión sanitaria y de la historia clínica hospitalaria"*. Editores Médicos, Madrid, 2000. Pág. 20.

[184] CENTENO SORIANO, Cristina: *"Operaciones administrativas y documentación sanitaria"*. Formación Alcalá, Jaén, 2007. Pág. 107.

[185] Ibídem.

[186] Ibídem. Pág. 110.

[187] Ibídem. Pág. 111.

pudiendo producirse algún olvido en el traslado de la información. Si lo pensamos así, es todo un mérito que al cabo del día todos esos informes estén completos al 100%, pero la realidad es que esto es algo que forma parte del trabajo del personal sanitario; tanto el hacer una cura, como anotar la evolución de unos puntos de sutura, son necesarias para que el informe sea real, completo y útil para la evolución del paciente, ya que unas décimas de fiebre podrían despistar, si no sabemos que existe una herida infectada. Por eso es tan importante el trabajo de unos como el de otros.

En este sentido, algunos autores manifiestan que *"se puede constatar, que en muchos de nuestros centros sanitarios hoy día la historia clínica, en general, es una colección desestructurada de documentos en soporte papel, contenidos en una carpeta a la que solo se aspira a almacenar y encontrar cuando se solicite"*[188]*.* Insistiendo este mismo sector en que *"…la HC es documento que contiene toda la información de utilidad clínica sobre el estado de salud o enfermedad del individuo o persona atendida en un centro sanitario, y tiene que reunir las siguientes condiciones: debe ser útil al profesional de la salud para reflejar sus conocimientos en el proceso asistencial, debe también ser fiable, de modo que la información reflejada en ellos indique la realidad, y además debe ser accesible, estando siempre localizable y disponible"*[189]*.*

Esto dista mucho de la historia clínica única que se pretende sostener hoy en día en el sistema sanitario español, y que está cada vez más conseguida gracias al uso de las tecnologías.

Otra parte de la doctrina ha manifestado que *"así, la historia clínica se confecciona con "los datos de identificación del paciente, el informe del examen físico, las órdenes de diagnóstico con el paso del tiempo, las órdenes de diagnóstico y tratamiento, las*

[188] CURRIEL HERRERO, J y ESTÉVEZ LUCAS, J: *"Manual para la gestión sanitaria y de la historia clínica hospitalaria"*. Editores Médicos, Madrid, 2000. Pág. 33.

[189] Ibídem.

observaciones clínicas, el informe sobre los procedimientos, pruebas y resultados y la epicrisis así como la anamnesis", por lo que podría ser calificarla como "archivo, registro, base o banco de datos", lo que lleva a encuadrarla dentro de la protección de datos)"[190]*.* Y que, *"precisamente, al tratarse de datos sensibles, se requiere que gocen de una especial protección a la hora de su recogida y tratamiento. No podemos obviar que estamos ante datos cuya publicidad o conocimiento por terceras personas podría traer repercusiones familiares, sociales y profesionales no deseadas por el paciente titular de los mismos. De ahí la relevancia de proteger estos datos"*[191]*. "Así, los datos relativos a la salud se van acumulando a lo largo de la vida, es un itinerario vital en el que aparece todo lo que hemos vivido, los tratamientos y sus consecuencias"*[192]*.*

Samprón López, por su parte, manifiesta en este sentido que *"debido a la inseguridad jurídica a las que están sometidas muchas actuaciones de los profesionales sanitarios, se tiende a una medicina defensiva, tanto a cerca de las actuaciones sanitarias, como acerca de la información y documentación contenida en la Historia Clínica, con lo cual pierde esta su riqueza en datos que serían cuando menos interesantes para procesos posteriores del paciente"*[193]*.*

Otro sector doctrinal ha expresado en cambio que *"Los datos que contiene una historia clínica han dependido siempre del médico que la realiza y el centro donde se realiza, existiendo en ellas diferencias de formato y contenido. Esta disparidad está desapareciendo con la informática y el proyecto de una historia clínica única y común informatizada a nivel nacional y europeo. La normalización de los documentos, elaborada de forma equilibrada y*

[190] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores): *"La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural"*. Tirant Lo Blanch, Valencia, 2014. Pág. 332.

[191] Ibídem.

[192] Ibídem.

[193] SAMPRÓN LÓPEZ, David: *"Los derechos del paciente a través de la información de la historia clínica"*. Edisofer, Madrid, 2002. Pág. 39.

flexible, porque la falta de normalización puede significar la ausencia sistemática de recogida de datos, y una estandarización muy rígida y detallada puede dificultar el registro de datos no previstos y producir una disgregación lógica de la información en muchos documentos específicos complementarios (Comb, 1994)"[194]*.*

Este mismo sector doctrinal manifiesta al respecto que *"la normalización de la HC tiene por objeto definir y hacer cumplir las características que deben tener los documentos clínicos y los que deben tener su reproducción, así como de su empleo y uso"*[195].

Respecto al contenido de la historia clínica, este debe ser un documento íntegro, veraz y actualizado, al que todo paciente tiene derecho, debiendo contener unos mínimos de cuya cumplimentación serán responsables los profesionales que intervengan en cada proceso. Esta información la contiene el artículo 15 de la Ley del paciente, que establece en su punto primero que *"la historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. Todo paciente o usuario tiene derecho a que quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada".* Todo ello con la finalidad de, como establece el punto segundo *"…facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud".* Y sigue estableciendo este artículo en su punto tercero que *"la cumplimentación de la historia clínica, en los aspectos relacionados con la asistencia directa al paciente, será responsabilidad de los profesionales que intervengan en ella".* De

[194] CRIADO DEL RÍO, María Teresa y SEOANE PRADO, Javier: "*Aspectos médico-legales de la historia clínica"*. Colex, Madrid, 1999. Pág. 54.

[195] CURRIEL HERRERO, J y ESTÉVEZ LUCAS, J*: "Manual para la gestión sanitaria y de la historia clínica hospitalaria"*. Editores Médicos, Madrid, 2000. Pág. 49.

modo que la información a la historia clínica la incorporan varios profesionales, según les asistan o realicen pruebas; así se conseguirá un documento completo y fiable de la situación de los pacientes, con el compromiso y la colaboración de todos ellos. No en vano, el punto cuarto de este artículo establece que *"la historia clínica se llevará con criterios de unidad y de integración, en cada institución asistencial como mínimo, para facilitar el mejor y más oportuno conocimiento por los facultativos de los datos de un determinado paciente en cada proceso asistencial".*

Pero pese a todo ello, se establecen una información mínima que deben contener estos documentos, en relación a las diferentes situaciones que puedan darse en el ámbito sanitario, según establece también el artículo 15 en su punto segundo *"…el contenido mínimo de la historia clínica será el siguiente: a) La documentación relativa a la hoja clínicoestadística. b) La autorización de ingreso. c) El informe de urgencia. d) La anamnesis y la exploración física. e) La evolución. f) Las órdenes médicas. g) La hoja de interconsulta. h) Los informes de exploraciones complementarias. i) El consentimiento informado. j) El informe de anestesia. k) El informe de quirófano o de registro del parto. l) El informe de anatomía patológica. m) La evolución y planificación de cuidados de enfermería. n) La aplicación terapéutica de enfermería. ñ) El gráfico de constantes. o) El informe clínico de alta"* Especificando el último párrafo de este artículo que *"los párrafos b), c), i), j), k), l), ñ) y o) sólo serán exigibles en la cumplimentación de la historia clínica cuando se trate de procesos de hospitalización o así se disponga".*

Que la información que consta en los centros sanitarios esté lo más actualizada posible es una cuestión esencial para la curación del paciente, al igual que lo es que se corresponda con la realidad. En este sentido Aberasturi Gorriño manifiesta que *"todo tratamiento médico tiene que partir necesariamente de una información veraz, completa y actual sobre el paciente. Desde que nace, e incluso*

desde antes de nacer hasta la muerte, e incluso después de ésta, las personas son fuente constante de información en el sector sanitario. Esta información resulta imprescindible para la realización de las tareas vinculadas a la protección de la salud. Este hecho no constituye por sí mismo ninguna novedad, pues la importancia de la información en este ámbito siempre ha sido especialmente destacable"[196]*.*

Y reflexiona, este autor*: Lo verdaderamente reseñable en la actualidad es que se ha puesto más que nunca de manifiesto la dificultad de los sistemas sanitarios para manipular esta información. Cada vez son más los servicios que se prestan desde los centros sanitarios, la población envejece cada vez más, la movilidad de los ciudadanos aumenta, aparecen nuevas fuentes de información como la genética, la especialización es también cada vez mayor, a la información sanitaria hay que sumarle la administrativa, etc. Todo esto hace que la gestión sanitaria en general y la manipulación de la información sanitaria en particular, constituyan actividades cada vez más complejas. El volumen de datos que hay que manipular y la agilidad con la que hay que hacerlo para otorgar un servicio de calidad hacen que sean prácticamente imprescindibles herramientas que posibiliten este tratamiento fácil, rápido y seguro de la información sanitaria, un «sistema de información» que ponga a disposición del personal que lo necesite la información que sea precisa para llevar a cabo su labor, cuándo y cómo lo requiera. La implantación de un sistema de información capaz de responder a las necesidades actuales de transmisión y manejo de datos pasa por la informatización del sistema"*[197]*.*

Este mismo autor, ha manifestado también respecto de la veracidad de los datos que *"la responsabilidad de que se cumpla con*

[196] ABERASTURI GORRIÑO, Unai*: "La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 26.

[197] Ibídem.

este principio es, evidentemente, tanto de la Administración sanitaria como de los propios usuarios"[198]*.*

Así mismo, David Samprón López recoge en este sentido que: *"El documento de 26 de noviembre de 1997, del Grupo de Expertos credo por el Ministerio de Sanidad y Consumo para definir y fijar criterios en relación con los derechos y obligaciones de los pacientes, establece que siendo el fin principal de la historia clínica facilitar la asistencia sanitaria al ciudadano, esta finalidad es la razón de ser de la Historia Clínica y la única que puede justificar su creación y actualización, la naturaleza de los datos que puede contener, y su carácter especialmente sensible en relación con la necesaria protección legal que asume la confidencialidad de su contenido y por tanto la intimidad de la persona sobre cuya salud hace referencia la información en ella contenida"*[199]*.*

Vale la pena dividir el artículo 16 de la Ley del paciente, para diferenciar que, sus último cuatro puntos, se refieren al personal que incorpora la información en la historias clínicas, y hace una gran diferenciación entre personal administrativo y sanitario. Así el punto cuarto de este artículo establece que *"el personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones".* Y el punto quinto que *"el personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria".* Este es un hecho que en la mayoría de los casos no se

[198] ABERASTURI GORRIÑO, Unai: *"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 110.

[199] SAMPRÓN LÓPEZ, David: *"Los derechos del paciente a través de la información de la historia clínica"*. Edisofer, Madrid, 2002. Pág. 55.

lleva a cabo, ya que suele ser el personal administrativo quien transcribe los datos de los pacientes, muchas veces por falta de tiempo de los propios profesionales. Esto tiene que ser informado sin duda en las funciones y obligaciones del personal, tema que se examinará más adelante.

El informe jurídico de la AEPD 0656/2008 versa sobre si el personal de enfermería de un centro sanitario debe acceder a todos los datos médicos del paciente, ante lo que se establece que *"…únicamente sería posible establecer una regla mínima de acceso, en cuya virtud el personal de enfermería que desarrolla su actividad en funciones de hospitalización debería acceder a la totalidad de los datos de la historia clínica que o bien se encuentren directamente vinculados al episodio que ha dado lugar a la hospitalización y que se obtengan durante la misma y a aquéllos otros datos de la historia clínica que hubieran sido considerados relevantes para el tratamiento llevado a cabo en relación con la hospitalización concreta respecto de la que se prestan los servicios asistenciales".* Lo que ocurre es que en la realidad, y tratándose sobre todo de centros pequeños, la mayoría de las veces privados, esto resulta difícil de llevar a la práctica porque los accesos no se encuentran tan fragmentados o porque el personal es escaso y realiza varias funciones, aunque estas no les correspondan.

Respecto del acceso a los datos del diferente tipo de personal que encontramos en los centros sanitarios, hay una parte de la doctrina que ha manifestado que frecuentemente *"…aparecen otros factores sobreañadidos al proceso asistencial, tales como las labores de gestión y administración (personal de justicia, compañías aseguradoras, riesgos laborales, certificaciones de calidad, etc.) que obligan a que otro tipo de personal no sanitario, puedan tener acceso*

a la documentación clínica, dando lugar a otro tipo de secreto que se conoce como "secreto médico derivado"[200]*.*

Se hace necesario citar aquí una referencia doctrinal *"tanto la creación como la actualización de la HC, que nadie discute, y que se desprende de la normativa sanitaria, en cuanto a la creación intelectual, corresponde al médico que presta la atención al paciente, si bien ciertos tipos documentales estandarizados a modo de formularios, corresponde su propiedad intelectual al Centro, Comités o Comisiones que los hayan elaborado"*[201]*.* Así, "*en cuanto a la propiedad de los datos referentes a la salud corresponde al paciente tal y como se establece en la normativa sanitaria tanto estatal como autonómica, y en la LOPD*"[202].

Respecto de la diferenciación entre datos administrativos y sanitarios, el CDM establece en su artículo 27.4 que *"en las instituciones sanitarias informatizadas los médicos directivos velarán por una clara separación entre la documentación clínica y la administrativa".*

Igualmente esta misma norma en su artículo 19.1 recoge que *"los actos médicos quedarán registrados en la correspondiente historia clínica. El médico tiene el deber y el derecho de redactarla. La historia clínica incorporará la información que se considere relevante para el conocimiento de la salud del paciente, con el fin de facilitar la asistencia sanitaria".*

Se regula también en la Ley del paciente el deber de secreto de los profesionales en el ejercicio de sus funciones, respecto del uso

---

[200] BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: *"Manual de ética y deontología médica".* Organización Médica Colegial de España, 2012. Pág. 100.

[201] SAMPRÓN LÓPEZ, Davi:. *"Los derechos del paciente a través de la información de la historia clínica"*. Edisofer, Madrid, 2002. Pág. 63.

[202] Ibídem.

de la historia clínica, así establece su artículo 16.6 que *"el personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto".* Cuestión, la del deber de secreto, ampliamente tratada en el apartado dedicado a esta materia.

La Ley del paciente, establece respecto al acceso a los datos de nivel alto, que *"las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso".* Este es un requisito establecido por el RLOPD, que en sus artículos 103 y 113, dependiendo del tipo de soporte en que se recojan los datos. El artículo 103 se refiere a los datos que constan en soporte informático y establece el concepto de registro de accesos, del que, según se establece en su punto primero *"de cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado".* El punto segundo dice que además *"en el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido".* Y según establece el punto tercero *"los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos".* De modo que habrá un responsable que se encargue de dicha gestión. Dicho responsable, denominado "*responsable de seguridad*", definido en el 5.2 l) de este reglamento como *"persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables".* Esto, sabiendo que el "*responsable del fichero*", es definido en el artículo 3d de la LOPD como *"persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".*

Pues bien, una vez claras estas figuras, este responsable de seguridad, se encargará además, según establece el punto quinto del comentado artículo 103 del RLOPD, que *"…se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados".* Habrá, para todo lo establecido, un plazo de conservación que marca el punto cuarto de este artículo estableciendo que *"el período mínimo de conservación de los datos registrados será de dos años".*

Y existe también una excepción a lo anteriormente establecido, regulado en el punto sexto, según el cual *"no será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias: a) Que el responsable del fichero o del tratamiento sea una persona física. b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales"*. Debiendo además, dejar constancia de ello en el documento de seguridad, según establece el último párrafo de este último punto comentado que establece que *"la concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad".* Y respecto de los datos de nivel alto que constan en soporte papel, el artículo 113.1 establece como norma general que *"el acceso a la documentación se limitará exclusivamente al personal autorizado".* Pero además, se recoge en el punto segundo que *"se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios".* Esta es una tarea difícil, ya que habría que habilitar unos formularios en los que los profesionales hiciesen constar esta información, quizás dentro de cada historia clínica, o de cada dispositivo que la almacene, pero en definitiva, una complicada cuestión, que deberá inculcarse al personal, para que con la gran actividad diaria de los centros

sanitarios, sobre todo de los grandes, se conciencien de sacar el tiempo para realizarlo.

Sobre la conservación de la documentación clínica se establece el plazo general de cinco años en el soporte original, para la propia atención al paciente por los centros sanitarios, pero se establece además la conservación a efectos judiciales. Así se establece en el artículo 17.1 de la Ley del Paciente que *"los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial".* Recogiendo el punto tercero que *"los profesionales sanitarios tienen el deber de cooperar en la creación y el mantenimiento de una documentación clínica ordenada y secuencial del proceso asistencial de los pacientes".* Para los pacientes hospitalizados en concreto, se establece en el punto cuarto que *"la gestión de la historia clínica por los centros con pacientes hospitalizados, o por los que atiendan a un número suficiente de pacientes bajo cualquier otra modalidad asistencial, según el criterio de los servicios de salud, se realizará a través de la unidad de admisión y documentación clínica, encargada de integrar en un solo archivo las historias clínicas. La custodia de dichas historias clínicas estará bajo la responsabilidad de la dirección del centro sanitario".* En el caso de profesionales independientes serán ellos los responsables de la gestión y custodia, según el punto quinto del comentado artículo. Y acaba este artículo de la siguiente forma en el punto sexto diciendo que, *"son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal".* Existe una especialidad de conservación de la historia clínica, que se

regula en el punto segundo estableciendo que *"la documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas".*

Publica el periódico El País publica que *"Protección de Datos investiga por primera vez un caso de bebé robado"*, y asegura una de las afectadas en este caso que: *"En el hospital me respondieron que no tenían la historia clínica de mi madre porque todos los archivos se destruyen pasados cinco años"*[203]. En cualquier caso plazo genérico y mínimo que en la mayoría de los centros se supera con creces, por la utilidad de la información a posteriori, cosa que en este caso no interesaba.

El informe jurídico de la AEPD 0551/2008 establece en relación a la conservación de la historia clínica que *"…el deber de custodia de la historia clínica debería subsistir al menos durante el período de tiempo establecido por la normativa estatal o autonómica reguladora de la materia, teniendo en cuenta la propia finalidad de la historia, por cuanto, como también ha señalado esta Agencia en informe de 1 de octubre de 2003, "la voluntad del legislador en este caso no es la de que se proceda a la destrucción inmediata de los datos, sino, al contrario, que dichos datos sean conservados en cuanto pudieran resultar necesarios para la salvaguardia de la vida e integridad física del paciente".*

También en relación a la conservación de la historia clínica, el informe jurídico de la AEPD 0443/2010, establece en relación al artículo 17.1 de la Ley del paciente que *"…la Ley permite la conservación de la historia clínica en un soporte distinto del original,*

[203] JUNQUERA, Natalia: *"Protección de Datos investiga por primera vez un caso de bebé robado"*. El País, lunes 28 de mayo de 2012, vida & artes, Madrid, sociedad. Pág 38.

siempre que quede preservada su autenticidad, seguridad e integridad". Pero puntualiza este informe que *"al propio tiempo, la Ley obliga a conservar los datos de la historia clínica incluso con posterioridad al alta del paciente o al último episodio asistencial, durante el tiempo adecuado para la debida asistencia sanitaria del mismo y, como mínimo, durante cinco años desde cada fecha de alta".* Y finalmente señala que: *"Por último, en relación con la posible constancia del consentimiento informado del paciente u otros documentos mediante el empleo de dispositivos de firma electrónica, el mismo será posible en garantías que permitan acreditar la integridad de los documentos objeto de firma. En este sentido, y desde la perspectiva de la aplicación de las normas de protección de datos, debe indicarse que cuando sea preciso el consentimiento del interesado para el tratamiento de sus datos de carácter personal, lo que no sucederá en relación con el tratamiento de la historia clínica, al encontrarse el mismo habilitado por el artículo 8 de la Ley Orgánica 15/1999, corresponderá al responsable del tratamiento, en este caso el centro sanitario, la prueba de la debida obtención del consentimiento a través de cualquier medio válido en derecho, dado que reiterada jurisprudencia de la Audiencia Nacional y del Tribunal Supremo ha declarado que es al responsable al que corresponde la carga de la prueba en este caso".*

Y en referencia a los plazos de conservación establecidos por la Ley del paciente, recoge otro informe jurídico 0149/2008 de la AEPD que *"en lo que no fuera de aplicación el artículo 17.1 de la Ley 41/2002, deberá tenerse en cuenta que, conforme al artículo 4.5 de la Ley Orgánica 15/1999, "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".*

Juan Mejía expresa en este sentido que *"la conservación de las HC debe orientarse a preservar la información clínica de interés*

desde el punto de vista asistencial y no necesariamente el documento original en el que se plasmó"[204]*.*

Otra parte de la doctrina recoge que *"un aspecto importante para el área de archivo de HC es local y mobiliario específico del mismo. En el local de archivo de HC debe disponerse de tres zonas principales de actividad: un espacio abierto al usuario sanitario interno del centro, un espacio reservado al personal, y un espacio para almacenar"*[205]*.* Este sector doctrinal, señala además un plazo temporal del almacenamiento que deben cumplir estos lugares, según el que *"el espacio de almacenamiento de HC debe concebirse ante todo, en función de la seguridad. Su acceso debe ser fácil y su capacidad suficiente para colocar HC durante al menos 10 años. El embotellamiento en las zonas de almacenamiento conduce inevitablemente a una desorganización del trabajo"*[206]*.* De hecho, *"El informe 80370 de la OMS indica el tiempo de vida de la HC en 10 años"*[207]*.*

Luís Mejía por su parte, sigue manteniendo que *"en mi opinión debe conservarse un plazo al menos de 5 años, como documento administrativo que es. Ahora bien, razones de oportunidad pueden aconsejar un plazo superior, así de 8 a 10 años, por considerarse el periodo activo de las HC. Y por último, solo un criterio garantista justificaría extenderla conservación de las historias hasta los 15 años, que es el plazo máximo para la prescripción de las acciones…"*[208]*.*

En relación a la custodia de la historia clínica, un sector doctrinal sostiene en cambio que *"respecto a la custodia de la HC,*

---

[204] MEJÍA, Juan: *"Hacia un estatuto jurídico desarrollado de la Historia Clínica"*. Diario La Ley 5638 de octubre de 2002.

[205] CURRIEL HERRERO, J y ESTÉVEZ LUCAS, J: *"Manual para la gestión sanitaria y de la historia clínica hospitalaria"*. Editores Médicos, Madrid, 2000. Pág. 20.

[206] Ibídem.

[207] Ibídem. Pág. 90.

[208] MEJÍA, Juan: *"Hacia un estatuto jurídico desarrollado de la Historia Clínica"*. Diario La Ley 5638 de octubre de 2002.

en relación con la propiedad de la misma. Por un lado, será responsabilidad del centro propietario de la historia clínica, su custodia siempre que la asistencia médica al paciente se esté llevando a cabo por un facultativo o facultativos del propio centro. Y por otro. La custodia será responsabilidad del médico que preste sus servicios por cuenta propia. Es decir, que propiedad y custodia de la historia clínica van de la mano…"[209].

A este respecto conviene citar que según fuentes de la Agencia Española de Protección de datos: *"La mayoría de infracciones en la custodia de las historias clínicas descubiertas son sistemáticas: obedecen a la manera en que día a día se manejan. Es el caso de la sanción impuesta por la Agencia de Protección de Datos en 2008 a la Agencia Valenciana de Salud, porque almacenaba los historiales médicos en lugares inseguros y los transportaba en carros como los de los supermercados que quedaban al alcance de cualquiera"*[210].

Respecto a la propiedad de la historia clínica, Juan Mejía hace una reflexión muy interesante, *"hay un sector que sostiene que la propiedad de la HC pertenece al paciente, si bien la institución sanitaria tiene la obligación de su conservación y custodia. Otros estiman que su propiedad pertenece al médico, especialmente en la medicina privada, al ser fruto de su trabajo intelectual. Un tercer grupo estima que su propiedad en la medicina por cuenta ajena es del centro sanitario para el que trabaja el facultativo, al ser aquel quien abona a los médicos un salario por la realización de su trabajo"* [211]. Y en realidad, según manifiesta el autor, *"más que de derecho de propiedad hay que hablar de distintos derechos, (de acceso, de uso*

[209] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso: *"La protección de datos personales en el ámbito sanitario"*. Editorial Aranzadi, Navarra 2002. Pág. 74.

[210] DE BENITO, Emilio: "La mayoría de hospitales públicos custodia mal las historias clínicas". El País, jueves 14 de octubre de 2010, vida & artes, Madrid. Pág. 28.

[211] MEJÍA, Juan: *"Hacia un estatuto jurídico desarrollado de la Historia Clínica"*. Diario La Ley 5638 de octubre de 2002.

y disposición y de las correlativas obligaciones, de secreto, de custodia, de conservación…)"[212]. Por lo que *"Estaríamos en un supuesto de titularidad compartida con una parte tangible y una parte moral que conlleva a ejercitar diversas facultades por distintos titulares"*213. Concluyendo, con mucha razón, que *"Al fin estamos como siempre ante el principio de proporcionalidad"*[214]*.*

El derecho a la custodia se encuentra además regulado en el artículo 19 de la ley del paciente, *"el paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido por el artículo 16 de la presente Ley".* Que como se aprecia hace referencia a la ya citada confidencialidad del artículo 16, que recordemos, se encuentra también regulada en el artículo 10 de la LOPD, que establece que *"el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".*

A propósito de la custodia de la historia clínica, otra parte de la doctrina asegura que *"en todo caso, se otorga al paciente el derecho de que los centros sanitarios "establezcan un mecanismo de custodia activa y diligente de las historias clínicas" (art. 19); y hay una remisión a la LOPD en relación a las medidas técnicas de seguridad (art. 17.6)"*[215]*.*

---

[212] Ibídem.
[213] Ibídem.
[214] Ibídem.
[215] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores): *"La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural"*- Tirant Lo Blanch, Valencia, 2014. Pág. 356.

Respecto a la conservación y custodia de la historia clínica que se viene examinando, parte de la doctrina ha manifestado que *"no hay ninguna duda respecto al deber de conservación y custodia de la historia clínica, y los problemas principalmente son dos: la posesión de medios eficaces que garanticen la custodia y seguridad de los datos conservados, lo cual crea el problema de la preservación de la intimidad, y por otra parte el periodo de conservación de la historia clínica, para lo que hay que fijarse en la finalidad asistencial. Al menos 15 años por responsabilidad profesional"*[216].

Mucho se ha hablado y se va a hablar a lo largo de este estudio, de la conservación de los datos. Conviene resaltar en este punto, que la Recomendación sobre protección de datos médicos, dedica el punto décimo de su apéndice a este tema, estableciendo en su punto primero que *"en general, los datos médicos no deben conservarse más tiempo del necesario para alcanzar el propósito para el que se recogieron y procesaron".* Lo cual viene a coincidir con la LOPD, la cual en su punto 4.5, respecto de la calidad de los datos establece que *"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".* Estableciendo el segundo párrafo de este mismo punto que *"no serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados".*

En cambio, la Recomendación, va más allá en su punto segundo, en el que dice que *"cuando se acredite la necesidad de conservar los datos médicos que ya no tienen uso alguno para el fin con el que se recabaron por un interés legítimo de la salud pública o de la ciencia médica, o de la persona a cargo del tratamiento médico*

[216] CRIADO DEL RÍO, María Teresa y SEOANE PRADO, Javier: *"Aspectos médico-legales de la historia clínica"*. Colex, Madrid, 1999. Pág. 227.

o del controlador del archivo en orden a permitirles la defensa en o el ejercicio de una reclamación legal, o por razones históricas o estadísticas, se adoptarán las medidas técnicas oportunas para asegurar su correcta conservación y seguridad, teniendo en cuenta la intimidad del paciente".

Y el tercer párrafo del 4.5 de la LOPD, en similitud establece que: *"Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos".* Así, ambas normas, respecto de la conservación de datos fuera de los plazos establecidos, requieren unos criterios para su conservación, que el RLOPD establece respecto a la protección de datos en su artículo 9, que será comentado en el apartado correspondiente al tratamiento de datos con estos fines. La recomendación establece sobre esto en el 10.3 de su apéndice que: *"A petición del afectado, sus datos médicos deben ser eliminados, a menos que se hayan anonimizado o concurran intereses superiores y legítimos para no hacerlo, en particular los reseñados en el Principio 10.2, o si existe una obligación de conservar los datos grabados".* Vemos también que coinciden ambas normas en que la conservación debe ser con motivos históricos o estadísticos, aunque además la LOPD establece el uso científico y la recomendación el uso con fines legales.

Pero también el punto 12 de apéndice de la recomendación sobre protección de datos médicos, se refiere en su apartado primero a la investigación científica que se hará, en la medida de lo posible, de forma anónima *"siempre que sea posible, los datos médicos usados para fines de investigación científica deben ser anónimos. Los profesionales y organizaciones científicas y las autoridades públicas deben promover el desarrollo de técnicas y procedimientos para asegurar el anonimato".* Estableciendo su apartado segundo las situaciones en que se hará excepción a lo

anteriormente establecido, recogiendo que *"sin embargo, si tal anonimización hiciese imposible un proyecto científico de investigación, y el proyecto se va a realizar con fines legítimos, podría llevarse a cabo con datos personales a condición de que: a. el titular de los datos haya dado su consentimiento informado para uno o más fines de investigación; o b. otorguen el consentimiento el representante legal o la autoridad o persona u órgano previstos por la ley cuando el afectado sea una persona legalmente incapacitada e incapaz de una decisión libre, y la ley nacional no le permita actuar en su propia representación, siempre que este consentimiento se dé en el marco de un proyecto de investigación relacionado con la condición médica o la enfermedad del afectado; o c. el órgano u órganos designados por la ley nacional hayan autorizado la revelación de los datos con el fin de llevar a cabo un proyecto de investigación médica relacionado con un interés público importante, pero sólo si: i. el titular de los datos no se ha opuesto expresamente a la revelación; y ii. a pesar de los esfuerzos razonables que se puedan adoptar, sería impracticable contactar con el titular de los datos para pedir su consentimiento; y iii. el interés del proyecto de investigación justifica la autorización; o d. la investigación científica está prevista por la ley y constituye una medida necesaria por razones de salud pública*".

Respecto de la investigación científica, establece el apartado tercero a favor de los profesionales sanitarios para la utilización de la información, previo consentimiento de los afectados que *"bajo las previsiones complementarias que la ley nacional establezca, debe permitirse a los profesionales sanitarios habilitados para realizar su propia investigación médica el uso de los datos médicos que tienen en la medida en que el sujeto afectado haya sido informado de esta posibilidad y no se haya opuesto".* Pero el apartado quinto hace una matización, *"los datos personales usados para investigación científica no pueden publicarse en forma que permita identificar a los titulares de los datos, salvo que éstos hayan dado su consentimiento*

a la publicación y ésta sea permitida por la ley nacional". De modo que premiará el anonimato, salvo consentimiento expreso o autorización por ley para la publicación de dichos datos.

Lucas Murillo de la Cueva manifiesta respecto a la recopilación de la información que *"…sobre la captación de datos personales, la primera facultad es la de que no se recojan en ningún caso las informaciones sensibles que le afecten sin que medie su consentimiento previo y por escrito, que habrá debido solicitarle quien pretende recabarlos con indicación del destino que van a tener"*[217]*.*

También a este respecto el artículo 19.3 del CDM recoge que *"el médico y, en su caso, la institución para la que trabaja, están obligados a conservar la historia clínica y los elementos materiales de diagnóstico, mientras que se considere favorable para el paciente y, en todo caso, durante el tiempo que dispone la legislación vigente estatal y autonómica. Es muy recomendable que el responsable de un servicio de documentación clínica sea un médico."* Y así mismo el punto cuarto recoge que *"Cuando un médico cesa en su trabajo privado, las historias clínicas se pondrán a disposición de los pacientes que lo soliciten para que éstos puedan aportarlas al médico al que encomienden su continuidad asistencial. En caso de duda deberá consultar a su Colegio".* Es decir, que acabe la finalidad o el ejercicio del médico, la documentación clínica tiene previsto un destino.

Sobre este tema el Informe jurídico 496/2007 de la AEPD sobre conservación de la historia clínica e caso de jubilación o fallecimiento del médico. De él hay que resaltar que propone la celebración de un contrato, para quienes ejercen la medicina de forma privada, con un tercero que le prestase unos servicios entre

[217] LUCAS MURILLO DE LA CUEVA, Pablo: *"La protección de los datos personales frente al uso de la informática"*. Editorial Tecnos, Madrid, 1990. Pág. 185.

los que se encontrarían las comunicaciones en caso de jubilación o fallecimiento sobre el destino de las historias clínicas. Es decir, que tendrían que aplicarse los requisitos del artículo 12 de la LOPD. Así, se recoge que *"…en caso de jubilación del colegiado que hubiese firmado el contrato, podría incorporarse al mismo en el momento en que aquélla tuviera lugar una adenda en que el colegiado encomendase al Colegio el envío de un escrito similar en que se hiciera constar el hecho de la cesación del colegiado en el ejercicio de la profesión y la posibilidad de solicitar el traslado de la historia a otro facultativo".* Y en caso de fallecimiento *"…podría encomendarse al Colegio la prestación de un servicio adicional mediante el cual al conocerse por la Corporación el fallecimiento del colegiado, ésta se pusiera, en nombre de aquél en contacto con los pacientes para comunicarles el hecho mismo del fallecimiento de su médico, recordarles la posibilidad de ejercicio de sus derechos, en los términos que ya aparecen recogidos en el contrato (con las aclaraciones ya efectuadas en cuanto al acceso a los datos por los herederos) y plantearles la posibilidad de que soliciten el traslado de su historia clínica a otro colegiado en activo si así lo estimasen conveniente".*

Respecto a la gestión de la información sanitaria, encontramos en el quinto párrafo del Real Decreto sobre receta médica y órdenes de dispensación que: *"La receta médica y las órdenes de dispensación como documentos normalizados, suponen un medio fundamental para la transmisión de información entre los profesionales sanitarios y una garantía para el paciente, que posibilita un correcto cumplimiento terapéutico y la obtención de la eficiencia máxima del tratamiento, ello sin perjuicio de su papel como soporte para la gestión y facturación de la prestación farmacéutica que reciben los usuarios del Sistema Nacional de Salud".* De hecho, y según dice el séptimo párrafo, *"este real decreto se dicta en desarrollo de los artículos 19.6 y 77.6 y 8 de la Ley sobre el uso de los medicamentos, y al amparo de las competencias exclusivas que*

en materia de legislación sobre productos farmacéuticos y bases para la coordinación general de la sanidad atribuye al Estado el artículo 149.1.16.ª de la Constitución".

Esta norma ha sido sometida, entre otros organismo al informe previo de la AEPD y viene a regular los conceptos relevantes y el ámbito de aplicación del mismo, así como los requisitos comunes de las recetas médicas públicas y privadas, así como el sistema de la receta médica electrónica oficial del Sistema Nacional de Salud y la orden de dispensación hospitalaria pública y privada, además de la conservación y custodia de la receta médica. Así lo establece el octavo párrafo del Real Decreto que nos ocupa *"de conformidad con lo dispuesto en los artículos 37 h) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, y 5 b) del Estatuto de la Agencia, aprobado por Real Decreto 428/1993, de 26 de marzo, la presente norma ha sido sometida al informe previo de la Agencia Española de Protección de Datos".*

Entrando de lleno en el articulado de esta norma se establecen tres conceptos fundamentales, el de receta médica, el de orden de dispensación y el de orden de dispensación hospitalaria, en los que se apoya gran parte del texto. Todos ellos se definen como documentos sanitarios, que es necesario gestionar, y en los que los profesionales sanitarios expenden medicamentos a los pacientes, a través de las farmacias, en el último de los casos por farmacéuticos y pudiendo obtenerse también en botiquines dependientes de las farmacias; en los dos primeros casos será en farmacias ya sean hospitalarias, como en el segundo de los casos o no hospitalaria como en el primero.

Por la importancia de estos conceptos, en necesario es necesario citar el artículo primero que los define de la siguiente forma: *"A los efectos de este real decreto, se entenderá por: a) Receta médica: la receta médica es el documento de carácter sanitario, normalizado y obligatorio mediante el cual los médicos,*

odontólogos o podólogos, legalmente facultados para ello, y en el ámbito de sus competencias respectivas, prescriben a los pacientes los medicamentos o productos sanitarios sujetos a prescripción médica, para su dispensación por un farmacéutico o bajo su supervisión, en las oficinas de farmacia y botiquines dependientes de las mismas o, conforme a lo previsto en la legislación vigente, en otros establecimientos sanitarios, unidades asistenciales o servicios farmacéuticos de estructuras de atención primaria, debidamente autorizados para la dispensación de medicamentos. b) Orden de dispensación hospitalaria: la orden de dispensación hospitalaria para pacientes no ingresados es el documento de carácter sanitario, normalizado y obligatorio para la prescripción por los médicos, odontólogos y podólogos de los servicios hospitalarios, de los medicamentos que exijan una particular vigilancia, supervisión y control, que deban ser dispensados por los servicios de farmacia hospitalaria a dichos pacientes. c) Orden de dispensación: la orden de dispensación, a la que se refiere el artículo 77.1, párrafo segundo de la Ley sobre el uso de los medicamentos, es el documento de carácter sanitario, normalizado y obligatorio mediante el cual los profesionales enfermeros, en el ámbito de sus competencias, y una vez hayan sido facultados individualmente mediante la correspondiente acreditación, contemplada en la disposición adicional duodécima de la referida ley, indican o autorizan, en las condiciones y con los requisitos que reglamentariamente se establezcan, la dispensación de medicamentos y productos sanitarios por un farmacéutico o bajo su supervisión, en las oficinas de farmacia y botiquines dependientes de las mismas o, conforme a lo previsto en la legislación vigente, en otros establecimientos sanitarios, unidades asistenciales o servicios farmacéuticos de estructuras de atención primaria, debidamente autorizados para la dispensación de medicamentos".

Todas estas recetas, para ser correctamente gestionadas, deberán llevar obligatoriamente un mismo formato y datos

necesarios consistentes en datos del paciente, del prescriptor, del medicamento y otros datos como las fechas de prescripción y dispensación o el número de orden. Así lo marca dentro del capítulo segundo dedicado a los requisitos comunes de las recetas médicas públicas y privadas, el artículo 3.1, el cual establece que *"las recetas médicas, públicas o privadas, pueden emitirse en soporte papel, para cumplimentación manual o informatizada, y en soporte electrónico, y deberán ser complementadas con una hoja de información al paciente, de entrega obligada al mismo, en la que se recogerá la información del tratamiento necesaria para facilitar el uso adecuado de los medicamentos o productos sanitarios prescritos".*

Fijando a continuación en su punto segundo que el prescriptor deberá consignar en la receta y en la hoja informativa del paciente, ciertos datos necesarios para que este documento sea válido, en primer lugar *"a) Datos del paciente: 1.º El nombre, dos apellidos, y fecha de nacimiento. 2.º En las recetas médicas de asistencia sanitaria pública, el código de identificación personal del paciente, recogido en su tarjeta sanitaria individual, asignado por su Servicio de Salud o por las Administraciones competentes de los regímenes especiales de asistencia sanitaria. En el caso de ciudadanos extranjeros que no dispongan de la mencionada tarjeta, se consignará el código asignado en su tarjeta sanitaria europea o su certificado provisional sustitutorio (CPS) o en el formulario europeo de derecho a la asistencia que corresponda, o el número de pasaporte para extranjeros de países no comunitarios. En todo caso se deberá consignar, asimismo, el régimen de aportación que corresponda al paciente. 3.º En las recetas médicas de asistencia sanitaria privada, el número de DNI o NIE del paciente. En el caso de que el paciente no disponga de esa documentación se consignará en el caso de menores de edad el DNI o NIE de alguno de sus padres o, en su caso, del representante legal, y para ciudadanos extranjeros el número de pasaporte".*

En segundo lugar *“b) Datos del medicamento: 1.º Denominación del/los principio/s activo/s. 2.º Denominación del medicamento si se trata de un medicamento biológico o el profesional sanitario prescriptor lo considera necesario desde un punto de vista médico, siempre de conformidad con lo establecido en la Ley sobre el uso de los medicamentos. En tal caso, en la receta se justificará brevemente el uso del nombre comercial. 3.º Dosificación y forma farmacéutica y, cuando proceda, la mención de los destinatarios: lactantes, niños, adultos. 4.º Vía o forma de administración, en caso necesario. 5.º Formato: número de unidades por envase o contenido del mismo en peso o volumen. 6.º Número de envases o número de unidades concretas del medicamento a dispensar. 7.º Posología: número de unidades de administración por toma, frecuencia de las tomas (por día, semana, mes) y duración total del tratamiento. Los datos referidos en los epígrafes 5.º y 6.º sólo serán de obligada consignación en las recetas médicas emitidas en soporte papel. En las recetas médicas emitidas en soporte electrónico sólo serán de cumplimentación obligada por el prescriptor cuando el sistema electrónico no los genere de forma automática”.*

En tercer lugar *“c) Datos del prescriptor: 1.º El nombre y dos apellidos. 2.º Datos de contacto directo (correo electrónico y teléfono o fax, estos con el prefijo internacional). 3.º Dirección profesional, incluyendo la población y el nombre de España. La referencia a establecimientos, instituciones u organismos públicos solamente podrá figurar en las recetas médicas oficiales de los mismos. 4.º Cualificación profesional. 5.º Número de colegiado o, en el caso de recetas médicas del Sistema Nacional de Salud, el código de identificación asignado por las Administraciones competentes y, en su caso, la especialidad oficialmente acreditada que ejerza. En las recetas médicas de la Red Sanitaria Militar de las Fuerzas Armadas, en lugar del número de colegiado podrá consignarse el número de Tarjeta Militar de Identidad del facultativo. Asimismo se hará constar, en su caso, la especialidad oficialmente acreditada que ejerza. 6.º La*

firma será estampada personalmente una vez cumplimentados los datos de consignación obligatoria y la prescripción objeto de la receta. En las recetas electrónicas se requerirá la firma electrónica, que deberá producirse conforme con los criterios establecidos por la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. En las recetas del Sistema Nacional de Salud, los datos del prescriptor, a los que se refieren los epígrafes 3.º y 5.º se podrán consignar además de forma que se permita la mecanización de dichos datos por los servicios de salud y las mutualidades de funcionarios". Y en cuarto lugar "d) Otros datos: 1.º La fecha de prescripción (día, mes, año): fecha del día en el que se cumplimenta la receta. 2.º La fecha prevista de dispensación (día, mes, año): fecha a partir de la cual corresponde dispensar la receta, en el caso de dispensaciones sucesivas de tratamientos crónicos o medicamentos de dispensación renovable. 3.º N.º de orden: Número que indica el orden de dispensación de la receta, en el caso de dispensaciones sucesivas de tratamientos crónicos o medicamentos de dispensación renovable. Los datos referidos en los epígrafes 2.º y 3.º solo serán de obligada consignación en las recetas médicas en soporte papel. Además de los datos señalados en los epígrafes anteriores, en su caso, deberá ser consignado el visado por las Administraciones sanitarias, de acuerdo con el Real Decreto 618/2007, de 11 de mayo, por el que se regula el procedimiento para el establecimiento, mediante visado, de reservas singulares a las condiciones de prescripción y dispensación de los medicamentos. En caso de recetas electrónicas, el visado se realizará en la forma prevista en el artículo 8.7 de este real decreto. En las recetas médicas en soporte papel y en la hoja de información al paciente para el caso de receta electrónica se incluirá una cláusula que informe al paciente en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal".

Pero además, el punto tercero de este comentado artículo tres, establece que *“la hoja de información para el paciente estará diferenciada de la receta pudiendo ser separable de la misma, o bien constituir un impreso independiente, donde el prescriptor podrá relacionar todos los medicamentos y productos sanitarios prescritos, facilitando al paciente la información del tratamiento completo y el diagnóstico, si procede, a juicio del prescriptor”.* Y su punto quinto que *“todos los datos e instrucciones consignados en la receta médica deberán ser claramente legibles, sin perjuicio de su posible codificación adicional con caracteres ópticos. Las recetas médicas no presentarán enmiendas ni tachaduras en los datos de consignación obligatoria, a no ser que éstas hayan sido salvadas por nueva firma del prescriptor”.* De modo que tanto correcta cumplimentación y consignación de los datos como la copia de la receta y su legibilidad, podrían también considerarse en el apartado de calidad de datos sanitarios en lo que se refiere a este documento, la receta.

IV. PRINCIPIOS GENERALES DE LA PROTECCIÓN DE DATOS.

Antes de entrar a analizar las razones que llevan a la creación de una base de datos médicos, es necesario partir de unos principio que deben respetarse cuales quiera que sean estos fundamentos.

La LOPD en sus artículos 4 a 12 habla de calidad, información, consentimiento, datos protegidos, datos relativos a la salud, seguridad de datos, deber de secreto, comunicación de datos y acceso a los datos por cuenta de terceros.

Y por su parte, el reglamento de desarrollo de dicha Ley Orgánica en los artículos 8 a 22 lo hace en relación a la calidad de los datos, el consentimiento para el tratamiento de los datos y deber de información y la figura del encargado del tratamiento.

Encontramos conceptos coincidentes entre ambas normas, (calidad, información, consentimiento, comunicación y acceso a datos por cuenta de terceros) y otros que regula el RLOPD y que la LOPD cita como principios (datos protegidos, datos relativos a la salud, seguridad de datos y deber de secreto).

IV.1.CALIDAD:

El Convenio 108, ya establecía en su artículo 5 que *"los datos de carácter personal que sean objeto de un tratamiento automatizado: a) se obtendrán y trataran leal y legítimamente; b) se registraran para finalidades determinadas y legitimas, y no se utilizaran de una forma incompatible con dichas finalidades; c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado; d) serán exactos y si fuera necesario puestos al día; e) se conservaran bajo una forma que permita la identificación de las personas concernidas durante un*

periodo de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado".

El autor Unai Aberasturi Gorriño, ha expresado en relación a estos principios que *"la virtualidad de estos derechos va más allá de su consideración como facultades indispensables de control sobre los datos de cada uno. Su relevancia deriva también de la importancia que tienen a la hora de asegurar la calidad de la información y garantizar así, que la finalidad que se persigue con el tratamiento de datos, pueda verse cumplida. En el ámbito sanitario se ha repetido en numerosas ocasiones que es fundamental guardar la calidad de la información. No hay un buen servicio sin información de calidad"*[218]*.*

El DCM también se expresa de una forma más general en su artículo 7.2, el cual recoge que *"el médico, principal agente de la preservación de la salud, debe velar por la calidad y la eficiencia de su práctica, principal instrumento para la promoción, defensa y restablecimiento de la salud".* De aquí podemos deducir, que la calidad de la atención sanitaria, presupone una calidad en el tratamiento de los datos personales relativos a la salud, de modo que dentro de la calidad sanitaria estaría incluida la calidad en el tratamiento de datos.

Respecto a la calidad de los datos, Aberasturi Gorriño ha manifestado que *"…la LOPD, cuando regula los principios que determinan la «calidad de los datos», se refiere a los principales criterios que tiene que seguir todo tratamiento de datos. Parece, por lo tanto, que el contenido de estos preceptos se refiere a auténticos principios básicos de la protección de datos"*[219]*.*

Hay un sector doctrinal que se manifiesta en referencia a la informatización de los mismos sosteniendo que *"…la informatización*

[218] ABERASTURI GORRIÑO, Unai: *"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 281.

219 Ibídem. Pág. 74.

de la HC tendrá que estar sustentada en todo momento en los preceptos de la LOPD. Además se debe tener en cuenta la Recomendación núm. 5. El cumplimiento de los principios de calidad de los datos personales, lealtad, exactitud y veracidad de la información serán junto con la confidencialidad y las medidas de seguridad de nivel alto los pilares básicos a la hora de informatizar la historia clínica…"[220]*.*

Otros manifiestan por su parte que *"la calidad de la relación del médico con los pacientes incide decisivamente en la calidad de la asistencia sanitaria y la imagen de los médicos y de la Medicina ante la sociedad. La normativa legal sobre la relación médico-paciente, es extensa y exigente pero no suficiente para agotar el ideal de perfección que se exige desde la ética al trato mutuo médico-paciente"*[221]*.*

Y hay otra parte de la doctrina que mantiene en este sentido que *"la relación médico-paciente establece entre ellos un doble vínculo. Uno científico y humano y otro patrimonial que es un auténtico intercambio de bienes de diferente naturaleza"*[222]*.*

Además, el jurista Mariano Avilés, manifiesta en Diario Médico, respecto de la calidad y cohesión del sistema sanitario que "…el sistema sanitario actual tiene un modelo difícil de ser encuadrado en un Estado de Derecho cuyo objetivo sea el interés general. Estamos ante un Estado de intereses particularistas donde la cohesión brilla por su ausencia y la calidad será analizada en función del lugar

220 JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso: "La protección de datos personales en el ámbito sanitario". Editorial Aranzadi, Navarra 2002. Pág. 79.

221 BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: *"Manual de ética y deontología médica".* Organización Médica Colegial de España, 2012. Pág. 45.

222 Ibídem.

donde tenga lugar la prestación y dependiendo de la capacidad normativa cedida por el Estado a favor de los intereses territoriales"[223].

El artículo 42 de la Ley de Investigación Biomédica, establece en su punto segundo, en referencia al Banco Nacional de Líneas Celulares que: *"El Banco Nacional de Líneas Celulares promoverá la calidad y seguridad de los procedimientos sobre los que ejerza su competencia, mantendrá la confidencialidad de los datos y demás exigencias respecto de las actuaciones que lleve a cabo, de acuerdo con lo establecido en la Ley 14/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida, y en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y contemplará en sus actuaciones los principios de precaución, proporcionalidad y ausencia de lucro".*

Así mismo el artículo 45 de esta norma establece unos principios rectores específicos que se suman a las garantías establecidas en el título I de esta Ley, y que son los siguientes: *"a) Accesibilidad y equidad: deberá garantizarse la igualdad en el acceso a los análisis genéticos sin consideraciones económicas y sin requisitos previos relativos a posibles opciones personales. b) Protección de datos: se garantizará el derecho a la intimidad y el respeto a la voluntad del sujeto en materia de información, así como la confidencialidad de los datos genéticos de carácter personal. c) Gratuidad: todo el proceso de donación, cesión, almacenaje y utilización de muestras biológicas tanto para los sujetos fuente como para los depositantes, deberá estar desprovisto de finalidad o ánimo de lucro. Los datos genéticos de carácter personal no podrán ser utilizados con fines comerciales. d) Consentimiento: deberá obtenerse previamente el consentimiento escrito del sujeto fuente o en su caso de sus representantes legales para el tratamiento de*

[223] AVILÉS, Mariano: "La buena administración y la cuestión sanitaria". Diario Médico, viernes 16 de julio de 2010. Año XIX, Núm.4155, Pág 9.

muestras con fines de investigación o de datos genéticos de carácter personal. e) Calidad de los datos: los datos obtenidos de los análisis genéticos no podrán ser tratados ni cedidos con fines distintos a los previstos en esta Ley".

La Directiva sobre protección en el tratamiento de datos, respecto de las condiciones generales para la licitud del tratamiento de datos personales, establece en el capítulo segundo los principios relativos a la calidad de los datos que deberán ser adecuados, actualizados, y correctamente conservados para la identificación de los interesados durante el periodo necesario para el cumplimiento de los fines para los que sean recogidos, y siendo siempre tratados de forma lícita y leal, con fines concretos y legítimos, no siendo incompatible el tratamiento posterior si estos son históricos, estadísticos o científicos. Así su artículo 6.1 establece que *"los Estados miembros dispondrán que los datos personales sean: a) tratados de manera leal y lícita; 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 de los interesados 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".*

Hay que tener siempre presente que *"en el ámbito de la protección de datos deben respetarse siempre unos principios que se refieren a que estos sean pertinentes y no excesivos, a la confidencialidad de los mismos, a que estos sean recabados con el consentimiento del interesado y que la recogida no se haga por medios fraudulentos, desleales o ilícitos, que asistan en todo caso a los afectados los derechos de acceso, rectificación, cancelación y oposición, además del derecho de información previo a la recogida, directamente relacionado con los fines para los que fueron prestados"* [224].

Todo esto debe ser visto desde la perspectiva estatal, mirando hacia las comunidades autónomas, así, según publica Diario Médico: *"El Ministerio de Sanidad y Política Social se mantiene como elemento vertebrador del Sistema Nacional de Salud (SNS) y el Consejo Interterritorial, del que forman parte el propio ministerio y las autonomías, se reúne de forma periódica para favorecer la cohesión en la sanidad del país, pero las regiones se han desarrollado de forma dispar"*[225].

De modo que de forma generalizada, existe un consenso sobre la necesidad de unos parámetros que rijan en materia de protección de datos, veámoslos.

IV.1.a. Principios:

Respecto de la calidad de los datos médicos, cabría decir que siempre tendrían que tener los requisitos legales en materia de protección de datos, ya que, por el ámbito y circunstancias en que se recogen siempre van a ser adecuados, pertinentes y no excesivos, siendo su finalidad determinada, explícita y legítimas en relación a su obtención; según marca el 4.1 LOPD *"los datos de*

[224] VIDAL RASO, Marta: *"Entorno de la Ley de Protección de Datos de Carácter Personal"*. Revista Top Franquicias Nº 7, Madrid, 2003. Págs. 52-53.

[225] JUÁREZ, José María: "Un sistema en constante evolución". Diario Médico, jueves 22 de julio de 2010. Año XIX, Núm.4159, Pág 1-Especial "Quien es Quien Sanidad.

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". Todo ello, dado que hablamos en el sector sanitario y de cada paciente en concreto.

En este sentido manifiesta el profesor Sánchez de Diego "*Cuantos más datos se tengan del paciente mejor"*; de este modo, el principio de proporcionalidad sería plano, ya que todos los datos referentes al proceso asistencial del paciente, serán adecuados, pertinentes y no excesivos, sin que puedan utilizarse para finalidades distintas de aquellas que motivaron su recogida, no considerándose estas, el tratamiento con fines históricos, estadísticos o científicos, como se ha expuesto anteriormente en referencia al art. 4.2 LOPD[226].

Y este es otro de los pilares de mi estudio, ya que puede considerarse científica la utilización posterior de la historia clínica disociada, por otros profesionales sanitarios, de modo que su uso sería lícito en relación al modelo que propongo en la parte final de este estudio. Todo ello en consonancia con el ya citado artículo 4.5 LOPD, según el cual *"…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"*. Es necesario acudir aquí a las leyes sectoriales, en este caso las sanitarias, para averiguar durante cuánto tiempo deben ser conservados, teniendo en cuenta que la finalidad común y principal para todos los pacientes es su curación.

En muchos casos la necesidad podría durar toda la vida del paciente, incluso habría que valorar la protección de datos de las personas fallecidas, por ejemplo en enfermedades hereditarias, cuya

[226] SÁNCHEZ DE DIEGO, Manuel: *"cuantos más datos se tengan del paciente mejor".* Diario Médico, martes 17 febrero 2009. Pág.24.

información pudiera servir para posteriores generaciones. Y sigue diciendo este artículo que *"…no serán conservados de forma que permita la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados"*, de modo que los datos deben ser disociados cuando acabe la finalidad para la que fueron recogidos, es decir, la curación del paciente. Concluyendo el quinto apartado con una excepción a la disociación de los datos, en atención a sus valores históricos, estadísticos o científicos, siempre y cuando se establezca reglamentariamente un procedimiento para mantener su integridad, que debería hacerse con más cautela en el sector médico por la naturaleza y sensibilidad de los datos que se tratan.

Sobre la disociación de datos de los individuos, hay una parte de la doctrina que se expresa, en concreto en relación a los datos médicos *"respecto a los datos personales y en contra del criterio seguido por la LOPD, merece la pena destacar que no se considerará identificable a un individuo –no considerándose sus datos como personales a los efectos de la Recomendación- siempre que la identificación, aun siendo posible, requiera una cantidad de tiempo y de medios no razonables. Tal precisión es significativa sobre todo en el ámbito de los datos médicos disociados. Es evidente que cualquier colección de datos previamente disociados, pueden volver a asociarse –y dejar de ser anónimos- si se conservan ambas tablas y se conoce o descifra la clave o relación que permita tal reasociación. Pero si el tiempo y los medios necesarios para descifrar esa clave no son razonables, los datos no podrán ser considerados, por el mero hecho de su posible reasociación, personales a los efectos de la recomendación nº5 de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados Miembros sobre Protección de Datos Médico"*[227]. Así

[227] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso: *"La*

mismo,*"…la Recomendación también permite la recogida y tratamiento de los datos a otros profesionales (administradores de archivos) siempre que queden igualmente sujetos a normas de confidencialidad comparables a las que pesan sobre el personal sanitario…"*[228].

Sobre si los datos sanitarios son adecuados o no, Unai Aberasturi Gorriño ha manifestado que *"en cuanto a la adecuación o idoneidad, en general, este criterio simplemente requiere que el medio que se emplea se entienda, atendiendo a presupuestos empíricos, como adecuado para la consecución del fin que se pretende. Se trata de averiguar si a ojos de la realidad conocida, en base a criterios puramente científicos, el medio utilizado puede servir para alcanzar la finalidad perseguida, siempre y cuando el medio sea realizable"*[229].

Habría que pensar en qué casos, la recogida desproporcionada de información, pudiese perjudicar la protección de los datos personales del paciente, siempre con las debidas medidas de seguridad. Por ejemplo si un menor no quisiera revelar su orientación sexual, en un proceso en el que existen afecciones infecciosas graves para él y su pareja, de la que posiblemente, tampoco quisiera revelar su identidad.

Respecto a la proporcionalidad en materia sanitaria, *"la inclusión del principio de proporcionalidad en el ordenamiento español es un hecho incuestionable. El sistema de control de los límites a los derechos fundamentales que supone el principio de proporcionalidad tal como hoy se conoce, recala en el ordenamiento*

---

protección de datos personales en el ámbito sanitario". Editorial Aranzadi, Navarra 2002. Pág. 37.

[228] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso: *"La protección de datos personales en el ámbito sanitario"*. Editorial Aranzadi, Navarra 2002. Pág. 39.

[229] ABERASTURI GORRIÑO, Unai: *"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 95.

español principalmente a través de su aplicación por el TEDH y por el TJUE"[230]*.*

Cabe recordar en este punto, que el RLOPD, habla de datos relativos a la salud pasada, presente y futura del paciente. Podría pensarse en relación con este planteamiento, que el dato futuro no es dato, sino mera conjetura, sospecha o consecuencia de algo que se conoce en la actualidad, pero no un dato cierto al cien por cien. Aunque pensándolo bien, hay enfermedades que con el paso de los años, y con la experiencia comparativa de cientos de casos iguales, se "*sabe*", que acabarán degenerando en ciertas patologías, con lo que tendríamos el dato cierto. Pero también es cierto que sería precipitado asegurar un dato futuro, ya que este puede llegar a no ser cierto nunca, por una muerte repentina del paciente. De modo que sería muy necesaria la información pasada y presente de un paciente, pero quedaría en entredicho la información futura.

Encontramos además una sentencia del Tribunal Superior de Justicia de Madrid, en cuyos fundamentos de derecho se establece que: *"En fecha 26 de enero de 1998, LA MERCANTIL "A" disponía en su fichero automatizado "Clientes" de datos relativos a la salud de Dña.....(esposa del inicialmente denunciante), no habiéndose acreditado que la entidad aseguradora dispusiese del consentimiento previo de la afectada para la automatización de tales datos. Por otra parte, tales datos, así como otros relativos a su número de DNI, domicilio, profesión, características antropométricas, antecedentes familiares y hábitos de consumo, no eran necesarios en tal fecha para la tramitación de una solicitud de seguro presentada a esta entidad por la afectada en diciembre de 1990"*[231]*.* Datos absolutamente excesivos según lo expuesto.

[230] Ibídem. Pág. 94.

[231] Sentencia del Tribunal Superior de Justicia de Madrid de 29-01-2003. Sala de lo contencioso-administrativo. Sección novena. Tratamiento de datos especialmente protegidos sin las debidas garantías previstas en la Ley.

Y en relación a lo ya referido sobre el 4.2 en relación a que las finalidades para las que se recogen los datos no sean incompatibles, puede referirse aquí el artículo segundo de la ley del paciente, en el que se regulan la autonomía de la voluntad y la intimidad; así establece su punto primero que *"la dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica"*. El previo consentimiento, como establece su punto segundo, regula que *"toda actuación en el ámbito de la sanidad requiere, con carácter general, el previo consentimiento de los pacientes o usuarios. El consentimiento, que debe obtenerse después de que el paciente reciba una información adecuada, se hará por escrito en los supuestos previstos en la Ley".* El derecho a una información adecuada y a la libre decisión, se contiene en el punto tercero, estableciéndose que *"el paciente o usuario tiene derecho a decidir libremente, después de recibir la información adecuada, entre las opciones clínicas disponibles".* La opción de negativa al tratamiento, como recoge el punto cuarto contempla que *"todo paciente o usuario tiene derecho a negarse al tratamiento, excepto en los casos determinados en la Ley. Su negativa al tratamiento constará por escrito".* Sobre el deber de aportar datos reales el punto quinto establece que *"los pacientes o usuarios tienen el deber de facilitar los datos sobre su estado físico o sobre su salud de manera leal y verdadera, así como el de colaborar en su obtención, especialmente cuando sean necesarios por razones de interés público o con motivo de la asistencia sanitaria".* Los deberes de información y documentación clínica, los recoge su punto sexto, regulando que *"todo profesional que interviene en la actividad asistencial está obligado no sólo a la correcta prestación de sus técnicas, sino al cumplimiento de los deberes de información y de documentación*

clínica, y al respeto de las decisiones adoptadas libre y voluntariamente por el paciente". Así como la debida reserva de la información sobre la que punto séptimo contempla que *"la persona que elabore o tenga acceso a la información y la documentación clínica está obligada a guardar la reserva debida".* Todos ellos como principios básicos de esta norma, pudiendo observarse una gran similitud con muchos de los principios recogidos en la actual normativa de protección de datos personales.

La información, consentimiento y comunicación de datos del afectado, así como sus derechos, la seguridad, la conservación de los mismos y los derechos de los afectados, son puntos que se recogen en la Recomendación nº R (97), de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre Protección de Datos Médicos, al igual que la regulación del flujo transfronterizo de datos, cuestiones después desarrollados por la normativa en materia de protección de datos de nuestro país. En cambio hay un par de puntos que regula este texto y no han sido desarrollados específicamente en nuestra normativa relativa a protección de datos personales. Me refiero a los datos de los niños no nacidos, que gozarán de la misma protección que los datos médicos de un menor. Igualmente los datos genéticos solo podrán usarse en beneficio del afectado o de la investigación científica. Aunque sí se habla de información genética, como datos de nivel alto, y de los datos relativos a los menores de edad en el reglamento de desarrollo de la LOPD. Todos estos puntos serán desarrollados a continuación en los apartados correspondientes.

Respecto de la finalidad, encuentra Aberasturi Gorriño una carencia, *"las normas que regulan la materia de protección de datos no entran a definir el principio de finalidad. No obstante, puede entenderse que cuando la LOPD se refiere a la finalidad está hablando de los objetivos que se persiguen con la manipulación de los datos, al porqué concreto del tratamiento. En definitiva, la*

finalidad se refiere a los motivos en que se fundamenta la utilización de los datos por parte del que será el responsable del fichero, a la actividad a la que dirige dicho responsable la manipulación de la información"[232]*.*

"A priori, cualquier dato solicitado en referencia a una atención sanitaria, sería adecuado, pertinente y no excesivo, ya que se referirían a un proceso asistencial concreto y sería necesaria la mayor información posible para su gestión, según se ha dicho anteriormente. No podrían utilizarse para finalidades incompatibles para las que se recogieron, quedando fuera de esta consideración los fines históricos, estadísticos o científicos"[233]*.* En cambio, *"en el sector sanitario es difícil referirnos a datos exactos y puestos al día, que es otro de los requisitos de calidad exigidos, ya que precisamente el cuerpo humano está en constante cambio. De modo que serán exactos y puestos al día en la medida en que se vayan conociendo los resultados de las pruebas y el paciente informe a su médico, de esa forma se mantendrán las historias clínicas vivas y actuales"*[234]*.* También *"en el tratamiento de un paciente es posible que un dato en principio inconexo y que pudiera parecer irrelevante pueda tener importancia posteriormente, por ello es difícil referirnos a información desproporcionada en la recogida de datos"*[235]*.*

Pero en cambio se hace difícil imaginar un dato exacto y puesto al día, como marca el art. 4.3 LOPD, ya que precisamente en la medicina muchas veces no se conocen los datos exactos; de este modo la medicina sería casi automática, pero el cuerpo humano, que es lo que estudia la medicina, está en constante cambio, y no es posible conocer muchas veces la evolución de los pacientes a

[232] ABERASTURI GORRIÑO, Unai, *"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013.Pág. 76.

[233] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

[234] Ibídem.

[235] Ibídem.

tiempo real, porque pensemos que muchos de los pacientes que acuden a tratarse a un centro sanitario siguen sus tratamientos o evolución fuera de los centros sanitarios, a los que acuden puntualmente a revisarse, en cuyo momento si se conocen datos más exactos sobre la evolución del paciente, pero lógicamente esto no sería posible de forma constante. De modo que los datos serán puestos al día en la medida en la medida en que se vayan conociendo los resultados de la evolución del estado clínico en el que se encuentren los pacientes.

Así, si *"los datos de carácter personal registrados, resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados…"*, según marca el art. 4.4 LOPD. Con esto serán los profesionales sanitarios los encargados de mantener la historia clínica actualizada, con la ayuda ineludible del paciente que les debe trasladar sus sensaciones, para que estos con las pruebas necesarias actualicen este documento. Pensemos que un médico puede actualizar en un informe de un paciente con artritis reumatoide, el valor de una PCR, marcador de inflamación, pero no saber, si el paciente no se lo traslada, si el paciente siente dolor en las articulaciones con esos resultados.

Muchas veces, la falta de información, puede llevar a la desprotección de los datos personales. Si partimos de una situación en que el profesional médico no puede conocer los antecedentes, ya sea porque el paciente se encuentra inconsciente, por que se trate de un menor que no los conoce, o bien porque se trate de una persona que no entiende el idioma, esto puede generar un posible diagnóstico en el que puedan aparecer datos inexactos o erróneos. Por ejemplo, la información clínica sobre un hígado, que aparezca alterada en una persona adulta que llega inconsciente, podría hacer pensar en una afición del paciente al alcoholismo o a un fallo multifuncional, pero sin embargo, esto puede deberse a alguna otra

causa genética o funcional. En este sentido, la falta de información podría dar lugar a la aparición de datos inexactos o erróneos, asociados a un paciente, con lo que se estaría violando el principio de calidad de los datos personales.

Cuando un paciente entra en una UCI inconsciente, el personal sanitario, intenta recabar de la familia toda la información posible sobre esa persona, como hábitos de vida, alimentación, aficiones, etc., para intentar asociar a sus dolencias una causa, y así poder actuar de la forma más adecuada.

Por este motivo, los datos personales es necesario que sean conocidos por el personal sanitario y puestos al día, para que la información clínica sea lo más íntegra posible.

Por otro lado, el 4.7 de la LOPD establece que *"se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos".* Aunque en el sector sanitario se haga difícil imaginar esta situación.

El artículo 8 del RLOPD, se dedica en pleno a esta cuestión, empezando por establecer en su punto primero que *"los datos de carácter personal deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos".* El punto segundo concreta así mismo que *"los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento".* Y el punto tercero limita imponiendo que *"los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos".* No obstante, el punto cuarto sigue puntualizando *"sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".* El punto quinto de este artículo se refiere, por su parte, a la actualización de los datos y establece que *"Los datos de carácter personal serán exactos y puestos al día de forma que*

respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste". De modo que los datos deben ser correctos y actuales, utilizarse para una finalidad concreta y tratados de forma lícita para cumplir los requisitos de calidad respecto de su tratamiento.

IV.1.b. Fines históricos, estadísticos y científicos:

Ya se ha venido comentando a lo largo del estudio, y se seguirá haciendo de forma puntual la utilización de los datos con estos fines, y que no conviene traer a este punto de forma conjunta porque perderían el interés para el que se refirieron.

Lo que si se hará en este apartado es apuntar que el artículo 9.1del RLOPD regula esta materia y establece que *"no se considerará incompatible, a los efectos previstos en el apartado 3 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos".* Puntualizando el segundo párrafo de este artículo que *"para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias"*.

No obstante, el punto segundo de este artículo recoge que *"por vía de excepción a lo dispuesto en el apartado 6 del artículo anterior, la Agencia Española de Protección de Datos o, en su caso, las autoridades de control de las comunidades autónomas podrán, previa solicitud del responsable del tratamiento y conforme al procedimiento establecido en la sección segunda del capítulo VII del título IX del presente reglamento, acordar el mantenimiento íntegro*

de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas a las que se refiere el apartado anterior". Recordemos que este artículo 8.6 se citó ya en el apartado II.2 de este estudio al abordar el tema de la disociación de los datos.

Hay una parte de la doctrina que se ha manifestado respecto de la utilización de los datos médicos con fines científicos observando que *"cuando por motivos de publicación científica o formación continuada, así como investigación científica de la salud, etc., se tenga que utilizar la HC y al objeto de conservar la confidencialidad de la documentación clínico-sanitaria, no deberá contener aquellos datos que permitan la identificación del paciente, y en caso de ser necesario, será imprescindible su autorización expresa y por escrito, siendo autorizada también esta publicación por la dirección del hospital"*[236].

Por su parte Noelia de Miguel, ve un aspecto negativo en cuanto a protección de datos se refiere en el ámbito de la investigación afirmado que existe *"…el debate ya iniciado con la propuesta de lo que sería la Directiva 95/46/CE, en el que se ha dejado escuchar las voces de los investigadores, reiterando que un excesivo sistema de protección de datos personales puede tener una incidencia negativa para el desarrollo científico"*[237]*.* Esta opinión es compartida por el personal sanitario que trabaja en los hospitales y ve las trabas que supone al avance de la ciencia, sobre todo en relación a la disociación de datos de los sujetos.

El DCM recoge en su artículo que *"la historia clínica se redacta y conserva para la asistencia del paciente. Es conforme a la Deontología Médica el uso del contenido de la historia clínica para su*

[236] CURRIEL HERRERO, J y ESTÉVEZ LUCAS, J: "*Manual para la gestión sanitaria y de la historia clínica hospitalaria*". Editores Médicos, Madrid, 2000. Pág. 77.

[237] DE MIGUEL SÁNCHEZ, Noelia: "*Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público*". Tirant lo Blanch, Valencia, 2004. Pág. 60.

análisis científico, estadístico y con fines docentes y de investigación, siempre que se respete rigurosamente la confidencialidad de los pacientes y las restantes disposiciones de este Código que le puedan afectar".

La Ley General de Sanidad, establecen su artículo 10.7, como un derecho del paciente *"a ser advertido de si los procedimientos de pronóstico, diagnóstico y terapéuticos que se le apliquen pueden ser utilizados en función de un proyecto docente o de investigación, que, en ningún caso, podrá comportar peligro adicional para su salud. En todo caso será imprescindible la previa autorización y por escrito del paciente y la aceptación por parte del médico y de la Dirección del correspondiente Centro Sanitario".*

Esta misma norma, marca en su artículo 68 que *"los centros hospitalarios desarrollarán, además de las tareas estrictamente asistenciales, funciones de promoción de salud, prevención de las enfermedades e investigación y docencia, de acuerdo con los programas de cada Área de Salud, con objeto de complementar sus actividades con las desarrolladas por la red de atención primaria".*

E igualmente establece en su artículo 69.2 respecto a la calidad de la atención sanitaria que *"la evaluación de la calidad de la asistencia prestada deberá ser un proceso continuado que informará todas las actividades del personal de salud y de los servicios sanitarios del Sistema Nacional de Salud. La Administración sanitaria establecerá sistemas de evaluación de calidad asistencial oídas las Sociedades científicas sanitarias. Los Médicos y demás profesionales titulados del centro deberán participar en los órganos encargados de la evaluación de la calidad asistencial del mismo".*

El artículo 50 de la Ley de Investigación Biomédica, que trata el acceso a los datos genéticos por personal sanitario, establece en su punto segundo que *"los datos genéticos de carácter personal sólo podrán ser utilizados con fines epidemiológicos, de salud pública, de investigación o de docencia cuando el sujeto interesado haya*

prestado expresamente su consentimiento, o cuando dichos datos hayan sido previamente anonimizados". Y el punto tercero dice que *"en casos excepcionales y de interés sanitario general, la autoridad competente, previo informe favorable de la autoridad en materia de protección de datos, podrá autorizar la utilización de datos genéticos codificados, siempre asegurando que no puedan relacionarse o asociarse con el sujeto fuente por parte de terceros".*

Respecto de los fines históricos de la información médica hay que atender a lo que establece una corriente doctrinal, que considera que *"la historia clínica documental contiene una serie de procesos que por la patología atendida, las características del paciente, el valor históricos de la tipología del documento, etc., constituyen con el tiempo una historia clínica con material de interés científico y cultural para las ciencias de la salud. Son el fondo histórico documental del archivo de historia clínica"*[238]*.* A este mismo respecto sigue expresando este sector que *"…la carátula de la HC que pasa a fondo histórico documental contiene los siguientes elementos. Nº de HC, fecha de inclusión y las siguientes rúbricas: «dado el valor científico y documental, esta HC está custodiada en el archivo de HC denominado Fondo Histórico documental>, <nunca se destruirá: su conservación está sometida a los criterios establecidos a nivel de comisión de HC del centro»"*[239]*.*

El artículo 23 de esta Ley del paciente hace referencia a la obligatoriedad de cumplimentación por parte de los profesionales de unos datos complementarios sobre información técnica, estadística y administrativa que se encuentren en relación con los procesos en los que intervengan, estableciendo que *"los profesionales sanitarios, además de las obligaciones señaladas en materia de información clínica, tienen el deber de cumplimentar los protocolos, registros, informes, estadísticas y demás documentación asistencial o*

[238] CURRIEL HERRERO, J y ESTÉVEZ LUCAS, J: "*Manual para la gestión sanitaria y de la historia clínica hospitalaria*". Editores Médicos, Madrid, 2000. Pág. 93.

[239] Ibídem. Pág. 95.

administrativa, que guarden relación con los procesos clínicos en los que intervienen, y los que requieran los centros o servicios de salud competentes y las autoridades sanitarias, comprendidos los relacionados con la investigación médica y la información epidemiológica".

IV.1.c. Supuestos que legitiman el tratamiento o la cesión de datos:

La LOPD no regula conjuntamente estos supuestos, solo lo hace en el artículo 27 con el título "comunicación de la cesión de datos", recogiendo en su punto primero que *"el responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario".* Y en su punto segundo que *"la obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley".* Así se regula la exención de consentimiento en la comunicación de datos, que será expuesta a continuación en el apartado correspondiente.

Sin embargo el artículo 10 del RLOPD bajo el título "*supuestos que legitiman el tratamiento o cesión de los datos*", regula estas dos acciones a realizar con los datos personales y las condiciones que deben darse para que pueda producirse cada una de ellas. El artículo 10.1 del RLOPD establece recto del consentimiento para el tratamiento de los datos personales que *"los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello".*

Pero como en casi todo hay excepciones, el punto segundo posibilita el tratamiento de los datos del interesado sin su consentimiento cuando *"…lo autorice una norma con rango de ley o*

una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes: El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre…", o cuando *"…el tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas".*

Igualmente el punto tercero establece otra excepción en este sentido que *"los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando: a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario. b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento. c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre".*

Respecto de la cesión de datos, el punto cuarto del artículo 10 establece los requisitos que deben darse y establece que *"será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando: a) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. b) La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones*

autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente. c) La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos: Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos. Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra. La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias".

Y en concreto respecto de los datos especialmente protegidos, entre los que se encuentran los datos de salud, establece que este artículo que "*los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre…",* recogiendo su último párrafo que *"…en particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud".*

Karla Cantoral ha manifestado en este sentido que *"en el derecho comparado tenemos que en la normativa de protección de datos tanto España como los demás países europeos han optado mayoritariamente por categorías cerradas de datos sensibles, a las que otorgan una tutela reforzada frente a los datos ordinarios…"*[240].

Respecto a los datos de salud, Aberasturi Gorriño ha manifestado que *"desde una interpretación restrictiva el derecho a proteger la salud sería la facultad de exigir al Estado una acción dirigida a proteger la salud individual de cada uno. Desde un punto*

[240] CANTORAL DOMÍNGUEZ, Karla: "Derecho *de protección de datos personales en la salud*". Editorial Novum, MEXICO D.F., 2012. Pág. 86.

de vista más amplio este derecho abrazaría medidas tanto individuales como colectivas. Si bien el concepto de salud ha ido cambiando constantemente de contenido, hoy día parece que hay acuerdo en asumir la interpretación amplia"[241]*.* Además, este autor establece que *"El principio de pertinencia pone en relación los datos que se recogen y la finalidad concreta para la que se recogen: tiene que haber una coherencia o relación entre dicho medio y el fin. Esta coherencia se traduce en la necesidad de que el tratamiento de datos que se vaya a llevar a cabo para cumplir con el objetivo de proteger la salud afecte en la menor medida posible al derecho fundamental a la autodeterminación informativa. El tratamiento por un agente que no sea el titular de unos datos supone siempre una afección al derecho a la autodeterminación informativa. Esta afección necesariamente ha de estar justificada"*[242]*.*

El Real Decreto Ley sobre sostenibilidad del sistema sanitario establece a este respecto en su nuevo artículo tres bis, punto tercero, segundo párrafo que añade el artículo 1.2, que *"… el Instituto Nacional de la Seguridad Social podrá tratar los datos obrantes en los ficheros de las entidades gestoras y servicios comunes de la Seguridad Social o de los órganos de las administraciones públicas competentes que resulten imprescindibles para verificar la concurrencia de la condición de asegurado o beneficiario. La cesión al Instituto Nacional de la Seguridad Social de estos datos no precisará del consentimiento del interesado".* Y en el antepenúltimo párrafo que *"el Instituto Nacional de la Seguridad Social tratará la información a la que se refieren los dos párrafos anteriores con la finalidad de comunicar a las administraciones sanitarias competentes los datos necesarios para verificar en cada momento que se mantienen las condiciones y los requisitos exigidos para el reconocimiento del derecho a la asistencia sanitaria, sin*

[241] ABERASTURI GORRIÑO, Unai: *"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 87.

[242] Ibídem. Pág. 92.

precisar para ello del consentimiento del interesado". Y por fin afirma en el último de sus párrafos que *"Cualquier modificación o variación que pueda comunicar el Instituto Nacional de la Seguridad Social deberá surtir los efectos que procedan en la tarjeta sanitaria individual»".* De modo que todo este cruce de información, finalmente quedará registrado en las tarjetas sanitarias, pudiendo convertir a este documento en un arma de doble filo; provechosa porque contiene toda nuestra información sanitaria, pero peligrosa si cae en manos de extraños que puedan manipularla y darle un uso indebido, quedando los datos personales al descubierto, lo cual tiene directa relación con la confidencialidad.

Así mismo, el precepto que nos ocupa se refiere a la protección de datos personales, y literalmente su artículo cuatro, que añade el 94 ter, dice en su punto primero que *"el Instituto Nacional de la Seguridad Social o, en su caso, el Instituto Social de la Marina, podrá tratar los datos obrantes en los ficheros de las entidades gestoras y servicios comunes de la Seguridad Social y de las entidades que colaboran con las mismas que resulten imprescindibles para determinar la cuantía de la aportación de los beneficiarios en la prestación farmacéutica. Dicho tratamiento, que no requerirá el consentimiento del interesado, se someterá plenamente a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y sus disposiciones de desarrollo".* Este tratamiento, previa cesión de datos, que no requiere el consentimiento del interesado, se somete plenamente a la normativa existente en materia de protección de datos. Y sigue diciendo el punto segundo de este artículo que *"del mismo modo, y con la finalidad a la que se refiere el apartado anterior, la administración competente en materia tributaria podrá comunicar al Instituto Nacional de la Seguridad Social, o, en su caso, el Instituto Social de la Marina, sin contar con el consentimiento del interesado, los datos que resulten necesarios para determinar el nivel de renta requerido. Igualmente, los órganos de las*

administraciones públicas que resulten competentes para determinar la concurrencia de los requisitos establecidos para la exención de la aportación previstos en el apartado 8 del artículo 94 bis de esta ley, podrán comunicar esta circunstancia al Instituto Nacional de la Seguridad Social o, en su caso, el Instituto Social de la Marina, sin contar con el consentimiento del interesado".

Así, y con la misma carencia de consentimiento, la Administración Tributaria requerirá al INSS los datos indispensables para determinar el nivel de renta de los usuarios, sin hacer referencia a la cuantía concreta de las rentas, comunicando así el dato relativo a nivel de aportación, para incorporarlo a la tarjeta sanitaria de los pacientes, de acuerdo a la normativa que regula las recetas médicas y órdenes de dispensación. De esta forma, los sistemas de información aportarán datos de las adquisiciones y de la facturación, que serán recogidos de forma manual e informática, para su comunicación a diferentes organismos dependientes del Sistema Nacional de Salud. El punto tercero de este 94 ter acaba diciendo que *"el Instituto Nacional de la Seguridad Social o, en su caso, el Instituto Social de la Marina, comunicará al Ministerio de Sanidad, Servicios Sociales e Igualdad y éste, a su vez, a las demás administraciones sanitarias competentes el dato relativo al nivel de aportación que corresponda a cada usuario de conformidad con lo establecido en la normativa reguladora de las recetas médicas y órdenes de dispensación. En ningún caso, dicha información incluirá el dato de la cuantía concreta de las rentas. Los datos comunicados de conformidad con lo dispuesto en el párrafo anterior serán objeto de tratamiento por la administración sanitaria correspondiente a los solos efectos de su incorporación al sistema de información de la tarjeta sanitaria individual»".* Habrá que estar en este punto también a lo establecido sobre la transmisión de datos entre Administraciones.

De modo que, cada ejercicio, la administración tributaria comunicará al órgano de la Administración pública encargado del reconocimiento de la condición de asegurado o beneficiario, los datos de sus niveles de renta necesarios para determinar los citados porcentajes de aportación de los servicios de la cartera común que lo requieran, respetándose siempre los principios establecidos en la normativa de protección de datos. De este modo lo establece la disposición adicional tercera de este Real Decreto que nos ocupa, dedicado a la cesión de información tributaria, según marca su disposición adicional tercera, *"la administración tributaria facilitará, dentro de cada ejercicio, al órgano de la administración pública responsable del reconocimiento y control de la condición de asegurado o de beneficiario del mismo, los datos relativos a sus niveles de renta en cuanto sean necesarios para determinar el porcentaje de participación en el pago de las prestaciones de la cartera común de servicios sujetas a aportación. En el tratamiento de estos datos la administración cesionaria deberá respetar la normativa sobre protección de datos de carácter personal".*

Artículo 69.6 de la Ley de Investigación Biomédica establece que *"La cesión de muestras podrá ir acompañada de la información clínica asociada, en cuyo caso los datos estarán protegidos según lo dispuesto en la Ley de Autonomía del Paciente y la Ley de Protección de Datos de Carácter Personal".*

IV.2. INFORMACIÓN:

El Convenio 108 ya establecía en su artículo 8 que *"cualquier persona deberá poder: a) conocer la existencia de un fichero, automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la resistencia habitual o el establecimiento principal de la autoridad controladora del fichero; b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible; c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente convenio; d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo".*

Y el artículo 9 establece una serie de restricciones; en su punto primero se establece que *"no se admitirá excepción alguna en las disposiciones de los artículos 5, 6 y 8 del presente convenio, salvo que sea dentro de los límites que se definen en el presente artículo".* Y en el segundo que *"será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente convenio cuando tal excepción, prevista por la ley de la parte, constituya una medida necesaria en una sociedad democrática: a) para la protección de la seguridad del estado, de la seguridad pública, para los intereses monetarios del estado o para la represión de infracciones penales; b) para la protección de la persona concernida y de los derechos y libertades de otras personas"* Especificando el punto tercero que *"podrán preverse por la ley restricciones en el ejercicio de los derechos a que se refieren los párrafos b), c) y d) del artículo 8 para*

los ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas".

De igual modo la LOPD regula este principio de información en el 5.1, que será analizado unas líneas más adelante en comparación con lo que dice la normativa sanitaria sobre la información médica. Y es que, es imprescindible en el sector sanitario, tanto para el médico, como para el paciente, más para este último, que exista un acto de información correcta y completa tanto de los datos personales, como de los datos médicos, en definitiva de los datos personales relativos a la salud.

El capítulo II de la ley del paciente regula el derecho a la información asistencial, así como quienes son los titulares del mismo. El derecho a la información asistencial aparece en concreto en el artículo 4, y es distinto del derecho de acceso a la historia clínica, por idéntico que parezca. En el primer caso, según marca su punto 1: *"Los pacientes tienen derecho a conocer, con motivo de cualquier actuación en el ámbito de su salud, toda la información disponible sobre la misma, salvando los supuestos exceptuados por la Ley. Además, toda persona tiene derecho a que se respete su voluntad de no ser informada"*, y en el segundo, el artículo 18.1 de la LAP, que será comentado más adelante en el apartado correspondiente, recoge el derecho de acceso del paciente a su historia médica.

Surge aquí además otra discrepancia entre estos dos artículos, ya que el 4.1 sigue diciendo que *"la información, que como regla general se proporcionará verbalmente dejando constancia en la historia clínica, comprende, como mínimo, la finalidad y la naturaleza de cada intervención, sus riesgos y sus consecuencias"*, y en el 18.1 existe el derecho de acceso a la historia clínica, también regulado en la Ley de protección de datos en su artículo 15, cuyo punto primero

establece que *"el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos".* La distinción está sin duda en los conceptos, en el primero de los casos se refiere a la información clínica, concepto más restringido que el segundo, la historia clínica integrada por diversa información, ambos conceptos están regulados en el artículo 3 de la ley del paciente y comentados en apartados anteriores de este trabajo. El abanico de posibilidades en la forma de obtención de la información que se observa en los distintos artículos, lo encontramos también en el citado artículo 15.2 de la LOPD, el cual establece en su punto segundo, respecto al derecho de acceso, que *"la información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos".*

Respecto al comentado derecho de acceso a la historia clínica es ampliamente comentado por una parte de la doctrina según quien lo ejercite, manifestando este sector que *"…de la aplicación de la LGS se desprende el derecho-deber de acceso a los datos contenidos en la HC por los responsables de los centros, para satisfacer el derecho del paciente a la información y documentación requerida, así como para información estadística sanitaria, adoptando las medidas precisas para garantizar los deberes relativos a la intimidad personal y familiar y al secreto de quien, en virtud de sus competencias, tengan acceso a la HC"*[243]*. "Respecto al derecho de acceso a la historia clínica por parte de los pacientes, tanto el art. 10.5.8.11, 61, RD 63/95 de 20 de enero, sobre ordenación de prestaciones sanitarias del Sistema Nacional de Salud*

[243] SAMPRÓN LÓPEZ, David: "*Los derechos del paciente a través de la información de la historia clínica*". Edisofer, Madrid, 2002. Pág. 69.

apartado 5, así como la LOPD en su art. 15, acreditan tal derecho"[244]*.* Así, *"respecto al derecho de acceso por parte de el investigador y el docente, parece que tanto la LGS arts. 104,18.5, 68 ,10.4, y 61 y la LOPD arts 4.2,7.3 y 8 lo contemplan, así como la normativa autonómica, y el grupo de expertos que lo considera necesario"*[245]*.* Y respecto a las consideraciones del Grupo de Expertos surgido en el año 1997 respecto de la necesidad de regular los derechos de los pacientes en materia de información y documentación clínica, este mismo autor expresa que *"el grupo de expertos considera que el acceso a la información clínica de una persona debe justificarse por motivos de asistencia sanitaria del titular de la misma, y que el paciente tendrá acceso de manera ordenada y según la norma existente al efecto en el centro, señalando el grupo de expertos que en este apartado podría surgir conflicto con la LOPD"*[246].

Respecto al contenido hay también diferencias entre el 15.1 de la LOPD y el 4.1 de la ley del paciente, ya que la primera establece, según se acaba de comentar que el acceso al origen y comunicaciones de sus datos será gratuito. Y la segunda, según podemos leer unos renglones más arriba y de forma mucho más específica, referida al ámbito sanitario, contempla la finalidad, naturaleza, riesgos y consecuencias de las intervenciones.

En cuanto a la forma, parecen coincidir algo más ambas normas, ya que el 4.2 de la Ley del paciente establece que *"la información clínica forma parte de todas las actuaciones asistenciales, será verdadera, se comunicará al paciente de forma comprensible y adecuada a sus necesidades y le ayudará a tomar decisiones de acuerdo con su propia y libre voluntad"*, y el ya comentado 15.2 de la LOPD, hemos visto que habla de información

[244] SAMPRÓN LÓPEZ, David: "*Los derechos del paciente a través de la información de la historia clínica*". Edisofer, Madrid, 2002. Pág. 71.

[245] Ibídem. Pág. 78.

[246] Ibídem. Pág. 77.

que se pueda leer y ser entendida. De modo que aquí la pequeña diferencia es que la información sea real, como plus establecido por la ley del paciente. Pero encontramos también en el artículo 4.3 de la LOPD que *"los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado".* Así, habría casi plena coincidencia en este punto. Hay que especificar, que el derecho de acceso que tiene el paciente a sus datos, será en cierta forma limitado, según marca el punto tercero del artículo 15 de la LOPD, *"el derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes".*

Y entre este embrollo de comparaciones que intentan aclarar cómo debe ser el contenido y la forma de obtención de la información, con más o menos acuerdo entre las normas analizadas, tenemos que atender a las excepciones establecidas en el 18.3 de la ley del paciente arriba mencionadas y que merecen un análisis aparte. Este artículo establece que *"el derecho al acceso del paciente a la documentación de la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas".*

De modo que si hace unos renglones sacábamos en claro que el paciente, que es el titular del derecho a la información, salvando los casos establecidos en el art 5.4 de la ley paciente, podía tener conocimiento de la naturaleza y origen de la información sobre su salud, así como su finalidad, recogiéndose que *"el derecho a la información sanitaria de los pacientes puede limitarse por la existencia acreditada de un estado de necesidad terapéutica. Se*

entenderá por necesidad terapéutica la facultad del médico para actuar profesionalmente sin informar antes al paciente, cuando por razones objetivas el conocimiento de su propia situación pueda perjudicar su salud de manera grave. Llegado este caso, el médico dejará constancia razonada de las circunstancias en la historia clínica y comunicará su decisión a las personas vinculadas al paciente por razones familiares o de hecho".

También el punto tercero del artículo 5 establecía limitaciones en caso de incapacidad *"cuando el paciente, según el criterio del médico que le asiste, carezca de capacidad para entender la información a causa de su estado físico o psíquico, la información se pondrá en conocimiento de las personas vinculadas a él por razones familiares o de hecho. El paciente será informado, incluso en caso de incapacidad, de modo adecuado a sus posibilidades de comprensión, cumpliendo con el deber de informar también a su representante legal",* pero incluso en esta circunstancia, y según establece el punto segundo de este mismo artículo, *"el paciente será informado, incluso en caso de incapacidad, de modo adecuado a sus posibilidades de comprensión, cumpliendo con el deber de informar también a su representante legal".* No obstante la norma general regulada en el 5.1 fija que: *"El titular del derecho a la información es el paciente. También serán informadas las personas vinculadas a él, por razones familiares o de hecho, en la medida que el paciente lo permita de manera expresa o tácita".*

Tras la lectura de estos artículos vemos que esto será posible salvando los datos de terceros que consten en la historia clínica, así como las anotaciones subjetivas de los profesionales que atendieron en cada momento al paciente, o incluso de cualquier dato objetivo si ello va en detrimento de la salud del propio paciente. Si lo pensamos detenidamente podemos llegar al caso de que la mayor parte de nuestra propia historia clínica no tenemos derecho a conocerla, aún siendo los titulares de tales derechos de acceso y de información.

Una parte de la doctrina se expresa en este sentido manifestando que *"al médico prácticamente el único derecho que le queda es demostrar su inocencia y buena praxis, y sin poder vetar o limitar el acceso a una información contenida en la documentación clínica que él ha generado con la sana intención de no solo proporcionar la asistencia al paciente en ese episodio clínico, sino también facilitar una información muy útil para episodios posteriores del paciente*[247]*.* Matizando este mismo sector que *"es por eso, que el médico adopta una posición defensiva que contribuye tristemente a privar de riqueza la historia clínica, al no formular opiniones propias ni aplicar otros tratamientos, que dados los conocimientos científicos, podría muy bien aplicar"*[248]*.*

Por su parte, el CDM recoge en su artículo 19.5 que *"el médico tiene el deber de facilitar, al paciente que lo pida, la información contenida en su historia clínica y las pruebas diagnósticas realizadas. Este derecho del paciente quedaría limitado si se presume un daño a terceras personas que aportaron confidencialmente datos en interés del paciente. Las anotaciones subjetivas que el médico introduzca en la historia clínica son de su exclusiva propiedad".* Igualmente el artículo 20.1 del CDM establece que *"cuando proceda o el paciente lo solicita, es deber del médico proporcionar un informe o un certificado sobre la asistencia prestada o sobre los datos de la historia clínica. Su contenido será auténtico y veraz y será entregado únicamente al paciente, a la persona por él autorizada o a su representante legal"*. Y concluye el punto médico de este artículo, que *"están éticamente prohibidos los certificados médicos de complacencia".*

[247] SAMPRÓN LÓPEZ, David: "*Los derechos del paciente a través de la información de la historia clínica*". Edisofer, Madrid, 2002. Pág. 58.

[248] Ibídem.

Pero el propio paciente no es el único titular del derecho a la información, el artículo 6 de la ley del paciente establece que nuestros datos de salud pueden ser conocidos por la colectividad de los ciudadanos si suponen un riesgo para la salud pública, al regular el derecho a la información epidemiológica, según el cual *"los ciudadanos tienen derecho a conocer los problemas sanitarios de la colectividad cuando impliquen un riesgo para la salud pública o para su salud individual, y el derecho a que esta información se difunda en términos verdaderos, comprensibles y adecuados para la protección de la salud, de acuerdo con lo establecido por la Ley".* Y por supuesto, serán partícipes de la información aquellas personas autorizadas tácita o expresamente por el propio paciente, según acabamos de leer que establece 5.1 de esta misma norma.

Samprón López manifiesta al respecto que *"el controvertido aspecto de la titularidad de la Historia Clínica no está resuelto con la normativa existente a nivel estatal. Sin embargo, a través del derecho de uso y acceso tanto a la información como a los documentos contenidos en ella por el paciente, por el médico, por el centro, por el investigador y el docente, por la Administración sanitaria, por el Ministerio Fiscal, por los Jueces y Tribunales, y por otros centros en donde pudiera ser tratado el paciente, la atribución concreta del derecho de propiedad tiene una menor relevancia*".[249]

Noelia de Miguel ha opinado a este propósito que *"por desgracia sigue siendo usual que se piense que el propietario de los datos que se recogen en un fichero es el titular del fichero…"*[250], y es que el titular de los datos es siempre la persona a la que estos pertenecen y no quien los almacene, trate o recoja; otra cosa es la titularidad de los documentos en que estos datos se plasmen.

[249] SAMPRÓN LÓPEZ, David: "*Los derechos del paciente a través de la información de la historia clínica*". Edisofer, Madrid, 2002. Pág. 57.

[250] DE MIGUEL SÁNCHEZ, Noelia: "*Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público*". Tirant lo Blanch, Valencia, 2004. Pág. 14.

A propósito de la titularidad de la historia clínica otro sector doctrinal sostiene que *"…si el facultativo está trabajando bajo dependencia de un centro sanitario, la propiedad de la HC pertenecerá al centro sanitario sin perjuicio del derecho de acceso que ostenta el paciente, así como el médico o médicos que le asistan. Por otro lado es lógico que si un médico tiene su propia consulta privada, las HC de los pacientes a que asista, pertenezcan al mismo, ostentando igualmente el paciente el derecho de acceso a su HC"*[251].

Y es que en este sector, el sanitario, como en muchos, el profesional que realiza el trabajo de creación de la documentación, la siente como suya, cuando son muchos los factores que intervienen en la misma. A este aspecto hay que volver a citar a Samprón López: *"respecto al derecho de propiedad que se puede ostentar a favor del centro sanitario cuando e allí generada, se basa en que dicho centro pone los medios materiales para su creación, así como el diseño del soporte donde se contiene la misma. Además el centro, trata dicha historia, la custodia y retribuye a los profesionales que crean y actualizan la información y documentación de la Historia Clínica"*[252]. Y por otro lado, *"…la atribución del derecho de propiedad a favor del paciente tendría su fundamento principal en que es el paciente el origen de la historia clínica, y toda la información en ella contenida está referida al paciente, sin perjuicio de su utilización por el centro y por el médico que la crea y la actualiza. Sin embargo el paciente no tiene potestad para introducir ni quitar ningún dato de la Historia Clínica, ni para custodiarla"*[253].

---

[251] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso: "*La protección de datos personales en el ámbito sanitario*". Editorial Aranzadi, Navarra 2002. Pág. 73.

[252] SAMPRÓN LÓPEZ, David. "*Los derechos del paciente a través de la información de la historia clínica*". Edisofer, Madrid, 2002. Pág. 59.

[253] Ibídem.

El derecho a la información, nombrado desde la exposición de motivos, y citado en el ya comentado artículo 7.2 de la ley de calidad sanitaria, es regulado concretamente en el artículo 26 esta norma, en referencia a la Ley básica reguladora de la autonomía del paciente y de los derechos y obligaciones existentes en materia de información y documentación clínica. Así establece concretamente este último artículo en su punto primero que *"los servicios de salud informarán a la ciudadanía de sus derechos y deberes, de las prestaciones y de la cartera de servicios del Sistema Nacional de Salud, de los requisitos necesarios para el acceso a éstos y de los restantes derechos recogidos en la Ley básica reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica, así como de los derechos y obligaciones establecidos en la Ley General de Salud Pública y en las correspondientes normas autonómicas, en su caso".* Y concreta en su punto segundo que *"el Registro general de centros, establecimientos y servicios sanitarios del Ministerio de Sanidad y Consumo, de carácter público, permitirá a los usuarios conocer los centros, establecimientos y servicios, de cualquier titularidad, autorizados por las comunidades autónomas. Dicho registro se nutrirá de los datos proporcionados por los correspondientes registros de las comunidades autónomas".* De modo que, de acuerdo a esto, los ciudadanos recibiremos la información de nuestros derechos y deberes en materia sanitaria a través de los centros a los que acudamos, y previsiblemente, a través del personal que en ellos nos atienda, sea sanitario o de otra naturaleza, lo cual presupone también la formación de los mismos en esta materia.

Otro sector doctrinal manifiesta que *"el médico que realiza la historia, además de incluir los datos e informes del paciente y de los especialistas que han realizándolas pruebas complementarias, realiza una actividad intelectual para realizar un interrogatorio adecuado en la anamnesis del paciente, solicitar las pruebas diagnósticas que considera necesarias, elaborando un juicio*

diagnóstico, en base al razonamiento científico de los datos del paciente y sus conocimientos médicos, cuyos resultados son de exclusiva propiedad intelectual del médico que es su autor material"[254]*.* Pero este mismo sector doctrinal manifiesta que *"…el centro considera que a él le pertenece la HC en base a que proporciona el espacio físico y los medios instrumentales para que la relación médico-paciente llegue a término y la historia sea completa (Gisbert,J.A. y Castellano,M.1998)"*[255]*.*

Y es el artículo 53 el que establece que el Ministerio de Sanidad y Consumo garantizará un sistema en el que la información sea fluida entre las Administraciones sanitarias, informando a los ciudadanos sobre sus cuidados y los riesgos de no llevarlos, así como de los servicios de salud que se encuentran a su disposición, pudiendo sugerir cualquier cuestión al respecto. Y de esta forma lo expresa literalmente en su texto el punto primero del citado artículo, a propósito de la regulación del sistema de información sanitaria en el Sistema Nacional De Salud, estableciendo que *"el Ministerio de Sanidad y Consumo establecerá un sistema de información sanitaria del Sistema Nacional de Salud que garantice la disponibilidad de la información y la comunicación recíprocas entre las Administraciones sanitarias. Para ello en el seno del Consejo Interterritorial del Sistema Nacional de Salud se acordarán los objetivos y contenidos de la información".* Puntualizándose en el segundo párrafo de este precepto que *"el objetivo general del sistema de información sanitaria del Sistema Nacional de Salud será responder a las necesidades de los siguientes colectivos, con la finalidad que en cada caso se indica: a) Autoridades sanitarias: la información favorecerá el desarrollo de políticas y la toma de decisiones, dándoles información actualizada y comparativa de la situación y evolución del Sistema Nacional de Salud. b) Profesionales: la*

[254] CRIADO DEL RÍO, María Teresa y SEOANE PRADO, Javier: "*Aspectos médico-legales de la historia clínica"*. Colex, Madrid, 1999. Pág. 82.

[255] Ibídem. Pág. 85.

información irá dirigida a mejorar sus conocimientos y aptitudes clínicas. Incluirá directorios, resultados de estudios, evaluaciones de medicamentos, productos sanitarios y tecnologías, análisis de buenas prácticas, guías clínicas, recomendaciones y recogida de sugerencias. c) Ciudadanos: contendrá información sobre sus derechos y deberes y los riesgos para la salud, facilitará la toma de decisiones sobre su estilo de vida, prácticas de autocuidado y utilización de los servicios sanitarios y ofrecerá la posibilidad de formular sugerencias de los aspectos mencionados. d) Organizaciones y asociaciones en el ámbito sanitario: contendrá información sobre las asociaciones de pacientes y familiares, de organizaciones no gubernamentales que actúen en el ámbito sanitario y de sociedades científicas, con la finalidad de promover la participación de la sociedad civil en el Sistema Nacional de Salud". Concluye informando este artículo en su punto sexto que *"la cesión de los datos, incluidos aquellos de carácter personal necesarios para el sistema de información sanitaria, estará sujeta a la legislación en materia de protección de datos de carácter personal y a las condiciones acordadas en el Consejo Interterritorial del Sistema Nacional de Salud".* De modo que una vez más, vemos que como tónica general en la normativa sanitaria, se pide el respeto de la normativa de protección de datos.

Una parte de la doctrina define el sistema de información sanitaria de la siguiente forma *"Por sistema de información sanitaria se entiende, siguiendo a la OMS, todo sistema o mecanismo utilizado para la recopilación, procesamiento, análisis y transmisión de la información que se precisa para organizar los servicios sanitarios o centros asistenciales"*[256]*.*

El artículo 54 matiza que estos datos estarán en una *"red segura de comunicaciones"* para el intercambio de la información

[256]CURRIEL HERRERO, J y ESTÉVEZ LUCAS, J: "*Manual para la gestión sanitaria y de la historia clínica hospitalaria*", Editores Médicos, Madrid, 2000. Pág. 157.

exclusivamente sanitaria, que requerirá certificación electrónica, firma electrónica y cifrado, como medidas de seguridad de nivel alto establecidas en la actual legislación de protección de datos. Así lo expresa literalmente este precepto, el cual estipula que *"el Ministerio de Sanidad y Consumo, a través de la utilización preferente de las infraestructuras comunes de comunicaciones y servicios telemáticos de las Administraciones públicas, pondrá a disposición del Sistema Nacional de Salud una red segura de comunicaciones que facilite y dé garantías de protección al intercambio de información exclusivamente sanitaria entre sus integrantes. La transmisión de la información en esta red estará fundamentada en los requerimientos de certificación electrónica, firma electrónica y cifrado, de acuerdo con la legislación vigente. A través de dicha red circulará información relativa al código de identificación personal único, las redes de alerta y emergencia sanitaria, el intercambio de información clínica y registros sanitarios, la receta electrónica y la información necesaria para la gestión del Fondo de cohesión sanitaria, así como aquella otra derivada de las necesidades de información sanitaria en el Sistema Nacional de Salud".*

Con el fin de garantizar la correcta gestión de la información en todo el territorio nacional, el Ministerio de Sanidad y Consumo gestionará el intercambio de información necesario entre los distintos organismos de las comunidades autónomas, garantizando que el acceso a la historia clínica de los pacientes por parte de los profesionales que tengan que participar en este proceso, sea bajo los principios de calidad, confidencialidad e integridad, estableciendo para ello un procedimiento telemático de gestión de la información, respetando siempre lo establecido en la Ley de Protección de Datos y la Ley del Paciente. Así lo regula el artículo 56 de la Ley de calidad sanitaria, *"con el fin de que los ciudadanos reciban la mejor atención sanitaria posible en cualquier centro o servicio del Sistema Nacional de Salud, el Ministerio de Sanidad y Consumo coordinará los mecanismos de intercambio electrónico de información clínica y de*

salud individual, previamente acordados con las comunidades autónomas, para permitir tanto al interesado como a los profesionales que participan en la asistencia sanitaria el acceso a la historia clínica en los términos estrictamente necesarios para garantizar la calidad de dicha asistencia y la confidencialidad e integridad de la información, cualquiera que fuese la Administración que la proporcione. El Ministerio de Sanidad y Consumo establecerá un procedimiento que permita el intercambio telemático de la información que legalmente resulte exigible para el ejercicio de sus competencias por parte de las Administraciones públicas. El intercambio de información al que se refieren los párrafos anteriores se realizará de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en la Ley 41/2002, de 14 de noviembre".

Dependiente también del Ministerio de Sanidad y Consumo se crea el Instituto de Información Sanitaria encargado de vigilar el sistema de información sanitaria ya comentado, y que se establece en el artículo 58.1 de esta norma *"se creará el Instituto de Información Sanitaria, órgano dependiente del Ministerio de Sanidad y Consumo que desarrollará las actividades necesarias para el funcionamiento del sistema de información sanitaria establecido en el artículo 53"*, garantizándose en el punto cuarto de la misma, la seguridad y confidencialidad de los datos de acuerdo a la LOPD, que: *"El Instituto velará por la integridad y seguridad de los datos confiados, garantizando su confidencialidad con arreglo a lo dispuesto en la Ley Orgánica 15/1999".*

En el 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, hecho en Oviedo el 4 de abril de 1997 (CDHB- Convenio de Derechos Humanos y Biomedicina), el derecho a la información y la vida privada también son tenidos en cuenta; su artículo 10.1 establece que *"toda persona tendrá derecho a que se*

respete su vida privada cuando se trate de informaciones relativas a su salud". Y el 10.2 que *"toda persona tendrá derecho a conocer toda información obtenida respecto a su salud. No obstante, deberá respetarse la voluntad de una persona de no ser informada".* Y por último el punto tercero regula excepciones, al establecer que *"de modo excepcional, la ley podrá establecer restricciones, en interés del paciente, con respecto al ejercicio de los derechos mencionados en el apartado 2".* El genoma humano también es tenido en cuenta en esta norma prohibiéndose la discriminación a causa de la información genética en el artículo 11, donde *"se prohíbe toda forma de discriminación de una persona a causa de su patrimonio genético".*

La Declaración sobre derechos de los pacientes, se centra, respecto del derecho de información sobre los servicios sanitarios, en la identidad de los profesionales que atienden al paciente y su situación profesional, sobre el estado de salud concreto de los mismos, incluso resumido por escrito, si fuese necesario, adecuado a la capacidad de comprensión de cada paciente, que podrá elegir a la persona que la reciba, así como la reserva del personal sanitario a no comunicarla excepcionalmente, o el derecho del paciente a no recibirla o a recibir una segunda opinión. Concretamente dice el texto en su punto segundo que *"la información sobre los servicios sanitarios y cómo utilizarlos adecuadamente debe ser proporcionada al público para beneficio de todos a quienes concierne. Los pacientes tienen derecho a ser informados en detalle sobre su estado de salud, incluyendo los datos médicos sobre su estado; sobre los procedimientos médicos propuestos, junto a los riesgos potenciales y beneficios de cada procedimiento; sobre alternativas a los procedimientos propuestos, incluyendo el efecto de no aplicar un tratamiento; y sobre el diagnóstico, pronóstico y progreso del tratamiento. La información podrá ser ocultada a los pacientes de forma excepcional, cuando existan buenas razones para pensar que esta información les causaría un gran daño, sin ningún efecto*

positivo. La información debe ser comunicada al paciente de forma adecuada a su capacidad de comprensión, minimizando el uso de terminología técnica poco familiar. Si el paciente no habla el idioma común, debe buscarse a un intérprete para ayudarle. Los pacientes tienen derecho a no ser informados, según su petición explícita. Los pacientes tienen derecho a elegir a la persona, si así lo desean, a la que se debe informar en su lugar. Los pacientes deberían tener la posibilidad de obtener una segunda opinión. Cuando sean admitidos en un centro sanitario, los pacientes deberían ser informados de la identidad y estatus profesional de los profesionales de la salud que se están ocupando de ellos y de las reglas y rutinas que se aplicarán durante su estancia y cuidados. Los pacientes deberían poder solicitar y obtener un resumen escrito de sus diagnóstico, tratamiento y cuidados recibidos al ser dados de alta de un centro sanitario".

La Ley de calidad sanitaria, establece en su artículo 7.2, a propósito de las personas que reciban prestaciones de atención sanitaria del Servicio Nacional de Salud que, *"…tendrán derecho a la información y documentación sanitaria y asistencial de acuerdo con 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".*

La Recomendación sobre protección de datos médicos, regula en el punto quinto de su apéndice la información a los afectados, y dice literalmente en su punto primero que *"los afectados deben ser informados de los siguientes extremos: a. la existencia de un archivo que contiene sus datos médicos y el tipo de datos recogidos o que se van a recoger; b. el fin o fines para los que son o serán procesados; c. en su caso, el individuo u organismos de los que han sido o serán obtenidos; d. las personas u órganos a los que pueden ser comunicados y con qué fines; e. la posibilidad, si existe, de que el afectado niegue su consentimiento o retire el ya dado, y las consecuencias de tal cesación del consentimiento; f. la identidad del*

administrador del archivo y de su representante, si existe, así como las condiciones bajo las que se puede ejercer el derecho de acceso y de rectificación".

Estas exigencias, puede observarse que coinciden bastante con las establecidas en el 5.1 de la LOPD, según el cual *"los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".*

Si bien, la recomendación que nos ocupa, puntualiza en sus puntos posteriores el modo de informar, ya que en el 5.2 establece que *"se debe informar al afectado, como muy tarde, en el momento de recogerlos. Sin embargo, cuando los datos no se obtengan del afectado, se le debe comunicar tal recogida tan pronto como sea posible y, en una forma apropiada, la información a que hace referencia el Principio 5.1, salvo que claramente sea no razonable o impracticable, o salvo que el afectado haya recibido ya la información"*. En diferencia a la LOPD en la que se establece que la información tiene que ser previa, como se acaba de ver en el 5.1 de la LOPD. En cambio, y según sigue afinando el punto 5.3 de la recomendación *"la información al afectado será apropiada y adaptada a las circunstancias. La información se dará preferiblemente a cada uno de los afectados de forma individual".* Esto puede deducirse también del 5.1de la LOPD, aunque este

último no especifique si la información ha de hacerse necesariamente de forma individual.

Ante todos los extremos establecidos anteriormente, respecto de la información, por la recomendación, caben revocaciones según marca el punto 5.6 de su apéndice: *"Cabe hacer derogaciones a los principios 5.1, 5.2 y 5.3 en los siguientes casos: a. la información al sujeto de los datos puede restringirse si así lo dispone la ley y constituye una medida necesaria en una sociedad democrática: i. para prevenir un peligro real o reprimir un crimen. ii. por razones de salud pública; iii. para proteger al afectado y los derechos y libertades de otros; b. en emergencias médicas, los datos considerados necesarios para el tratamiento médico pueden recogerse previamente a la información".* Además, y dentro del apartado quinto del apéndice de la recomendación que nos ocupa, dedicado a la información a los afectados, su punto cuarto establece que *"antes de llevar a cabo un análisis genético, se debe informar al afectado sobre los objetivos del análisis y la posibilidad de hallazgos inesperados".* Y también el 5.5 regula la información a las personas incapacitadas, estableciendo que *"si el afectado es una persona legalmente incapacitada, incapaz de tomar una decisión libre y consciente, y la ley nacional no le permite actuar en su propia representación, la información se facilitará a la persona reconocida como legalmente habilitada para actuar en interés del afectado. Si una persona legalmente incapacitada es capaz de entender, se le debe informar antes de recoger o procesar sus datos".*

Así he manifestado en otras ocasiones que respecto de la información a los interesado, en materia sanitaria *"habría que empezar con el cumplimiento de la normativa de protección de datos en el momento de su recogida. El artículo 5.1 de la LOPD obliga a informar, de forma previa a la recogida de los datos, de modo expreso, preciso e inequívoco sobre la existencia del fichero de datos, su finalidad y los destinatarios de los mismos, así como de la*

identidad y dirección del responsable del fichero. Esto se ha de hacer, por un procedimiento "que permita acreditar su cumplimiento". Es decir, que este trámite habrá que realizarlo de forma clara, exacta y que no admita duda, si acudimos a las definiciones de estos adjetivos en el diccionario de la Real Academia Española. Habría además que conservar el soporte en el que conste, para lo que se podrán utilizar medios informáticos de almacenamiento. Es cierto que si de las circunstancias en que se recogen los datos y de la naturaleza de los mismos se deduce de forma clara la finalidad, no será necesario informar de una serie de extremos o advertencias al titular de los datos personales (artículo 5.3 LOPD). Esto podría resultar obvio en la recogida de los en el sector sanitario"[257]*. "Pero en cambio, la legislación sanitaria contempla como medio preestablecido de información el verbal, de modo que aquí podrían chocar las leyes sanitarias y de protección de datos, en el sentido en que no se conservaría el soporte que acredite dicha información, a no ser que se grabasen las conversaciones, cosa que no es habitual en este sector"*[258].

La Directiva sobre protección en el tratamiento de datos, regula por su parte, en la sección cuarta regula la información al interesado tanto si la información ha sido recabada de él como si no. Así el artículo 10 de la directiva establece que para la Información en caso de obtención de datos recabados del propio interesado que *"los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello: a) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del tratamiento de que*

[257] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos"*. Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

[258] Ibídem.

van a ser objeto los datos; c) cualquier otra información tal como: - los destinatarios o las categorías de destinatarios de los datos, - el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder, - la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado".

Y el artículo 11.1 de esta norma puntualiza que *"cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información que se enumera a continuación, salvo si el interesado ya hubiera sido informado de ello: a) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del tratamiento de que van a ser objeto los datos; c) cualquier otra información tal como: - las categorías de los datos de que se trate, - los destinatarios o las categorías de destinatarios de los datos, - la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado".* Recogiéndose en el segundo de este mismo artículo establece como excepción que *"las disposiciones del apartado 1 no se aplicarán, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente*

prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas".

La Ley de Investigación Biomédica recoge en varios de sus artículos el tema de la información. El 27.3 a propósito de la información de los resultados, establece que *"los investigadores deberán hacer públicos los resultados generales de las investigaciones una vez concluidas, atendiendo a los requisitos relativos a los datos de carácter personal a los que se refiere el artículo 5.5 de esta Ley y sin menoscabo de los correspondientes derechos de propiedad intelectual e industrial que se pudieran derivar de la investigación".* Como también se referirá más adelante en relación a la confidencialidad, el 5.5 establece que *"si no fuera posible publicar los resultados de una investigación sin identificar a la persona que participó en la misma o que aportó muestras biológicas, tales resultados sólo podrán ser publicados cuando haya mediado el consentimiento previo y expreso de aquélla".*

Respecto a la Información a los sujetos participantes en la investigación que se regula en el artículo 15, el punto 2d) establece que *"la información incluirá el propósito, el plan detallado, las molestias y los posibles riesgos y beneficios de la investigación. Dicha información especificará los siguientes extremos: d) Medidas para asegurar el respeto a la vida privada y a la confidencialidad de los datos personales de acuerdo con las exigencias previstas en la legislación sobre protección de datos de carácter personal".*

El artículo 47 regula en relación a la información, previa a la realización de análisis genéticos con fines de investigación en el ámbito sanitario que *"sin perjuicio de lo establecido en la legislación sobre protección de datos de carácter personal, antes de que el sujeto preste el consentimiento en los términos previstos en el artículo 48, deberá recibir la siguiente información por escrito: 1.º Finalidad del análisis genético para el cual consiente. 2.º Lugar de realización del análisis y destino de la muestra biológica al término*

del mismo, sea aquél la disociación de los datos de identificación de la muestra, su destrucción, u otros destinos, para lo cual se solicitará el consentimiento del sujeto fuente en los términos previstos en esta Ley. 3.º Personas que tendrán acceso a los resultados de los análisis cuando aquellos no vayan a ser sometidos a procedimientos de disociación o de anonimización. 4.º Advertencia sobre la posibilidad de descubrimientos inesperados y su posible trascendencia para el sujeto, así como sobre la facultad de este de tomar una posición en relación con recibir su comunicación. 5.º Advertencia de la implicación que puede tener para sus familiares la información que se llegue a obtener y la conveniencia de que él mismo, en su caso, transmita dicha información a aquéllos. 6.º Compromiso de suministrar consejo genético, una vez obtenidos y evaluados los resultados del análisis".

También se recoge el derecho a la información y derecho a no ser informado en el 49.1, el cual establece *que "el sujeto fuente será informado de los datos genéticos de carácter personal que se obtengan del análisis genético según los términos en que manifestó su voluntad, sin perjuicio del derecho de acceso reconocido en la legislación sobre protección de datos de carácter personal, que podrá suponer la revocación de la previa manifestación de voluntad libre otorgada".*

Y el artículo 59 regula la Información previa a la utilización de la muestra biológica, una vez realizados los análisis y, establece en su punto primero que *"sin perjuicio de lo previsto en la legislación sobre protección de datos de carácter personal, y en particular, en el artículo 45 de esta Ley, antes de emitir el consentimiento para la utilización de una muestra biológica con fines de investigación biomédica que no vaya a ser sometida a un proceso de anonimización, el sujeto fuente recibirá la siguiente información por escrito: a) Finalidad de la investigación o línea de investigación para la cual consiente. b) Beneficios esperados. c) Posibles*

inconvenientes vinculados con la donación y obtención de la muestra, incluida la posibilidad de ser contactado con posterioridad con el fin de recabar nuevos datos u obtener otras muestras. d) Identidad del responsable de la investigación. e) Derecho de revocación del consentimiento y sus efectos, incluida la posibilidad de la destrucción o de la anonimización de la muestra y de que tales efectos no se extenderán a los datos resultantes de las investigaciones que ya se hayan llevado a cabo. f) Lugar de realización del análisis y destino de la muestra al término de la investigación: disociación, destrucción, u otras investigaciones, y que en su caso, comportará a su vez el cumplimiento de los requerimientos previstos en esta Ley. En el caso de que estos extremos no se conozcan en el momento, se establecerá el compromiso de informar sobre ello en cuanto se conozca. g) Derecho a conocer los datos genéticos que se obtengan a partir del análisis de las muestras donadas. h) Garantía de confidencialidad de la información obtenida, indicando la identidad de las personas que tendrán acceso a los datos de carácter personal del sujeto fuente. i) Advertencia sobre la posibilidad de que se obtenga información relativa a su salud derivada de los análisis genéticos que se realicen sobre su muestra biológica, así como sobre su facultad de tomar una posición en relación con su comunicación. j) Advertencia de la implicación de la información que se pudiera obtener para sus familiares y la conveniencia de que él mismo, en su caso, transmita dicha información a aquéllos. k) Indicación de la posibilidad de ponerse en contacto con él/ella, para lo que podrá solicitársele información sobre el modo de hacerlo". Se hace necesario nombrar aquí que el artículo 45 de la LOPD se refiere a los tipos y cuantía de las sanciones que corresponden a las diferentes infracciones en materia de protección de datos.

Artículos que la LOPD prácticamente replica, en el ya citado 5.1 para los recogidos del interesado, y en el artículo 5.4 para aquellos recogidos de persona distinta del interesado, y el cual dice

literalmente que *"cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo".* Estos puntos recordemos que se refieren a la existencia de un fichero, finalidad y destinatarios de la información, al ejercicio de los derechos y a la identificación y localización del responsable del fichero.

No obstante, el 5.5 de la LOPD matiza que *"no será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten".*

Y por último hay que referir, que igualmente el CDM en su artículo 12.1, establece que *"el médico respetará el derecho del paciente a decidir libremente, después de recibir la información adecuada, sobre las opciones clínicas disponibles. Es un deber del médico respetar el derecho del paciente a estar informado en todas y cada una de las fases del proceso asistencial. Como regla general,*

la información será la suficiente y necesaria para que el paciente pueda tomar decisiones". Y sin duda, esa información debe ir referida al tratamiento de sus datos personales, ya que inevitablemente la información sanitaria va ligada a ellos.

Establece igualmente este código, respecto del tratamiento de los datos personales de los no capacitados para entender la información, ya sea por menores o por incapaces legalmente, que se encuentran igualmente contemplados en el artículo 13.1 del CDM, que *"cuando el médico trate a pacientes incapacitados legalmente o que no estén en condiciones de comprender la información, decidir o dar un consentimiento válido, deberá informar a su representante legal o a las personas vinculadas por razones familiares o de hecho".* Matizado por el 13.2, según el cual *"el médico deberá ser especialmente cuidadoso para que estos pacientes participen en el proceso asistencial en la medida que su capacidad se lo permita".*

A este respecto el artículo 14.2 de este mismo texto establece que *"el mayor de 16 años se considera capacitado para tomar decisiones sobre actuaciones asistenciales ordinarias".* Y el punto segundo de este artículo que *"la opinión del menor de 16 años será más o menos determinante según su edad y grado de madurez; esta valoración supone para el médico una responsabilidad ética".* Pero según marca el 14.3, *"En los casos de actuaciones con grave riesgo para la salud del menor de 16 años, el médico tiene obligación de informar siempre a los padres y obtener su consentimiento. Entre 16 y 18 años los padres serán informados y su opinión será tenida en cuenta".*

Como vemos se modula el deber de información de acuerdo a la edad y condiciones del menor, aunque no siempre, ya que el punto cuarto del artículo 14 dice lo siguiente *"cuando los representantes legales tomen una decisión que, a criterio del médico, sea contraria a los intereses del representado, el médico solicitará la intervención judicial".* Las condiciones en que debe darse

dicha información se encuentran igualmente recogidas en el artículo 15 del CDM que establece que *"el médico informará al paciente de forma comprensible, con veracidad, ponderación y prudencia. Cuando la información incluya datos de gravedad o mal pronóstico se esforzará en transmitirla con delicadeza de manera que no perjudique al paciente"* .Puntualizando el punto segundo de este artículo que *"la información debe transmitirse directamente al paciente, a las personas por él designadas o a su representante legal. El médico respetará el derecho del paciente a no ser informado, dejando constancia de ello en la historia clínica".*

Respecto de la información proporcionada a los menores de edad, Elena Urso manifiesta que *"…se adoptan también las cautelas necesarias para proporcionar la información adecuada sobre las condiciones de salud, describiendo la naturaleza y la duración de las terapias con lenguaje comprensible no sólo para los padres, sino también, si la edad lo permite, al niño. En el caso de los adolescentes, en cambio, se impone la obtención de su consentimiento, después de una completa información"*[259]*.*

IV.2.a. Generalidades:

Como se ha visto ampliamente, el artículo 5.1 LOPD obliga en la recogida de los datos, a la previa información a los interesados, de forma expresa, precisa e inequívoca, sobre la existencia del fichero de datos, su finalidad y los destinatarios de los mismos, así como de la identidad y dirección del responsable del fichero, eximiendo el punto 3 de este artículo 5, incluir en esta información el carácter obligatorio o facultativo a las preguntas planteadas, así como las consecuencias de la negativa a suministrar dichos datos, y la posibilidad de ejercitar los derechos de acceso, rectificación,

[259] Urso, Elena, traducción Torre, E: *"Infancia, adolescencia y derecho a la salud en el hospital: el papel clave de los derechos fundamentales"*. Revista europea de derechos fundamentales. ISSN 1699-1524. Núm. 14/2ºsemestre 2009. Páginas 183-229.

cancelación y oposición, si estos extremos pueden deducirse de forma clara, de las circunstancias en que se recogen los datos personales y la naturaleza de los mimos. Literalmente dice este artículo *"no será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban".* De modo que dicho lo anterior sobre la información al interesado, vemos que hay excepciones dependiendo de la obviedad de las circunstancias.

Teniendo en cuenta que la recogida de datos en un centro sanitario puede efectuarse de distintas formas, dependiendo, por ejemplo, de si el titular de los mismos se encuentra consciente en ese momento, o si corresponden a un menor o incapacitado; el caso es que habrá que respetar unos mínimos legales, anteponiendo siempre la salud del paciente.

Y respecto de la finalidad, para la cual los datos fueron recogidos, en el caso de los datos médicos, puede considerarse de forma general, la finalidad de la curación total del paciente, y no parcial, por lo que, en principio, no debería ser incompatible iniciar la investigación y el tratamiento de los datos del paciente en otro servicio o rama distinta a aquel por el que se acude al centro sanitario en primera instancia, si durante el proceso, se conocen datos de salud distintos, y que corresponden a otros servicios, siempre con la previa información al paciente. En cambio pueden existir incompatibilidades no relacionadas con las finalidades, pero sí con otro tipo de datos especialmente protegidos, como el origen racial, las creencias o la orientación sexual. El origen racial y la vida sexual podrían estar exentos de consentimiento por razones de interés general, incluso también los de salud, según el 7.3 LOPD, existiendo también la excepción sobre la necesidad de prevención y diagnóstico médicos del 7.6, con lo que se plantea una dualidad de excepciones.

IV.2.b. Supuestos especiales:

El artículo 19 del RLOPD, establece respecto del tema de la información que *"en los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre".* Esto obviamente en el ámbito sanitario solo podría producirse en el sector privado, ya que en el público no es nada habitual, y no me refiero al traslado de expedientes entre comunidades autónomas, ya que es finalmente el estado, el gestor nacional de todas ellas, aunque cada centro sanitario tenga, de forma independiente, registrados sus ficheros y elaborados sus documentos de seguridad, para manejarse en la operativa diaria.

Encaja aquí perfectamente el artículo publicado por el diario El País sobre la venta de empresas y las consecuencias del correspondiente traspaso de información, que debe ser informado a los usuarios para que manifiesten su consentimiento al respecto, ya que se trata de entidades diferentes, aunque su actividad sea la misma, cosa que no siempre ocurre. Así publica este diario que: *"La Agencia Española de Protección de Datos investigará de oficio la actuación de la empresa Stacks, que desarrolla el nuevo sistema informático de los 400 centros de salud de la región. La investigación de abre tras la venta de Stacks, que tendrá acceso a los datos médicos de seis millones de madrileños, a otra empresa dedicada a la venta de datos médicos a la industria farmacéutica"*[260].

[260] GÜEL, Oriol: "Protección de Datos investiga el nuevo sistema informático de los centros de salud". EL País, viernes 23 de febrero de 2007. Madrid. Pág. 31.

IV.2.c. Ejercicio de derechos:

El título III de la LOPD regula los derechos de las personas. Así, en primer lugar, respecto de la información que, de acuerdo al artículo 26 LOPD (buscar y referir en el inicio de los principios), todas las entidades tienen la obligación de registrar en la AEPD, el artículo 14 establece que *"cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita".*

Los derechos ARCO, de acceso, rectificación, cancelación y oposición, se encuentran también regulados en la LOPD. El RLOPD, por su parte, establece en el artículo 23 el carácter personalísimo de estos derechos. Su punto primero establece que *"los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado".* Y el segundo que *"tales derechos se ejercitarán: a) Por el afectado, acreditando su identidad, del modo previsto en el artículo siguiente. b) Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición. c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél".* Estableciendo el último párrafo de este artículo que *"Cuando el responsable del fichero sea un órgano de las Administraciones públicas o de la Administración de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante*

declaración en comparecencia personal del interesado". Y como norma general, aunque luego se especifica en cada uno de ellos, el 23.3 establece que *"los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél".*

Respecto del ejercicio de derechos, hay un sector doctrinal que ha manifestado que: *"El art. 6.1 LAESP «reconoce a los ciudadanos el derecho a relacionarse con las Administraciones públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la LRJ-PAC, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos»"*[261]*.*

El derecho de acceso se encuentra regulado en el artículo 15 de la LOPD, y aunque ya ha sido ampliamente comentado en apartados anteriores a propósito de la información a los interesados, en relación con otras normas, lo veremos aquí, puesto que es el apartado que le corresponde. Su punto primero establece que *"el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos".* Y el punto segundo por su parte regula que *"la información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada*

[261] RODOTA, Stefano, DUPRAT, Jean-Pierre, PIÑAR MAÑAS, José Luis, NIETO GARRIDO, Eva, HERNÁNDEZ CORCHETE, Juan Antonio: *"Transparencia, acceso a la información y protección de datos"*. Editorial Reus, S.A., Madrid, 2014. Pág. 111.

o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos". Es decir que será gratuito y a elección de cada persona la forma de ejercitarlo. Sin embargo, el punto tercero de este artículo establece una limitación, que *"el derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes"*. De modo que no podremos solicitarlo cuantas veces queramos sin más, lo cual tiene su lógica una vez conocidos los datos.

Es interesante señalar aquí, para ver la realidad de lo que ocurre en los centros sanitarios, la consulta que recoge el informe jurídico 0473/2012 de la AEPD, sobre el cobro de una contraprestación por la emisión de una copia de la historia clínica. Ante lo que la AEPD contesta que *"este derecho de acceso a la historia clínica particulariza, para el ámbito que le es propio, el derecho de acceso a los datos de carácter personal, que es uno de los derechos de las personas consagrados en el Título III LOPD y forma parte del contenido esencial de este derecho fundamental, considerando la Sentencia del Tribunal Constitucional 292/2000 y su desarrollo por la meritada ley orgánica.*

Así, el artículo 15 LOPD señala que *"el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos".* Y tras remitirse a la regulación reglamentaria para el desarrollo del procedimiento para ejercitar el derecho de acceso, el artículo 17 LOPD dispone*: "No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación".* Recogiendo además que *"por su parte, el Reglamento de desarrollo de la LOPD (RDLOPD) aprobado por Real Decreto 1720/2007 de 21 de diciembre consagra también este*

sistema de gratuidad, ni siquiera permitiendo el cobro de los gastos generados por el derecho de acceso, como las fotocopias, al señalar en su artículo 24.2: "Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición". Como bien dice la petición de informe, reitera el art. 24.3 RDLOPD que *"el ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan. No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado".*

Respecto al ejercicio del derecho de acceso, el informe jurídico 0162/2010 de la AEPD, establece que *"…si el centro sanitario consultante ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, aquél no responderá por los posibles riesgos que para la seguridad de la información pudieran derivarse de la elección".*

El RLOPD, por su parte, realiza una definición en el artículo 27.1: *"El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos"*; que parece tomar como patrón el 15.1 de la LOPD ya comentado. Y el 27.2 especifica que *"en virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento*

información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento. No obstante, cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos".

Y el artículo 28.1 del RLOPD, establece que *"al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero: a) Visualización en pantalla. b) Escrito, copia o fotocopia remitida por correo, certificado o no. c) Telecopia. d) Correo electrónico u otros sistemas de comunicaciones electrónicas. e) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable"*; parece reflejar igualmente, de forma más ampliada, el 15.2 de la LOPD arriba citado. No obstante, el 28.2 establece que *"los sistemas de consulta del fichero previstos en el apartado anterior podrán restringirse en función de la configuración o implantación material del fichero o de la naturaleza del tratamiento, siempre que el que se ofrezca al afectado sea gratuito y asegure la comunicación escrita si éste así lo exige".* De modo que siempre que no se exija contraprestación, podrá ser por el medio más conveniente, aunque no haya sido el elegido por el afectado.

El RLOPD establece por su parte el plazo para el ejercicio de este derecho que no contempla la LOPD, lo que si hace con los de rectificación y cancelación para los que esta última concede un plazo de diez días. Pues bien el 29.1 fija que *"el responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, el interesado podrá interponer la reclamación prevista en el artículo 18*

de la Ley Orgánica 15/1999, de 13 de diciembre. En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo". Y el 29.2 fija además otro plazo *"si la solicitud fuera estimada y el responsable no acompañase a su comunicación la información a la que se refiere el artículo 27.1, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación".* Además en clara referencia al 15.2 de la LOPD, dice el 29.4: *"La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos"*. Concretando el último párrafo de este artículo que *"dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos".*

Pero también cabe la posibilidad de que este derecho de acceso sea denegado. El artículo 30.1 del RLOPD establece que *"el responsable del fichero o tratamiento podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto".* Según recogía el 15.3 de la LOPD, pero además contempla el 30.2 otro supuesto de denegación *"podrá también denegarse el acceso en los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso".* Y para ambos casos, establece el 30.3 del RLOPD que *"en todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades*

autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre".

Además como marca el artículo 18.1 de la Ley de atención al paciente, *"el paciente tiene el derecho de acceso, con las reservas señaladas en el apartado 3 de este artículo, a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella. Los centros sanitarios regularán el procedimiento que garantice la observancia de estos derechos".* Este punto tercero referido a las reservas será comentado más adelante.

En este sentido hay un sector doctrinal que ha manifestado que *"estamos ante un derecho del paciente, pero no exclusivo"*[262]*.* Y afirman que *"en todo caso, corresponde a los centros sanitarios regular el procedimiento que garantice la observancia del derecho de acceso y obtención de copia de los datos obrantes en la historia clínica…"*[263]. Establecen además que *"en caso de pacientes fallecidos, los centros sanitarios y los facultativos sólo facilitarán el acceso a su historia clínica a las personas vinculadas a él, por razones familiares o de hecho, salvo prohibición expresa del fallecido que debe estar acreditada. No obstante, el acceso de un tercero a la historia clínica por motivos de riesgo para la salud estará limitado a los datos pertinentes. Y en ningún caso se facilitará "información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros" (art. 18.4 LAP)"*[264]*.* Pero además *"también se prevé el acceso al historial clínico por parte de los profesionales asistenciales, puesto que la finalidad de la historia clínica es precisamente "garantizar una asistencia adecuada al paciente", por ello "los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a*

[262] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores): "*La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural*". Tirant Lo Blanch, Valencia, 2014. Pág. 352.

[263] Ibídem. Pág. 353.

[264] Ibídem.

la historia clínica de éste como instrumento fundamental para su adecuada asistencia" (art. 16.1 LAP)"[265]*.*

Igualmente manifiestan estos autores que *"en este sentido, será cada centro sanitario el encargado de establecer "los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten"*[266]*.* Y que *"por su parte, el art 16.3 prevé el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, que se rige por lo dispuesto en la LOPD y la LGS. En dicho caso, sería necesario preservar de forma separada los datos de identificación personal de los clínicos, salvo consentimiento del informado del paciente"*[267]*.* Sosteniendo igualmente que *"también queda previsto el acceso a la historia clínica por parte del personal de administración y gestión de los centros sanitarios, pero sólo "a los datos de la historia clínica relacionados con sus propias funciones" (art, 16.4 LAP); así como para el personal sanitario que ejerza funciones de inspección, evaluación, acreditación y planificación (art. 16.5 LAP)"*[268]*.*

Y concluye esta corriente respecto del ejercicio del derecho de acceso que *"en todo caso, y para garantizar la protección de los datos, se establece el deber de secreto del personal que accede a los datos (art. 16.6 LAP) y se introduce un mandato a las CCAA para regular el procedimiento para que quede constancia del acceso a la historia clínica y su uso (art, 16.4 LAP)"*[269]*.* Asegurando que *"para*

[265] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores): *"La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural*". Tirant Lo Blanch, Valencia, 2014. Pág. 353.

[266] Ibídem.

[267] Ibídem.

[268] Ibídem. Pág. 354.

[269] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores): *"La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural*". Tirant Lo Blanch, Valencia, 2014. Pág. 354.

poder garantizar el acceso al historial clínico esté debe estar guardado y protegido"[270]*.*

No obstante, en relación al acceso a la información, otra parte de la doctrina ha manifestado que *"…el Grupo de Expertos sobre Información e Historia Clínica, señaló a modo de conclusión que los datos personales de la HC de un paciente deben disponerse de modo que permitan su consulta integrada de manera que por medio de una búsqueda única puedan recuperarse todos los datos de la HC de un mismo enfermo, y ello con independencia de su origen en el tiempo o de la Unidad de donde se recogieron. Además su consulta debe ser coherente y ordenada indicando fecha, persona que hace las anotaciones y unidad a la que pertenece, así como selectiva y diferenciada por episodios asistenciales"*[271]*.*

Mejía opina respecto al derecho de acceso que *"… el paciente tiene un derecho de acceso íntegro a la HC pero con tres limitaciones: las anotaciones personales del médico, la confidencialidad de los datos de otras personas y por interés terapéutico del propio paciente"*[272]*.* Ya que dice que *"El acceso íntegro solo se predica respecto a los datos objetivos y a los resultados de las pruebas, pero no a las muestras clínicas o a las propias pruebas complementarias, y ello en orden a garantizar los principios de unidad e integridad de la historia cínica"*[273]*.*

Los derechos de rectificación y cancelación, por sui parte, se encuentran regulados en el artículo 16 de la LOPD, es cual establécela respecto en su primer apartado que *"el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días".* Estableciendo el punto segundo que *"serán rectificados o*

[270] Ibídem. Pág. 355.

[271] MEJÍA, Juan: "*Hacia un estatuto jurídico desarrollado de la Historia Clínica*". Diario La Ley 5638 de octubre de 2002.

[272] Ibídem.

[273] Ibídem.

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". Y el punto tercero, aunque ya ha sido comentado anteriormente en relación con la disociación de los datos, recogía que *"la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión".*

Respecto de los datos que se hubiesen comunicado a terceros antes del ejercicio del derecho, el punto cuarto de este artículo establece que *"si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación".* Así mismo, en relación con la obligación de conservarlos para atender obligaciones legales marcadas por otras normas, establece el punto quinto que *"los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado".*

Y como ya ha sido comentado respecto de la disociación de datos anteriormente, *"del mismo modo marca el Reglamento de Protección de Datos que, "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", conservándose en el caso de que se pudiera exigir algún tipo de responsabilidad. Es necesario acudir también aquí a las leyes sanitarias para ver que el periodo de conservación que se marca en este caso no es acorde a una finalidad, sino a un periodo de tiempo*

preestablecido de cinco años, contemplándose también su conservación a efectos judiciales, sin que sea necesario que se haga en el soporte original"[274]*.*

Conviene hacer una última referencia respecto de la diferencia entre cancelación y bloqueo de los datos que sostiene parte de la doctrina que manifiesta que *"…la LOPD en el capítulo de definiciones del artículo 3c) incluye dentro de las operaciones y procedimientos comprendidos en la categoría de tratamiento de datos las de "bloqueo y cancelación" (no así la de destrucción). Acerca de los principios de protección de datos, el artículo 4 impone en sus números 4 y 5 la cancelación de los datos inexactos, incompletos o que hayan dejado de ser necesarios o pertinentes. Por último, el arto 16.3 dispone ya se ha visto en el apartado correspondiente el bloqueo y supresión de los datos una vez concluidos los plazos establecidos. También aquí aparece clara la diferencia entre el bloqueo y las restantes expresiones utilizadas"*[275]*.*

El artículo 31.1 del RLOPD, define el derecho de rectificación como *"el derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos".* Y el 31.2 el de oposición como *"el ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento. En los supuestos en que el interesado invoque el ejercicio del derecho de cancelación para revocar el consentimiento previamente prestado, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente reglamento".*

[274] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

[275] ARZOZ SANTIESTEBAN, Xavier, CALONGE CRESPO, Iñaki, ESPARZA LEIBAR, Iñaki, ETXEBERRIA GURIDI, José Francisco, GONZÁLEZ LÓPEZ, Juan José, ORDEÑANA GEZURAGA, Ixusco, PECHARROMÁN FERRER, Begoña, PÉREZ GIL, Julio, SUBIJANA ZUNZUMEGUI, Ignacio José: "*Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de datos personales*". Tirant Lo Blanch, Valencia, 2011. Pág. 234.

A este respecto, un sector doctrinal ha puesto de manifiesto que *"…la cancelación de los datos incluidos en la documentación clínica no procederá cuando existiese una obligación de conservarlos, debiendo preservarse para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha de alta de cada proceso asistencial. A estos efectos, para justificar un mayor plazo, interesa tener en cuenta el principio de conservación ajustada la finalidad, previsto en el artículo 4.5 de la Ley Orgánica 15/1999…"*[276].

Otros en cambio sostienen que *"la Ley de Autonomía del Paciente no prevé un derecho de rectificación y cancelación, pero lógicamente, sería aplicable la LOPD en el sentido de que los datos inexactos deberían poder rectificarse y cancelarse, y esto tanto respecto a los datos de identificación personal como respecto de los clínico-asistenciales cuando su tratamiento no se haya ajustado a la legislación o bien resulten inexactos"*[277]. Argumentando que *"Salvo estas circunstancias muy específicas, el deber de conservación de la historia clínica que establece el art. 17.1 LAP, chocaría con los derechos de rectificación y cancelación, pero debemos entender que prevalece la finalidad de la salvaguardia de la salud del paciente que su voluntad; así como el derecho de custodia que establece el art. 19 LAP"*[278].

Juan Mejía, por su parte, mantiene respecto al ejercicio de este derecho que *"con relación al derecho de cancelación, no debe ejercitarse mientras la HC permanezca viva. Si bien la LO 15/99*

[276] ATELA BILBAO, Alfonso, BENAC URROZ, Mariano, CODÓN HERRERA, Alfonso, GARAY ISASI, Josu, GONZÁLEZ SALINAS, Pedro, HERNÁNDEZ-MARTÍNEZ CAMPELLO, Carlos, LIZARRAGA BONELLI, Emilio, MARTÍ MONTESINOS, Cristina, PELLEJERO GARCÍA, Carlos, PIDEVAL BORRELL, Ignasi, VILLAR ABAD, Gloria, GONZÁLEZ PÉREZ, Jesús: *"Autonomía del paciente, información e historia clínica"*. Editorial Aranzadi, Madrid 2004. Pág. 190.

[277] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores): "*La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural*". Tirant Lo Blanch, Valencia, 2014. Pág. 357.

[278] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores): "La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural". Tirant Lo Blanch, Valencia, 2014. Pág. 357.

(art.4.5), en mi opinión no es aplicable al dato de salud, pues no puede cancelarse por el paciente"[279]*.*

Pero además el artículo 32, regula el modo en que deben ejercitarse estos derechos. Así el 32.1 establece que *"la solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado. En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso".* Y por su parte el 32.2 dice que *"el responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre. En el caso de que no disponga de datos de carácter personal del afectado deberá igualmente comunicárselo en el mismo plazo"*; en similitud a lo establecido 16.1 de la LOPD. E igual que hace el 16.4 de la LOPD, el RLOPD, también contempla los supuestos en que los datos hayan sido previamente cedidos en su artículo 32.3 Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar o cancelar los datos.

La rectificación o cancelación efectuada por el cesionario no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre".

[279] MEJÍA, Juan: "Hacia un estatuto jurídico desarrollado de la Historia Clínica". Diario La Ley 5638 de octubre de 2002

Y también los derechos de rectificación y cancelación pueden ser denegados. El artículo 33 del RLOPD se encarga de recogerlo. En su punto primero establece que *"la cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos".* El punto segundo recoge que *"podrá también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso".* Estableciendo el punto tercero de este artículo para ambos que *"en todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre".*

El derecho de oposición, no viene regulado en la LOPD como tal, aunque sí se cita en el artículo 6.4, que será analizado más adelante, y en el 17, cuyo título es "Procedimiento de oposición, acceso, rectificación o cancelación." El punto primero de este artículo establece que *"los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente",* de modo que estará regulado en el RLOPD. Y el punto segundo establece que *"no se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación"*.

Así pues, el RLOPD, establece en los artículos 24 y 25 las condiciones y procedimientos que le confiere la LOPD. El 24.1 en concreto recoge que *"los derechos de acceso, rectificación,*

cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro". Y el 24.2 que *"deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición".* De modo que son independientes y gratuitos, cuestión, esta última en la que redunda el siguiente punto de este mismo artículo al establecer que *"el ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan"*. Especificando el segundo párrafo de este artículo que *"no se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado".* Y sigue el punto cuarto del mismo artículo ahondando en este tema al decir que *"cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos".* Concluyendo este artículo estableciendo en su punto quinto que *"el responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aún*

cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente".

Del procedimiento a seguir para el ejercicio de los derechos ARCO se encarga el artículo 25 del RLOPD, que establece en su punto primero que a excepción de quienes dispongan de un lugar de atención al público al efecto, como se ve a continuación que *"salvo en el supuesto referido en el párrafo 4 del artículo anterior, el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá: a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente. El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos. b) Petición en que se concreta la solicitud. c) Dirección a efectos de notificaciones, fecha y firma del solicitante. d) Documentos acreditativos de la petición que formula, en su caso".*

Así mismo el punto segundo del artículo 25 requiere la aparición del responsable del fichero que *"…deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros".* Y además según establece el punto quinto *"…deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros".* Además

el tercer apartado establece que *"en el caso de que la solicitud no reúna los requisitos especificados en el apartado primero, el responsable del fichero deberá solicitar la subsanación de los mismos".*

Por su parte el artículo 26 establece que *"cuando los afectados ejercitasen sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición".*

Donde sí se regula el derecho de oposición es en el RLOPD, al que este le dedica un capítulo entero dentro del Título III, dedicado a los derechos de acceso, rectificación, cancelación y oposición, y en el que este último derecho se encuentra recogido en los artículos 34 a 36. El artículo 34 define así que *"el derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos: a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario. b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación. c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento".*

Y el artículo 35 establece la forma de ejercitarlo, diciendo en su punto primero que *"el derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento. Cuando la oposición se realice con base en la letra a) del artículo anterior, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho".* Recogiendo el punto segundo la forma de proceder al respecto, estableciendo que *"el responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre. En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo".* Y el punto tercero recoge la conclusión al recoger que *"el responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado 2 de este artículo".*

Hay que referir en este punto respecto del derecho de oposición y los datos de salud, que el artículo 6, dedicado al consentimiento, establece en su punto cuarto que *"en los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectad".*

En este sentido expresa también parte de la doctrina que *"el derecho de oposición está previsto en el arto 6.4 LOPD, para los supuestos en los que no sea necesario el consentimiento del*

afectado para el tratamiento de los datos, y siempre que no se prevea legalmente otra cosa, entonces se podrá oponer al tratamiento existiendo motivos fundados y relativos a su situación personal"[280].

Vistos los derechos ARCO, no puede cerrarse este apartado de la normativa existente en materia de protección de datos, sin referir el derecho de tutela recogido en el artículo 18 de la LOPD, que asiste a los interesados en caso de vulnerarse la normativa de protección de datos. Este precepto establece en su punto primero que *"las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine".* Puntualizando en el segundo apartado que *"el interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación".* Respecto al plazo de resolución se encarga el punto tercero que recoge que *"el plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses".* Y concluye el punto cuarto diciendo que *"contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo".*

El ejercicio de derechos es también tratado en la Recomendación sobre protección de datos médicos en el apartado 8 de su apéndice; esta norma regula únicamente los derechos de acceso y rectificación, recogiendo su punto primero que *"se permitirá*

[280] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores). "*La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural.*" Tirant Lo Blanch, Valencia, 2014. Pág. 356.

a toda persona el acceso a sus datos médicos, ya directamente o a través de un profesional sanitario o, si lo permite la ley nacional, a través de una persona designada por el titular de los datos. La información debe ser facilitada de modo inteligible". Igualmente prevé este texto la negativa a hacerlo por imperativo legal en su punto segundo, estableciendo que *"el acceso a los datos médicos puede ser denegado, limitado o rechazado sólo si lo prevé la ley y si: a. constituye una medida necesaria en una sociedad democrática por su interés en proteger la seguridad del Estado, la seguridad pública o la represión de crímenes; o b. el conocimiento de la información es probable que cause un serio daño a la salud del afectado; o c. la información sobre el afectado revela también información sobre terceros o, respecto a los datos genéticos, si esta información es probable que cause un serio daño a un pariente consanguíneo o uterino o a una persona que tiene un vínculo directo en línea germinal; o d. los datos son empleados para fines de investigación científica o estadística y se aprecia con nitidez que no hay riesgo alguno de violación de la intimidad del afectado, especialmente el de usar los datos en decisiones o medidas que afecten a un individuo en particular".*

Como vemos, en definitiva por bien del estado, de los afectados o de terceros. Y en el punto cuarto de este apartado octavo, se regula, el derecho de rectificación, según el cual, *"el afectado puede pedir la rectificación de los datos erróneos sobre su persona y, en caso de negativa, tendrá la capacidad de recurrir la decisión".*

La Directiva sobre protección en el tratamiento de datos, regula en su sección quinta los derechos de acceso y oposición, en los artículos 12 a 15. El artículo 12 regula el derecho de acceso y establece que: *"Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: - la confirmación de la existencia o*

inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran Y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; - la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; - el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizados a que se refiere el apartado 1 del artículo 15; b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos; c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado".

El artículo 13.1 blinda este derecho de acceso en determinadas circunstancias en las que *"los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f) tina función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); g) la protección del interesado o de los derechos y libertades de otras personas".*

Y especifica el punto segundo que *"sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas*

El artículo 14 de este texto, por su parte, regula el derecho de oposición, y establece que *"los Estados miembros reconocerán al interesado el derecho a: a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos; b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente, el derecho de oponerse, sin gastos, a dicha comunicación o utilización. Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b)".*

El artículo 15.1, bajo la curiosa rúbrica de decisiones individuales automatizados, establece que *"los Estados miembros*

reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.". Y el punto segundo que *"los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión: a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado".*

El artículo 66.3 de la Ley de Investigación Biomédica establece a este respecto que *"el responsable del fichero atenderá las solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación u oposición formuladas por los sujetos fuente, de conformidad con lo dispuesto en la normativa vigente sobre protección de datos de carácter personal".*

IV.3. CONSENTIMIENTO:

La LOPD recoge el consentimiento en su artículo 6.1, el cual establece que *"el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa".* Y por supuesto, con la posibilidad de revocarlo en los supuestos establecidos en el 6.3, según el cual *"el consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos*

retroactivos". Pero el punto segundo, exime del deber de prestarlo en determinadas circunstancias, ya que *"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, apartado 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 libertades fundamentales del interesado".*

Así el 7.6 establece que los datos especialmente protegidos, podrán ser tratados *"… los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento 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 dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto".* Los apartados 2 y 3 referidos tratan de los especialmente protegidos, recogiendo el apartado segundo establece en concreto que *"sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias…"*, y el apartado tercero el tratamiento y cesión, entre otros, de los datos de salud, especificando que *"los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y*

cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente".

De modo que en el tema que nos ocupa, no será necesario el consentimiento del interesado cuando exista un riesgo para la vida del legalmente incapacitado o de otra persona.

Y a propósito del consentimiento, pero en directa relación con el tratamiento de datos por cuenta de tercero, y por ende, en este caso, con la privatización de la sanidad, el informe jurídico de la AEPD 0600/2009, recoge el caso de una entidad sanitaria privada que colabora con la autonómica pública tenga que recabar el consentimiento de los pacientes para poder tratar sus datos. Ante lo que la Agencia concluye que *"…aún no formando parte integrante del sistema Nacional de Salud, los centros concertados desarrollan acciones asistenciales directamente vinculadas con el sistema, pudiendo incluso entenderse que las mismas constituyen, en cuanto sea objeto de concierto, servicios propios del mencionado Sistema." Y que "En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud".*

Así, *"según el artículo 7.3 de la LOPD, los datos relativos a la salud de las personas, al igual que el origen racial o la vida sexual, solo podrán recogerse, tratarse y cederse con el consentimiento expreso del afectado o por disposición legal. Pero en cambio se exige además un requisito específico -que se haga por escrito-, para otro tipo de datos especialmente protegidos, como son los de ideología, afiliación sindical, religión y creencias; esto se debe sin duda al especial tratamiento que les da el artículo16.2 CE. En la realidad, cualquiera de los datos protegidos, tanto los que exigen el*

consentimiento escrito, como los que no, podrían figurar en un informe médico y, en cambio, se requieren diferentes formas para recabarlo, de modo que lo mejor sería unificar y tomar la más exigente, en forma expresa y por escrito para todos ellos. Además, si no es por escrito, está también el tema de la carga de la prueba, que recae en el responsable del fichero"[281]*.* De modo que *"mientras las leyes sanitarias establecen la información verbal como norma general, para el trámite de la recogida del consentimiento, requiriéndose solo por escrito en determinados casos, como en las intervenciones quirúrgicas. Una vez más podrían chocar ambas normas. En cambio, para el caso de la revocación del consentimiento se exige que se haga por escrito, lo cual no concuerda con la forma en que se obtuvo dicho consentimiento, en la mayoría de los casos"*[282].

Otro sector de la doctrina manifiesta en este aspecto que *"…no cabe duda de que, ante una situación de riesgo para la vida o la salud del paciente, ha de prevalecer siempre la protección de ésta frente a la salvaguarda de los derechos que tiene reconocidos como titular de los datos de carácter personal…"*[283]*.*

Y volviendo a los primeros apartados del artículo 7, en los que se establecen los distintos tipos de datos especialmente protegidos y las distintas formas de obtención del mismo respecto a estos, se pueden establecer dos grandes grupos. Uno en el 7.2 que requiere consentimiento expreso y por escrito para el tratamiento de los datos de ideología, afiliación sindical, religión y creencias. Y otro en el 7.3 que se requiere para los datos de origen racial, salud y vida sexual,

[281] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos"*. Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

[282] Ibídem.

[283] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso: "*La protección de datos personales en el ámbito sanitario*". Editorial Aranzadi, Navarra 2002. Pág. 100.

únicamente consentimiento expreso, pero no escrito, además de poder ser recabados, tratados y cedidos por razones de interés general, o cuando así lo disponga una ley.

Aunque pareciese tener menos categoría este segundo grupo, por no exigirse el consentimiento escrito, el caso es que, datos de cualquiera de los dos grupos pueden figurar en un informe médico, por lo que habría que aunar los criterios a la hora de recoger el consentimiento, aplicando a todos los datos los criterios más exigentes, expreso y por escrito.

Hay que referir aquí también el apartado primero del artículo 7.1, que aunque no está directamente relacionado con los datos relativos a la salud, recoge que *"de acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo".* Pensemos que en un informe médico es posible que consten este tipo de datos, por lo que habrá que ponderar indeterminados casos si prevalece el interés vital del afectado o su derecho a no pronunciarse sobre sus creencias o incluso oponerse al tratamiento de sus datos por este tema.

El requisito del consentimiento es también ampliamente regulado en la ley del paciente, que habla del término "*consentimiento informado*", y lo define en el artículo 3 como *"la conformidad libre, voluntaria y consciente de un paciente, manifestada en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar una actuación que afecta a su salud".* El artículo 8 dedicado en pleno a este concepto, puntualiza en su punto primero que *"toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado, una vez que, recibida la información prevista en el artículo 4, haya valorado las opciones propias del caso".* De modo

que se requiere además, que haya sido proporcionada una información previa; recordemos además que el artículo 4 se refiere a la información asistencial a la que tienen derecho los pacientes.

Sobre el consentimiento informado, cabe aquí citar el informe jurídico 0012/2013 de la AEPD en que se recoge una interesante consulta que plantea *"…si es conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en adelante LOPD, y su normativa de desarrollo, la inclusión de información personal de cualquier paciente en una pequeña medalla colgada del cuello en el que se pueda visualizar un Código QR con fines sanitarios. En particular, la consulta indica que se podrían incluir todos los datos personales del portador, incluyendo la historia clínica del paciente, de modo que "ante cualquier emergencia o accidente que pueda tener un determinado paciente, los servicios sanitarios que le asistan, con un simple escaneo de un móvil (Smartphone) sobre el Código que cuelga de su cuello pueden conocer en breves minutos todo el historial médico sanitario del paciente".* La respuesta es la siguiente *"…no existe obstáculo en la inclusión de datos personales en un código QR, siempre que, existiendo consentimiento informado del portador de la medalla en los términos indicados, sólo se incluyan en el mismo los datos estrictamente necesarios para el cumplimiento de las finalidades pretendidas, lo que dependerá de cada tipo de usuario y de enfermedad. Asimismo, deberán adaptarse las medidas de seguridad que correspondan en cada caso, en los términos del Título VIII del Real Decreto 1720/2007 de 21 de diciembre. Y si la finalidad es que únicamente accedan a dichos datos el personal sanitario que vaya atender al paciente en situación de emergencia o accidente, deberían implantarse medidas que no permitieran el acceso a esta información por terceros".* Suponiendo que esto último se refiera al caso de pérdida del citado dispositivo, lo cual podría causar un grave daño al paciente, de no contener el mismo medidas de encriptado o similares, como se exigen para los datos de nivel alto de seguridad;

y aún en tal caso, seguro que con los avances de la informática la información podría ser accedida. De utilizarse este método habría que ver en qué momento se le proporcionaría al paciente, si a la llegada de un centro sanitario, o al igual que la tarjeta sanitaria lo tendría en su casa para llevarlo encima cuando lo considere necesario.

A este respecto, parte de la doctrina ha manifestado que *"la LAP a la hora de regular el consentimiento informado en el art, 8 pero referido a las actuaciones médicas, no a la recogida de los datos. Está la salvedad de que el art. 8.4 sí prevé que se le informe de la posibilidad de utilizar los procedimientos de pronóstico, diagnóstico y terapéuticos que se le apliquen en un proyecto docente o de investigación que en ningún caso podrá comportar riesgo adicional para la salud; y lo previsto en el art. 16.3 respecto a la posibilidad de dar consentimiento en no separar los datos de identificación personal del paciente de los clínico-asistenciales respecto al acceso con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia"*[284]*.* Y producto de este análisis argumentan que *"entendemos, sin embargo, que sí cabría la oposición respecto al tratamiento de los datos precisamente no c1ínicoasistenciales referidos a la identificación personal, como datos relativos a circunstancias sociales o personales (situación familiar, etc.) que por la situación personal del sujeto podría legitimarle a oponerse a su tratamiento"*[285]*.*

Nuria Terribas recuerda en este sentido que "*…en el año 1986 se promulga la Ley General de Sanidad, donde por primera vez se recoge con rango de ley un listado de derechos de los pacientes. Esta ley es la que introduce la obligatoriedad del consentimiento*

[284] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores): "*La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural*". Tirant Lo Blanch, Valencia, 2014. Pág. 356.

[285] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores): "*La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural*". Tirant Lo Blanch, Valencia, 2014. Pág. 356.

informado…". Y que *"la consecuencia de esta imposición legal fue que el consentimiento informado se convirtió en una obligación que si no se cumplía podía dar lugar a demandas judiciales, perdiendo entonces la esencia de lo que debía ser: una herramienta con la que, mediante un proceso de comunicación y dentro de la relación médico-paciente, se propiciase el respecto del derecho del paciente a ser informado, comprender dicha información y, finalmente, dar su autorización para un determinada actuación…"*[286]*.*

Los límites del consentimiento informado los establece el artículo 9.1, en el caso de los que pueda poner el paciente al establecer que *"la renuncia del paciente a recibir información está limitada por el interés de la salud del propio paciente, de terceros, de la colectividad y por las exigencias terapéuticas del caso. Cuando el paciente manifieste expresamente su deseo de no ser informado, se respetará su voluntad haciendo constar su renuncia documentalmente, sin perjuicio de la obtención de su consentimiento previo para la intervención".* Y el 9.2 recoge los límites que puedan poner los facultativos que los atiendan, estableciendo *"los facultativos podrán llevar a cabo las intervenciones clínicas indispensables en favor de la salud del paciente, sin necesidad de contar con su consentimiento, en los siguientes casos: a) Cuando existe riesgo para la salud pública a causa de razones sanitarias establecidas por la Ley. En todo caso, una vez adoptadas las medidas pertinentes, de conformidad con lo establecido en la Ley Orgánica 3/1986, se comunicarán a la autoridad judicial en el plazo máximo de 24 horas siempre que dispongan el internamiento obligatorio de personas. b) Cuando existe riesgo inmediato grave para la integridad física o psíquica del enfermo y no es posible conseguir su autorización, consultando, cuando las circunstancias lo*

[286] TERRIBAS I SALA, Núria*: "Aspectos legales de la atención a los menores de edad".* Institut Borja de Bioética. Universitat Ramon Llull. FMC. 2008. Barcelona. España. Pags 367-73.

permitan, a sus familiares o a las personas vinculadas de hecho a él".

Un sector doctrinal, manifiesta a propósito del consentimiento informado que *"a pesar de la evolución, el médico sigue adoptando a veces una postura paternalista en la que considera que el ejercicio de sus deberes es un privilegio que el médico puede conceder o no al paciente en función de su criterio y de lo que él considera más adecuado. Otras veces el médico, desde una perspectiva legalista, afirma que es necesario informar, por imperativo legal, porque la Ley otorga a los pacientes un derecho que se traduce en la aparición de un documento jurídico, el consentimiento informado, actitud que es expresión de una medicina defensiva, que no traduce el verdadero sentido del consentimiento informado. Por otro lado están los que adoptan una actitud moral y normativa y consideran que ejercer estos deberes es una obligación moral del médico, que lleva a considerar al paciente como persona y entender que tiene capacidad para elegir de acuerdo a su propio sistema de valores"*[287]*.* Y así mismo reflexiona en este aspecto esta parte de la doctrina, asegurando que *"la profesión médica aún no es del todo consciente de la importancia que tienen el ejercicio de estos derechos, puesto que en los últimos años se ha evidenciado que una de las cusas que ha generado más demandas contra los médicos es el incumplimiento del deber de informar"*[288]*.*

Otros autores, en cambio, ponen su atención en que *"…la recogida de datos debe realizarse dando cumplimiento al principio de consentimiento informado. Este principio es el resultante de conjugar*

[287] CRIADO DEL RÍO, María Teresa y SEOANE PRADO, Javier: "*Aspectos médico-legales de la historia clínica"*. Colex, Madrid, 1999. Pág. 102.

[288] CRIADO DEL RÍO, María Teresa y SEOANE PRADO, Javier: "*Aspectos médico-legales de la historia clínica"*. Colex, Madrid, 1999. Pág. 107.

los principios de información previa y consentimiento del afectado que están íntimamente ligados"[289]*.*

Aberasturi Gorriño expresa así su opinión respecto al consentimiento informado, sosteniendo que *"los principios básicos que determinan la calidad de los datos, y en particular el principio de finalidad, constituyen uno de los pilares de la regulación de la protección de los datos de carácter personal. Junto a estas figuras, y en el mismo nivel de relevancia, es decir, en el núcleo del derecho a la autodeterminación informativa, se encuentra otro principio: «el consentimiento informado», que, sin duda alguna se erige en la principal facultad de control sobre los datos de carácter personal".*[290] Y establece igualmente que *"En el ámbito de la protección de datos el consentimiento informado reconoce la capacidad del titular de los datos de autorizar o no un determinado tratamiento de los mismos. Esta institución constituye la principal facultad de control que los ciudadanos tienen sobre la información que les concierne"*[291]*. Además señala este autor que "El derecho a ser informado constituye, en términos generales, la facultad de toda persona a conocer las características que van a rodear a los tratamientos de datos que le conciernen o afectan. La regulación que la LOPD realiza respecto de este derecho se recoge fundamentalmente en su artículo 5"*[292]*.*

Elena Urso ha sostenido al respecto de este tema que *"…el desafío a afrontar y tratar de vencer, es el de una medicina que no sea nostálgica de la antigua visión paternalista exaltada en aquellos textos o proyectos legislativos que, en hipótesis de contradicción,*

[289] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso: "*La protección de datos personales en el ámbito sanitario*". Editorial Aranzadi, Navarra 2002. Pág. 91.

[290] ABERASTURI GORRIÑO, Unai: *"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 115.

[291] Ibídem. Pág. 118.

[292] ABERASTURI GORRIÑO, Unai: *"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 123.

dejan al médico la «última palabra», y que sepa en cambio poner sólidos márgenes a la siempre peligrosa tendencia a «delegar» al paciente- con capacidad de autodeterminarse, o los familiares que lo representan legalmente, si está inconsciente o incapaz-, decisiones tomadas ciertamente en nombre de la autonomía o del consentimiento que, sin embargo, cuanto más se define éste como «informado», rígidamente formalizado, y extensivo a cualquier posible consecuencia no deseada, tanto más deja vacía la función esencial protectora que debería desarrollar"[293]*.*

Existe una reciente e interesante sentencia de la Primera Sala de la Suprema Corte de Justicia de la Nación de México, publicada el 7 de julio de 2015, en México D.F., que *"…determinó que la falta de información suficiente acerca de los riesgos y beneficios del procedimiento quirúrgico al cual una persona será cometida hace precedente la acción de daño moral, pues con base en el derecho de la autodeterminación del paciente se le debe otorgar toda aquella que le resulte suficiente para ponderar sus alternativas y elegir la que considere más benéfica. Por ende, se determinó que resulta insuficiente la existencia de documentos genéricos y abstractos firmados por los pacientes que no reúnan los requisitos mínimos establecidos en la Norma Oficial Mexicana 168-SSA-1998"*[294].

Según la Ley sobre el uso de los medicamentos, a propósito del tratamiento de información en la receta médica, tanto electrónica como manual, en cuanto a la inclusión de los datos en los sistemas de información, no se necesitará el consentimiento de los interesados, según lo dispuesto en la LOPD, siempre con el fin de controlar las prestaciones y proporcionar asistencia médica y farmacéutica a los pacientes. Así lo recoge su artículo 77.8

[293] Urso, Elena, traducción Torre, E: *"Infancia, adolescencia y derecho a la salud en el hospital: el papel clave de los derechos fundamentales"*. Revista europea de derechos fundamentales. ISSN 1699-1524. Núm. 14/2ºsemestre 2009. Páginas 183-229.

[294] http://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=140471

estableciendo que *"el Gobierno determinará con carácter básico los requisitos mínimos que han de cumplir las recetas médicas extendidas y/o editadas en soporte informático con el fin de asegurar la accesibilidad de todos los ciudadanos, en condiciones de igualdad efectiva en el conjunto del territorio español, a la prestación farmacéutica del Sistema Nacional de Salud"* Además, según sigue diciendo este precepto*, "no será necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica en soporte papel o electrónico, de conformidad con lo dispuesto en los artículos 7, apartados 3 y 6; 8; y 11, apartado 2.a), de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Las citadas actuaciones deberán tener por finalidad facilitar la asistencia médica y farmacéutica al paciente y permitir el control de la prestación farmacéutica del Sistema Nacional de Salud"*.

El Convenio de Derechos Humanos y Biomedicina de 1997, respecto del consentimiento lo considere esencial, y regula el de las personas sin capacidad, donde, siempre en redundancia del beneficio del paciente, la opinión del menor será toma en cuenta de acuerdo a su grado de madurez, con autorización de su tutor legal. Incluso se gradúa el de las personas con trastornos mentales hasta el punto en que les perjudique, así como en las situaciones de urgencia, tomando en cuenta siempre los deseos expresados anteriormente. En concreto, el artículo 5 de esta norma marca como regla general que *"una intervención en el ámbito de la sanidad sólo podrá efectuarse después de que la persona afectada haya dado su libre e informado consentimiento. Dicha persona deberá recibir previamente una información adecuada acerca de la finalidad y la naturaleza de la intervención, así como sobre sus riesgos y consecuencias. En cualquier momento la persona afectada podrá retirar libremente su consentimiento".*

Y respecto de la protección de las personas que no tengan capacidad para expresa su consentimiento, establece el artículo 6.1, a excepción de los establecido en los artículos 17 y 20, que regulan la protección de las personas que no tengan capacidad para expresar su consentimiento en lo relativo a experimentos y trasplante de órganos respectivamente, que *"a reserva de lo dispuesto en los artículos 17 y 20, sólo podrá efectuarse una intervención a una persona que no tenga capacidad para expresar su consentimiento cuando redunde en su beneficio directo"*.

Así mismo el punto segundo de este artículo dice que *"Cuando, según la ley, un menor no tenga capacidad para expresar su consentimiento para una intervención, ésta sólo podrá efectuarse con autorización de su representante, de una autoridad o de una persona o institución designada por la ley. La opinión del menor será tomada en consideración como un factor que será tanto más determinante en función de su edad y su grado de madurez".*

No obstante, el punto 3 del referido artículo, puntualiza que *"cuando, según la ley, una persona mayor de edad no tenga capacidad, a causa de una disfunción mental, una enfermedad o un motivo similar, para expresar su consentimiento para una intervención, ésta no podrá efectuarse sin la autorización de su representante, una autoridad o una persona o institución designada por la Ley. La persona afectada deberá intervenir, en la medida de lo posible, en el procedimiento de autorización"*. Redundando en la participación el punto cuarto al establecer que *"el representante, la autoridad, persona o institución indicados en los apartados 2 y 3, recibirán, en iguales condiciones, la información a que se refiere el artículo 5."*, y en la información que pueda darse en estas situaciones, en la medida de lo posible, establece el punto quinto de este artículo sexto que *"la autorización indicada en los apartados 2 y 3 podrá ser retirada, en cualquier momento, en interés de la persona afectada".* Esto puede relacionarse con lo expuesto más adelante en

el apartado referido al consentimiento para el tratamiento de los menores de edad.

Respecto la protección de las personas que sufran trastornos mentales, establece el artículo 7 que *"la persona que sufra un trastorno mental grave sólo podrá ser sometida, sin su consentimiento, a una intervención que tenga por objeto tratar dicho trastorno, cuando la ausencia de este tratamiento conlleve el riesgo de ser gravemente perjudicial para su salud y a reserva de las condiciones de protección previstas por la ley, que comprendan los procedimientos de supervisión y control, así como los de recurso".*

Y el artículo 8 establece para las situaciones de urgencia que *"cuando, debido a una situación de urgencia, no pueda obtenerse el consentimiento adecuado, podrá procederse inmediatamente a cualquier intervención indispensable desde el punto de vista médico a favor de la salud de la persona afectada". Y* respeto de los deseos expresados anteriormente, en relación a las situaciones comentadas, según el artículo 9 *"serán tomados en consideración los deseos expresados anteriormente con respecto a una intervención médica por un paciente que, en el momento de la intervención, no se encuentre en situación de expresar su voluntad".*

Así lo recoge también parte de la doctrina, estableciendo que *"según el artículo 9 de Convenio, se tomarán en consideración los deseos expresados anteriormente, con respecto a una intervención médica, por un paciente que, en el momento de la intervención, no se encuentre en situación de expresar su voluntad"*[295].

Se regula igualmente, la investigación científica en la experimentación con embriones "*in vitro*" donde se garantizará la adecuada protección del embrión, prohibiéndose su constitución con tales fines, así establece el artículo 18.1 que *"cuando la*

[295] SAMPRÓN LÓPEZ, David: "*Los derechos del paciente a través de la información de la historia clínica*". Edisofer, Madrid, 2002. Pág. 32.

experimentación con embriones «in vitro» esté admitida por la ley, ésta deberá garantizar una protección adecuada del embrión". Estableciendo el punto segundo de este artículo que *"Se prohíbe la constitución de embriones humanos con fines de experimentación".* Así mismo, la extracción de órganos y tejidos de donantes vivos para trasplantes con el debido consentimiento se regula en el artículo 19 que establece como regla general que *"la extracción de órganos o de tejidos para trasplantes sólo podrá efectuarse de un donante vivo en interés terapéutico del receptor y cuando no se disponga del órgano o del tejido apropiados de una persona fallecida ni de un método terapéutico alternativo de eficacia comparable".* Y a continuación en el punto segundo, y en referencia al consentimiento general establecido anteriormente, dice que *"el consentimiento a que se refiere el artículo 5 deberá ser expresa y específicamente otorgado, bien por escrito o ante una autoridad".* Recordemos que los fines científicos ya fueron referidos en el principio de calidad, que podemos relacionar también con lo establecido en este apartado.

No olvidemos la carencia de consentimiento que marca el Real Decreto- Ley sobre sostenibilidad, respecto de las comunicaciones de datos entre las distintas administraciones, principalmente la tributaria y la sanitaria, a propósito del establecimiento de los porcentajes aplicables al pago de los medicamentos.

La Declaración Universal sobre Bioética y Derechos Humanos de 19 de octubre de 2005, por su parte, establece como premisa en su artículo 6.1 que *"yoda intervención médica preventiva, diagnóstica y terapéutica sólo habrá de llevarse a cabo previo consentimiento libre e informado de la persona interesada, basado en la información adecuada. Cuando proceda, el consentimiento debería ser expreso y la persona interesada podrá revocarlo en todo momento y por cualquier motivo, sin que esto entrañe para ella desventaja o perjuicio alguno"*. Añadiendo el punto segundo de este artículo que *"la investigación científica sólo se debería llevar a cabo previo*

consentimiento libre, expreso e informado de la persona interesada. La información debería ser adecuada, facilitarse de forma comprensible e incluir las modalidades para la revocación del consentimiento. La persona interesada podrá revocar su consentimiento en todo momento y por cualquier motivo, sin que esto entrañe para ella desventaja o perjuicio alguno…".

No obstante, no deja de lado el consentimiento de las personas carentes de su capacidad para darlos, y que se recoge en el artículo 7 que *"de conformidad con la legislación nacional, se habrá de conceder protección especial a las personas que carecen de la capacidad de dar su consentimiento: a) la autorización para proceder a investigaciones y prácticas médicas debería obtenerse conforme a los intereses de la persona interesada y de conformidad con la legislación nacional. Sin embargo, la persona interesada debería estar asociada en la mayor medida posible al proceso de adopción de la decisión de consentimiento, así como al de su revocación; b) se deberían llevar a cabo únicamente actividades de investigación que redunden directamente en provecho de la salud de la persona interesada, una vez obtenida la autorización y reunidas las condiciones de protección prescritas por la ley, y si no existe una alternativa de investigación de eficacia comparable con participantes en la investigación capaces de dar su consentimiento. Las actividades de investigación que no entrañen un posible beneficio directo para la salud se deberían llevar a cabo únicamente de modo excepcional, con las mayores restricciones, exponiendo a la persona únicamente a un riesgo y una coerción mínimos y, si se espera que la investigación redunde en provecho de la salud de otras personas de la misma categoría, a reserva de las condiciones prescritas por la ley y de forma compatible con la protección de los derechos humanos de la persona. Se debería respetar la negativa de esas personas a tomar parte en actividades de investigación".*

La Recomendación sobre protección de datos médicos, regula en el punto sexto de su apéndice el tema del consentimiento, y establece como premisa en su punto primero que al *"…solicitar el consentimiento del afectado, éste debe ser libre, expreso e informado".* La LOPD por su parte, establece en su artículo 6.1, como ya se ha dicho anteriormente que *"el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa".* De modo que, los requisitos son diferentes, pero cuando se trata de datos especialmente protegidos, la LOPD exige además en el 7.3, analizado ya al comienzo de este apartado, que *"los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente".*

Así vemos que recomendación y Ley Orgánica coinciden en que el consentimiento para los datos de salud debe ser expreso, exigiendo además la primera los requisitos de libre e informado. Pero si acudimos a las definiciones del artículo 3 de la LOPD, vemos que en su letra h define como *"consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen".* Y aquí coinciden los otros dos requisitos exigidos por la recomendación, de libre e informado, de modo, que con la recopilación de todos estos artículos de la LOPD vemos que los requisitos serían coincidentes. Y así mismo, el apartado 6.2 del apéndice de la recomendación, respecto al consentimiento establece en este sentido que *"los resultados de cualquier análisis genético se deben formular dentro de los límites de los objetivos de la consulta, el diagnóstico o el tratamiento para el que se obtuvo el consentimiento".* Estableciéndose en el 6.3, que *"cuando se trate de procesar datos médicos de una persona legalmente incapacitada que es incapaz de una decisión libre, y*

cuando la ley nacional no le permita actuar en su propia representación, es preciso obtener el consentimiento de la persona legalmente habilitada para actuar en interés de éste, o de la autoridad o persona u órgano designados por la ley con este fin. Si, de acuerdo con el Principio 5.5, una persona legalmente incapacitada ha sido informada de la intención de recoger o procesar sus datos médicos, sus deseos deben tenerse en cuenta, a menos que la ley nacional disponga otra cosa".

El informe jurídico 0617/2008 de la AEPD en el que se plantea el acceso por los informáticos que realizarán pruebas con datos reales para la implantación de un programa que almacenará datos de salud, se recoge que *"…aún cuando no se va a llevar a cabo una efectiva asistencia sanitaria a los afectados cuyos datos reales sean empleados en las pruebas a las que se refiere la consulta, la legitimación para el tratamiento procederá en este caso de la aplicación del artículo 7.3 de la Ley Orgánica 15/1999, en conexión con el artículo 56 de la Ley 16/2003, no siendo en consecuencia preciso el consentimiento del afectado para que se proceda al mencionado tratamiento".* De modo que personal no sanitario también podrá acceder esporádica y justificadamente a los datos de salud.

La Directiva sobre protección en el tratamiento de datos establece igualmente los principios relativos a la legitimación para el tratamiento de datos, basados fundamentalmente en el consentimiento inequívoco, que no será necesario si existe contrato, obligación jurídica, un interés vital del interesado un interés público o hay que proteger un interés legítimo del interesado o de terceros a los que les hayan sido comunicados los datos.

Así su artículo 7 recoge que *"los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: a) el interesado ha dado su consentimiento de forma inequívoca, b) es necesario para la ejecución de un contrato en el que el interesado*

sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o c)es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o d)es necesario para proteger el interés vital del interesado, o e)es necesario 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, o f)es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva".

El CDM recoge a este respecto en el artículo 16.2 que *"el consentimiento se expresa habitualmente de forma verbal, dejando constancia en la historia clínica. Cuando las medidas propuestas supongan para el paciente un riesgo significativo se obtendrá el consentimiento por escrito".*

La Declaración sobre derechos de los pacientes, por su parte, establece que el consentimiento debe ser informado, siendo necesario para la preservación de cualquier sustancia, diagnóstico, tratamiento y cuidado del paciente o para su participación en la enseñanza clínica o la investigación científica pudiendo ser rechazado o incluso presunto en determinadas situaciones, teniendo en cuenta las situaciones de representación.

De este modo establece este texto en los puntos 1 a 10 de su apartado tercero que *"el consentimiento informado del paciente es el requisito previo a toda intervención médica. El paciente tiene el derecho a negarse o a detener una intervención médica. Las implicaciones de negarse a recibir o detener tal intervención deben ser cuidadosamente explicadas al paciente. Cuando el paciente sea incapaz de expresar su voluntad y se necesite urgentemente llevar a*

cabo una intervención, se puede presumir el consentimiento del paciente, a menos que resulte obvio por una declaración de voluntades anticipadas previa que en dicha situación el consentimiento sería denegado. Cuando el consentimiento de un representante legal sea requerido y la intervención propuesta sea urgentemente necesitada, dicha intervención puede realizarse a pesar de que no se pueda conseguir dicho consentimiento del representante a tiempo. Cuando se requiera el consentimiento legal del representante, los pacientes (ya sean menores o adultos) deberán estar también implicados en el proceso de toma de decisiones, al nivel máximo que permita su capacidad. Si un representante legal se niega a dar su consentimiento y el médico u otro profesional de la salud opina que la intervención beneficia al paciente, entonces la decisión debe ser referida a un tribunal o alguna forma de arbitrio. En todas las demás situaciones en las que el paciente sea incapaz de dar un consentimiento informado y donde no exista un representante legal o representante designado por el paciente para este propósito, deben tomarse medidas apropiadas para un proceso de toma de decisiones diferente, teniendo en cuenta todo lo que se conoce y, hasta lo más posible, lo que puede presumirse acerca de los deseos del paciente. El consentimiento del paciente es requerido para la preservación y uso de todas las sustancias del cuerpo humano. Se puede presumir el consentimiento cuando las sustancias deban ser utilizadas en el curso actual del diagnóstico, tratamiento y cuidado del paciente. El consentimiento informado del paciente es necesario para su participación en la enseñanza clínica. El consentimiento informado del paciente es un requisito previo para la participación en la investigación científica. Todos los protocolos deben ser sometidos a unos procedimientos de revisión éticos adecuados. Dicha investigación no debe llevarse a cabo en aquellas personas incapaces de expresar su voluntad, a no ser que se haya obtenido el consentimiento de un representante legal y la investigación pudiera redundar en beneficio del paciente.

Como una excepción al requerimiento de que la participación redundara en beneficio del paciente, una persona incapacitada puede formar parte de una investigación observacional que no beneficie directamente su salud, mientras que dicha persona no ponga objeción, que el riesgo o carga sea mínimo y que la investigación tenga un valor significativo y no existan métodos alternativos ni haya otros sujetos para investigar disponibles".

El artículo 2.1 de la Ley Orgánica sobre protección del honor, intimidad e imagen establece que *"la protección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia".* Especificando en el punto segundo que *"no se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por Ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso…".* Y recogiendo en el tercero que *"el consentimiento a que se refiere el párrafo anterior será revocable en cualquier momento, pero habrán de indemnizarse en su caso, los daños y perjuicios causados, incluyendo en ellos las expectativas justificadas".*

A este respecto, el artículo séptimo de este mismo texto, hace la siguiente mención respecto de las intromisiones ilegítimas, al establecer en su punto primero que *"el emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas".* El punto segundo por su parte establece que *"la utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción".* Y el punto quinto que *"la captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la*

imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo octavo, dos".

El referido artículo 8.2 establece en concreto que *"en particular, el derecho a la propia imagen no impedirá: a) Su captación, reproducción o publicación por cualquier medio cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público. b) La utilización de la caricatura de dichas personas, de acuerdo con el uso social. c) La información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoria. Las excepciones contempladas en los párrafos a) y b) no serán de aplicación respecto de las autoridades o personas que desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza".*

A propósito de la video vigilancia, que podría estar relacionada con el derecho a la propia imagen anteriormente referido, es práctica habitual que en los centros sanitarios, tanto públicos como privados, se instalen cámaras de video vigilancia, que también podrían grabar datos de salud sobre el aspecto físico que capten de las personas.

A este respecto, se manifiesta parte de la doctrina estableciendo que *"entre las diversas formas de tratamiento de datos de carácter personal, la captación y grabación de imágenes de personas físicas identificadas o identificables por medio de sistemas de cámaras o videocámaras, constituye una de las novedades más importantes experimentadas en los últimos años con importante incidencia en materia de protección de datos"*[296]. Y sigue manteniendo este sector que *"…los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre, por*

[296] BANDRÉS MOYÁ, Fernando Y DELGADO BUENO, Santiago: "*Biomedicina y derecho sanitario*". Ademas Comunicación, S.L., 2009. Pág. 397.

lo que siempre que se utilicen sistemas de cámara o videocámaras con fines de vigilancia, resultara de aplicación la Instrucción 1 /2006. Y se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita la simple captación de imágenes que no se graban"[297]*.* No obstante mantienen que *"en el ámbito hospitalario, nos encontramos con la paradoja de que el usuario, no se preocupa de la recogida de su imagen por dichas cámaras y si en algún caso las percibe, las considera también elementos de seguridad, en este caso para la protección del propio Centro Sanitario y por el carácter público del mismo imprescindible para su vigilancia. No obstante dicho usuario está más preocupado por encontrar el sitio y los profesionales que le resuelvan su problema, que por la protección de su propia imagen personal"*[298]*.*

Sobre a video vigilancia, otro sector de la doctrina sostiene que *"El arto 18.4 CE es fiel reflejo de esta preocupación disponiendo 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". Se ha discutido en la doctrina española acerca de si el precepto transcrito permite sostener el surgimiento de un nuevo derecho autónomo o si, por el contrario, estaríamos en presencia de una nueva dimensión del derecho a la intimidad. Se trata, en todo caso, de articular los adecuados mecanismos de garantía frente a las posibilidades de acopio de información, relativa a las personas, derivadas del progreso tecnológicos"*[299]*.* Y nos recuerdan que *"el tratamiento de datos personales por medio de la imagen y el sonido es objeto de particular atención en la Directiva 95/46/CE del*

[297] BANDRÉS MOYÁ, Fernando Y DELGADO BUENO, Santiago: "*Biomedicina y derecho sanitario*". Ademas Comunicación, S.L., 2009. Pág. 415.

[298] Ibídem. Pág. 424.

[299] ARZOZ SANTIESTEBAN, Xavier, CALONGE CRESPO, Iñaki, ESPARZA LEIBAR, Iñaki, ETXEBERRIA GURIDI, José Francisco, GONZÁLEZ LÓPEZ, Juan José, ORDEÑANA GEZURAGA, Ixusco, PECHARROMÁN FERRER, Begoña, PÉREZ GIL, Julio, SUBIJANA ZUNZUMEGUI, Ignacio José:" *Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de datos personales*". Tirant Lo Blanch, Valencia, 2011. Pág. 188.

Parlamento Europeo y del Consejo de la Unión Europea, en la medida en que se estiman como datos personales toda información sobre una persona física identificada o identificable, siendo aquélla identificable cuando su "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"[300]*.* Así, *"la LOPD, al igual que la derogada LORTAD, elude toda referencia expresa a la imagen y sonido como elementos constitutivos de datos de carácter personal, pero la definición que de éstos se recoge en el arto 3.a) no impide su consideración como tales: "cualquier información concerniente a personas físicas identificadas o identiflcables". También de forma similar a lo que acontecía con el derogado Reglamento de desarrollo de la LORTAD, el RD 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LO 15/1999, define los datos de carácter personal de forma prácticamente idéntica incluyendo, pues, las informaciones gráficas, fotográficas o acústicas (art. 5.1.f)"*[301]*.*

Recordemos que la video vigilancia encuentra su origen en 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 de la AEPD, que será aplicable por tanto a aquellos dispositivos instalados en centro sanitarios.

Del mismo modo, los datos de imagen también se incluyen en la normativa de protección de datos, y deben cumplirla. No hay que olvidar que en el ámbito sanitario también se recogen datos de imagen como resonancias magnéticas, gammagrafías, mamografías, ecografías, radiografías, tac, etc.; son las llamadas pruebas de diagnóstico por imagen, que entrañan la recogida de datos relativos

[300] Ibídem. Pág. 191.
[301] Ibídem. Pág. 193.

a la salud de las personas. Además en los quirófanos, salas de curas, salas de rehabilitación, consultas etc., pueden también grabarse imágenes con valor docente o de investigación, siempre con el consentimiento del paciente.

Se hace necesario citar aquí un curioso hallazgo producto del avance de la ciencia en relación con los datos que pueden aportar las pruebas médicas a través de imágenes; Malen Ruiz de Elvira titula su artículo publicado en el periódico El País: *"La resonancia magnética se destapa como detector de mentiras"*[302], y asegura que el uso forense de las imágenes cerebrales plantea problemas de privacidad.

Finalmente el punto tercero de la LO sobre protección del honor, intimidad e imagen, en su punto tercero recoge por su parte que *"la divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo".* El punto cuarto que *"la revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela".* Lo cual puede estar en relación con el deber de secreto que será analizado más adelante.

La Ley de Investigación Biomédica, por su parte, regula ampliamente el tema del consentimiento. El artículo 4.5 establece que *"toda persona tiene derecho a ser informada de sus datos genéticos y otros de carácter personal que se obtengan en el curso de una investigación biomédica, según los términos en que manifestó su voluntad. El mismo derecho se reconoce a la persona que haya aportado, con la finalidad indicada, muestras biológicas, o cuando se hayan obtenido otros materiales biológicos a partir de aquello*". Y el artículo 48 se dedica en pleno a él estableciendo en su

[302] RUIZ DE ELVIRA, Malen: "La resonancia magnética se destapa como detector de mentiras". El País, miércoles 16 de junio de 2010, vida & artes, Madrid. Pág. 35.

punto primero que *"será preciso el consentimiento expreso y específico por escrito para la realización de un análisis genético".* Además el punto tercero requiere que *"para acceder a un cribado genético será preciso el consentimiento explícito y por escrito del interesado. El Comité de Ética de la Investigación determinará los supuestos en los que el consentimiento podrá expresarse verbalmente. En todo caso, cuando el cribado incluya enfermedades no tratables o los beneficios sean escasos o inciertos, el consentimiento se obtendrá siempre por escrito".* Y en relación a la realización de estos procedimientos en el embarazo, el punto cuarto establece que *"la realización de análisis genéticos sobre preembriones in vivo y sobre embriones y fetos en el útero requerirá el consentimiento escrito de la mujer gestante. El análisis genético de un preembrión in vitro no transferido se regirá por lo establecido en la Ley sobre técnicas de reproducción humana asistida".*

Además el artículo 58 establece en su punto segundo sobre la obtención de muestras que *"el consentimiento del sujeto fuente será siempre necesario cuando se pretendan utilizar con fines de investigación biomédica muestras biológicas que hayan sido obtenidas con una finalidad distinta, se proceda o no a su anonimización".* Pero además el último párrafo en su letra d) perfila que *"no obstante lo anterior, de forma excepcional podrán tratarse muestras codificadas o identificadas con fines de investigación biomédica sin el consentimiento del sujeto fuente, cuando la obtención de dicho consentimiento no sea posible o represente un esfuerzo no razonable en el sentido del artículo 3.i) de esta Ley. En estos casos se exigirá el dictamen favorable del Comité de Ética de la Investigación correspondiente, el cual deberá tener en cuenta, como mínimo, los siguientes requisitos: d) Que se garantice la confidencialidad de los datos de carácter personal".*

Recordemos respecto al consentimiento, como se ha examinado en el inicio de este apartado, que la LOPD establece que

debe ser inequívoco, salvo que la ley disponga otra cosa, según marca el art.6 con un sinfín de excepciones, entre las que se encuentra la finalidad de proteger intereses vitales del afectado. Esto respetando lo dispuesto en los apartados precedentes, en los que establecen las distintas formas de otorgar el consentimiento, de acuerdo cada tipo de dato protegido en concreto. En este sentido el apartado tercero, se refiere, entre otros, a los datos de salud que solo podrán ser recabados, tratados y cedidos por razones de interés general, por disposición legal o cuando el afectado consienta expresamente.

Parte de la doctrina ha dejado constancia de que *"a nivel Jurisprudencial, el Consentimiento informado se considera como un Derecho Humano Fundamental, tras la Sentencia del Tribunal Supremo de 12 de enero de 2001, que resuelve recurso de casación contra la sentencia de la Audiencia Provincial de Madrid de 10 de octubre de 1995 y en cuyo Fundamento de Derecho Primero, establece que esta aportación realizada a la teoría de los Derechos Humanos, es consecuencia necesaria o explicación de los clásicos derechos a la vida, a la integridad física y a la libertad de conciencia"*[303]*.*

IV.3.a. Principios generales sobre su obtención:

Recordemos que la LOPD regulaba el consentimiento en su artículo 6, ya analizado. No obstante, cabe citar aquí la definición del mismo que esta norma hace en su artículo 3h), como *"toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen".* En cambio esta norma no recoge las formas en que el consentimiento debe prestarse.

[303] SAMPRÓN LÓPEZ, David: "Los derechos del paciente a través de la información de la historia clínica". Edisofer, Madrid, 2002. Pág. 32.

El artículo 12 del RLOPD establece unos principios generales para la obtención del consentimiento. Su punto primero, dice en concreto sobre el tratamiento que *"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 del 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".* Y por su parte el punto segundo regula la cesión *"cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo".* Y en cualquiera de los dos casos, y según marca el punto tercero de este artículo, *"corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho".*

Recordemos que también el 10.5 del RLOPD establecía que *"los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre".* Cuestión que ya se vio cuando al analizar la calidad de los datos en relación a los supuestos que legitimaban el tratamiento y la cesión de los datos.

IV.3.b. Consentimiento para el tratamiento de datos de menores de edad:

Respecto del consentimiento para el tratamiento de los datos de los menores de edad, el artículo 13.1 del RLOPD, establece un límite respecto de los años que estos deben tener para prestarlo, estableciendo que *"podrá procederse al tratamiento de los datos de*

los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores". Pero hay que respetar lo establecido en el punto tercero sobre la forma de informarles, ya que *"cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo".* Y también lo que dice el punto cuarto sobre la comprobación de edad de los mismos que *"corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales".*

Y el punto segundo de este artículo hace lo propio al establecer otra limitación, pero esta vez para la protección de otras personas y dice que *"en ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior".*

El artículo 12.3 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico, establece respecto de su uso que los proveedores de servicios de acceso a internet que *"…informarán sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos*

para la juventud y la infancia". Se aprecia aquí la importancia de este texto en el sentido en que la tecnología permita acceder al menor a información que sus médicos o tutores no hayan querido darle por razones clínicas, ya sea debido a su madurez, o por la conveniencia física o psíquica para el propio menor.

Según establece la Ley del paciente, el consentimiento podrá ser representado en caso de menores o incapaces y revocado en cualquier momento, y no será necesaria su obtención en caso de riesgo para la salud pública o para la del propio paciente. Así lo recoge el artículo 9.3 de esta norma, estableciendo que *"se otorgará el consentimiento por representación en los siguientes supuestos: a) Cuando el paciente no sea capaz de tomar decisiones, a criterio del médico responsable de la asistencia, o su estado físico o psíquico no le permita hacerse cargo de su situación. Si el paciente carece de representante legal, el consentimiento lo prestarán las personas vinculadas a él por razones familiares o de hecho. b) Cuando el paciente esté incapacitado legalmente. c) Cuando el paciente menor de edad no sea capaz intelectual ni emocionalmente de comprender el alcance de la intervención. En este caso, el consentimiento lo dará el representante legal del menor después de haber escuchado su opinión si tiene doce años cumplidos".* No obstante lo dicho, el último párrafo de este punto abre un poco los varemos de edades y establece que *"cuando se trate de menores no incapaces ni incapacitados, pero emancipados o con dieciséis años cumplidos, no cabe prestar el consentimiento por representación. Sin embargo, en caso de actuación de grave riesgo, según el criterio del facultativo, los padres serán informados y su opinión será tenida en cuenta para la toma de la decisión correspondiente".*

El punto cuarto se refiere a casos específicos con especial regulación, especificando que *"la práctica de ensayos clínicos y de técnicas de reproducción humana asistida se rige por lo establecido*

con carácter general sobre la mayoría de edad y por las disposiciones especiales de aplicación".

Y el punto quinto da rienda a los menores en su capacidad de decisión y estipula que *"la prestación del consentimiento por representación será adecuada a las circunstancias y proporcionada a las necesidades que haya que atender, siempre en favor del paciente y con respeto a su dignidad personal. El paciente participará en la medida de lo posible en la toma de decisiones a lo largo del proceso sanitario. Si el paciente es una persona con discapacidad, se le ofrecerán las medidas de apoyo pertinentes, incluida la información en formatos adecuados, siguiendo las reglas marcadas por el principio del diseño para todos de manera que resulten accesibles y comprensibles a las personas con discapacidad, para favorecer que pueda prestar por sí su consentimiento".*

Respecto del tratamiento de el acceso a los datos de las historias clínicas de los menores de edad, la AEPD resuelve en su informe jurídico 0222/2014 sobre la base de que *"el consentimiento para el tratamiento de los datos de los menores de edad en las historias clínicas queda supeditado a lo dispuesto en el artículo 9.3 c) de la Ley 41/2002".* Que *"el menor de edad mayor de catorce años podrá, en general, ejercitar por sí solo el derecho de acceso a la historia clínica".* Que *"los titulares de la patria potestad podrán también acceder a los datos del menor de edad sujeto a aquélla mientras esa situación persista, para el cumplimiento de las obligaciones previstas en el Código Civil".* Y que *"no podrá oponerse a ese acceso la mera oposición del menor salvo que así lo reconociera una norma con rango de Ley".*

Nuria Terribas estudia de forma profunda el tema del consentimiento de los menores de edad y la bioética publicando interesantes documentos. Resalta la autora de este artículo que la Ley Básica 41/2002 en consonancia con el Convenio Europeo de

Biomedicina y Derechos Humanos, *"…establece en su art.9 lo que ha venido a llamarse «mayoría de edad sanitaria», dando legitimidad a la figura del «menor maduro» en el ejercicio de los derechos de información y decisión en el contexto sanitario"*[304].

Esta misma autora entiende *"…por «capacidad» entendemos el reconocimiento de la plena madurez legal de la persona para obrar de forma vinculante en derecho…"*[305]. Así podría entenderse otro de los términos que maneja esta autora que afirma que *"…una persona competente es la que tiene suficiente madurez psicológica y cognitiva para apreciar su situación (p.ej., en caso de enfermedad), comprender la información relevante acerca de la elección o decisión que debe tomarse, ponderando los riesgos y beneficios, y comunicar su elección…"*[306].

Además es interesante citar en este apartado sobre la mayoría de edad que Nuria Terribas que se refiere a que en *"…la regulación en la Ley 41/2002 de autonomía del paciente y homólogas leyes autonómicas, introducen de forma clara la figura del menor maduro, marcando una distinción nítida de los 16 años como «mayoría de edad sanitaria» para gestionar todos los procesos de información y toma de decisiones, y entre los 12 y 16 años debiendo ponderar el profesional el grado de madurez de ese menor a fin de concretar su grado de implicación y protagonismo…"*[307].

A este respecto se manifiesta también una parte de la doctrina que sostiene que *"el paciente menor de edad es el que tiene menos de 18 años, en que se adquiere la plena capacidad civil y puede tomar decisiones sobre su persona y los bienes. No obstante, en sanidad la Ley 41/2002 reconoce a los menores entre 16 y 18 años*

[304] TERRIBAS I SALA, Núria*: "Aspectos legales de la atención a los menores de edad".* Institut Borja de Bioética. Universitat Ramon Llull. FMC. 2008. Barcelona. España. Pags 367-73.

[305] Ibídem.

[306] Ibídem.

[307] TERRIBAS I SALA, Núria: *"La confidencialidad en la relación terapéutica"*. Revista de psiquiatría infanto-juvenil número 2/2012 especia congreso, sábado 12 de mayo. Barcelona, 2012.

capacidad para tomar decisiones sobre su salud"[308]*.* Sosteniendo igualmente que *"… en general para las actuaciones asistenciales ordinarias se considera capaz al mayor de 16 años; en los menores de 16 años, y siguiendo al Convenio Europeo de Bioética, "la opinión del menor será tomada en consideración como un factor que será tanto más determinante en función de su edad y su grado de madurez". Esto significa que el médico debe "meterse en la piel" de cada uno de sus pacientes menores y evaluar su nivel comprensivo respecto de sí mismo y de su entorno, valorando, conforme a esto sus opiniones y decisiones sobre su salud"*[309]*.* Así que no se deja de lado al paciente ni mucho menos, *"Cuando un paciente está incapacitado, la relación médico-paciente se establece entre el paciente que es el objeto de la atención y los cuidados del médico, pero cuando hay que tomar decisiones y cuando éstas quedan por escrito, es el tutor/a quién firma el documento y decide por el incapacitado Judicialmente"*[310]*.*

A propósito de la mayoría de edad, refiero de nuevo a Nuria Terribas, quien argumenta que *"…el Código Civil establece la mayoría de edad a los 18 años o por emancipación, excepto cuando "…haya conflicto de intereses entre los padres y el menor…", o en los "actos relativos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y sus condiciones de madurez, pueda realizar por sí mismo"*[311]*.* Y sigue diciendo que en este contexto que, *"… cabe interpretar que las decisiones en salud son actos relativos a derechos de la personalidad, y como tales no necesariamente*

[308] BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: *"Manual de ética y deontología médica".* Organización Médica Colegial de España, 2012. Pág. 49.

[309] Ibídem. Pág. 50.

[310] Ibídem. Pág. 51.

[311] TERRIBAS I SALA, Núria*: "Aspectos legales de la atención a los menores de edad".* Institut Borja de Bioética. Universitat Ramon Llull. FMC. 2008. Barcelona. España. Pags 367-73.

requieren la representación de los padres o tutores si se dan condiciones de madurez suficientes…"[312]. Comentando también, en referencia al art.5.1 de la Ley 1/1996 de 5 de enero, de Protección Jurídica del Menor, que *"…los menores tienen derecho a buscar, recibir y utilizar la información adecuada a su desarrollo"* y que *"los padres o tutores y los poderes públicos respetarán estos derechos y les protegerán ante posibles ataques de terceros"*[313]*.* E igualmente recoge respecto a este tema *que "…Merece destacarse también la Ley 15/1999 de Protección de Datos de Carácter Personal, así como el Real Decreto 1720/2007 que la desarrolla. Este último texto jurídico recoge una mención especial del consentimiento para el tratamiento de datos de menores de edad y dispone en su artículo 13 que « podrá procederse al tratamiento de datos de los mayores de 14 años con su consentimiento, salvo en los casos en que la Ley exija la asistencia de los titulares de la patria potestad. En el caso de menores de 14 años se requerirá el consentimiento de los padres o tutores»"*[314]*.*

Además esta autora ,mantiene que *"por otra parte, debemos admitir la falta de madurez social en los temas de salud de los menores, que da lugar a una paradójica realidad: por un lado la sociedad en general ha dado un altísimo grado de permisividad a los jóvenes y adolescentes, en el contexto lúdico y social, aceptando la autogestión de su propia vida sin a penas control ni supervisión; por otro lado, reclama o reivindica un ámbito de intervención máximo y estrictamente paternalista respecto a ellos, en cuanto estos contactan con el sistema sanitario, hasta el punto de no aceptar que puedan decidir por sí mismos ante ciertas situaciones de su esfera más íntima y personal (p.ej. salud sexual y reproductiva) y, por*

[312] TERRIBAS I SALA, Núria*: "Aspectos legales de la atención a los menores de edad".* Institut Borja de Bioética. Universitat Ramon Llull. FMC. 2008. Barcelona. España. Pags 367-73.

[313] Ibídem.

[314] Ibídem.

tanto, negándoles el derecho a su propia autodeterminación como individuos en formación y desarrollo"[315]*.*

Respecto a la autodeterminación de los menores, Elena Urso ha manifestado que *"…solo muy progresivamente se ha llegado a reconocer plena subjetividad jurídica a los niños y a los adolescentes, si bien graduando la amplitud de su esfera de autodeterminación, en consideración al nivel de madurez alcanzado…"*[316]*.*

Sobre el tema de la incapacidad del paciente, existe en la ley del paciente el término "instrucciones previas", como anticipación de la voluntad del mismo llegado el caso de que no pueda expresar sus deseos, y podrán ser revocadas en cualquier momento. El artículo 11.1 establece que *"por el documento de instrucciones previas, una persona mayor de edad, capaz y libre, manifiesta anticipadamente su voluntad, con objeto de que ésta se cumpla en el momento en que llegue a situaciones en cuyas circunstancias no sea capaz de expresarlos personalmente, sobre los cuidados y el tratamiento de su salud o, una vez llegado el fallecimiento, sobre el destino de su cuerpo o de los órganos del mismo. El otorgante del documento puede designar, además, un representante para que, llegado el caso, sirva como interlocutor suyo con el médico o el equipo sanitario para procurar el cumplimiento de las instrucciones previas".*

El punto segundo regula la forma en que deben constar las mismas, definiendo que *"por el documento de instrucciones previas, una persona mayor de edad, capaz y libre, manifiesta anticipadamente su voluntad, con objeto de que ésta se cumpla en el momento en que llegue a situaciones en cuyas circunstancias no sea*

[315] TERRIBAS I SALA, Núria*: "Aspectos legales de la atención a los menores de edad".* Institut Borja de Bioética. Universitat Ramon Llull. FMC. 2008. Barcelona. España. Pags 367-73.

[316] Urso, Elena, traducción Torre, E: *"Infancia, adolescencia y derecho a la salud en el hospital: el papel clave de los derechos fundamentales"*. Revista europea de derechos fundamentales. ISSN 1699-1524. Núm. 14/2ºsemestre 2009. Páginas 183-229.

capaz de expresarlos personalmente, sobre los cuidados y el tratamiento de su salud o, una vez llegado el fallecimiento, sobre el destino de su cuerpo o de los órganos del mismo. El otorgante del documento puede designar, además, un representante para que, llegado el caso, sirva como interlocutor suyo con el médico o el equipo sanitario para procurar el cumplimiento de las instrucciones previas".

El punto tercero, por su parte, marca los límites a las mismas recogiendo que *"no serán aplicadas las instrucciones previas contrarias al ordenamiento jurídico, a la «lex artis», ni las que no se correspondan con el supuesto de hecho que el interesado haya previsto en el momento de manifestarlas. En la historia clínica del paciente quedará constancia razonada de las anotaciones relacionadas con estas previsiones".* Haciendo lo propio el punto cuarto sobre la posibilidad de revocarlas, como una forma de manifestación del consentimiento que son, y establece que *"las instrucciones previas podrán revocarse libremente en cualquier momento dejando constancia por escrito".*

Finalmente el punto quinto, establece una generalidad para su regulación, ya que cada comunidad autónoma deberá gestionarlas por separado *"con el fin de asegurar la eficacia en todo el territorio nacional de las instrucciones previas manifestadas por los pacientes y formalizadas de acuerdo con lo dispuesto en la legislación de las respectivas Comunidades Autónomas, se creará en el Ministerio de Sanidad y Consumo el Registro nacional de instrucciones previas que se regirá por las normas que reglamentariamente se determinen, previo acuerdo del Consejo Interterritorial del Sistema Nacional de Salud".*

Respecto a las instrucciones previas se manifiesta una parte de la doctrina al establecer que *"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*

regula, en su artículo 11, las instrucciones previas, disponiendo que:«Por el documento de instrucciones previas, una persona mayor de edad, capaz y libre, manifiesta anticipadamente su voluntad, con objeto de que ésta se cumpla en el momento en que llegue a situaciones en cuyas circunstancias no sea capaz de expresarlos personalmente, sobre los cuidados y el tratamiento de su salud o, una vez llegado el fallecimiento, sobre el destino de su cuerpo o de los órganos del mismo»"[317]*.* Y continúa especificando este sector que *"como acto autónomo y libre de una persona, y tal como dispone el número 4 del artículo 11 de la Ley 41/2002, «las instrucciones previas podrán revocarse libremente en cualquier momento dejando constancia por escrito». Aunque la normativa estatal no indica nada al respecto, hay que entender que el acto de revocación, así como el de modificación, exige la concurrencia del requisito de capacidad en el otorgante"*[318].

A propósito del tema de los menores de edad, la Ley Orgánica sobre protección del honor, intimidad e imagen establece en el artículo 3.1 que *"el consentimiento de los menores e incapaces deberá prestarse por ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil"*. Y sobre el resto de casos, especifica en el punto segundo que *"…el consentimiento habrá de otorgarse mediante escrito por su representante legal, quien estará obligado a poner en conocimiento previo del Ministerio Fiscal el consentimiento proyectado. Si en el plazo de ocho días el Ministerio Fiscal se opusiere, resolverá el Juez".*

Además, el artículo 7 Real Decreto-Ley sobre células y tejidos, establece en su punto primero que *"la obtención de células y tejidos de una persona viva para su ulterior aplicación alogénica en seres humanos podrá realizarse si el donante es mayor de edad, cuenta con plena capacidad de obrar y estado de salud adecuado y ha*

[317] BANDRÉS MOYÁ, Fernando Y DELGADO BUENO, Santiago: "*Biomedicina y derecho sanitario*". Ademas Comunicación, S.L., 2009. Pág. 469.

[318] Ibídem. Pág. 480.

prestado por escrito su consentimiento informado. La información que recibirá el donante del médico que haya de realizar la extracción o sea responsable de esta, debe cubrir el objetivo y la naturaleza de la obtención de las células y tejidos; sus consecuencias y riesgos; las pruebas analíticas que se han de realizar; el registro y protección de los datos; y los fines terapéuticos. Asimismo se informará de las medidas de protección aplicables al donante y de los beneficios que con el uso del tejido o grupo celular extraído se espera que haya de conseguir el receptor. El consentimiento podrá ser revocado en cualquier momento antes de la obtención de la célula y/o el tejido, excepto en los casos de obtención de progenitores hematopoyéticos de sangre periférica o de médula ósea, en que la revocación sólo podrá producirse antes del inicio del tratamiento de acondicionamiento en el receptor. No podrán obtenerse células y tejidos de personas menores de edad o de personas que por deficiencias psíquicas, enfermedad mental, incapacitación legal o cualquier otra causa, no puedan otorgar su consentimiento, salvo cuando se trate de residuos quirúrgicos o de progenitores hematopoyéticos u otros tejidos o grupos celulares reproducibles cuya indicación terapéutica sea o pueda ser vital para el receptor. En estos casos, el consentimiento será otorgado por quien ostente la representación legal".

Tema el de los menores, antes no contemplado en la normativa de protección de datos, de gran actualidad e interés en todos los sectores que tratan datos de este colectivo, especialmente en el sector médico, que como se ha visto, cuenta con gran cantidad de normativa que regula esta materia.

IV.3.c. Forma de recabar el consentimiento:

La LOPD, como ya se ha visto, recogía en su artículo 7.3 la condición de que el consentimiento sea expreso para el tratamiento de los datos relativos a la salud. El RLOPD por su parte, no contiene ninguna disposición aplicable a los datos de salud que ocupan este

estudio respecto a la forma de obtención del consentimiento, más que lo establecido en el tantas veces nombrado 10.5 en clara referencia a lo establecido en los artículo 7 y 8 de la LOPD como claras referencias respecto de los datos de salud.

El punto segundo del artículo 8 de la Ley del paciente, establece además la forma en que ha de otorgarse el consentimiento, y dice que *"el consentimiento será verbal por regla general. Sin embargo, se prestará por escrito en los casos siguientes: intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente".* Es decir que no valdrá la norma general para casos invasivos o de riesgo para la salud del paciente. Y puntualiza el punto tercero a continuación que *"el consentimiento escrito del paciente será necesario para cada una de las actuaciones especificadas en el punto anterior de este artículo, dejando a salvo la posibilidad de incorporar anejos y otros datos de carácter general, y tendrá información suficiente sobre el procedimiento de aplicación y sobre sus riesgos".* El punto quinto finalmente, habla de la posibilidad de revocarlo, estableciendo que *"el paciente puede revocar libremente por escrito su consentimiento en cualquier momento".*

El artículo 10 de la Ley del paciente, establece por su parte, las condiciones de la información y consentimiento por escrito. Así, su punto primero, *"el facultativo proporcionará al paciente, antes de recabar su consentimiento escrito, la información básica siguiente: a) Las consecuencias relevantes o de importancia que la intervención origina con seguridad. b) Los riesgos relacionados con las circunstancias personales o profesionales del paciente. c) Los riesgos probables en condiciones normales, conforme a la experiencia y al estado de la ciencia o directamente relacionados con el tipo de intervención. d) Las contraindicaciones".* Y establece

además su punto segundo que *“el médico responsable deberá ponderar en cada caso que cuanto más dudoso sea el resultado de una intervención más necesario resulta el previo consentimiento por escrito del paciente”.* Por lo que pudiera parecer más necesario en unas situaciones que en otras, tema ya debatido en el apartado general del consentimiento.

IV.3.d. revocación del consentimiento:

Acabamos de ver en el 6.3 que el consentimiento otorgado puede ser revocado con causa justificada y siempre que no haya efectos retroactivos.

Por su parte, el RLOPD, establece en su artículo 17 la revocación del consentimiento, recogiendo en su punto primero que *“el afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido. No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado”.* Es decir, a través de un medio gratuito, como ya se estableciera para el ejercicio de los derechos.

El punto segundo de este artículo, establece por su parte el plazo para hacer efectiva la revocación solicitada, estableciendo que *“el responsable cesará en el tratamiento de los datos en el plazo*

máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre". Cumpliendo además el requisito establecido en el 17.3 *"cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a la solicitud".* Al igual que ocurría en el ejercicio del derecho de rectificación, que establece el último punto de este artículo al recoger que *"si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el plazo previsto en el apartado 2, para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre".*

IV.4. DATOS ESPECIALMENTE PROTEGIDOS: DATOS RELATIVOS A LA SALUD:

Los datos relativos a la salud de las personas, regulados de forma específica por la legislación española y europea, han sido referidos de forma puntual en todos los apartados de este estudio, con el fin de dar una visión amplia sobre el tratamiento de este tipo de datos personales en los centros sanitarios.

Recordemos no obstante en este punto, por su importancia, que el Convenio 108 recoge en su artículo 6 que *"los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales"*.

Asimismo los artículos 7 y 8 de la LOPD referidos respectivamente a los datos especialmente protegidos y a los datos de salud, hay sido ya inevitablemente referidos a lo largo de este estudio a las alturas que estamos, tanto en referencia al consentimiento en cuanto a los datos especialmente protegidos, como en referencia a la cesión de datos en cuanto a los datos de salud, que también fueron referidos en la introducción.

No obstante, no se puede olvidar en este punto, debido a su relevancia en este estudio, que el artículo 8 establece que *"…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".* Y por su parte el 7.3 recogía que *"los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente".*

Respecto del consentimiento necesario para el tratamiento de los datos de salud, es interesante nombrar que el informe de la AEPD 0242/2010 establece que *"…atendiendo al principio de finalidad contemplado en el artículo 4.1 de la LOPD que dice 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 finalidades determinadas, explícitas y legítimas para las que se hayan obtenido", nos lleva a concluir que la comunicación o acceso a los datos de la historia clínica con finalidades distintas de las que señala el artículo 14.2 de la Ley 41/2002, como es el presente supuesto, en el que el acceso a los datos tendría una finalidad de control del cumplimiento de la normativa fiscal por los profesionales*

que atendieron al paciente, no tendría cabida en las previsiones del artículo 7.3 de la LOPD, salvo consentimiento expreso del afectado".

Otro informe jurídico de la AEPD, el 0438/2012 habla de los datos sensibles en el concreto caso de *"…aquellos supuestos en que una persona que tenga acceso a la historia clínica por razones profesionales, considere que debe poner en conocimiento del órgano consultante que un persona carece de las condiciones psíquicas o físicas precisas para conducir, a fin de que se inicie el oportuno expediente de retirada del permiso de conducción".* Ante lo que la AEPD resuelve que *"…a falta de una norma con rango de ley que ampare la comunicación de datos objeto de consulta solamente sería conforme a lo establecido en la Ley Orgánica 15/1999 dicha cesión de datos en caso de que se haya obtenido el consentimiento expreso del interesado".*

Es oportuno reseñar la Sentencia de la Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 29-03-2006 referida a Datos de salud, cesión de datos, consentimiento expreso y acceso de datos por cuenta de terceros, en cuyos fundamentos de derecho se recoge que *"en el presente caso, especifica dicha resolución impugnada, el tratamiento de datos de carácter personal lo realiza la franquiciada con sede en (.....), recabando los datos personales de los pacientes y realizándose los tratamientos sanitarios de los mismos. Estos tratamientos se registran en ficheros que son enviados a las dos entidades actoras, las franquiciadoras, con sedes ambas en ....., quienes reciben esa información a tenor de lo pactado en los contratos de franquicia con el fin del control de la facturación. Continua el acto recurrido indicando que el contenido de esa información es el que se recoge en el hecho probado segundo, lo que supone que ese tratamiento que las franquiciadoras efectúan de los datos de pacientes que les remiten las franquiciadas no es el recogido en el artículo 7.6 de la LOPD, pues dicho tratamiento no es necesario para la prevención o*

para el diagnóstico médico, ni para la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, ni para la preservación de la salud de los pacientes, sino para el control de facturación entre mercantiles asociadas; por lo que no procede el tratamiento de los referidos datos relativos a la salud sin el consentimiento expreso de los afectados"[319]*.* Una prueba más del acceso indebido a los datos personales, más grave en estas situaciones en que se refieren a datos de salud de las persona

Otra sentencia de la Audiencia Nacional, recoge en sus fundamentos de derecho que *"el 17 de mayo de 1999 se presentó denuncia ante la Agencia de Protección de Datos (APD) por representantes sindicales de los trabajadores de La Entidad Pública "B". En dicha denuncia se indicaba, entre otras cosas, que varios trabajadores en situación de baja habían recibido visitas de médicos que decían actuar en nombre de la empresa, personándose en su domicilio, y con datos relativos a los mismos facilitados por la citada entidad. Con el fin de explorar al trabajador en situación de baja. Posteriormente se adjunto documentación referida a la celebración de un convenio suscrito entre la entidad citada y otras sociedades con el fin, entre otros, de realizar visitas médicas domiciliarias al personal que se encuentra en situación de baja por enfermedad"*[320]*.* Esto a mi parecer invade la intimidad del paciente que no ha sido avisado previamente.

Y es que *"…parece que cuando se trata de los datos relativos a nuestra salud, vemos más importante su vigilancia; no en vano gozan de una especial protección en la legislación actual, en materia de protección de datos. Pero no es menos cierto que, aunque queramos que se protejan, queremos a la vez que sean conocidos*

[319] Audiencia Nacional. Sentencia de 29-03-2006. Sala de lo Contencioso-Administrativo, sección primera. Datos de salud. Cesión de datos. Consentimiento expreso. Acceso de datos por cuenta de terceros.

[320] Sentencia de la Audiencia Nacional de 10-05-2002. Sala de lo contencioso administrativo. Sección Primera. Tratamiento de datos médicos para el control del absentismo.

por el personal sanitario. ¿Quién no ha deseado al entrar en un centro sanitario, que los profesionales que le atienden sepan cuanto antes todo sobre el paciente, para lograr un mayor éxito en el proceso asistencial, evitando con ello horas de incertidumbre? Seguramente quien se haga esta pregunta comprenderá que tan importante es el mantener una reserva sobre la información de los pacientes, como que esa información sea conocida, por supuesto por el personal adecuado y con las cautelas debidas"[321].

A este respecto otra referencia jurisprudencial establece entre sus fundamentos de derecho que *"la legislación española, como anticipamos, se encuadra dentro de las que consideran que determinados datos son especialmente sensibles "per se" y como se dice en la Exposición de Motivos en este tipo de datos "los contornos del principio del consentimiento se refuerzan singularmente". Principio regulador que permanece estable tanto en la LO 5/1992, como en la 15/1999, si bien esta última ha introducido las precisiones contenidas en la Directiva95/46/CEE"*[322].

Herrán Ortiz opina al respecto que *"…por datos sensibles debe entenderse una categoría especial de datos de carácter personal que encuentran en la Ley un régimen jurídico de protección reforzado debido no solo a su proximidad con la esfera más interior o privada de la persona, sino fundamentalmente a que constituyen la esencia misma de la persona como individuo y fundamentan su desarrollo personal, de suerte que en ocasiones nada tienen que ver con la intimidad en el sentido de ocultamiento, sino más bien se refieren a otras facetas de la persona, como la dignidad y la personalidad individual que adquieren especial relevancia en su*

[321] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012.

[322] Sentencia de la Audiencia Nacional de 10-05-2002. Sala de lo contencioso administrativo. Sección Primera. Tratamiento de datos médicos para el control del absentismo.

relación con los demás, y que por tanto, no son necesariamente íntimas o reservadas aunque sí privadas" [323]*.*

Nuria Terribas opina en cambio que "*… la sensibilidad de un dato que pertenece a un tercero no podemos juzgarla desde nuestro propio criterio individual"*[324].

Otro sector doctrinal, establece por su parte que "*…la expresión "datos médicos" se refiere a todos los datos personales relativos a la salud de un individuo. Se refiere también a los datos que tengan una clara y estrecha relación con la salud y los datos genéticos…"*[325]*.*

Otros autores en cambio manifiestan respecto a estos conceptos que *"en primer lugar debemos identificar de qué hablamos cuando nos referimos a los datos, y particularmente cuando hablamos de datos clínicos y relativos a la propia salud. Los datos personales están formados por la información referida a personas físicas identificadas o identificables (persona concernida), y dentro de los mismos hay dos tipos de datos en función de su naturaleza: datos no sensibles, y datos "sensibles" o "especialmente protegidos" conforme al Convenio 108 del Consejo de Europa, de 28 de enero de J 981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Tol 554957), en adelante Convenio 108*"[326]. "*Por tanto, cuando hablamos de los datos clínicos referidos a la propia salud nos estamos refiriendo a datos de carácter personal y específicamente a unos*

[323]HERRÁN ORTIZ, Ana Isabel: "*La violación de la intimidad en la protección de datos personales*". Dykinson, Madrid 1.999. Pág. 263.

[324] TERRIBAS SALA, Núria: "*Los avances del derecho ante los avances de la medicina. Confidencialidad de los datos sanitarios: de la norma a la práctica médica*". In Salomé Adroher Biosca- Thomson Aranzadi, 2008. Pags 796-802.

[325] ATELA BILBAO, Alfonso, BENAC URROZ, Mariano, CODÓN HERRERA, Alfonso, GARAY ISASI, Josu, GONZÁLEZ SALINAS, Pedro, HERNÁNDEZ-MARTÍNEZ CAMPELLO, Carlos, LIZARRAGA BONELLI, Emilio, MARTÍ MONTESINOS, Cristina, PELLEJERO GARCÍA, Carlos, PIDEVAL BORRELL, Ignasi, VILLAR ABAD, Gloria, GONZÁLEZ PÉREZ, Jesús: *"Autonomía del paciente, información e historia clínica"*. Editorial Aranzadi, Madrid 2004. Pág. 166.

[326] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores): "*La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural*". Tirant Lo Blanch, Valencia, 2014. Pág. 331.

datos que gozan del carácter de sensibles, y dentro de los mismos, a la información relativa a la salud de la persona, que será recogida e incorporada en la historia clínica"[327]. Concepto, el de historia clínica, ampliamente analizado en apartados precedentes.

Pero hay otros que sostienen que *"como no es posible limitar una clasificación determinada de datos sensibles, debe tratarse entonces de reconocer la sensibilidad de ciertos datos atendiendo a su utilización, es decir, de datos que a priori son irrelevantes desde el punto de vista de su calidad, pero que interrelacionados pueden dar lugar a un perfil de la personalidad del individuo"*[328]*.* Sobre este tema *"en el derecho comparado, tenemos que en la normativa de protección de datos, en España, así como en los países europeos, han optado mayoritariamente por categorías cerradas de datos sensibles, a las que otorga una tutela reforzada frente a los datos ordinarios. Una excepción lo constituye la Ley Suiza, que recogió expresamente el perfil de la personalidad como dato sensible. Ésta consideró datos sensibles las siguientes informaciones: "Los datos personales acerca de las opiniones o actividades religiosas, filosóficas, políticas y sindicales, la salud, la esfera íntima o la pertenencia a una raza, medidas de asistencia social, investigaciones o sanciones penales o administrativas y el perfil de la personalidad, como un conjunto de datos que permiten apreciar las características esenciales de la personalidad de una persona física"*[329].

La sección tercera de la Directiva sobre protección en el tratamiento de datos, se encarga de las categorías especiales de

---

[327] FERNÁNDEZ-CORONADO, Ana y PÉREZ-ÁLVAREZ, Salvador (directores): "*La protección de la salud en tiempos de crisis. Nuevos retos del bioderecho en una sociedad plural*". Tirant Lo Blanch, Valencia, 2014. Pág. 332.

[328] PÉREZ FUENTES, Gisela María (coordinadora): *"Temas selectos de derecho a la información, derecho a la intimidad, transparencia y datos personales".* Editorial Sista, S.A. Tabasco, México, 2010. Pág. 121.

[329] Ibídem.

tratamientos, entre los que se encuentran los datos relativos a la salud que ocupan este estudio. Y su tratamiento queda prohibido salvo, en el caso de los datos médicos, para la prevención o diagnóstico médicos, asistencia o tratamiento sanitario o gestión de tales servicios siempre que el tratamiento se lleve a cabo por personal sanitario sujeto al secreto profesional, exista consentimiento explícito, o la necesidad de proteger un interés vital del interesado incapacitado o de un tercero. Se deja la puerta abierta a otras excepciones por interés público importante y bajo el control de la autoridad nacional de control.

Así su artículo 8.1 bajo la rúbrica de categorías especiales de tratamientos establece 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".*

En el punto segundo de este mismo artículo que *"lo dispuesto en el apartado 1 no se aplicará cuando: a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los 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, 0 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".

Además el punto tercero que *"el apartado 1 no se aplicará cuando el tratamiento de datos 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 dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto".*

Pero esta no es la única excepción, ya que el punto cuarto establece otras excepciones *"siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control".* Excepciones ampliadas también en el apartado quinto el cual establece que *"el tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos. Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones*

administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos". Y por último el apartado sexto establece que "Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión".

IV.5. SEGURIDAD DE DATOS:

El Convenio 108 ya se encargó de regular este tema en su artículo 7, el cual establece *que "se tomaran medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la perdida accidental, así como contra el acceso, la modificación o la difusión no autorizados".*

"La seguridad de los datos es uno de los pilares de la protección de datos, regulado en el artículo 9 de la LOPD, que establece que se "deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural", y por otro lado, que *"no podrán mantenerse ficheros, que no reúnan las condiciones y requisitos establecidas por vía reglamentaria, en relación a los datos personales, y recursos que los alberguen, ya sean centros de tratamiento, locales, equipos, programas o sistemas, y a las personas que intervengan en su tratamiento". Y cito literalmente este artículo, porque es muy explicativo de las circunstancias y recursos que pueden afectar a los datos. Esto ha sido desarrollado reglamentariamente por RLOPD,*

que divide la protección en niveles básico, medio y alto, incluso para los datos en soporte papel"[330]*.*

El artículo 9 de la LOPD, que regula este tema, ya fue referido en la introducción de este estudio y será a continuación comentado en relación con la Recomendación sobre protección de datos médicos, por lo que no redundaré ahora más en su literatura.

Establece la Recomendación sobre protección de datos médicos, por su parte que *"recordando los principios generales sobre protección de datos de la Convención para la Protección de los Individuos en relación al Tratamiento Automatizado de Datos Personales (Series Tratados Europeos, n. 108) y en particular su artículo 6, que estipula que los datos personales relativos a la salud no pueden ser procesados automatizadamente a menos que el ordenamiento nacional proporcione medidas de seguridad apropiadas; Consciente del incremento del uso de datos médicos tratados automatizadamente por sistemas de información, no sólo para la asistencia médica, la investigación médica, la gestión hospitalaria y la salud pública, sino también fuera del sector sanitario; Convencido de la importancia de la calidad, integridad y disponibilidad de los datos médicos para el afectado por tales datos y su familia; Consciente de que el progreso de la ciencia médica depende en buena medida de la disponibilidad de datos médicos sobre individuos; Convencido de que es deseable regular la recogida y procesamiento de datos médicos, salvaguardar la confidencialidad y la seguridad de los datos personales relativos a la salud, y asegurar que se emplean de acuerdo con los derechos y libertades fundamentales del individuo, y en particular con el derecho a la intimidad; Consciente de que el progreso en la ciencia médica y los avances en la tecnología informática desde 1981 hacen necesario*

[330] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

revisar varias disposiciones de la Recomendación N. R (81) sobre la regulación de los bancos de datos médicos automatizados…".

Se establece en concreto en la comentada recomendación que *"den pasos para asegurar que los principios contenidos en el apéndice a esta recomendación se reflejen en sus leyes y en la práctica; aseguren una amplia difusión de los principios contenidos en el apéndice a esta recomendación entre las personas implicadas, por razón de su profesión, en la recogida y procesamiento de datos médicos…".*

Sobre el ámbito de aplicación de esta norma, recoge su artículo 2.1 que *"esta recomendación es aplicable a la recogida y tratamiento automatizado de datos médicos, salvo que la ley nacional, en un contexto específico fuera del sector sanitario, proporcione otras medidas de seguridad apropiadas"*. Puntualizando el punto segundo que *"un Estado miembro puede extender los principios establecidos en esta recomendación a datos médicos no procesados automatizadamente"*.

De modo que ya se adelantaba en su tiempo a la normativa existente, previendo que la regulación en materia médica podía extenderse también a los datos en soporte papel. Y respecto a la intimidad el artículo 3.1 dice que *"se garantizará el respecto a los derechos y libertades fundamentales, y en particular al derecho a la intimidad, durante la recogida y procesamiento de datos médicos"*. Anotando el 3.2 que *"los datos médicos sólo pueden recogerse y procesarse si existen medidas de protección adecuadas establecidas por la ley nacional".* No obstante, el penúltimo párrafo de este artículo sigue diciendo que *"en principio, los datos médicos deben ser recogidos y procesados sólo por profesionales sanitarios o por individuos u órganos que trabajen en representación de profesionales sanitarios. Los individuos u órganos que trabajen en representación de profesionales sanitarios recogiendo y procesando datos médicos deben estar sujetos a las mismas normas de*

confidencialidad que pesan sobre los profesionales sanitarios o a normas de confidencialidad comparables". Esto desde luego está en directa relación con las funciones y obligaciones del personal, así como con la subcontratación de servicios que supongan el acceso a los datos de los pacientes por cuenta de terceros, temas anteriormente comentados. Y sigue insistiendo el último párrafo en que *"los administradores de archivos que no son profesionales sanitarios sólo deben recoger y procesar datos médicos cuando estén sujetos a normas de confidencialidad comparables a las que pesan sobre el profesional sanitario o a medidas de seguridad igualmente eficaces proporcionadas por la ley nacional"*.

La recogida y procesamiento de datos médicos debe respetar los fines para los que se recogieron, según establece el 4.1 de esta recomendación, *"los datos médicos deben ser recogidos y procesados honrada y legalmente y sólo para fines especificados"*. Obteniéndolos del afectado o de persona distinta solo en determinadas circunstancias, ya que según recoge el 4.2, *"los datos médicos deben obtenerse, en principio, del afectado. Sólo pueden ser obtenidos de otras fuentes si se hace de acuerdo con los Capítulos 4, 6 y 7 y si esto es necesario para alcanzar los fines del procesamiento o si el afectado no está en posición de proporcionarlos".* Recordemos a este respecto que los puntos 4,6 y 7 se refieren respectivamente de la recogida y procesamiento de datos médicos, consentimiento y comunicación, y se encuentran reubicados en los apartados correspondientes de este estudio.

Dentro de esta misma norma a la que vengo refiriéndome ya largo rato, se encuentra regulado en el apartado nueve la seguridad, a la que hace referencia el título del apartado en el que estamos. Pues bien, su punto primero establece como premisa que *"se tomarán las medidas técnicas y de organización adecuadas para proteger los datos personales procesados de acuerdo con esta recomendación contra su destrucción accidental o ilegal y su pérdida*

accidental, así como contra el acceso, alteración, comunicación o cualquier otra forma de procesamiento no autorizados". Estableciendo su segundo párrafo que *"Estas medidas asegurarán un nivel apropiado de seguridad, teniendo en cuenta, de una parte, el estado de la técnica y, de otra, la naturaleza sensible de los datos médicos y la evaluación de los riesgos potenciales".* Y es en su punto tercero donde se establece que *"estas medidas serán revisadas periódicamente".*

Como puede observarse, este texto coincide en gran parte con el apartado primero del artículo nueve de la LOPD, que ya ha sido citado, pero que es necesario referir de nuevo en este punto para ver la similitud con la regulación sanitaria en este aspecto y recordar que *"el responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".* Ambas coinciden en que la tecnología y la naturaleza de los datos, así como los posibles riesgos, son factores fundamentales a tener en cuenta. Lo que no dice la referida recomendación, pero sí la LOPD en su punto segundo es que *"no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas".* De modo que por vía reglamentaria deben establecerse las normas que deben cumplir los lugares o dispositivos que alojen los datos personales. Y además en su punto tercero se establece que *"reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley"*. Esto último, en expresa referencia al artículo 7 de la

LOPD que regula los datos especialmente protegidos, dentro de los cuales se encuentran los datos de salud.

En cambio, la recomendación, hace unas estipulaciones en el apartado segundo del punto noveno de su apéndice para la protección de los pacientes que dice así literalmente, *"en orden a asegurar en particular la confidencialidad, integridad y exactitud de los datos procesados, así como la protección de los pacientes, se tomarán medidas apropiadas para: a. impedir que cualquier persona no autorizada tenga acceso a las instalaciones de procesamiento de datos personales (control de entrada a las instalaciones); b. impedir que el soporte de los datos sea leído, copiado, alterado o retirado por personas no autorizadas (control del soporte de los datos); c. impedir la introducción no autorizada de datos en el sistema de información, y cualquier consulta, modificación o borrado no autorizados de datos personales procesados (control de memoria); d. impedir que los sistemas de procesamiento automatizado de datos sean usados por personas no autorizadas a través de equipos de transmisión de datos (control de utilización); e. asegurar -teniendo en cuenta, por un lado, el acceso selectivo a los datos y, por otro, la seguridad de los datos médicos- que el diseño del sistema de procesamiento, como norma general, es tal que permite la separación de: - identificadores y datos relativos a la identidad de las personas, - datos administrativos, - datos médicos, - datos sociales, - datos genéticos (control de acceso); f. garantizar la posibilidad de comprobar y verificar a qué personas u órganos se pueden comunicar los datos a través de equipos de transmisión de datos (control de comunicación); g. garantizar que es posible comprobar y establecer 'a posteriori' quién ha tenido acceso al sistema y qué datos personales han sido introducidos en el sistema de información, cuándo y por quién (control de introducción de datos); h. impedir la lectura, copia, alteración o borrado no autorizados de datos personales durante la comunicación de datos personales y el*

traslado de soportes de datos (control de transporte); i. salvaguardar los datos mediante copias de seguridad (control de disponibilidad)".

Como se ve una relación de controles, algunos coincidentes con los establecidos en los capítulos tercero y cuarto del RLOPD, que como normativa reglamentaria de desarrollo de la LO, vienen a establecer respectivamente Medidas de seguridad aplicables a los ficheros y tratamientos automatizados y no automatizados, lo que pudiera estar en relación con los comentados 9.2 y 9.3 de la LOPD.

Contempla por último la recomendación, en relación a la seguridad de los datos médicos, la figura de los administradores de archivos, regulada igualmente en el ya comentado apartado nueve del apéndice de este texto. Así, el punto tercero del comentado artículo nueve, dice que *"los administradores de archivos médicos deben, de acuerdo con la ley nacional, elaborar normas internas apropiadas que respeten los principios pertinentes de esta recomendación".* Y su punto cuarto establece igualmente que *"cuando sea necesario, los administradores de archivos de procesamiento de datos médicos deben designar a una persona independiente como responsable de la seguridad de los sistemas de información y de la protección de los datos, y que sea competente para asesorar en estas materias"*. Donde, como vemos, aparece la figura del responsable de seguridad, esta sí, regulada ampliamente en la normativa de protección de datos.

Obviamente, esta disposición es anterior al RLOPD, en el cual además de los datos en soporte informático se regulan los datos en soporte papel; y sí, efectivamente, en España es precisamente el citado reglamento el que establece las medidas de seguridad a tomar en cada tratamiento de datos, como ya se ha dicho anteriormente en la parte general.

La Ley 14/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida hace referencia a las auditorías técnicas y legales de los centros de reproducción humana asistida

en el artículo 19, como medida de seguridad aplicable en los niveles altos de protección.

Así mismo, establece la Ley de Calidad Sanitaria, que la calidad de las mencionadas prestaciones la lleva a cabo la Agencia de Calidad del Sistema Nacional de Salud, dependiente del Ministerio de Sanidad y consumo, el cual deberá garantizar además la realización de una auditoría externa que garantice la calidad de los servicios. Además, dependerá de este último organismo el Observatorio del Sistema Nacional de Salud, que analizará de forma permanente la gestión de los servicios sanitarios de las comunidades autónomas. Existiendo además, el Consejo Interterritorial del Sistema Nacional de Salud, a instancia de la Ley General de Sanidad, como intermediario entre el Estado y las comunidades autónomas.

Así lo expresa el párrafo segundo del octavo apartado de la exposición de motivos, *"dentro de la Administración General del Estado, se encomienda a la Agencia de Calidad del Sistema Nacional de Salud, órgano dependiente del Ministerio de Sanidad y Consumo, la elaboración de los elementos de la infraestructura de la calidad, sin perjuicio de las actuaciones en este orden de las comunidades autónomas. Estos elementos estarán a disposición de las propias comunidades y de los centros sanitarios públicos y privados, con la finalidad de contribuir a la mejora de la calidad de los servicios que prestan a los pacientes".*

Continuando el párrafo cuarto diciendo que *"asimismo se encomienda al Ministerio de Sanidad y Consumo el fomento de la auditoría externa periódica de los centros y servicios sanitarios, en garantía de su seguridad y de la calidad de dichos servicios".* Y por último, en relación a este organigrama, concluye el último párrafo que *"…el Observatorio del Sistema Nacional de Salud, órgano igualmente integrado en el Ministerio de Sanidad y Consumo, proporcionará un análisis permanente del sistema, mediante*

estudios comparados de los servicios de salud de las comunidades autónomas en el ámbito de la organización, de la provisión de servicios, de la gestión sanitaria y de los resultados".

Por su parte, el apartado XII establece que *"…el Consejo, órgano de cooperación entre el Estado y las comunidades autónomas, tiene encomendada la misión de promover la cohesión del sistema…*". Cuestiones todas estas abordadas y desarrolladas por legislaciones posteriores, como se ha venido observando a lo largo del estudio.

Según la Ley sobre el uso de los medicamentos, la recogida de datos necesaria para que el mercado de medicamentos esté abastecido, y se pueda garantizar una seguridad en el suministro de los mismos a los ciudadanos, debe respetar en todo caso la LOPD, siendo titulares de dichos ficheros las diferentes administraciones estatales, autónomas y locales que corresponda en cada caso. Así lo recoge su artículo 87.1 *"con el fin de lograr un adecuado abastecimiento del mercado y establecer garantías de seguridad para los ciudadanos, los laboratorios, los almacenes mayoristas, las oficinas de farmacia, los establecimientos comerciales detallistas y las entidades o agrupaciones ganaderas autorizadas para la dispensación de medicamentos veterinarios, están sujetos a las obligaciones de información a que se refiere este artículo".* Y puntualiza su punto sexto de este artículo que *"la recogida y tratamiento de datos a que se refiere este artículo deberá adecuarse a la normativa vigente en materia de seguridad y protección de datos de carácter personal, en cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, teniendo la consideración de responsables de sus respectivos ficheros de titularidad pública la Administración General del Estado, las Administraciones sanitarias competentes de las Comunidades Autónomas y, en su caso, las Administraciones corporativas correspondientes".*

El artículo 41.1 de la Ley de Telecomunicaciones, por su parte, se dedica en pleno a la protección de datos de carácter personal, estableciendo la obligación de adoptar las medidas necesarias de seguridad a los operadores de servicios de comunicaciones electrónicas que los pongan a disposición del público, o los comercialicen a través de redes públicas, incluidas aquellas que dan soporte a dispositivos de identificación o recopilación de datos. Así lo expresa concretamente este precepto estableciendo que *"los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar la protección de los datos de carácter personal…".*

Y los mínimos establecidos a este respecto consisten en restringir el acceso al personal autorizado, establecer medidas para la destrucción, alteración o pérdidas accidentales y para los accesos a datos no autorizados o que estén fuera de la ley, así como el establecimiento de una política de seguridad para el tratamiento de datos personales que se aplique de forma efectiva. Así lo sigue manifestando este mismo precepto, que recoge que *"dichas medidas incluirán, como mínimo: a) La garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la Ley. b) La protección de los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos. c) La garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales".*

Pero estas medidas podrán ser revisadas por la AEPD, quien igualmente podrá hacer recomendaciones para asegurar el adecuado nivel de seguridad, como establece el último párrafo del comentado precepto, *"la Agencia Española de Protección de Datos, en el ejercicio de su competencia de garantía de la seguridad en el tratamiento de datos de carácter personal, podrá examinar las medidas adoptadas por los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público y podrá formular recomendaciones sobre las mejores prácticas con respecto al nivel de seguridad que debería conseguirse con estas medidas".*

Si se detecta un riesgo concreto para los abonados de los servicios de comunicaciones electrónicas, deberán ser avisados del mismo así como de las medidas que se vayan a adoptar, ya que así lo establece el segundo punto del artículo 41 *"en caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar".*

Y por último, si existiera una violación de los datos personales, se deberá poner en conocimiento de la AEPD, incluso al abonado si se pudiera ver dañada su intimidad, y no han quedado probadas las pertinentes medidas de seguridad, según establece el primer párrafo del punto tercero del artículo 41. Todo ello, sin perjuicio, según establece el punto cuarto del artículo 41, de la aplicación de la normativa existente en materia de protección de datos, que recoge que: *"Lo dispuesto en el presente artículo será sin perjuicio de la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo".* Todas estas medidas afectan, por supuesto, a los datos médicos, siempre que se utilicen las redes de telecomunicaciones

para su gestión, de modo que, es una normativa a la que también pueden acogerse los pacientes.

En relación con la seguridad de los datos y por la sensibilidad de los datos a tratar, es necesario cita aquí lo recogido en el artículo 21 de la LO 2/2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo (LA- Ley del aborto), el cual recoge que, que regula el tratamiento de los datos, que según establece su punto primero *"en el momento de la solicitud de información sobre la interrupción voluntaria del embarazo, los centros, sin proceder al tratamiento de dato alguno, habrán de informar a la solicitante que los datos identificativos de las pacientes a las que efectivamente se les realice la prestación serán objeto de codificación y separados de los datos de carácter clínico asistencial relacionados con la interrupción voluntaria del embarazo".*

Puntualizando su punto segundo que *"los centros que presten la interrupción voluntaria del embarazo establecerán mecanismos apropiados de automatización y codificación de los datos de identificación de las pacientes atendidas, en los términos previstos en esta Ley. A los efectos previstos en el párrafo anterior, se considerarán datos identificativos de la paciente su nombre, apellidos, domicilio, número de teléfono, dirección de correo electrónico, documento nacional de identidad o documento identificativo equivalente, así como cualquier dato que revele su identidad física o genética".*

El punto tercero, por su parte, sigue insistiendo en la seguridad de los datos tratados y establece que *"en el momento de la primera recogida de datos de la paciente, se le asignará un código que será utilizado para identificarla en todo el proceso"*.

Y el punto cuarto que *"los centros sustituirán los datos identificativos de la paciente por el código asignado en cualquier información contenida en la historia clínica que guarde relación con la práctica de la interrupción voluntaria del embarazo, de forma que*

no pueda producirse con carácter general, el acceso a dicha información".

Concluyendo finalmente su punto quinto que *"las informaciones relacionadas con la interrupción voluntaria del embarazo deberán ser conservadas en la historia clínica de tal forma que su mera visualización no sea posible salvo por el personal que participe en la práctica de la prestación, sin perjuicio de los accesos a los que se refiere el artículo siguiente"*. Como puede observarse, queda claro que el tratamiento debe ser codificado, lo cual presume la confidencialidad de la información, lo cual enlaza con el apartado siguiente de este estudio.

Incluso cabría aquí citar el artículo 23.1 de esta misma norma, que regula la cancelación de los datos, los cual también podría tener directa relación con la confidencialidad de los mismos, al establecer que *"los centros que hayan procedido a una interrupción voluntaria de embarazo deberán cancelar de oficio la totalidad de los datos de la paciente una vez transcurridos cinco años desde la fecha de alta de la intervención. No obstante, la documentación clínica podrá conservarse cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud, en cuyo caso se procederá a la cancelación de todos los datos identificativos de la paciente y del código que se le hubiera asignado como consecuencia de lo dispuesto en los artículos anteriores".* Refiriéndose su punto segundo en relación directa a la protección de datos que *"Lo dispuesto en el apartado anterior se entenderá sin perjuicio del ejercicio por la paciente de su derecho de cancelación, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal".*

IV.5.a. Medidas de seguridad:

El Convenio 108 ya recogía en su artículo 4.1, que *"…cada parte tomara, en su derecho interno, la medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capitulo",* especificando en el punto segundo que *"dichas medidas deberán adoptarse a mas tardar en el momento de la entrada en vigor del presente convenio con respecto a dicha parte".*

El RLOPD se encarga de regular estas medidas de seguridad en el tratamiento de datos de carácter personal en su título VIII, estableciéndose en el artículo 79 el alcance de las mismas, el cual establece que *"los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cuál sea su sistema de tratamiento".*

Seguidamente el artículo 80 hace una clasificación de los niveles de seguridad estableciendo que *"las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto".*

Esto servirá de base para establecer las medidas a continuación para los distintos tipos de ficheros, fijando el artículo 81.1, en relación a aplicación de dichos niveles, y como premisa general que *"todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico"*.

Pero además, establece el punto segundo de este artículo que *"deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal: a) Los relativos a la comisión de infracciones administrativas o penales. b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999,*

de 13 de diciembre. c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias. d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros. e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social. f) Aquéllos 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".

Y por último, establece el 81.3 que *"además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal: a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas. c) Aquéllos que contengan datos derivados de actos de violencia de género".* De modo, que según se viene comentando a lo largo de todo el estudio, a los datos de salud les corresponde la aplicación del nivel alto de seguridad. No obstante, los puntos quinto y sexto contienen reducciones de los niveles entre las que se encuentran incluidos los datos de salud.

Así el punto quinto establece que *"en caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando: a) 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. b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad".

Y el punto sexto por su parte dice 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".*

Y respecto de todo lo dicho anteriormente sobre la aplicación de las distintas medidas, concluye el 81.7 que *"las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero".* E igualmente el punto octavo establece de forma general que *"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".*

El Real Decreto-Ley sobre Células y Tejidos, recoge al respecto en su artículo 6.2 que *"los establecimientos de tejidos deberán adoptar, en el tratamiento de los datos relacionados con los donantes, las medidas de seguridad de nivel alto previstas en el Reglamento de medidas de seguridad de los ficheros automatizados*

que contengan datos de carácter personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre".

Recordemos que el Convenio 108 recogía en su artículo 11 que *"ninguna de las disposiciones del presente capitulo se interpretara en el sentido de que limite la facultad, o afecte de alguna otra forma a la facultad de cada parte, de conceder a las personas concernidas una protección más amplia que la prevista en el presente convenio".*

Por su parte el capítulo tercero del referido título octavo del RLOPD, se encarga de regular las medidas de seguridad para los ficheros automatizados y las divide en los tres niveles ya mencionados.

Las medidas de seguridad de nivel básico contemplan en primer lugar las funciones y obligaciones del personal que les serán comunicadas en la medida que afecten al desarrollo de sus funciones, estando claramente definidas y documentadas, incluyendo las consecuencias ante su incumplimiento. Asimismo se describirán las autorizaciones delegadas si existiesen; esta primera medida se encuentra regulada en el artículo 89 del RLOPD, cuyo punto primero establece que *"las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad. También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento".* Estableciendo el punto segundo de este artículo que *"el responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento".*

Existirá también un registro de incidencias que contemple un procedimiento de notificación y gestión de incidencias especificando el tipo de incidencia, el momento en que se ha producido, o detectado, la persona que la notifica y a la que se le comunica, los efectos derivados de la misma y medidas correctoras aplicadas; todo ello se encuentra recogido en el artículo 90 del RLOPD el cual establece que *"deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas".*

Igualmente debe haber un control de acceso para los usuarios exclusivamente a los recursos necesarios para el desarrollo de sus funciones, existiendo una persona autorizada expresamente para conceder, alterar o anular los accesos autorizados, conforme a lo que establezca el responsable del fichero. Será también éste, quien elabore una relación actualizada de usuarios y perfiles de usuarios con los accesos autorizados para cada uno de ellos, estableciendo mecanismos para evitar el acceso a recursos con derechos distintos de los autorizados. El personal ajeno estará sometido a las mismas normas; esta regulación se encuentra recogida en el artículo 91 del RLOPD, ya citado en la introducción de este estudio, y el cual recoge en su punto primero que *"los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones".* Y en su punto cuarto, respecto de este personal que *"exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero".* También el punto quinto contempla el personal no incluido en los puntos anteriores *"en caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá*

estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio". Y por su parte los puntos tercero y cuarto atribuyen funciones en este sentido al responsable del fichero, estableciendo el 91.2 que *"el responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos".* Y el 91.3 que *"el responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados".*

Por otro lado, la gestión de los soportes y documentos que contengan datos de carácter personal, debe permitir identificar el tipo de información que contienen, ser inventariados y estar solo accesibles por el personal autorizado en el documento de seguridad; las características físicas que posibiliten este cumplimiento, quedarán motivadas en el documento de seguridad; esto se encuentra recogido en el 92.1 que recoge que *"los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad. Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad".*

Las salida de soportes y documentos estará autorizada por el responsable del fichero y anotada a su vez en el documento de seguridad; quedando estos términos regulados en el 92.2 que contempla *"la salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad".*

Y el traslado de documentación con medidas que eviten su sustracción, pérdida o acceso indebido, se regula en el 92.3 el cual recoge que *"en el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte".*

Respecto al desecho de documentos deberá conllevar medidas que impidan el acceso a la información en ellos contenida o su posterior recuperación, y se encuentra recogido en el 92.4 que establece que *"siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior".*

Los soportes con datos especialmente sensibles deberán contar con un sistema especial de etiquetado comprensible para los usuarios con acceso autorizado a los mismo y sin significado para el resto de personas; ello se encuentra establecido en el artículo 92.5 que recoge que *"la identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas".*

La identificación y autenticación la llevará a cabo el responsable del fichero, ya que según establece el 93.1: *"El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios".* Y establecerá mecanismos para que se realice de forma inequívoca y personalizada, verificando que el usuario está autorizado, según establece el 93.2, facultando para que *"el responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación*

de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado". Si se hace mediante contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento que garanticen su confidencialidad e integridad, ya que de acuerdo al 93.3: *"Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad".* Además existe un periodo, no superior a un año, de cambio de las mismas, almacenándola ininteligiblemente mientras estén vigentes, al establecer el 93.4 que: *"El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible".*

Respecto de las copias de respaldo y recuperación, existirán procedimientos para la realización de copias de respaldo al menos semanales, salvo que en dicho periodo no se hayan producido actualizaciones de los datos; según lo establecido en el 94.1 *"deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos".* Se establecen igualmente procedimientos para la recuperación de datos que garanticen la reconstrucción de los datos al tiempo de producirse la pérdida o destrucción, dejando constancia motiva en el documento de seguridad si se procediera a graba manualmente datos en caso de pérdida en ficheros parcialmente automatizados; de acuerdo a esto el 94.2 marca que *"asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que*

la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad". El responsable del fichero verificará además cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de respaldo y recuperación de datos, en cumplimiento del 94.3, que recoge literalmente que *"el responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos".* Y cuando se vayan a implantar sistemas de información, no se utilizarán datos reales salvo que se asegure el nivel de seguridad acorde al tratamiento realizado y dejando constancia de ello en el documento de seguridad; igualmente, las pruebas con datos reales se harán previa copia de seguridad; Así marca el 94.4 que *"las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad".*

En cuanto a las medidas de seguridad de nivel medio, se recogen las siguientes. En primer lugar, hace necesaria la existencia de uno o varios responsables de seguridad nombrados en el documento de seguridad, y que supervisarán las medidas definidas en el mismo; Así, de acuerdo a lo establecido en el 95 del RLOPD *"en el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el*

documento de seguridad. En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento".

En segundo lugar, a partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento en materia de protección de datos, realizándose una auditoría extraordinaria cuando se produzcan modificaciones sustanciales en los sistemas de información que repercutan en las medidas de seguridad implantadas, marcando el cómputo de dos años señalado; todo ello se encuentra recogido en el 96.1, según el cual *"a partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título. Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior".* La auditoría dará lugar a un informe sobre la adecuación de las medidas y controles, identificando las deficiencias y proponiendo medidas correctoras al respecto, incluyendo los hechos, datos y observaciones en que se basen los dictámenes y recomendaciones; de acuerdo al 96.2: *"El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas".* Y además, dicho informe será analizado por el responsable de

seguridad, que comunicará las conclusiones al responsable del fichero para que adopte las medidas correctoras, recogiendo el 96.3 que *"los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas".*

En tercer lugar, la gestión de soportes dará lugar a la existencia de un registro de entrada y otro de salida de soportes, que permita conocer el tipo de documento o soporte, la fecha y hora, el emisor o destinatario, el número de soportes o documentos incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la recepción o entrega. El 97.1 regula la entrada y especifica que *"deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada".* Y el 97.2 regula la salida estableciendo que *"igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada".*

En cuarto lugar, respecto a la Identificación y autenticación, el artículo 98 establece que *"el responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información".*

Además existirá un control de acceso físico por el que, de acuerdo al artículo 99, *"exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información".*

Por último, será obligatorio un registro de incidencias que además de lo establecido en el artículo 90, consignará los procedimientos de recuperación de datos, indicando quien los ejecutó, los datos restaurados y si ha sido necesario grabarlos manualmente en el proceso de recuperación, de acuerdo al artículo 100.1 *"en el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación".* Sin olvidar que el 100.2 exige que *"será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos".*

Y respecto de las medidas de seguridad de nivel alto, tendrá que existir un procedimiento de gestión y distribución de soportes; los soportes se identificarán utilizando sistemas de etiquetado que permita identificar su contenido a los usuarios autorizados a su acceso, dificultándoselo al resto de usuarios. Según marca el 101.1 *"la identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas".* La distribución de estos soportes se hará mediante mecanismos que garanticen que la información no sea accesible o manipulada durante su transporte, como el cifrado de datos; el 101.2 establece al respecto que *"la distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro*

mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte. Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero". Se cifrarán también los datos contenidos en dispositivos portátiles que salgan fueras de las instalaciones bajo el control del responsable del fichero, evitándose el tratamiento de datos en dispositivos que no permitan esta medida, y se motivará en el documento de seguridad, si fuese estrictamente necesario, adoptando medidas de acuerdo a los riesgos del tratamiento en entornos desprotegidos; el 101.3 recoge en este sentido que *"deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos*".

Existirá además la obligación de realizar copias de respaldo y recuperación de datos; por el procedimiento establecido en el artículo 102 *"deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación".*

El registro de accesos es otra de las obligaciones de este nivel, todo ello según marca el artículo 103, ya analizado en un bloque anterior de este estudio a propósito de la incorporación de los datos médicos a la historia clínica. Pese a esto, se hace necesario volver a citar este artículo en este punto en el que estamos, para no dejar un vacío en la continuidad de las medidas a aplicar. Pues bien, según

recogía el 103.1, *"de cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado".* Además el 103.2 establece que *"en el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido".* Y el 103.3, por su parte, que *"los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos".* Fijándose además en el punto cuarto de este artículo que *"el período mínimo de conservación de los datos registrados será de dos años".* No obstante el punto quinto apunta que *"el responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados".* Y por último, el punto sexto hace una exención a lo hasta ahora establecido, marcando que *"no será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias: a) Que el responsable del fichero o del tratamiento sea una persona física. b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales. La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad".*

Como última medida a tomar respecto de los datos informatizados de nivel alto, establece el artículo 104 del RLOPD que *"cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros".*

Respecto de los ficheros no automatizados, el RLOPD recoge igualmente las medidas adaptadas a los distintos tipos de niveles.

En cuanto a las medidas de seguridad para este tipo de ficheros, existen unas obligaciones comunes a los ficheros y tratamientos automatizados, ya que además de lo que será expuesto a continuación para los ficheros no automatizados en exclusiva, les serán de aplicación a este tipo de ficheros, las normas establecidas en los artículos 79 a 92 anteriormente descritas, según establece el artículo 105 RLOPD. Dicho precepto recoge en su punto primero que *"además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a: a) Alcance. b) Niveles de seguridad. c) Encargado del tratamiento. d) Prestaciones de servicios sin acceso a datos personales. e) Delegación de autorizaciones. f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento. g) Copias de trabajo de documentos. h) Documento de seguridad".* Este primer grupo de medidas comunes será expuesto a continuación, según consta en el índice. Pero además, el 105.2 recoge que *"asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a: a) Funciones y obligaciones del personal. b) Registro de incidencias. c) Control de acceso. d) Gestión de soportes".* Es decir que también les son aplicables a los ficheros no automatizados de nivel básico, lo establecido para los automatizados en los artículos 89 a 92 arriba analizados.

Bien, pues además de este paquete de medidas de nivel básico, comunes a los ficheros no automatizados, existen unas específicas establecidas por el RLOPD que hay que ver detenidamente, pese a que la tendencia es que los ficheros en soporte papel desaparezcan con el tiempo.

Respecto de los criterios de archivo de soportes o documentos, se realizará de acuerdo a los criterios previsto en la legislación

específica, en cuya ausencia el responsable deberá establecer criterios y procedimientos para el archivo, que en cualquier caso, deberán garantizar la correcta conservación de documentos, así como la localización y consulta de la información, posibilitando el ejercicio de los derechos. Esto lo marca el 106, el cual establece que *"al archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo".*

Los dispositivos de almacenamiento de los documentos que contengan datos personales, dispondrán de mecanismos que obstaculicen su apertura, siendo necesario en su defecto, adoptar medidas que impidan el acceso de personas no autorizadas, dadas las características físicas del dispositivo en cuestión. Así lo recoge el 107 regulando que *"los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas".*

Y respecto de la custodia de los soportes, cuando la documentación con datos personales no se encuentre archivada en los dispositivos de almacenamiento, por estar en procesos de revisión o tramitación, ya sea previo o posterior a su archivo, la persona a cargo de la misma, deberá custodiarla e impedir que sea accedida por persona no autorizadas, marca el artículo108 que *"mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento*

establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada".

Las medidas de seguridad de nivel medio, por consisten en la existencia de un responsable de seguridad según el 109 que contempla que *"se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento".* Y además en la realización de una revisión bienal de acuerdo al 110, según el que *"los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título".*

Y por último, las medidas de seguridad de nivel alto se concretan en las siguientes.

En cuanto al almacenamiento de la información, los elementos en los que se almacenen ficheros no automatizados con datos personales, deberán estar en áreas de acceso protegido con puertas de acceso dotadas de sistemas que obstaculicen su apertura, mediante llave u otro dispositivo equivalente, que permanecerán cerradas cuando no sea preciso el acceso a los documentos en ellas incluidos; así lo recoge el 111.1, especificando que *"los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero".* Si esto no fuese posible, debido a las características de los locales, el responsable del fichero tomará medidas alternativas, debidamente motivadas en el documento de seguridad, según establece el 111.2 que contempla la posibilidad de

que: *"Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad".*

La generación de copias o reproducción de documentos solo podrá ser realizada bajo el control del personal autorizado en el documento de seguridad; según el 112.1: *"La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad".* Procediéndose a la destrucción de aquellas que sean desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior, ya que de acuerdo al 112.2, *"deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior".*

Respecto al acceso a la documentación, ya referido anteriormente en la introducción de este estudio, marca el 113.1 que *"el acceso a la documentación se limitará exclusivamente al personal autorizado".* Estableciendo de acuerdo al 113.2 *"…mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios"*. Y con otra particularidad más recogida en el 113.3, *"el acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad".*

Finalmente, el 114 establece respecto al traslado de documentación que *"siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado".*

"Pues bien, esas medidas "técnicas y organizativas", ya citadas, deben plasmarse en un documento de seguridad, de obligado cumplimiento para el personal con acceso a los datos. En el caso de los datos de salud habría que cumplir todas las medidas, ya que dichos datos corresponden al nivel alto de seguridad, y los niveles son acumulativos"[331].

De modo que, según lo expuesto, los ficheros deberán cumplir las medidas que les correspondan de acuerdo al soporte en el que se encuentre la información y de acuerdo a nivel de seguridad que tengan.

"Se trataría de no romper la cadena de protección de los datos personales, que deben iniciar los responsables de los ficheros previamente a la creación de los mismos, involucrando en ello a cuantos intervengan en su tratamiento, desde los médicos, hasta el personal de limpieza que pueda acceder a documentos que se encuentren en las papeleras. En varias ocasionas han aparecido informes médicos en cubos de basura situados en la vía pública, lo cual denota que ni el médico fue informado de que no se pueden tirar documentos sin destruir, ni el personal de limpieza que no se podían dejar abandonados en este estado"[332].

El Real Decreto sobre receta médica establece por su parte que La confección, edición y distribución de las recetas en papel, ya se cumplimenten a través de medios manuales o electrónicos, deberán cumplir unas medidas de seguridad que puedan garantizar su autenticidad, dificultando los máximo posible su falsificación. Y así establece el artículo 4.1 que *"las recetas médicas en soporte papel para cumplimentación manual o informatizada se confeccionarán con*

[331] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

[332] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

materiales que impidan o dificulten su falsificación, o mediante la introducción de medidas de seguridad en el sistema que garanticen su autenticidad, y de acuerdo con los criterios establecidos en el anexo de este real decreto". Recogiéndose además en el punto cuarto que *"la edición, elaboración y distribución de los talonarios de recetas oficiales de estupefacientes se realizará de acuerdo con su normativa específica".*

El artículo 44 de la ley de investigación biomédica, establece en su punto primero del título en el que se ubica, dedicado a Análisis genéticos, muestras biológicas y biobancos, que tiene por objeto: *"… Establecer los requisitos que deben cumplir las instituciones y las personas que realicen los análisis genéticos y traten o almacenen datos genéticos de carácter personal y muestras biológicas".*

El Real Decreto sobre atención especializada recoge en su artículo 9.1, en relación con las medidas de seguridad en el tratamiento de los datos que *"el Ministerio de Sanidad, Servicios Sociales e Igualdad adoptará las medidas necesarias para asegurar que el tratamiento de los datos se realiza conforme a los fines previstos en el artículo 2 de este real decreto".* Donde se encuentran regulados los objetivos del registro ya definido anteriormente.

El punto segundo de este artículo 9 recoge así mismo que *"asimismo, dispondrá las medidas oportunas para garantizar la seguridad de los procesos de envío, cesión, custodia y explotación de la información, de acuerdo con lo previsto en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal"*.

Además específica sobre la cesión de los datos, en el punto tercero, que *"todo tratamiento que conlleve el acceso a los datos del registro o la cesión de los mismos, se efectuará en los términos que se acuerden en el Consejo Interterritorial del Sistema Nacional de Salud (CISNS), según se establece en el artículo 53 de la Ley*

16/2003, de 28 de mayo, y con las garantías que dispone la Ley Orgánica 15/1999, de 13 de diciembre. Para ello se aplicarán técnicas de disociación y encriptación, así como todos aquellos mecanismos que permitan garantizar la confidencialidad de los datos que obren en el registro".

Y concluye con el punto cuarto diciendo que *"tanto para el suministro como para la consulta de los datos del registro por parte de las comunidades autónomas, será necesario utilizar los sistemas de certificado electrónico reconocido. Para facilitar el acceso de los usuarios autorizados se establecerán perfiles distintos para cada uno de ellos".*

IV.5.b. Documento de seguridad:

En materia de protección de datos existen dos obligaciones principales que deben cumplir las entidades. Una de ellas es la declaración de ficheros, contemplada en el apartado relativo a la creación de las bases de datos, y la otra la elaboración del documento de medidas de seguridad, debiendo ambas, estar siempre actualizadas.

Respecto a esta última, la otra obligación fundamental para las entidades que procedan al tratamiento de datos de carácter personal, es la elaboración del documento de medidas de seguridad, que se encuentra regulada en el artículo 88 RLOPD, cuyo punto primero establece que *"el responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información".*

El punto segundo especifica un poco más que *"el documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad*

agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización".

El punto tercero, por su parte, recoge los mínimos que debe contener el documento *"el documento deberá contener, como mínimo, los siguientes aspectos: a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos. b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento. c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros. d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan. e) Procedimiento de notificación, gestión y respuesta ante las incidencias. f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados. g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos".*

Y además el punto cuarto exige unos requisitos para los ficheros de nivel medio y de nivel alto *"en caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además: a) La identificación del responsable o responsables de seguridad. b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento".*

Otra particularidad que se establece en relación al tratamiento por cuenta de terceros se establece en el punto quinto *"cuando exista un tratamiento de datos por cuenta de terceros, el documento*

de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo".

Y si los datos se tratasen solo en sistemas del encargado habrá que estar a lo establecido en el punto sexto, el cual establece que *"en aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados. En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento".* Lo que ocurre es que en el ámbito sanitario, hoy en día esto es poco probable, por muy informatizada que esté toda la información médica siempre hay papel de por medio en los centros sanitarios.

A propósito de la destrucción de documentos, y en concreto de la historia clínica como documento médico principal, la doctrina se manifiesta al respecto que *"la destrucción suele realizarse, previa autorización por el organismo pertinente y se emplea la incineración o destructores de papel depositados en las Unidades de Documentación y Archivo de las HC"*[333]*.*

[333] CURRIEL HERRERO, J y ESTÉVEZ LUCAS, J: *"Manual para la gestión sanitaria y de la historia clínica hospitalaria*". Editores Médicos, Madrid, 2000. Pág. 86.

Tanto registros como documento de seguridad deben permanecer siempre actualizados, según se ha dicho, para garantizar su utilidad. La obligación de actualización de registros la marca el 26.3 de la LOPD, y será cita do en el apartado relativo a creación de bases de datos. Y respecto a la obligación de la actualización del documento de medidas de seguridad la contempla el 88.7 del RLOPD, el cual recoge que *"el documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas".* Especificando además el octavo apartado de este mismo artículo que *"el contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal".*

Pensemos que el documento de seguridad es una guía de conducta promovida por unos responsables, de acuerdo a lo establecido en la normativa, que debe ser trasladada y servir al personal de la entidad, para que se lleve a cabo un correcto tratamiento de la información. Por otra parte, sería muy conveniente, que en el documento de seguridad se incluya un apartado con las notificaciones realizadas a la AEPD, para que se tengan siempre presentes los ficheros declarados en relación con las medidas establecidas en el documento de seguridad, para que la visión sea homogénea.

Según he manifestado en otras ocasiones, *"… la adaptación a la Ley, no pasa únicamente por adaptarse a la normativa efectuando la inscripción de los ficheros y elaboración del documento de*

seguridad obligatorio, en el cual se establecen todas las medidas tomadas para la protección de los datos. Tanto el registro como los documentos establecidos por la Ley, deben permanecer actualizados durante toda la vida del Organismo, empresa o profesional, reflejando en cada momento su realidad; incluso cuando dejen de existir, esta situación debe quedar también reflejada"[334].

La sección novena de la Directiva sobre protección en el tratamiento de datos regula, entre otros, el tema de la notificación a las autoridades de control y sanciones por incumplimiento de las normas. Respecto de la Obligación de notificación a la autoridad de control, establece el punto 1 del artículo 18 que *"los Estados miembros dispondrán que el responsable del tratamiento o, en su caso, su representante, efectúe una notificación a la autoridad de control contemplada en el artículo 28, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos, total o parcialmente automatizados, destinados a la consecución de un fin o de varios fines conexos".*

A este respecto establece el punto tercero de este artículo que *"los Estados miembros podrán disponer que no se aplique el apartado 1 a aquellos tratamientos cuya única finalidad sea la de llevar un registro que, en virtud de disposiciones legales o reglamentarias, esté destinado a facilitar información al público y estén abiertos a la consulta por el público en general o por toda persona que pueda demostrar un interés legítimo".*

Y esta obligación solo estará exenta bajo los criterios recogidos en el punto segundo de este artículo, que establece que *"los Estados miembros podrán disponer la simplificación o la omisión de la notificación, sólo en los siguientes casos y con las siguientes condiciones: - cuando, para las categorías de tratamientos que no*

[334] VIDAL RASO, Marta: *"¿Todavía no se ha adaptado a la Ley de Protección de Datos Personales?"*. Boletín Informativo nº57- Consulting Empresarial, Madrid 2005. Págs. 9 -10.

puedan afectar a los derechos y libertades de los interesados habida cuenta de los datos a que se refiere el tratamiento, los Estados miembros precisen los fines de los tratamientos, los datos o categorías de datos tratados, la categoría o categorías de los interesados, los destinatarios o categorías de destinatarios a los que se comuniquen los datos y el período de conservación de los datos y/o - cuando el responsable del tratamiento designe, con arreglo al Derecho nacional al que está sujeto, un encargado de protección de los datos personales que tenga por cometido, en particular: - hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la presente Directiva, - llevar un registro de los tratamientos efectuados por el responsable del tratamiento, que contenga la información enumerada en el apartado 2 del artículo 21, garantizando así que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados".

Además el punto cuarto del comentado artículo 18, establece que *"Los Estados miembros podrán eximir de la obligación de notificación o disponer una simplificación de la misma respecto de los tratamientos a que se refiere la letra d) del apartado 2 del artículo 8".*

Y finalmente el punto quinto, en relación a los ficheros no automatizados, que *"los Estados miembros podrán disponer que los tratamientos no automatizados de datos de carácter personal o algunos de ellos sean notificados eventualmente de una forma simplificada".*

El artículo 67 de la Ley de Investigación Biomédica, establece, por su parte, en su punto primero que *"una vez constituido el biobanco según el procedimiento anterior, la autoridad competente procederá a su registro en el Registro Nacional de Biobancos para Investigación Biomédica, bajo la dependencia del Instituto de Salud Carlos III. Previamente habrán de inscribirse en la Agencia Española*

de Protección de Datos, de conformidad con la legislación vigente. Los datos de este Registro se basarán en los que sean proporcionados por las autoridades competentes para autorizar los biobancos".

IV.5.c. Formación del personal: funciones y obligaciones y hojas informativas:

La formación del personal en las entidades, es un tema de candente actualidad. Se hacen cantidad de cursos de formación en todos los ámbitos, incluido el sanitario, y cada vez más también en relación a la de protección de datos, ya que es una materia obligatoria para el tratamiento de datos personales. Hoy en día cada vez es más habitual en los tablones de los centros sanitarios, carteles de cursos para el personal sanitario en materia de protección de datos, lo cual es alentador, ya que como he reiterado en diversas ocasiones, este es uno de los puntos débiles de la protección de datos relativos a la salud.

Respecto de la importancia de la información en las organizaciones manifiesta Ignacio Bell Mallén: *"Hoy en día es imposible sustraerse a la importancia que la comunicación tiene en la vida de las organizaciones. La sociedad actual, reflejada en el conjunto de las organizaciones que la forman, está colonizada hasta extremos insospechados por la información, como conjunto de contenidos que circulan a través de los canales de comunicación y no puede vivir a espaldas de ella. Las organizaciones públicas y privadas, grandes o pequeñas, con afán de lucro o sin él, saben que necesitan contar cada día más con la información. Es más, comprueban que en muchos casos dependen de ella, hasta el punto que en determinados casos las instituciones, las organizaciones, son lo que son en relación con el grado de conocimiento que se tiene de*

ellas".[335] Esto sin duda afecta también al ámbito sanitario, en el que, al igual que en otros, es necesario que fluya la información, a través de los distintos responsables, para todo el personal que la compone tenga conocimiento de los que le corresponde y pueda llevarlo a cabo y trasladarlo a los usuarios de las mismas, en este caso, a los pacientes.

El personal de acceso a los ficheros de datos, como ya se ha comentado en repetidas ocasiones, debe ser formado e informado de las funciones que le corresponden de acuerdo al acceso a los datos que vaya a tener en función de las necesidades que requiera su puesto de trabajo. Y digo necesidades, porque la mayoría de las veces, los usuarios de los datos personales, acceden a información que no necesitarían conocer para desarrollar sus funciones, y a la que simplemente acceden porque alguien no se ha molestado en controlar este aspecto. Por ejemplo acotando los accesos informáticos o simplemente ubicando en sitios de acceso común para los trabajadores de una empresa, determinada información en soporte papel.

Aunque también es verdad, que en otras ocasiones, el acotar la información a los usuarios, supone muchas trabas e incomodidades a la hora de trabajar, debido a que la información que tienen que manejar trabajadores de distinto rango de acceso, se encuentra en un único documento o dispositivo; cabe incluso poner como ejemplo la incomodidad de abrir y cerrar un armario que contiene información que otras personas no deberían conocer, pero que se encuentran ubicadas en una misma sala, cuando se abandona temporalmente el puesto de trabajo. Esto pasa todos los días en cientos de entidades, y por eso es tan importante la concienciación del personal, tanto a

[335] BELL MALLÉN, José Ignacio (Coord.): "Comunicar para crear valor. La dirección de comunicación en las organizaciones." EUNSA, Navarra, 2004.Pág. 155.

más que limitarle el acceso a los datos. Para ello, y según se ha visto en el apartado relativo al documento de medidas de seguridad, el artículo 89 marca este requisito como medida de seguridad de nivel básico, por lo que, como los niveles son absorbentes, afectaría a todos los ficheros. Es decir que, dentro de cada documento de seguridad, debe haber un apartado que contemple las funciones y obligaciones del personal, de acuerdo a las medidas en éste establecidas, dándose traslado de las mismas al personal que maneja los datos, en la medida que le correspondan de acuerdo a su puesto de trabajo.

En este sentido, y según he manifestado con anterioridad, *"es más o menos habitual, y casi nunca intencionado, que se falte al deber de secreto en el sector médico, la mayoría de las veces, debido a la frenética actividad diaria de los centros sanitarios. Varias son las circunstancias que motivan que los profesionales dejen fuera de su control la información médica, generalmente por una urgencia: porque se requiera temporalmente al profesional en otro lugar, por una duda o gestión que se ha de hacer en otro sitio, etc. La realidad es que, encontramos listados de pacientes en los mostradores a la vista del público, expedientes en las mesas de las consultas y, puertas abiertas fuera del horario de consultas, quizás para facilitar la entrada de otros turnos o simplemente del personal de limpieza. Esta ausencia frecuente del personal sanitario de sus puestos de trabajo durante la atención a los pacientes en las consultas médicas, podría mermar el deber de secreto al que están obligados. Como contrapartida, esa parte de desprotección, debería ser suplida con la buena fe de quien accidentalmente acceda a los datos, que podrían ser personas próximas o conocidas, lo cual incrementaría el grado de vulnerabilidad. Pero se trata de una cuestión de moral, por lo que quizás no solo habría que sensibilizar al personal que trabaja en los centros sanitarios de la importancia de la protección de los datos*

personales, sino a la población en general, para proteger los datos de los demás, y también los propios"[336]*.*

A este respecto se manifiesta también Nuria Terribas al sostener que *"…la información permite diseñar e implementar medidas de seguridad eficaces que den accesos controlados a los distintos profesionales, de modo que cada uno acceda sólo a aquellos datos que requiere para el desarrollo de su tarea"… "Sin embargo, en la práctica habitual se producen muchas situaciones que requieres cierta flexibilidad en estos accesos, si no queremos entorpecer la actividad asistencial"*[337] .Y en esta línea afirma que *"… si disponemos de un sofisticado sistema de accesos y medidas de seguridad pero no ponemos en práctica medidas de control y seguimiento, la eficacia se reduce enormemente ya que, como comentaba anteriormente, la consciencia entre los profesionales del valor de la confidencialidad es muy escasa"*[338]*.*

Y por otro lado habría que pensar en la reubicación de personas y recursos, para que estén los más reagrupados en la medida de lo posible, para evitar los accesos no autorizados a los datos. Hoy en día es muy común, ya sea por moda, por aprovechamiento del espacio o por cualquier otra circunstancia, que todos los trabajadores de una empresa se encuentren en espacios diáfanos y comunes para la realización de sus funciones (hablar por teléfono, trabajar con el ordenador, etc.), o que por ejemplo se encuentren bajo llave recursos, como el material de oficina, antes que las nóminas, porque desaparecen con mucha frecuencia. Todo

[336] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012.

[337] TERRIBAS SALA, Núria: "*Los avances del derecho ante los avances de la medicina. Confidencialidad de los datos sanitarios: de la norma a la práctica médica*". In Salomé Adroher Biosca- Thomson Aranzadi, 2008. Pags 796-802.

[338] TERRIBAS SALA, Núria: "*Los avances del derecho ante los avances de la medicina. Confidencialidad de los datos sanitarios: de la norma a la práctica médica*". In Salomé Adroher Biosca- Thomson Aranzadi, 2008. Pags 796-802.

esto entra dentro de la concienciación al personal para el correcto desarrollo de sus funciones y obligaciones.

A propósito de esta problemática de ubicación de los recursos en el sector sanitario *"se podrían buscar soluciones en este sentido, estableciendo un sistema de gestión de los recursos que almacenen los datos personales en un plano al que el público no alcance, ubicándolos en lugares a los que solo tenga acceso el personal sanitario o, redistribuyendo las mesas de atención y redirigiendo la orientación de los equipos informáticos. Se trata, en definitiva, de reorganizar los recursos buscando siempre el punto óptimo entre operatividad y confidencialidad".*[339] Seguramente *"La clave estaría en que esa transparencia se haga opaca en la frontera de la confidencialidad, de modo que se conozcan todos los datos posibles por aquellos profesionales que van a intervenir en el proceso asistencial, incluso que sean conocidos por un tercero si es realmente necesaria su intervención, pero que no trasciendan más allá"*[340]*.*

Las funciones y obligaciones del personal, están en directa relación con lo establecido en el documento de medidas de seguridad. Se trataría de sustraer las que afecten a cada persona que maneje datos personales, para que conozcan los recursos a los que pueden acceder y con qué limitaciones.

Todo el personal que acceda a los datos de carácter personal y a los sistemas de información que los tratan, está obligado a conocer y observar las medidas que afecten a las funciones que desarrolla. Asimismo sería conveniente que existiera una parte general informativa de conceptos a disposición de los usuarios en el

[339] VIDAL RASO, Marta, *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

[340] VIDAL RASO, Marta, *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

documento de medidas de seguridad, para complementar a las funciones y obligaciones que les sean comunicadas de forma específica a cada uno de ellos. Y por otro lado, deben conocer los ficheros a los que pertenecen los datos que manejan y que han debido ser declarados ante la AEPD.

Para asegurar estos extremos, se debería informar a los usuarios mediante un sistema y periodicidad establecidos, través de la persona pertinente nombrada por el responsable del fichero, o en su caso, por el responsable de seguridad.

De acuerdo a esto, las personas que tengan acceso a los datos del fichero, ya sea a través de medios informatizados o no informatizados, se encuentran obligadas a cumplir por ley lo establecido en las de funciones y obligaciones del personal, y sujetas a las consecuencias en que pudieran incurrir en caso de incumplimiento de las mismas, que deberán concretarse por el responsable oportuno.

Así, el responsable del fichero, debe hacer entrega de una copia de este documento en la parte que le afecte a cada uno, para su conocimiento, como persona autorizada a acceder a los datos del fichero, siendo aconsejable que quede constancia de la entrega; sería muy útil en este sentido, que existiera por cada usuario un manual de funciones y obligaciones, ya sea en soporte papel o informático, en el que se les fuesen comunicando las posibles variaciones en este sentido, especificando la fecha y aceptación de cada uno de los usuarios, lo que mantendría a los mismos claramente informados, a la vez que protegería al responsable del fichero sobre el cumplimiento de esta obligación.

Este tema ha sido anteriormente de mi interés, ante lo que he manifestado que *“el responsable del fichero debería así desarrollar el sistema de seguridad de los datos personales, concienciando a su personal de la importancia de la protección de datos. Es más, cuando alguien comienza a trabajar con datos personales, se le*

debería dar con carácter previo una formación en materia de protección de datos, en la que además de comprometerse al deber de secreto, sea informado de cuáles son sus funciones y obligaciones para con los datos personales, indicando a que recursos está autorizado a acceder y que normas de seguridad debe respetar para el manejo de los mismos, así como los protocolos que debe seguir cuando se produzcan contingencias en el tratamiento de los datos. Sería necesario en este punto distinguir los diferentes tipos de personas que pueden acceder a los datos personales, entre responsable de fichero, administradores del sistema, personal informático y el resto del distinto personal que acceda a los datos. Todos ellos tienen lógicamente funciones distintas, por el desarrollo de las distintas actividades les corresponden realizar. De modo que es necesario que cada grupo de profesionales esté informado, en la medida que le afecte, de las normas relativas a la seguridad requerida en los centros de tratamiento y locales, a sus puestos de trabajo, al entorno del sistema operativo y las comunicaciones, a los sistemas informáticos y aplicaciones o elementos de acceso al fichero, a la salvaguarda y protección de sus contraseñas personales, a la gestión de soportes o incidencias, a la entrada y salida de datos por red, a los procedimientos de respaldo y recuperación de datos, o sobre los controles periódicos de verificación del cumplimiento de la normativa, respecto al tratamiento de los datos de carácter personal que manejan"[341].

De acuerdo con establecido en las medidas de seguridad ya vistas para cada nivel en el apartado correspondiente, el manual de funciones y obligaciones del personal debería regular unos aspectos específicos que serán analizados a continuación.

En lo relativo a los centros de tratamiento y locales, el tipo de acceso de cada uno de acuerdo a su puesto de trabajo y perfil, que

[341] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

deberá ser comunicado por el responsable que corresponda en cada caso, de acuerdo a lo establecido por el responsable de seguridad, especificando los recursos a los que tenga acceso, ya sea en soporte informático o en soporte papel. Además, en caso de que los datos que se traten sean de nivel alto, constará el aviso de vigilancia de los dispositivos que contengan este tipo de información, tanto en su ubicación original para que permanezcan cerrados (como armarios, despachos…), como si se va a proceder a su traslado (en el caso de memorias externas, dispositivos portátiles…).

Y por último, respecto del personal que tenga que tener acceso a los locales por razones de mantenimiento o fuerza mayor, pero no tenga autorizada la entrada a los locales en los que se ubican los ficheros de datos de forma habitual, habría que constancia de ello en un registro de acceso a los locales, pero sin acceso al fichero de datos, que se configuraría al efecto para estas situaciones especiales; cosa distinta sería el personal de limpieza, que aún no estando a acceder al fichero de datos, si lo está de forma habitual a acceder a los locales en los que estos se encuentran para el desarrollo de sus funciones, lo que les obliga a guardar el deber de secreto de todos aquellos datos que de forma incidental pudieran conocer durante el desarrollo de las mismas (como documentos tirados en las papeleras o aquellos que hubieran podido quedar encima de las mesas), debiendo tener también un especial cuidado para que no se dañen los soportes tanto informáticos como en papel, ya que no sería la primera vez que se desenchufa un servidor para limpiar o cae agua en papeles que quedan ilegibles.

Se ha hablado en varias ocasiones de este tipo de personal, sobre todo del personal de limpieza, como personas no autorizadas a acceder a los datos personales, pero sí a los locales donde estos se encuentran para realizar sus labores. En este sentido hay que decir que el artículo 83 del RLOPD establece respecto a prestaciones de servicios sin acceso a datos personales que: *“El*

responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales". Puntualizando el segundo párrafo de este artículo que: *"Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio"*. En este sentido, por el hecho de acceder a los locales en los que se ubica la información, al igual que al personal que sí está autorizado para el manejo de datos, debería existir para el personal sin acceso a datos, una comunicación recordándoles los riesgos que conlleva su labor, en cuanto a la manipulación de recursos, conexiones y documentación; e igualmente sobre prohibición de acceder a los datos, así como la obligación de guardar secreto si tuviesen acceso a los mismos de forma accidental durante la realización de su trabajo.

Respecto de los puestos de trabajo, estarán descritos para cada usuario, que deberá encargarse de vigilarlo, para que la información que contengan no pueda ser vista por personas sin acceso autorizado a ella, por ejemplo mediante protectores de pantalla para el caso de los recursos informáticos, o mediante una ubicación que garantice la confidencialidad en el caso del soporte papel, como puedan ser bandejas o carpetas opacas; estas medidas tendrán un valor especial cuando se abandone el puesto de trabajo, cosa que ocurre de forma habitual, y supone un riesgo para la información. Igualmente habrá que prestar una especial atención a las impresoras o dispositivos compartidos en los que se puedan visualizar datos personales por personas no autorizadas, como el caso de impresoras o destructoras de papel. La conexión a redes exteriores debe estar debidamente autorizada por el responsable del fichero, quien autorizará específicamente a cada usuario y dejará

constancia de ello en el apartado correspondiente del documento de seguridad. Igualmente el responsable de seguridad establecerá la configuración de acceso a la base de datos para cada usuario, siendo cambiados solo con su autorización. Y por último, debe recalcarse en esta apartado el deber de secreto, comprometiéndose a la confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo, mediante la firma de un acuerdo de confidencialidad.

En relación a los sistemas de acceso al fichero, habrá que prestar especial atención a aquellos que tengan carácter temporal o sean copiados de otros, para que cumplan el nivel de seguridad adecuado y sean destruidos una vez haya concluido su utilidad. Del mismo modo, los dispositivos de almacenamiento de soportes, deben especificarse los mecanismos que obstaculicen su apertura, y si no es posible que dispongan de ellos, proponer medidas al respecto. En este sentido habrá que prestar especial atención a la documentación no informatizada que contenga datos y no se encuentre archivada en los dispositivos correspondientes por encontrarse en fase de tramitación o revisión, debiendo tomar la persona a cargo de la misma, medidas para su protección impidiendo que sea accedida por personal no autorizado. En todo caso, los usuarios tendrán acceso únicamente a los recursos necesarios para el desarrollo de sus funciones, que estarán claramente concretadas, existiendo una relación de usuarios autorizados a acceder al fichero de datos que el responsable del mismo deberá mantener actualizada, debiendo establecer mecanismos para que los usuarios no puedan acceder a recursos distintos de aquellos a los que fueron autorizados.

A propósito de la salvaguarda y protección de las contraseñas personales cada usuario será responsable de la confidencialidad de su contraseña, registrando como incidencia e informando al

responsable oportuno, en caso de que esta sea conocida por otras personas.

En cuanto a la gestión de incidencias, deberá existir un procedimiento de notificación y gestión de las mismas, que deje constancia del tipo de incidencia, fecha y hora en que se produjo, persona que realiza la notificación, persona a quien se comunica, efectos que puede producir, descripción detallada de la misma y medidas correctoras aplicadas. Los usuarios que tengan conocimiento de ellas deberán comunicarla al responsable oportuno y registrarla en un formulario establecido al efecto, de lo contrario, deberán ser apercibidos de ello dejando constancia de esta situación en el documento de seguridad como incidencia.

La gestión de soportes que contengan datos del fichero, ya sea por acciones intermedias habituales a través de los programas que los tratan o de las copias de seguridad, o bien por motivos esporádicos, deben identificarse de forma clara y ser inventariados a través de etiquetas externas indicando de que fichero proviene, los datos que contienen y la finalidad de tratamiento y la fecha de creación; si esta identificación no fuese posible debido a las características de los mismos, se tomarán medidas adicionales al respecto, haciéndolo constar en el documento de seguridad. A partir de los niveles medios de seguridad, y en relación a la información especialmente sensible, los soportes deben identificarse de forma que solo sea entendible por la persona que los creó y no por el resto, como medida de seguridad. En cualquier caso, los soportes descritos deben almacenarse en lugares de acceso restringido con el fin de que no sean accedidos por personas no autorizadas. Respecto de la salida de soportes deberá ser autorizada por el responsable del fichero, incluso a través de medios electrónicos, que adoptará los medios oportunos para que esta no sufra incidentes, debiendo además habilitar el oportuno formulario para su inventario; a partir de los niveles medios de protección, además se registrarán las entradas

de datos, que serán igualmente autorizadas, conteniendo tipo de soporte, fecha y hora, emisor y recetor, información que contiene y forma de envío de la misma. En el caso de que se trate de datos de nivel alto y vayan a salir, ya sea por medios físicos o electrónicos, se hará de forma cifrada, para que no puedan ser accedidos durante su transporte, quedando constancia igualmente del tipo de soporte y datos que contiene, fecha y hora del envío, así como los destinatarios de los mismos. En los dispositivos portátiles, deberán cifrarse los datos personales que contengan, evitando que en ellos se almacenen datos de nivel alto, cuya existencia deberá constar en el documento de medidas de seguridad, previa autorización del responsable oportuno, y tomando las medidas de seguridad correspondientes a su nivel de protección. Del mismo modo, la copia o reproducción de documentos no informatizados que contengan datos personales, debe estar autorizada por el responsable oportuno, siendo desechadas cuando haya concluido su finalidad. De cualquier modo, y para cada uno de los soportes descritos es obligatorio que cuando vayan a desecharse se utilicen medios para que la información que contuviesen no pueda ser accedida por terceros.

Por otro lado, internamente debería haber un responsable, que de acuerdo a la magnitud de la entidad será el responsable del fichero o cualquier otra persona o personas organizadas por departamentos, secciones, etc., a la que puedan ser comunicadas, entre otras cosas, las solicitudes relativas al ejercicio de derechos para su respuesta correcta. Igualmente estos responsables autorizarán el traslado de documentación fuera de los locales en los que se encuentre ubicado el fichero de datos, para su correcta protección durante su transporte.

El personal de acceso a los datos deberá actuar diligentemente con los soportes que contengan datos personales, prestando atención a la existencia de las oportunas leyendas informativas, en

especial cuando recojan el consentimiento de los titulares de los datos.

Y en definitiva, todas las personas que conozcan modificaciones en materia de protección de datos, deben comunicárselas a sus superiores, al igual que estos deben comunicar a sus subordinados cualquier cambio que afecte a la metodología implantada en la organización en materia de protección de datos; de esta forma se cumplirá con el requisito de mantener actualizado el documento de medidas de seguridad, tanto en su parte teórica, como en su parte práctica.

El artículo 25.6 del RLPD establece en este sentido, respecto del procedimiento relativo al ejercicio de derechos, que *"el responsable del fichero deberá adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos".*

Por su parte la Ley General de Sanidad, en relación a la formación del personal que accede a los datos, recoge en su artículo 18.1, entre las acciones que deben ejercer la Administraciones Públicas, a través de los órganos correspondientes, la *"adopción sistemática de acciones para la educación sanitaria como elemento primordial para la mejora de la salud individual y comunitaria, comprendiendo la educación diferenciada sobre los riesgos, características y necesidades de mujeres y hombres, y la formación contra la discriminación de las mujeres*. *Lo que presupone, además de la educación social de los individuos, para el aprovechamiento de los recursos, la formación del personal que trabaje en el sector sanitario a propósito del tratamiento de datos personales".* Y en este sentido, el punto 14 de este mismo artículo, matiza que *"La mejora y adecuación de las necesidades de formación del personal al servicio de la organización sanitaria, incluyendo actuaciones formativas*

dirigidas a garantizar su capacidad para detectar, prevenir y tratar la violencia de género".

Asimismo, el DCM, recoge en su artículo 7.3 que *"la formación médica continuada es un deber ético, un derecho y una responsabilidad de todos los médicos a lo largo de su vida profesional".* Queriendo entender, que dentro de la formación médica que reciban los profesionales sanitarios, debe estar obligatoriamente incluida la del tratamiento de los datos personales relativos a los pacientes.

IV.5.d. Delegación de autorizaciones:

Ya se ha hablado a lo largo de todo el texto de la existencia de responsables que dirijan y supervisen todo lo relativo al tratamiento de los datos personales en sus diferentes facetas. Y debido a la magnitud de cada entidad o a la rotación de personal que tenga, tanto de forma habitual, como en situaciones especiales o periodos de descanso, existe para estas situaciones, la posibilidad de que los nombrados responsables puedan delegar en otras personas las autorizaciones que les fueron concedidas, para que continúen aplicándose las normas de protección que afecten a los datos personales.

El artículo 84 del RLOPD regula esta materia fijando que *"las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero".*

IV.5.e. Acceso a los datos a través de redes:

Los accesos a datos a través redes de comunicaciones, se regulan en el artículo 85 del RLOPD, el cual establece que *"las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80".* Recordemos, que según acaba de exponerse hace algunos renglones, el referido artículo 80 establece los niveles de seguridad. De modo que, se manejen los datos a través de redes de comunicaciones o no, deberán, en cualquier caso, respetar las normas establecidas para cada nivel, e acuerdo a la categoría de datos que se traten.

IV.5.f. Régimen de trabajo fuera de los locales:

Este aspecto es un aspecto al que no suele prestarse demasiada atención, porque, por un lado requiere una inversión de tiempo, y por otro porque a veces es tal la cantidad de información que sale fuera de los locales que es simplemente imposible realizar tales gestiones.

Los requisitos para la realización del mismo se encuentra regulado en el artículo 86 del RLOPD, que en su punto primero recoge que *"cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado".* Pero puntualiza el punto segundo de este artículo que *"la autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas".* De modo que, de acuerdo a lo establecido en la normativa, cada vez

que vaya a salir información para realizar trabajos fuera de los locales en los que se ubica el fichero de datos, habría que hacer constar esta circunstancia en el documento de seguridad, previa autorización del responsable del fichero.

Esto es especialmente importante en el sector sanitario, en el que podrían salir datos de salud y llegar a extraviarse, por lo que es necesario prestar en este aspecto una especial atención. Pensemos por otro la lado, que con el movimiento de información que hay diariamente en los centros sanitarios, y sin llegar a que esa información salga de los mismos, esta recorre, por necesidades sanitarias varios departamentos o servicios dentro del mismo centro. No será la primera vez ni la última que se pierdan unos análisis o una radiografía; ya sea en soporte papel o informático, lo cierto es que esto ocurre, por lo que se requiere una vigilancia de la información y del recorrido que esta hace, ya sea dentro o fuera de los centros sanitarios. Todo esto se ve agravado, por la utilización para estas tareas de pequeñas memorias que manejan gran cantidad de información, y que por su reducido tamaño pueden llegar a perderse con una mayor facilidad. Así, cuando se reproducen copias del fichero de datos, ya sea en soporte papel o informático, hay que dejar un rastro de las mismas, para garantizar que los datos vuelvan a su origen y si no lo hacen, conocer el nuevo destino y utilidad concreta. Desgajar el fichero original en el que se encuentran los datos personales de esta forma, puede poner en riesgo la seguridad de los datos.

IV.6. DEBER DE SECRETO, CONFIDENCIALIDAD Y TRANSPARENCIA:

El Deber de secreto es uno de los grandes temas dentro de la actualidad en nuestra sociedad, cada día más corrupta. En la LOPD se encuentra regulado en el artículo 10 estableciendo éste que *“el*

responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo". Y aunque este precepto ya había sido analizado en el apartado de las bases de datos médicos e historial clínico, se hace necesario recordarlo también ahora en relación a la seguridad de los datos.

En este sentido, la Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales (LPRL- Ley de prevención de riesgos laborales), establece en su artículo 22.4, a propósito de la regulación de la vigilancia de la salud que *"los datos relativos a la vigilancia de la salud de los trabajadores no podrán ser usados con fines discriminatorios ni en perjuicio del trabajador".* Recogiendo el segundo párrafo que *"el acceso a la información médica de carácter personal se limitará al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador."* Pero se puntualiza además en el tercer párrafo que *"no obstante lo anterior, el empresario y las personas u órganos con responsabilidades en materia de prevención serán informados de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva".* Estos preceptos reflejan como los datos sanitarios no son comunicados a personas distintas de su titular en el ámbito laboral, pero si se comunica la situación de si tiene un estado de salud apto o no apto.

Es oportuno citar aquí también el informe jurídico de la AEPD 0424/2010, en el cual se recoge en relación con la arriba comentada Ley de prevención de riesgos laborales que *"…en cuanto a las cesiones de datos que sean objeto de tratamiento por los servicios médicos de la empresa, debe ante todo tenerse en cuenta la clara delimitación efectuada por el ya citado artículo 22 de la Ley 31/1995 que, tras indicar en su apartado 2 que "las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo respetando siempre el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud", declara tajantemente en el párrafo segundo de su apartado 4 que "el acceso a la información médica de carácter personal se limitará al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador".*

Según he puesto de manifiesto otras veces*, "esta norma afecta al tratamiento de cualquier tipo de datos, no exclusivamente a los sanitarios, lo cual obliga a cualquier persona que trate datos personales, ya sean médicos, administrativos, etc. En relación con los datos sanitarios la Ley 14/1986, de 25 de abril, General de Sanidad establece claramente que "el personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto"*[342]*.*

Unen opinión de otro sector de la doctrina "*…protección de datos asistenciales y confidencialidad de la HC son aspectos diferentes de un derecho de todo paciente que es la utilización de la HC para los fines que están previstos en la legislación vigente"*[343]*.*

[342] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

[343] CURRIEL HERRERO, J y ESTÉVEZ LUCAS, J: *"Manual para la gestión sanitaria y de la historia clínica hospitalaria*., Editores Médicos, Madrid, 2000. Pág. 42.

Así sostienen que *"la confidencialidad de la HC está en relación con una actitud de las personas, es una cultura de los profesionales que obliga a guardar o callar lo que han conocido en el desarrollo de su trabajo sanitario"*[344]*.* Y que por su lado *"La protección de datos en la HC, se encuentra en la SEGURIDAD que los datos clínico-sanitarios de ella solo se cederán a las personas autorizadas, no difundiendo su uso de forma indiscriminada y sin ningún criterio que preserve el principio de secreto profesional"*[345]*.*

Herrán Ortiz, sostiene en cambio que *"si la intimidad faculta al individuo a practicar un control eficaz sobre sus propias experiencias y vivencias, la confidencialidad constituye un medio o instrumento de protección de la intimidad"*[346]*.* De modo que para esta autora la confidencialidad es una herramienta para salvaguardar la intimidad: *"Así lo íntimo es lo más personal, siendo por tanto, todo lo íntimo secreto y reservado."*[347] De modo que: *"Cada persona puede desvelar por decisión propia parte de su intimidad a los demás, naciendo un deber de secreto en aquel a quien se ha confiado la intimidad"*[348]*.*

Entonces lo íntimo es secreto, pero este último también se puede referir a información no íntima. Y si confidencialidad y secreto se refieren a la intimidad, entonces la protección de datos personales también se puede referir a ella.

Otros autores en cambio se limitan a definir la confidencialidad de forma más escueta, manifestando que *"…la confidencialidad consiste precisamente en guardar reserva sobre las informaciones*

[344] Ibídem.

[345] Ibídem.

[346] HERRÁN ORTIZ, Ana Isabel: *"La violación de la intimidad en la protección de datos personales*". Dykinson, Madrid 1.999. Pág. 13.

[347] HERRÁN ORTIZ, Ana Isabel: "*La violación de la intimidad en la protección de datos personales*". Dykinson, Madrid 1.999. Pág. 15.

[348] Ibídem. Pág. 15.

que afectan a la vida privada de los individuos…"[349]*.* Y especificando que *"…la intimidad existe con independencia del carácter confidencial o secreto en que permanezca; y aquello que debe ser confidencial o secreto no es tan sólo el reducto interior y personal, sino que su contenido puede ser infinitamente más extenso…"*[350]*.*

Y este sector de la doctrina hace una reflexión que merece la pena leer, porque es el pensar de muchos que han visto al descubierto sus datos por la falta del sigilo del personal médico, y eso, una vez incumplido, es decir, una vez conocida la información por el resto, es irreversible. Así estos autores recuerdan *"la oportunidad de dar la tantas veces reclamada respuesta normativa, que no consista sólo en reforzar y sancionar la obligación de callar que tienen los médicos, sino que establezca mecanismos eficaces para garantizar el derecho de los pacientes a su intimidad, y, por consiguiente, a conocer, controlar y solicitar rectificaciones oportunas a la información registrada que se refiera a sí mismo, sin limitar inútilmente el progreso de la investigación científica y técnica…"*[351]*.*

Lo que está claro es que la confidencialidad tiene que ser mantenida constantemente, si no, no sería tal, en cuanto se rompa y un dato deje de ser confidencial, lo dejará de ser para siempre, es algo que no se puede olvidar que se ha desvelado. A este respecto Juan Mejía ha manifestado que *"Todo ello se traduce en la*

[349] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso: "La protección de datos personales en el ámbito sanitario., Editorial Aranzadi, Navarra 2002. Pág. 129.

[350] Ibídem.

[351] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso: "La protección de datos personales en el ámbito sanitario". Editorial Aranzadi, Navarra 2002. Pág. 134.

necesidad de un circuito de confidencialidad facilitando la gestión asistencial de modo que no se atrofie el sistema"[352].

Nuria Terribas ha manifestado respecto a la confidencialidad en materia sanitaria que *"… no podemos olvidar que en la práctica sanitaria la información fluye a dos niveles el verbal (en la relación entre profesionales y paciente, junto con su entorno familiar y social) y el escrito o documentado (historia clínica y resto de documentación). Respecto a ambos niveles obliga por igual la ley a profesionales sanitarios y no sanitarios, incluyendo bajo ese deber de confidencialidad a todo el personal de una institución, inclusive personal de limpieza, mantenimiento u otros servicios complementarios, pues no dejan de ser personas que tienen relación con los pacientes y, aunque sea directa o colateralmente, son receptores y transmisores de información, aún cuando no les competa…"*[353]. Hay que recordar que un tema tan cotidiano como es la limpieza de los lugares en los que se encuentran los datos personales, ha sido ya comentado en este estudio tanto respecto de las medidas de seguridad a tomar, a propósito del estudio realizado por la AEPD a los hospitales para ver su grado de cumplimiento, debido a su importancia.

Y sostiene esta autora que "*…respecto a la información que fluye a nivel estrictamente verbal, la quiebra del secreto profesional y las fugas a la confidencialidad son una realidad cotidiana en todos los centros sanitarios* de *nuestra red, pública y no pública, no quedando amparada por la LOPD…*"[354]. Aunque bien es verdad, que la normativa de protección de datos contempla en el artículo 44.3 d)

[352] MEJÍA, Juan. "*Hacia un estatuto jurídico desarrollado de la Historia Clínica*", Diario La Ley 5638 de octubre de 2002

[353] TERRIBAS SALA, Núria: "*Los avances del derecho ante los avances de la medicina. Confidencialidad de los datos sanitarios: de la norma a la práctica médica*". In Salomé Adroher Biosca- Thomson Aranzadi, 2008. Pags 796-802.

[354] TERRIBAS SALA, Núria: "*Los avances del derecho ante los avances de la medicina. Confidencialidad de los datos sanitarios: de la norma a la práctica médica*". In Salomé Adroher Biosca- Thomson Aranzadi, 2008. Pags 796-802.

de la LOPD, como infracción grave "*La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Le*.". Pero la realidad es que la fuga de información que se produce en este sentido es difícil de remediar, si no es con una contundente concienciación del personal. Lo que ocurre muchas veces es que las situaciones no acompañan, y las informaciones deben darse a los pacientes en habitaciones compartidas, en las que no se puede hacer, en muchas ocasiones, pedir al otro u otros pacientes que la abandonen para llevar a cabo tal cometido, porque necesiten, por ejemplo, estar conectados al oxígeno. Por ello, es un reto de la sociedad actual, según se apuntará más adelante, la instalación de habitaciones individuales para que los pacientes tengan garantizada tanto su intimidad, como la protección de sus datos personales, para los cuidados que puedan necesitar o las informaciones que deban recibir.

Discierne además Nuria Terribas sobre cuál es el problema, que considera que está, en *"la falta de conciencia profesional sobre la importancia de la información que manejan las personas que trabajan prestando asistencia sanitaria…"*[355]*.* Sosteniendo que por un lado *"… la ausencia de formación en temas de confidencialidad y secreto profesional en la mayoría de titulaciones universitarias de grado de estos profesionales"*[356]*.* Pero que además, por otro lado *"… la necesidad de trabajo en equipo que implica el «secreto compartido», la masificación de la asistencia con la escasez de medios con los que debe trabajarse y la falta de tiempo asistencial para hacer las cosas bien".* Achaca que *"…la información, gran parte de las veces se proporciona en pasillos, salas de espera o en habitaciones compartidas con el único obstáculo de una cortina, con*

[355] TERRIBAS SALA, Núria: "*Los avances del derecho ante los avances de la medicina. Confidencialidad de los datos sanitarios: de la norma a la práctica médica*". In Salomé Adroher Biosca- Thomson Aranzadi, 2008. Pags 796-802.

[356] Ibídem.

lo que lo reducido de los espacios dificulta gravemente la privacidad"[357]*.* Coincidiendo con la opinión manifestada en el párrafo anterior, y concluye que *"…cuando más ampliamos el círculo de la confidencialidad mayor riesgo de quiebras y vulneraciones a la intimidad de la persona y quizás en algún momento deberemos plantearnos sacrificar la eficiencia del sistema en aras al respeto de los derechos del ciudadano"*[358]*.*

El derecho a la intimidad cuenta dentro de la ley del paciente con un capítulo propio así titulado "*derecho a la intimidad*", que exalta la confidencialidad de los datos relativos a la salud, así como las medidas que lo garanticen a través de protocolos establecidos por los centros sanitarios, y se regula en concreto en el artículo 7.1 de la Ley del paciente, según el que *"toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley"*. Puntualizándose en el punto segundo que *"Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes".*

La sección octava de la Directiva sobre protección en el tratamiento de datos regula la confidencialidad y la seguridad del tratamiento, la primera, la confidencialidad, llamada deber de secreto en el artículo 10 de la LOPD, y recogida en el artículo 16 de la directiva que establece que *"las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal".* El concepto de encargado del

[357] Ibídem.

[358] Ibídem.

tratamiento, es definido en el artículo 3g) de esta norma como *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento…".*

La segunda, la seguridad del tratamiento, llamada en nuestra LOPD seguridad de datos y regulada en el artículo 9, contempla la figura del encargado del tratamiento, exigiendo que medie un contrato que vincule a ambas partes, cuestión abarcada en el artículo 12 de la LOPD, y que se recoge también en el artículo 17 de la Directiva que establecen su punto primero que *"los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse".* A este respecto establece el punto cuarto de este mismo artículo que *"A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente".* No obstante el punto segundo establece que *"los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas".* Y su punto tercero que *"la realización de tratamientos por encargo deberá estar*

regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular: - que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento; - que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste".

De modo que el encargo del tratamiento de los datos para la prestación de un servicio, deberá estar debidamente regulada en un contrato que garantice la aplicación de la normativa de protección de datos al respecto. De lo contrario, de no existir este contrato, se produciría una cesión de datos, que requeriría del consentimiento de los afectados, según se explicará más adelante.

La disposición adicional cuarta de la Ley de Telecomunicaciones, establece también que las autoridades nacionales podrán decidir motivadamente, mediante resolución, que información, amparada por la vigente legislación, pueda resultar amparada o no por la confidencialidad. Así establece este precepto que *"las personas físicas o jurídicas que aporten a alguna Autoridad Nacional de Reglamentación datos o informaciones de cualquier tipo, con ocasión del desempeño de sus funciones y respetando la legislación vigente en materia de protección de datos y privacidad, podrán indicar, de forma justificada, qué parte de lo aportado consideran confidencial, cuya difusión podría perjudicarles, a los efectos de que sea declarada su confidencialidad. Cada Autoridad Nacional de Reglamentación decidirá, de forma motivada y a través de las resoluciones oportunas, sobre la información que, según la legislación vigente, resulte o no amparada por la confidencialidad".* A este respecto, tanto la normativa de protección de datos como la sanitaria, protegen la confidencialidad de este tipo de información.

Respecto de la confidencialidad, un sector doctrinal ha establecido que *"... la HC tiene carácter confidencial, por lo que el*

hospital tiene la responsabilidad de garantizar el derecho a la intimidad de su proceso asistencial. Todo personal del hospital, tiene la obligación de no difundir la información referente al paciente atendido en el Centro"[359]*.*

Ya Hipócrates, médico de la antigüa Grecia, reflejaba el tema de la confidencialidad en sus obras. Basado en el juramento hipocrático, el CDM en su introducción comienza diciendo *"JURO POR APOLO médico y por Asclepio y por Higia y por Panacea y todos los dioses y diosas, poniéndoles por testigos, que cumpliré, según mi capacidad y mi criterio, este juramento y declaración escrita:… Y SI EN MI PRÁCTICA médica, o aún fuera de ella, viviese u oyere, con respecto a la vida de otros hombres, algo que jamás debas ser revelado al exterior, me callaré considerando como secreto todo lo de este tipo…".*

Respecto del juramento hipocrático Nuria Terribas comenta en la introducción de uno de sus artículos que, *"El llamado «juramento hipocrático», que puede ser considerado como el primer Código de Ética Médica, impuso durante siglos, la práctica del secreto médico, con su máxima: «todo lo que oiga y vea durante el ejercicio o fuera del ejercicio de mi profesión y que no deba ser divulgado, lo mantendré en secreto como algo sagrado»"*[360]*.*

Y *"desde luego es alentador que ya desde esa época hubiese alguna directriz respecto a la confidencialidad. Afortunadamente, por otro lado, hoy en día los términos están más acotados, para no dejar a la conciencia de cada uno, una libertad tan amplia como la que pueda marcar cada ser humano a su criterio; aunque en el fondo, por muchas normas de conducta que existan, es fundamental su*

[359] CURRIEL HERRERO, J y ESTÉVEZ LUCAS, J: "*Manual para la gestión sanitaria y de la historia clínica hospitalaria*", Editores Médicos, Madrid, 2000. Pág. 76.

[360] TERRIBAS SALA, Núria: "*Los avances del derecho ante los avances de la medicina. Confidencialidad de los datos sanitarios: de la norma a la práctica médica*". In Salomé Adroher Biosca- Thomson Aranzadi, 2008. Pags 796-802.

difusión, con el fin de concienciar a quien trata con los datos personales, ya que en última instancia será él quien decida, de acuerdo a sus razonamientos internos si va a respetar o no ese deber de secreto, aún a sabiendas de que pueda haber reprimendas o sanciones por no guardarlo debidamente"[361]*.* Además *"gran importancia en todo esto tiene los códigos deontológicos que existen en casi todas las profesiones, que dedican parte de su contenido a regular este aspecto"*[362]*.*

El articulado del CDM dedica su capítulo V exclusivamente al secreto profesional del médico, contemplándolo en los artículos 27 a 31. De entre ellos cabe destacar lo siguiente. El artículo 27.1 establece que *"el secreto médico es uno de los pilares en los que se fundamenta la relación médico-paciente, basada en la mutua confianza, cualquiera que sea la modalidad de su ejercicio profesional".* Estableciendo el punto segundo a modo de definición que *"el secreto comporta para el médico la obligación de mantener la reserva y la confidencialidad de todo aquello que el paciente le haya revelado y confiado, lo que haya visto y deducido como consecuencia de su trabajo y tenga relación con la salud y la intimidad del paciente, incluyendo el contenido de la historia clínica"* .Asimismo el punto quinto de este mismo artículo establece que *"el médico no puede colaborar en ninguna base de datos sanitarios si no está garantizada la preservación de la confidencialidad de la información depositada en la misma".* Y el punto séptimo que *"el médico preservará en su ámbito social, laboral y familiar, la confidencialidad de los pacientes".*

Un sector doctrinal ha manifestado en este sentido que *"el secreto médico, como parte del secreto profesional, se configura como una de las señas de identidad que ha caracterizado el ejercicio de la Medicina a lo largo de su historia. El sentir ético del médico con*

[361] Ibídem.

[362] Ibídem.

respecto al secreto debe ser tal que se le considera como una cualidad inherente a la profesión médica y uno de "los pilares en los que se fundamenta la relación médico-paciente", tal y como indica el artículo 27.1 del Código de Deontología Médica (CDM)"[363]*.* Y añaden que *"en España, la norma que regula el secreto médico es el Código de Deontología Médica de la Organización Médica Colegial (OMC), y más concretamente el capítulo V, artículos 27 a 35, indicando que tal obligación lo es para todos los médicos, con independencia de "cualquiera que sea la modalidad de su ejercicio"*[364]*.* Pero además sostienen que *"actualmente la asistencia se ejerce por equipos profesionales que necesitan compartir la información para poder dar al paciente una atención de calidad y donde los datos se recopilan de forma más o menos mecánica y por diferentes profesionales tanto sanitarios como no sanitarios que tienen acceso a dichos datos y todos ellos sujetos al secreto y aparecen los conceptos de "secreto médico compartido " y de "secreto médico derivado"*[365]*.*

El artículo 29.1, establece por su parte que *"el médico debe exigir a sus colaboradores sanitarios y no sanitarios absoluta discreción y observancia escrupulosa del secreto profesional." Puntualizando el punto segundo que "En el ejercicio de la medicina en equipo, cada médico tiene el deber y responsabilidad de preservar la confidencialidad del total de los datos conocidos del paciente".* Y el punto tercero establece finalmente que *"el médico*

[363] BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: *"Manual de ética y deontología médica".* Organización Médica Colegial de España, 2012. Pág. 97.

[364] Ibídem. Pág. 98.

[365] BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: *"Manual de ética y deontología médica".* Organización Médica Colegial de España, 2012. Pág. 99.

debe tener una justificación razonable para comunicar a otro médico información confidencial de sus pacientes". De modo que la regla general es la confidencialidad, ya lo dice el 30.1, pero también establece a continuación una serie de excepciones a la misma, según las cuales *"el secreto profesional debe ser la regla. No obstante, el médico podrá revelar el secreto exclusivamente, ante quien tenga que hacerlo, en sus justos límites, con el asesoramiento del Colegio si lo precisara, en los siguientes casos: a. En las enfermedades de declaración obligatoria. b. En las certificaciones de nacimiento y defunción. c. Si con su silencio diera lugar a un perjuicio al propio paciente o a otras personas, o a un peligro colectivo. d. Cuando se vea injustamente perjudicado por mantener el secreto del paciente y éste permita tal situación. e. En caso de malos tratos, especialmente a niños, ancianos y discapacitados psíquicos o actos de agresión sexual. f. Cuando sea llamado por el Colegio a testificar en materia disciplinaria. g. Aunque el paciente lo autorice, el médico procurara siempre mantener el secreto por la importancia que tiene la confianza de la sociedad en la confidencialidad profesional. h. Por imperativo legal: 1. En el parte de lesiones, que todo médico viene obligado a enviar al juez cuando asiste a un lesionado. 2. Cuando actúe como perito, inspector, médico forense, juez instructor o similar. 3. Ante el requerimiento en un proceso judicial por presunto delito, que precise de la aportación del historial médico del paciente, el médico dará a conocer al juez que éticamente está obligado a guardar el secreto profesional y procurará aportar exclusivamente los datos necesarios y ajustados al caso concreto".*

E igualmente, respecto a la confidencialidad recoge además el artículo 19.9 del CDM que *"la historia clínica electrónica sólo es conforme a la ética cuando asegura la confidencialidad de la misma, siendo deseables los registros en bases descentralizadas".* No debe olvidarse que las tecnologías multiplican los riesgos de fuga de los

datos a la par que sus posibilidades de transmisión, según se ha referido ya en la introducción de este estudio.

En este sentido, una parte de la doctrina manifiesta respecto al secreto médico que *"el secreto médico tiene una doble regulación ética y moral que deriva de la relación médico paciente, y que se basa en el deber de no hacer daño, además del deber de secreto legal, el capítulo IV del Código Deontológico se ocupa de ello"* [366]. De modo que el personal sanitario debe atender no solo al deber de secreto establecido tanto por la legislación sanitaria como por la normativa de protección de datos, sino que además la deontología de la profesión contempla además un deber ético y moral al respecto.

La cercanía entre ética y confidencialidad, es vista también por otra parte de la doctrina que asegura que *"sin lugar a dudas que el manejo de la confidencialidad en el trabajo clínico diario es un asunto mucho más privativo de la ética profesional que de las exigencias legales e incluso el uso de la información sanitaria fuera del marco estrictamente asistencial requiere de una serie de precauciones que permitan hacer efectivo el respeto a los derechos del propio paciente"*[367].

En el derecho comparado, encontramos una serie de autores que afirman respecto del secreto médico y la confección del historial clínico que *"Existe una tensión especialmente fuerte entre lo dispuesto en el Código penal francés y la realidad del funcionamiento de las instituciones sanitarias, debido a la cada vez mayor fragilidad que afecta al secreto médico, en especial cuando éste se comparte. Además, hay que tener en cuenta los múltiples*

[366] CRIADO DEL RÍO, María Teresa y SEOANE PRADO, Javier: "*Aspectos médico-legales de la historia clínica"*. Colex, Madrid, 1999. Pág. 157.

[367] BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: *"Manual de ética y deontología médica".* Organización Médica Colegial de España, 2012. Pág. 104.

intercambios de información por Internet entre los agentes sanitarios y sociales, los facultativos y los organismos de la Seguridad Social. A esto se añade la intervención de los proveedores de servicios de alojamiento de datos, que reciben los datos que componen el historial clínico personal, y que son empresas de informática"[368] .Además argumentan que *"el Código de deontología médica indica, para la profesión, el contenido del secreto (art. 4): «El secreto abarca todo lo que llega al conocimiento del médico en el ejercicio de su profesión, es decir no solamente lo que le ha sido confiado, sino también lo que él ha visto, escuchado o comprendido». Esta obligación tradicional se entiende en sentido amplio, a tenor de la Ley de 4 de marzo de 2002, como un derecho del que se beneficia el paciente y una obligación que pesa sobre los profesionales, los establecimientos y las redes sanitarias, así como sobre los organismos que participan en la prevención de la salud. Frente a esto, la persona tiene derecho «al respeto de su intimidad y al respeto de sus datos personales». El artículo L111O-4 del Código francés de salud pública otorga un sentido amplio a la obligación de respetar el secreto de los datos"*[369]*.*

Y aunque la normativa sobre protección de datos no alcanza a regular los datos de las personas fallecidas, hay que referir en este punto, que el mismo sector doctrinal que se acaba de comentar ha manifestado respecto de los datos médicos de las personas fallecidas que *"el deber de secreto profesional médico, no afecta solo al paciente en vida, sino que se prolonga aún después de su muerte, pues una vez muerto, posee aún derechos personalísimos"*[370]*.* Y en

[368] RODOTA, Stefano, DUPRAT, Jean-Pierre, PIÑAR MAÑAS, José Luis, NIETO GARRIDO, Eva, HERNÁNDEZ CORCHETE, Juan Antonio: *"Transparencia, acceso a la información y protección de datos"*. Editorial Reus, S.A., Madrid, 2014. Pág. 28.

[369] RODOTA, Stefano, DUPRAT, Jean-Pierre, PIÑAR MAÑAS, José Luis, NIETO GARRIDO, Eva, HERNÁNDEZ CORCHETE, Juan Antonio: *"Transparencia, acceso a la información y protección de datos"*. Editorial Reus, S.A., Madrid, 2014. Pág. 29.

[370] CRIADO DEL RÍO, María Teresa y SEOANE PRADO, Javier: "*Aspectos médico-legales de la historia clínica"*. Colex, Madrid, 1999. 161.

mi opinión, los datos personales de los fallecido deberían estar de alguna forma protegidos, ya que si una persona durante su vida ha expresado unos deseos sobre sí mismo, moralmente deberían ser respetados después de su muerte; aunque el RLOPD en su artículo 2 al regular el ámbito objetivo de aplicación del mismo, recordemos, que según se ha expresado anteriormente al hablar de las exclusiones de aplicación de esta norma, regula en su punto cuarto que *"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 óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos".*

En este sentido, el informe jurídico 0171/2008 de la AEPD, recoge que *"…una interpretación del artículo 18.4 de la Ley Orgánica 41/2002 coherente con el contexto normativo en el que la misma fue aprobada permitiría el ejercicio del derecho de acceso a la historia clínica del fallecido por parte de su cónyuge o persona vinculada con aquél por una relación de hecho similar, ascendientes y descendientes, así como las personas que hubieran sido designadas por el fallecido para ejercer las acciones a las que se refiere la Ley Orgánica 1/1982 y, en última instancia, sus herederos que además se encontrasen vinculados a aquél por relaciones familiares o de hecho análogas a la familiar".*

Respecto de los datos de personas fallecidas, Juan Mejía opina que *"… debe entregarse a los familiares solo la parte objetiva, excluyendo las informaciones de terceros y las anotaciones personales del médico, siempre que el fallecido no hubiera prohibido expresamente"*[371]*.* Hay que recordar que este tema ya ha sido

[371] MEJÍA, Juan. "*Hacia un estatuto jurídico desarrollado de la Historia Clínica*". Diario La Ley 5638 de octubre de 2002.

comentado respecto de la titularidad de la historia clínica en el capítulo correspondiente.

Por su parte la Carta de los Derechos de los Pacientes, recoge en su segunda parte, entre los catorce derechos del paciente, en sexto lugar el derecho a la privacidad y confidencialidad. Según este, *"Ttdo individuo tiene derecho a la confidencialidad sobre la información personal, incluyendo información sobre su estado de salud y diagnóstico potencial o procedimientos terapéuticos, así como a la protección de su privacidad durante la realización de los exámenes de diagnóstico, visitas de especialistas y tratamientos médicos o quirúrgicos en general. Toda la información relativa al estado de salud de un individuo y a los tratamientos médicos o quirúrgicos a los que está sujeto, deben ser considerados privados, y como tales, deben ser adecuadamente protegidos. La privacidad personal debe ser respetada, incluso a lo largo de tratamientos médicos o quirúrgicos (exámenes para establecer un diagnóstico, visitas de especialistas, medicaciones, etc.), que deben tener lugar en un medio apropiado y en presencia de las personas absolutamente necesarias (a menos que el paciente haya dado un consentimiento explícito o realizado una petición al respecto)".*

El Real Decreto-Ley 9/2014, de 4 de julio, por el que se establecen las normas de calidad y seguridad para la donación, la obtención, la evaluación, el procesamiento, la preservación, el almacenamiento y la distribución de células y tejidos humanos y se aprueban las normas de coordinación y funcionamiento para su uso en humanos (RDLCT- Real Decreto-Ley sobre Células y Tejidos), regula así mismo el tema de la confidencialidad. Recoge así en su punto primero que *"se garantizará a los donantes la confidencialidad de todos los datos relacionados con su salud y facilitados al personal autorizado, así como de los resultados y la trazabilidad de sus donaciones, de acuerdo con la Ley Orgánica 15/1999, de 13 de*

diciembre, de Protección de Datos de Carácter Personal". Concretando en su punto tercero que *"los datos de carácter personal tendrán carácter confidencial y estarán exclusivamente a disposición de los interesados, conforme a lo dispuesto en 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 y, en su caso, de la autoridad judicial para el ejercicio de las funciones que tiene encomendadas. Su utilización se limitará a fines asistenciales o de interés para la salud pública y será recogida y custodiada conforme a lo dispuesto en el artículo 10 de la Ley 14/1986, de 25 de abril, en la Ley Orgánica 15/1999, de 13 de diciembre, y en la Ley 41/2002, de 14 de noviembre".* Y remata en su punto quinto la cuestión de la confidencialidad estableciendo que *"no podrán facilitarse ni divulgarse informaciones que permitan la identificación de donantes y receptores de células y tejidos humanos, ni podrán facilitarse a los donantes o sus familiares los datos identificadores de los receptores o viceversa".* No obstante, el punto anterior, recoge la excepción, según la cual *"el deber de confidencialidad no impedirá la adopción de medidas preventivas cuando se sospeche la existencia de riesgos para la salud individual o colectiva en los términos previstos en los artículos 25 y 26 de la Ley 14/1986, de 25 de abril, o, en su caso, conforme a lo que establece la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública, la Ley 41/2002, de 14 de noviembre, y la Ley Orgánica 15/1999, de 13 de diciembre".*

También el artículo 28 del comentado Real Decreto-Ley, referido a los sistema de recogida y custodia de la información, recoge en su punto primero que "*Los centros y unidades autorizados para la aplicación en humanos de células o tejidos humanos deberán disponer de un sistema de recogida y custodia de información sobre las actividades realizadas en este ámbito, de acceso restringido y confidencial, donde constarán los usos y aplicaciones clínicos realizados con los datos necesarios para la identificación de los*

receptores, de los tejidos y/o células implantados así como su procedencia, de forma que se permita el adecuado seguimiento en caso necesario, conforme a lo especificado en el capítulo V".

Y por su parte el ANEXO I, de esta misma norma, que recoge los requisitos y condiciones mínimas para las autorizaciones de establecimientos de tejidos y centros o unidades de obtención y aplicación de células y tejidos, en su punto 1 j), establece lo siguiente *"los requisitos y condiciones mínimas para la autorización de centros sanitarios para obtener células y tejidos humanos para su uso en humanos son:… j) Disponer de un sistema de recogida y custodia de la información relativa a sus actividades, de acceso restringido y confidencial donde constarán las extracciones realizadas y los datos necesarios de los donantes, de las células o tejidos, así como el destino final o intermedio de los mismos. Se conservarán los datos relativos a las pruebas realizadas y características de los donantes, especificándose la fecha de realización y el resultado de las mismas, de forma que se permita el adecuado seguimiento de la información, en caso necesario, conforme a lo previsto en los artículos 13 y 31".* Con esto queda regulada de forma muy amplia esta materia en cuanto a la manipulación de las células y tejidos en el ser humano.

El deber de secreto respecto de los datos de los menores, es un tema que contempla Nuria Terribas, quien asegura que el art. 7 de la Ley 41/2002 *"…reconoce el derecho a la intimidad de toda persona, sin distinción de edad o nivel de competencia, obligando siempre al respeto a la confidencialidad de sus datos…",* pero matiza que el art. 5 de esta norma en relación al derecho a la información *"… si bien dispone como criterio general que el titular del derecho a la información es el paciente, también legitima el hecho de compartir la información con los familiares o personas vinculadas al paciente cuando éste no tiene plena competencia para entender dicha*

información"[372]*.* Y además señala que *"…la Ley 1/1996 de Protección Jurídica de Menor dispone claramente el derecho al «secreto de las comunicaciones» y, por ende, la transmisión de información en el contexto de la relación clínica debe entenderse como «comunicaciones» que atañen a la vida personal de ese menor…"*[373]*.*

A este respecto esta autora habla de un tercer factor socio-cultural, *"se trata de la intervención de las familias y personas del contexto del paciente en todo su proceso de salud, y por tanto también del acceso a la información sobre éste, al mismo nivel, o incluso por encima del propio paciente"*[374]*.* Resalta que el paciente *"…es el auténtico titular del derecho a la información y sólo cuando nos autorice, expresa o tácitamente, podremos informar también a familia o personas vinculadas…pero no a la inversa. En términos psicológicos, a este tipo de actitudes se denomina «conspiración del silencio»"*[375]*.*

En relación directa con la confidencialidad, aunque también con las medidas de seguridad de nivel básico para los ficheros no automatizados, o la gestión de soportes para los automatizados, se expresa Samprón López *"respecto de la custodia de la HC, los artículos 10.11.3.8, así como el 61, establecen el derecho a que conste por escrito la HC, esté a disposición de los enfermos, así como de las inspecciones y la ciencia. También el RD 63/95 de 20 de enero de ordenación de prestaciones sanitarias del sistema nacional de la salud, contempla la posibilidad de un ejemplar a*

[372] TERRIBAS I SALA, Núria*: "Aspectos legales de la atención a los menores de edad".* Institut Borja de Bioética. Universitat Ramon Llull. FMC. 2008. Barcelona. España. Pags 367-73.

[373] Ibídem.

[374] TERRIBAS SALA, Núria: "*Los avances del derecho ante los avances de la medicina. Confidencialidad de los datos sanitarios: de la norma a la práctica médica*". In Salomé Adroher Biosca- Thomson Aranzadi, 2008. Pags 796-802.

[375] TERRIBAS SALA, Núria: "*Los avances del derecho ante los avances de la medicina. Confidencialidad de los datos sanitarios: de la norma a la práctica médica*". In Salomé Adroher Biosca- Thomson Aranzadi, 2008. Pags 796-802.

petición del interesado. También la LOPD lo contempla en sus arts 9 y 10, y también lo garantiza la normativa autonómica"[376]*.*

Pensemos que la protección de datos dentro de los distintos servicios de un hospital o centro de salud plantea grandes diferencias, ya que los pacientes pueden ser derivados a nivel de consulta externa, servicio de urgencias, hospitalización, tratamientos de día como hospital de día, diálisis, Rx, rehabilitación, o transporte de enfermos mediante el servicio de ambulancias.

Las medidas de seguridad en los locales y equipos informáticos, la ubicación del mobiliario y equipos informáticos a través del cableado o la orientación de los mismos para la visualización de datos, el acceso a recursos en lo que se organice la documentación como cajones, estanterías, bandejas o carpetas organizadas por colores u otros distintivos, pueden ayudar a la fluidez en el trabajo, ya que la gestión de los datos de salud a menudo suele ser urgente.

De forma habitual, los profesionales sanitarios abandonan sus puestos de trabajo durante a atención a los pacientes en las consultas médicas, unas veces por causas externas a la atención que se está realizando en ese momento, con motivo de una urgencia o la consulta de un colega, y otras, porque es el propio médico que está atendiendo al paciente, a quien le surge una duda, gestión o comprobación que resolver con los distintos servicios.

El caso es que, comúnmente, queda a la vista y mano de los pacientes, información y recursos que almacenan datos médicos, tanto del paciente atendido en ese momento como de otros que han pasado recientemente por la consulta, y cuyos expedientes están pendientes de ser gestionados. Pero en la realidad, la rutina del trabajo día a día, puede hacer francamente complicado, que en una

[376] SAMPRÓN LÓPEZ, David. "*Los derechos del paciente a través de la información de la historia clínica*". Edisofer, Madrid, 2002. Pág. 83.

mesa en la que se atiende a los pacientes que acuden a sus consultas, no haya una historia del paciente anteriormente atendido, una anotación sobre algo que ha quedado pendiente, o simplemente un listado de las citas programadas para el día.

No resultaría posible ni operativo, guardar toda la información del paciente que ha sido atendido, una vez finalizada la consulta, porque, probablemente, haya que trasladar la información a otro departamento, realizar alguna gestión que haya quedado pendiente por lo apretado de la agenda diaria, o que simplemente queramos tener a la vista con el fin de no olvidar determinado trámite o consulta. Pero no es menos cierto, en un nivel al que la vista del paciente atendido no alcance, por ejemplo en casilleros rotulados con carteles que indiquen la prioridad, destino o trámite a realizar con la documentación pendiente de archivar, ubicándolos en estanterías a las que el paciente no tenga acceso. Habría que buscar el punto óptimo entre operatividad y confidencialidad.

Esto en cuanto respecta al tiempo que médico y paciente permanecen en la consulta, pero la realidad es que, como he comentado en el inicio, en numerosas ocasiones, el médico se ausenta del lugar en el que el paciente permanece, con la documentación a la vista.

Si en esta situación, por circunstancias del día a día, permaneciera información de otros paciente al alcance del que está siendo atendido, mermando la privacidad por parte del personal médico, parecería razonable pensar que, como contrapartida, esa parte de desprotección, sea suplida con la confidencialidad del paciente, evitando con ello tener que sacar al paciente de la consulta mientras el médico no permanezca en ella, lo cual resultaría claramente inadecuado, pudiendo perjudicar la confianza que se establece en las relaciones médico-paciente.

Resulta complicado en la realidad, llevar a cabo una confidencialidad absoluta con los datos de los pacientes, pero no es

menos cierto que, en algunas ocasiones, no se repara en mantener unos mínimos, como mantener la mesa de atención a los pacientes despejada, para con ello, mantener la confidencialidad de la información.

En este contexto conviene citar lo que recoge el informe jurídico 0501/2009 de la AEPD sobre la instalación de unas pantallas en las camas de un centro sanitario al que acceden mediante un lector de código de barras que se encuentra en la tarjeta identificativa de cada uno de los profesionales. Ante esta cuestión, expresa el informe que *"…las medidas indicadas en la consulta para evitar la visualización de los datos de salud del paciente por personas distintas al personal sanitario, resultan adecuadas a la finalidad perseguida, impidiéndose así que se produzca una cesión de datos sin el pertinente consentimiento del afectado".* Esto es sin duda una muestra de que los avances informáticos pueden beneficiar la confidencialidad.

El CDM en este sentido recoge en su artículo 28.1 que *"el director médico de un centro o servicio sanitario velará por el establecimiento de los controles necesarios para que no se vulnere la intimidad y la confidencialidad de los pacientes ni la documentación referida a ellos"*.

Sobre la intimidad y la confidencialidad cabe citar que el preámbulo de la Ley del Aborto, recoge que *"el desarrollo de la sexualidad y la capacidad de procreación están directamente vinculados a la dignidad de la persona y al libre desarrollo de la personalidad y son objeto de protección a través de distintos derechos fundamentales, señaladamente, de aquellos que garantizan la integridad física y moral y la intimidad personal y familiar …",* y establece más adelante que *"por otro lado, la Plataforma de Acción de Beijing acordada en la IV Conferencia de Naciones Unidas sobre la mujer celebrada en 1995, ha reconocido que «los derechos humanos de las mujeres incluyen el derecho a tener el control y a decidir libre y responsablemente sobre su*

sexualidad, incluida la salud sexual y reproductiva, libre de presiones, discriminación y violencia»….". De hecho, la citada norma recoge en su título II, bajo la rúbrica "*de la interrupción voluntaria del embarazo*", y dentro de éste en el capítulo segundo dedicado a las garantías, y en clara referencia a las exigencias establecidas en la normativa de protección de datos, la protección de la intimidad y confidencialidad, el tratamiento de datos, su acceso y cesión, así como la cancelación de los mismos. Es en concreto el artículo 20 el que se refiere la protección de la intimidad y confidencialidad, y dice literalmente *"1. Los centros que presten la interrupción voluntaria del embarazo asegurarán la intimidad de las mujeres y la confidencialidad en el tratamiento de sus datos de carácter personal. 2. Los centros prestadores del servicio deberán contar con sistemas de custodia activa y diligente de las historias clínicas de las pacientes e implantar en el tratamiento de los datos las medidas de seguridad de nivel alto previstas en la normativa vigente de protección de datos de carácter personal".*

Ley 14/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida, establece en su artículo 3.6 la confidencialidad de las historias clínicas en relación al proceso de aplicación de técnicas de reproducción asistida. Establece este precepto que *"todos los datos relativos a la utilización de estas técnicas deberán recogerse en historias clínicas individuales, que deberán ser tratadas con las debidas garantías de confidencialidad respecto de la identidad de los donantes, de los datos y condiciones de los usuarios y de las circunstancias que concurran en el origen de los hijos así nacidos. No obstante, se tratará de mantener la máxima integración posible de la documentación clínica de la persona usuaria de las técnicas".*

Además en referencia a los contratos de donación se establece el su artículo 5.5 el anonimato como garantía de la confidencialidad para los donantes, estableciéndose solo como excepción el riesgo para la salud del futuro hijo o por imperativo legislativo, sin comportar

que la identidad de los donantes sea pública. Así recoge este artículo en su párrafo primero que *"la donación será anónima y deberá garantizarse la confidencialidad de los datos de identidad de los donantes por los bancos de gametos, así como, en su caso, por los registros de donantes y de actividad de los centros que se constituyan".* Pero el segundo párrafo rompe parcialmente esta norma a favor de los descendientes y dice que *"los hijos nacidos tienen derecho por sí o por sus representantes legales a obtener información general de los donantes que no incluya su identidad. Igual derecho corresponde a las receptoras de los gametos y de los pre-embriones".* Y el tercer párrafo la rompe de forma total, ya que establece que *"sólo excepcionalmente, en circunstancias extraordinarias que comporten un peligro cierto para la vida o la salud del hijo o cuando proceda con arreglo a las Leyes procesales penales, podrá revelarse la identidad de los donantes, siempre que dicha revelación sea indispensable para evitar el peligro o para conseguir el fin legal propuesto. Dicha revelación tendrá carácter restringido y no implicará en ningún caso publicidad de la identidad de los donantes".* Es decir, que solo cuando haya en peligro una vida o así lo autorice una ley se permite el conocimiento restringido.

Estas condiciones de confidencialidad se mantendrán en los casos de utilización de pre-embriones con fines de investigación que sean cedidos a otros centros, como recoge el artículo 15.1e): *"La investigación o experimentación con pre-embriones sobrantes procedentes de la aplicación de las técnicas de reproducción asistida sólo se autorizará si se atiene a los siguientes requisitos: e) En el caso de la cesión de pre-embriones a otros centros, en el proyecto mencionado en el párrafo anterior deberán especificarse las relaciones e intereses comunes de cualquier naturaleza que pudieran existir entre el equipo y centro entre los que se realiza la cesión de pre-embriones. En estos casos deberán también mantenerse las condiciones establecidas de confidencialidad de los*

datos de los progenitores y la gratuidad y ausencia de ánimo de lucro".

Y respecto a las normas de funcionamiento en los centros y equipos, establece esta legislación en su artículo 18.2 que no se podrá revelar la identidad de los donantes, al regular que *"los equipos biomédicos y la dirección de los centros o servicios en que trabajan incurrirán en las responsabilidades que legalmente correspondan si violan el secreto de la identidad de los donantes, si realizan mala práctica con las técnicas de reproducción asistida o los materiales biológicos correspondientes o si, por omitir la información o los estudios establecidos, se lesionan los intereses de donantes o usuarios o se transmiten a los descendientes enfermedades congénitas o hereditarias, evitables con aquella información y estudio previos".* Además el punto tercero del citado artículo recoge que los datos de los donantes y usuarios, así como los consentimientos de unos y de otros se recogerán en una historia clínica protegida con las normas establecidas para mantener su confidencialidad. Y así lo expresa, *"los equipos médicos recogerán en una historia clínica, custodiada con la debida protección y confidencialidad, todas las referencias sobre los donantes y usuarios, así como los consentimientos firmados para la realización de la donación o de las técnicas".* Llegada la mayoría de edad, el hijo y los padres receptores de la donación podrán solicitar los datos de la historia clínica, pero no los datos de los donantes, ya que según se establece en el último párrafo de este artículo, *"los datos de las historias clínicas, excepto la identidad de los donantes, deberán ser puestos a disposición de la receptora y de su pareja, o del hijo nacido por estas técnicas o de sus representantes legales cuando llegue a su mayoría de edad, si así lo solicitan".*

Existe, un Registro nacional de donantes, adscrito al Ministerio de Sanidad y Consumo, el cual debe garantizar igualmente su confidencialidad, y según regula el artículo 21.1, *"el Registro*

nacional de donantes, adscrito al Ministerio de Sanidad y Consumo, es aquel registro administrativo en el que se inscribirán los donantes de gametos y pre-embriones con fines de reproducción humana, con las garantías precisas de confidencialidad de los datos de aquéllos".

Este registro, según regula el punto segundo de este mismo artículo se basa en datos administrados por las Comunidades Autónomas según les corresponda territorialmente, conteniendo el dato de la identidad de las mujeres o parejas receptoras, los hijos nacidos de cada donante, así como la localización de todos ellos desde la donación hasta la utilización de los tejidos donados. Así lo recoge el citado artículo, *"el Registro nacional de donantes, adscrito al Ministerio de Sanidad y Consumo, es aquel registro administrativo en el que se inscribirán los donantes de gametos y pre-embriones con fines de reproducción humana, con las garantías precisas de confidencialidad de los datos de aquéllos".* Almacenando información muy sensible, de acuerdo al segundo párrafo de este precepto que establece que *"este registro, cuyos datos se basarán en los que sean proporcionados por las comunidades autónomas en lo que se refiere a su ámbito territorial correspondiente, consignará también los hijos nacidos de cada uno de los donantes, la identidad de las parejas o mujeres receptoras y la localización original de unos y otros en el momento de la donación y de su utilización".*

Lo que sin duda requerirá de unas medidas de seguridad de nivel alto que deberán seguirse muy de cerca por la sensibilidad de los datos, que será regulado por el gobierno, ya que según marca el 21.3 *"el Gobierno, previo informe del Consejo Interterritorial del Sistema Nacional de Salud y mediante real decreto, regulará la organización y funcionamiento del registro nacional".* Incluso en el capítulo destinado a la regulación de las infracciones y sanciones, el artículo 24.4,2º protege la intimidad personal y familiar y la protección de los datos personales, si estos derechos resultasen afectados, a propósito de las medidas a tomar en casos de

sanciones, que deberán respetar; según marca este precepto *"… las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar y a la protección de los datos personales, cuando éstos pudieran resultar afectados".*

La Declaración sobre derechos de los pacientes en cuanto a la privacidad en la asistencia que reciban y en la confidencialidad sobre la información relativa al paciente, contenida en su historia, marca la pauta de no entrometerse en su vida privada a no ser necesario, así como a la protección de los sistemas que la contengan dicha información, respetando el derecho a conocerla y a obtener copia de ella. En el punto cuarto de este texto se establece respecto de la confidencialidad y privacidad que "4.1.*Toda información sobre el estado de salud del paciente, condición médica, diagnóstico, pronóstico, tratamiento y cualquier otra información de tipo personal debe ser confidencial, incluso tras la muerte. 4.2 La información confidencial sólo podrá ser revelada si el paciente da su consentimiento explícito o si la ley lo ordena expresamente. 4.3 Se presume el consentimiento cuando su revelación se hace a otros profesionales de la salud implicados en el tratamiento del paciente. 4.4 Todos los datos identificables del paciente deben ser protegidos. La protección de los datos debe ser apropiada a la hora de proceder a su archivo. 4.5 Las sustancias humanas de las cuales se pueda obtener datos identificables, deben ser asimismo protegidas. Los pacientes tienen derecho de acceso a sus expedientes médicos e informes técnicos y a cualquier otro expediente y registro pertinente para su diagnóstico, tratamiento y cuidado y a recibir una copia de su propio expediente y registros o partes del mismo. Tal acceso excluye datos concernientes a terceros. Los pacientes tienen derecho a requerir la corrección, finalización, supresión, clarificación y/o actualización de sus datos personales y médicos que sean incorrectos, incompletos, ambiguos o anticuados, o que no resulten relevantes para los propósitos de diagnóstico, tratamiento y cuidado.*

4.6 No puede darse la intrusión en la vida privada y familiar del paciente, a no ser, y sólo si además del consentimiento del paciente, puede justificarse como necesario para el diagnóstico del paciente y su tratamiento y atención. 4.7 Las intervenciones médicas sólo pueden llevarse a cabo cuando se muestre el respeto debido a la privacidad del individuo. Esto quiere decir que una intervención dada sólo podrá llevarse a cabo en presencia de aquellas personas necesarias para la intervención, a no ser que el paciente de su consentimiento o requiera otra cosa. 4.8 Los pacientes admitidos en un centro médico tienen derecho a esperar instalaciones físicas que aseguren su privacidad/intimidad, en particular cuando los profesionales de la salud les estén ofreciendo cuidados personales o estén llevando a cabo exámenes y tratamientos".

La Declaración Universal sobre Bioética y Derechos Humanos, se refiere al tema del consentimiento estableciendo en su artículo noveno que *"la privacidad de las personas interesadas y la confidencialidad de la información que les atañe deberían respetarse. En la mayor medida posible, esa información no debería utilizarse o revelarse para fines distintos de los que determinaron su acopio o para los que se obtuvo el consentimiento, de conformidad con el derecho internacional, en particular el relativo a los derechos humanos".*

La progresiva incorporación en todos los hospitales del Sistema Nacional de Salud de habitaciones individuales es un importante reto que recoge La Ley de calidad sanitaria, que establece en el artículo 28.1, párrafo tercero, establece que *"…los hospitales del Sistema Nacional de Salud procurarán la incorporación progresiva de habitaciones de uso individual".* Esto, según se ha comentado anteriormente, es muy beneficioso para la seguridad y confidencialidad de los datos de los pacientes.

La Ley General de Sanidad, regula entre los derechos de los pacientes, en su artículo 10.7, respecto a este tema que *"a la*

confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público". Por otro lado, cuando se ocupa de las infracciones sanitarias, y en relativa contradicción con lo anteriormente establecido, el artículo 35 A 1ª establece entre las leves *que "las simples irregularidades en la observación de la normativa sanitaria vigente, sin trascendencia directa para la salud pública"*. Y el punto B 5ª de este mismo artículo establece entre las graves que *"la resistencia a suministrar datos, facilitar información o prestar colaboración a las autoridades sanitarias, a sus agentes o al órgano encargado del Registro Estatal de Profesionales Sanitarios".* Y entre las muy graves el apartado C 5ª dice que *"la negativa absoluta a facilitar información o prestar colaboración a los servicios de control e inspección".* De modo que respetando la confidencialidad, hay casos en los que es obligatorio suministrar información, como ya he manifestado.

Según establece el Real Decreto sobre receta médica, en el momento de dispensación de la receta, el paciente podrá solicitar confidencialidad en ciertos tratamientos a través de procedimientos especiales establecidos al efecto. No obstante, el sistema de receta médica electrónica, debe garantizar en todo momento la seguridad y confidencialidad de la información de acuerdo a la LOPD, según se expresa concretamente en el articulado de esta norma. Así lo establece el artículo 8.1, el cual marca que *"el prescriptor accederá al sistema de receta médica electrónica a través de un equipo integrado en el Sistema de receta electrónica que deberá estar autentificado, garantizándose las comunicaciones cifradas. El prescriptor ha de acreditar su identidad y firmará electrónicamente la prescripción. Para prescribir la medicación del paciente, solicitará la tarjeta sanitaria individual para introducir en el sistema el código de identificación personal".* Puntualizándose además en el punto quinto de este mismo artículo que *"el paciente podrá solicitar en el momento de la prescripción, protección y confidencialidad en la*

dispensación de algún tratamiento. En estos casos el tratamiento se diferenciará para la dispensación, pudiéndose realizar a través de receta en soporte papel o a través de los procedimientos que se determinen por las Administraciones sanitarias".

Además el artículo 9.2 establece en este sentido, respecto de la dispensación farmacéutica en la receta médica electrónica que *"tras la identificación inequívoca del paciente, y en su caso de la persona en quien delegue, el farmacéutico sólo podrá acceder desde los equipos instalados en la oficina de farmacia, con los requisitos y condiciones que se establecen en el apartado siguiente, a los datos necesarios para una correcta dispensación informada y seguimiento del tratamiento y dispensará exclusivamente, de entre las prescripciones pendientes de dispensar, las que el paciente solicite".* Estableciendo a continuación en el punto tercero que *"sólo se permitirá el acceso de los farmacéuticos al sistema electrónico mediante la tarjeta sanitaria del paciente debidamente reconocida por el sistema de receta electrónica, debiendo ser devuelta de forma inmediata a su titular y sin que pueda ser retenida en la oficina de farmacia. El acceso del farmacéutico siempre quedará registrado en el mencionado sistema".*

Respecto de la receta médica electrónica, Aberasturi Gorriño dice que *"la receta electrónica es otro de los grandes proyectos en la aplicación de las TIC al ámbito sanitario. En los casos en que la dispensación de los medicamentos necesita de la intervención del médico, la receta constituye la prescripción del facultativo en la que se le indica al farmacéutico el medicamento y la dosis que ha de tomar un paciente determinado. Se trata, en lo que aquí interesa, por una parte, de un documento a través del cual culmina la asistencia médica, y, por otra, de un soporte en el que se integra información relativa a la salud además de otro tipo de datos, de un individuo determinado. Cuando se hace referencia a la receta electrónica se habla de la aplicación de la telemática a este instrumento. Ha*

subrayado la doctrina que lo característico de la receta electrónica es que la receta no tiene por qué imprimirse en un papel (lo que no quiere decir que no se imprima como comprobante para el paciente). Se supone que con este proyecto el médico prescribirá la receta a través del ordenador, ésta irá a una base de datos a la que estará conectado el farmacéutico, quien tendrá acceso a la misma a través de la Tarjeta Sanitaria Electrónica o magnética del paciente. Hoy día las leyes disponen de manera expresa la necesidad de tender a implantar esta herramienta, y tanto en el ámbito autonómico como estatal diversas normas la han incorporado"[377]*.*

Asimismo el artículo 11, dedicado a la protección de la confidencialidad de los datos, establece que *"el sistema de receta médica electrónica garantizará la seguridad en el acceso y transmisión de la información, así como la protección de la confidencialidad de los datos, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Se implantarán las medidas de seguridad de nivel alto, previstas en la referida normativa de protección de datos de carácter personal. Para garantizar dichos niveles de seguridad, esta información sólo será accesible desde la oficina de farmacia a efectos de dispensación, residirá de forma permanente en los sistemas de receta electrónica gestionados por las Administraciones sanitarias y no podrá ser almacenada en los repositorios o servidores ajenos a éstas, establecidos para efectuar la facturación, una vez esta se haya producido".*

Como vemos, tanto en las recetas médicas como en las órdenes de dispensación, se implantarán las medidas de seguridad establecidas en la LOPD y RLOPD, no siendo necesario el consentimiento en los procesos de implantación de los sistemas de información, ya sean en soporte papel o informático. Y en general se

[377] ABERASTURI GORRIÑO, Unai: *"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 32.

respetará la normativa de protección de datos en el tratamiento, cesión o custodia de los datos de carácter personal para las actuaciones previstas en este Real Decreto sobre la receta médica.

El capítulo IX de la Ley 33/2011, de 4 de octubre, General de Salud Pública y regulan los sistemas de información en Salud Pública, y su artículo 41 dedicado a la Organización de los sistemas de información, dice en el punto tercero que *"a los efectos indicados en los dos apartados anteriores, las personas públicas o privadas cederán a la autoridad sanitaria, cuando así se las requiera, los datos de carácter personal que resulten imprescindibles para la toma de decisiones en salud pública, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal".* Y es que el primer punto del referido artículo establece que *"las autoridades sanitarias con el fin de asegurar la mejor tutela de la salud de la población podrán requerir, en los términos establecidos en este artículo, a los servicios y profesionales sanitarios informes, protocolos u otros documentos con fines de información sanitaria".* Y continúa diciendo en el segundo que *"las Administraciones sanitarias no precisarán obtener el consentimiento de las personas afectadas para el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras Administraciones públicas sanitarias, cuando ello sea estrictamente necesario para la tutela de la salud de la población".*

Igualmente, hay que referir en este sentido la disposición final tercera de esta norma modifica la Ley del paciente, que en su artículo 16.3 pasa a decir que: *"El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en la Ley General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los*

de carácter clínicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos".

A este propósito, el informe 0065/2009 de la AEPD, apunta en este sentido, y respecto de las excepciones previstas en el ahora mencionado 16.3 de la Ley del Paciente que *"…. se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso".*

Son varios los artículos de la Ley de investigación biomédica que hacen referencia a este tema. El artículo segundo en referencia a los principios y garantías, establece en su letra c) que *"la realización de cualquier actividad de investigación biomédica comprendida en esta Ley estará sometida a la observancia de las siguientes garantías: c) Las investigaciones a partir de muestras biológicas humanas se realizarán en el marco del respeto a los derechos y libertades fundamentales, con garantías de confidencialidad en el tratamiento de los datos de carácter personal y de las muestras biológicas, en especial en la realización de análisis genéticos".*

Del mismo modo, el artículo 5, en relación a la protección de datos personales y garantías de confidencialidad, establece en su punto primero que *"se garantizará la protección de la intimidad personal y el tratamiento confidencial de los datos personales que resulten de la actividad de investigación biomédica, conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Las mismas garantías serán de aplicación a las muestras biológicas que sean fuente de información de carácter personal".* El punto segundo recoge respecto

al consentimiento que *"…la cesión de datos de carácter personal a terceros ajenos a la actuación médico-asistencial o a una investigación biomédica, requerirá el consentimiento expreso y escrito del interesado. En el supuesto de que los datos obtenidos del sujeto fuente pudieran revelar información de carácter personal de sus familiares, la cesión a terceros requerirá el consentimiento expreso y escrito de todos los interesados"*. Y en el punto tercero, también en este sentido *"… prohíbe la utilización de datos relativos a la salud de las personas con fines distintos a aquéllos para los que se prestó el consentimiento".* El punto cuarto establece , por su parte que *"quedará sometida al deber de secreto cualquier persona que, en el ejercicio de sus funciones en relación con una actuación médico-asistencial o con una investigación biomédica, cualquiera que sea el alcance que tengan una y otra, acceda a datos de carácter personal. Este deber persistirá aún una vez haya cesado la investigación o la actuación".* Y el punto quinto, como ya se refirió anteriormente con el tema de la información, sigue especificando que *"si no fuera posible publicar los resultados de una investigación sin identificar a la persona que participó en la misma o que aportó muestras biológicas, tales resultados sólo podrán ser publicados cuando haya mediado el consentimiento previo y expreso de aquélla".*

El artículo 51, dedicado en pleno al deber de confidencialidad y derecho a la protección de los datos genéticos, establece en su punto primero que *"el personal que acceda a los datos genéticos en el ejercicio de sus funciones quedará sujeto al deber de secreto de forma permanente. Sólo con el consentimiento expreso y escrito de la persona de quien proceden se podrán revelar a terceros datos genéticos de carácter personal. Si no es posible publicar los resultados de una investigación sin identificar a los sujetos fuente, tales resultados sólo podrán ser publicados con su consentimiento".* Y puntualiza el punto segundo que *"en el caso de análisis genéticos a varios miembros de una familia los resultados se archivarán y*

comunicarán a cada uno de ellos de forma individualizada. En el caso de personas incapacitadas o menores se informará a sus tutores o representantes legales".

El artículo octavo que habla sobre la trazabilidad y seguridad, recoge que *"deberá garantizarse la trazabilidad de las células, tejidos y cualquier material biológico de origen humano, para asegurar las normas de calidad y seguridad, respetando el deber de confidencialidad y lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal".*

Respecto del análisis genético en preembriones, embriones o fetos, establece el artículo 53 que *"los resultados de los análisis genéticos realizados en material embrionario o fetal estarán sometidos a los principios de protección de datos y de confidencialidad establecidos en esta Ley. El mismo criterio regirá en relación con cualquier otra muestra biológica que pueda contener información genética de la persona que aportó su propio material biológico para la obtención de aquél".*

La Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LT- Ley de Transparencia) dedica en pleno su artículo 15 a la protección de datos personales y establece concretamente en su punto segundo que *"si la información solicitada contuviera datos especialmente protegidos a los que se refiere el apartado 2 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso. Si la información incluyese datos especialmente protegidos a los que se refiere el apartado 3 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, o datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al*

infractor, el acceso sólo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquél estuviera amparado por una norma con rango de Ley". No obstante, el punto segundo dice que *"con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano".*

En Andalucía, cuentan a nivel autonómico con la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía, que proclama en el primer párrafo del primer bloque de la exposición de motivos que *"la transparencia es inherente a la democracia y constituye una pieza fundamental para el establecimiento de una sociedad democrática avanzada, que es uno de los objetivos proclamados en el preámbulo de nuestra carta magna".* Además dedica su artículo 26 a la protección de datos personales, en el que recoge que *"de conformidad con lo previsto en la legislación básica de acceso a la información pública, para la resolución de las solicitudes de acceso a la información pública que contengan datos personales de la propia persona solicitante o de terceras personas, se estará a lo dispuesto en la Ley 19/2013, de 9 de diciembre, y en la Ley Orgánica 15/1999, de 13 de diciembre".*

Un sector doctrinal mantiene a este propósito que *"el origen del acceso a la información pública lo podemos situar en Suecia, la primera Ley de Transparencia por así decirlo o el primer documento jurídico que habla de estos temas es de 1766; esta ley se llamó: "Ley para Libertad de Prensa y el Acceso a las Actas Públicas"*[378].

[378] PÉREZ FUENTES, Gisela María (coordinadora): *"Temas selectos de derecho a la información, derecho a la intimidad, transparencia y datos personales".* Editorial Sista, S.A. Tabasco, México, 2010. Pág. 146.

El 15.4 de la Ley de Transparencia establece que *“no será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas”.* Y el 15.5 que *“la normativa de protección de datos personales será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso”.*

Además, la disposición adicional quinta establece una colaboración directa con la Agencia Española de Protección de Datos que *“el Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos adoptarán conjuntamente los criterios de aplicación, en su ámbito de actuación, de las reglas contenidas en el artículo 15 de esta Ley, en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma, de conformidad con lo dispuesto en esta Ley y en la Ley Orgánica 15/1999, de 13 de diciembre”.*

En mi opinión, *“para conseguir esta armonía entre confidencialidad y transparencia de los datos sanitarios de los ciudadanos, habrá que empezar por respetar una serie principios, establecidos en la legislación específica en materia de protección de datos, que deben mantenerse durante toda la vida del dato, desde que se recoge, hasta que deja de ser útil. Los datos deben recogerse y tratarse con la debida seguridad y confidencialidad, respetando unos criterios de calidad, e informando a los titulares en la recogida de los mismos, así como recabando el consentimiento para su tratamiento, que será específico para los datos especialmente protegidos, entre los que se encuentran los datos relativos a la salud de las personas. Estos datos deberán adaptarse además a la legislación sanitaria existente, tanto si su tratamiento se hace exclusivamente en el centro sanitario, o por el profesional*

responsable, como si se comunican o son accedidos por cuenta de terceros"[379]*.*

Una parte de la doctrina mantiene en este sentido que *"el Reglamento (CE) n° 1049/2001 constituye hoy por hoy la principal norma sobre el régimen de acceso a los documentos de las Instituciones europeas. No regula con carácter general la transparencia y el derecho de acceso en el ámbito de la Unión Europea, pero sí constituye una referencia que debe tomarse en consideración"*[380]*.* Y explican que *"el principio general que da pie al Reglamento es el de "apertura". La apertura, señala su segundo considerando, «permite garantizar una mayor participación de los ciudadanos en el proceso de toma de decisiones, así como una mayor legitimidad, eficacia y responsabilidad de la Administración para con los ciudadanos en un sistema democrático. La apertura contribuye a reforzar los principios de democracia Y respeto de los derechos fundamentales contemplados en el artículo 6 del Tratado UE y en la Carta de los Derechos Fundamentales de la Unión Europea». Partiendo de lo anterior, pretende facilitar «el acceso más amplio posible a los documentos» (art. 1 a), al tiempo que determina los límites y excepciones a dicho acceso"*[381]*.*

Además mantienen estos autores que *"Es importante destacar que el acceso se extiende a «todos los documentos que obren en poder de una institución: es decir, los documentos por ella elaborado que estén en su posesión, en todos los ámbitos de actividad de la Unión Europea» (art. 2.3). Alcanza. Pues, a los tres pilares, y no sólo al ámbito propiamente comunitario. De hecho, en el Considerando*

[379] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

[380] RODOTA, Stefano, DUPRAT, Jean-Pierre, PIÑAR MAÑAS, José Luis, NIETO GARRIDO, Eva, HERNÁNDEZ CORCHETE, Juan Antonio: *"Transparencia, acceso a la información y protección de datos"*. Editorial Reus, S.A., Madrid, 2014. Pág. 55.

[381] RODOTA, Stefano, DUPRAT, Jean-Pierre, PIÑAR MAÑAS, José Luis, NIETO GARRIDO, Eva, HERNÁNDEZ CORCHETE, Juan Antonio: *"Transparencia, acceso a la información y protección de datos"*. Editorial Reus, S.A., Madrid, 2014. Pág. 55.

17 del Reglamento se afirma que el reconocimiento del derecho de acceso puede exigir que se modifiquen, entre otras disposiciones, «las normas de confidencialidad de los documentos de Schengen»"[382]*.*

Don Jesús Lizcano Álvarez, Presidente de Transparencia Internacional España y Catedrático de la Universidad Autónoma de Madrid mantiene en su artículo titulado *"Breve Diagnóstico de transparencia"*, que: *"La transparencia de las instituciones públicas españolas es tan necesaria como exigida actualmente por los ciudadanos, que demandan firmemente unas administraciones de cristal, en las que puedan ver todo lo que se hace y se gasta, o lo que se contrata y con quién, y lleguen con ello a conocer mejor e incluso a participar en el devenir cotidiano de esas instituciones que les representan y a las que sostienen económicamente"*[383].

Ha quedado ampliamente expuesto que el tema de la confidencialidad preocupa en todos los sectores del ámbito sanitario, siendo aquí, y fuera de éste, uno de los vértices de la protección de datos personales. Sin confidencialidad no es posible garantizar la protección.

Y concluyendo este apartado en relación al deber de secreto con el que comenzó, cabe referir aquí un artículo del periódico El País, apropósito de un juego de palabras muy oportuno: *"No hay médicos sin confianza, confianza sin confidencias ni confidencias sin secreto. La Academia Española define como confidencialidad <lo que se hace o se dice la confianza o con seguridad recíproca entre dos o más personas>. A su vez confianza tiene dos acepciones: <esperanza firme que se tiene de una persona o cosa> y <con reserva e intimidad>"*[384]. Como puede observarse, se recogen aquí

[382] Ibídem. Pág. 56.

[383] LIZCANO ÁLVAREZ, Jesús: "Breve Diagnóstico de transparencia". El País, viernes, actualidad, 29 de agosto de 2014.

[384] GÜEL, Oriol: Hallados en la calle los datos de 173 trasplantados en un hospital catalán". El País, martes 3 de noviembre de 2009, vida & artes, Barcelona. Pág. 30.

en pocas líneas muchos de los términos analizados en este apartado, y de lo que puede concluirse que intimidad, secreto y confianza van de la mano, siempre que esta última no se traicione.

Y con el título *"Los límites de la transparencia"*, publica este mismo periódico: *"Reclamamos transparencia mientras exigimos intimidad. Los imprecisos límites entre lo público y lo privado, sin embargo, hacen difícil atender esa demandas contrapuestas"*[385].

IV.7. COMUNICACIÓN DE DATOS:

El artículo 3i) de la LOPD define cesión o comunicación de datos como *"cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado".* Y se encuentra regulada en el artículo 11 de su texto, analizado a continuación en relación a otra normativa. Pero hay que recalcar que el punto quinto de este artículo establece que *"aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley".*

E igualmente hay que tener en cuenta que respecto al tema del consentimiento para la comunicación de datos, los apartados tercero y cuarto de este artículo establecen medidas al respecto. El primero de ellos sobre la nulidad del mismo recoge que *"será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar".* Y el segundo sobre la revocación, que *"el consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable".*

[385] FERNÁNDEZ-GALIANO, Luís: *"Los límites de la transparencia"*. El País, viernes 9 de agosto de 2013, opinión. Pág 27.

También se refiere este Real Decreto- Ley sobre sostenibilidad**,** a la protección de datos personales, y dice literalmente que *"el Instituto Nacional de la Seguridad Social podrá tratar los datos obrantes en los ficheros de las entidades gestoras y servicios comunes de la Seguridad Social y de las entidades que colaboran con las mismas que resulten imprescindibles para determinar la cuantía de la aportación de los beneficiarios en la prestación farmacéutica"*. Este tratamiento, previa cesión de datos, que no requiere el consentimiento del interesado, se somete plenamente a la normativa existente en materia de protección de datos. Y con la misma carencia de consentimiento, la Administración Tributaria requerirá al INSS los datos indispensables para determinar el nivel de renta de los usuarios, sin hacer referencia a la cuantía concreta de las rentas, comunicando así el dato relativo a nivel de aportación, para incorporarlo a la tarjeta sanitaria de los pacientes, de acuerdo a la normativa que regula las recetas médicas y órdenes de dispensación. De esta forma, los sistemas de información aportarán datos de las adquisiciones y de la facturación, que serán recogidos de forma manual e informática, para su comunicación a diferentes organismos dependientes del Sistema Nacional de Salud.

Así, cada ejercicio, la administración tributaria comunicará al órgano de la Administración pública encargado del reconocimiento de la condición de asegurado o beneficiario, los datos de sus niveles de renta necesarios para determinar los citados porcentajes de aportación de los servicios de la cartera común que lo requieran, respetándose siempre los principios establecidos en la normativa de protección de datos.

El Real Decreto Legislativo 1/1994, de 20 de junio, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social (LGSS- Ley General de la Seguridad Social), recoge en el artículo 36 sobre el deber de información por entidades financieras, funcionarios públicos, profesionales oficiales y autoridades que *"la*

cesión de aquellos datos de carácter personal que se deba efectuar a la Administración de la Seguridad Social conforme a lo dispuesto en este artículo o, en general, en cumplimiento del deber de colaborar para la efectiva liquidación y recaudación de los recursos de la Seguridad Social y de los conceptos de recaudación conjunta con las cuotas de la Seguridad Social, no requerirá el consentimiento del afectado". Sosteniendo en su segundo párrafo que *"…las autoridades, cualquiera que sea su naturaleza, los titulares de los órganos del Estado, de las Comunidades Autónomas y de las entidades locales; los organismos autónomos, las agencias y las entidades públicas empresariales; las cámaras y corporaciones, colegios y asociaciones profesionales; las mutualidades de previsión social; las demás entidades públicas y quienes, en general, ejerzan o colaboren en el ejercicio de funciones públicas, estarán obligados a suministrar a la Administración de la Seguridad Social cuantos datos, informes y antecedentes precise ésta para el adecuado ejercicio de sus funciones liquidatorias y recaudatorias, mediante disposiciones de carácter general o a través de requerimientos concretos y a prestarle, a ella y a su personal, apoyo, concurso, auxilio y protección para el ejercicio de sus competencias".* Además subraya en su último párrafo que *"la cesión de datos a que se refiere este artículo se instrumentará preferentemente por medios electrónicos".*

La Recomendación sobre protección de datos médicos, establece en el punto séptimo de su apéndice la regulación relativa a la comunicación de datos médicos, y en concreto en su punto primero dice que *"los datos médicos no se comunicarán, salvo en las condiciones establecidas en este capítulo y en el Capítulo 12, que se refiere a la utilización científica de los datos de forma anónima, como ya se ha comentado".*

Y sigue estableciendo el punto segundo del apartado séptimo del apéndice, en relación con la comunicación de datos que *"en particular, salvo que la ley nacional proporcione otras medidas de*

salvaguardia, los datos médicos sólo pueden comunicarse a una persona sujeta a las normas de confidencialidad que pesan sobre un profesional sanitario o a normas de confidencialidad comparables, y que acate las normas de esta recomendación". De modo que si nos basamos en el artículo 3i) de la LOPD, entenderemos como cesión o comunicación de datos *"…toda revelación de datos realizada a una persona distinta del interesado"*. Y en el artículo 11 de esta misma norma se recoge en su punto primero que *"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"*. Vemos que Recomendación y LO se refieren a cosas diferentes, ya que la primera basa la comunicación en la confidencialidad, haciendo referencia genérica al resto de normas de la recomendación, entre las que se encuentra el consentimiento; pero en cambio la segunda, supedita la comunicación directamente al consentimiento, y regula, como se ha visto, en artículo a parte la confidencialidad.

Pero este séptimo punto marca otro requisito para la comunicación de datos médicos en su punto tercero al decir que *"los datos médicos pueden comunicarse si son relevantes y: a. si la comunicación está prevista por la ley y constituye una medida necesaria en una sociedad democrática por: i. razones de salud pública; o ii. La prevención de un peligro real o la represión de un delito específico; o iii. Otro interés público importante; o iv. La protección de los derechos y las libertades de otros; o b. si la comunicación es permitida por la ley con fines de: i. protección del sujeto de los datos o de un pariente en línea genética; ii. Salvaguarda de intereses vitales del afectado o de una tercera persona; o iii. El cumplimiento de obligaciones contractuales específicas; o iv. el establecimiento, ejercicio o defensa de una reclamación legal; o c. si el afectado o su representante legal o la autoridad o persona u órgano previstos por la ley han dado su*

consentimiento para uno o más fines, y en la medida en que la ley nacional no disponga otra cosa; o d. sentado que el afectado o su representante legal o la autoridad, persona u órgano previstos por la ley no se ha opuesto explícitamente a cualquier comunicación no obligatoria, si los datos han sido recogidos en un contexto de prevención, diagnóstico o terapia libremente elegidos, y el propósito de la comunicación, en particular si se trata de la prestación de cuidado al paciente o del funcionamiento de un servicio médico que trabaje en interés del paciente, no es incompatible con el fin del procesamiento para los que los datos fueron recogidos". Así, los no relevantes no podrían comunicarse si esta información no está prevista por ley con todas las especificaciones recogidas anteriormente, o si media consentimiento o no hay oposición explícita a las comunicaciones no obligatorias, dentro de los establecido dentro del último punto de este apartado séptimo de la recomendación que se está comentando.

Como vemos, se ha restringido mucho el abanico para la comunicación de datos médicos, aproximándose a lo establecido en la LOPD, que por su parte, al contrario, recoge excepciones al consentimiento en el artículo 11.2, y establece que *"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 al 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 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 o 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".

Así mientras una norma cierra, otra abre las posibilidades de la comunicación de los datos, pero recordemos que la Recomendación se refiere a los datos médicos en especial, y la LO a los datos personales en general, quizás de ahí la diferencia. Tenemos que citar el artículo 8 de la LOPD, referido a los datos relativos a la salud, aunque ya se hiciera en la introducción, para recordar que "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." De modo que refiere a la normativa específica en sanidad sobre este tema.

Es interesante trasladar aquí lo establecido por el informe jurídico de la AEPD 0382/2012, a propósito de la aprobación de la entrada en vigor del Reglamento (UE) Nº1024/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, relativo a la cooperación administrativa a través del Sistema de Información del Mercado Interior y por el que se deroga la Decisión 2008/49/CE de la Comisión («Reglamento IMI»), ya que la AEPD establece al respecto que *"como ha señalado reiteradamente esta Agencia en sus informes, el hecho de que una norma con rango de Ley habilite el tratamiento o cesión de los datos no resulta por sí solo suficiente*

para considerar dicho tratamiento o cesión, sin más, como amparados por la Ley Orgánica 15/1999, siendo igualmente preciso que los mismos resulten conformes a lo dispuesto en la mencionada Ley y en particular a los principios consagrados por su artículo 4".

Hay otro informe jurídico que tiene interés respecto de la cesión de datos, es el 0300/2014, en el que el Servicio Andaluz de Salud, *"… plantea si resulta conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre, la cesión de datos de los profesionales funcionarios o laborales que desarrollan su actividad en el marco de la consultante a los colegios profesionales que requieren dicha información".* Así *"la cesión planteada deberá resultar conforme a lo dispuesto en artículo 11 de la Ley Orgánica 15/1999, bien contando con el consentimiento del interesado, bien encontrándose en alguno de los supuestos enumerados por su apartado 2".* De este modo se concluye que *"…si la colegiación en los Colegios Oficiales solicitantes resulta obligatoria para el ejercicio de las correspondientes profesiones la cesión de datos sería necesaria para poder acreditar el cumplimiento de los requisitos necesarios para ese ejercicio, encontrándose así amparada por lo dispuesto en la Ley Orgánica 15/1999"*.

A este respecto, una parte de la doctrina ha manifestado que *"como hemos venido apuntando a lo largo de la exposición, a nuestro entender, la LO 15/99, en su artículo 8, viene a establecer que la misma no es aplicable al tratamiento que los médicos efectúan de los datos relativos a la salud de sus pacientes, sino que en esta materia regirá la legislación estatal o autonómica sobre sanidad"*[386].

[386] ATELA BILBAO, Alfonso, BENAC URROZ, Mariano, CODÓN HERRERA, Alfonso, GARAY ISASI, Josu, GONZÁLEZ SALINAS, Pedro, HERNÁNDEZ-MARTÍNEZ CAMPELLO, Carlos, LIZARRAGA BONELLI, Emilio, MARTÍ MONTESINOS, Cristina, PELLEJERO GARCÍA, Carlos,

Aunque desde mi punto de vista esta reflexión no puede obviar que este artículo se encuentra dentro de la Ley de Protección de Datos, aplicable tanto a los datos de salud como a los que no lo son. Y por otro lado, no se puede aislar un precepto y sacarlo de su contexto, porque como se ha venido exponiendo a lo largo del estudio, a los datos médicos de una persona le acompañan otro tipo de datos, como puedan ser los administrativos, a los que no les sería aplicable la normativa sanitaria; entonces no tendría ningún sentido.

Por su parte, el CDM en su artículo 19.7 establece que *"es deber del médico, si el paciente lo solicita, proporcionar a otros colegas los datos necesarios para completar el diagnóstico o el tratamiento, así como facilitar el examen de las pruebas realizadas".*

Y en protección del ya citado artículo 8.3 del RD sobre atención especializada, a propósito del acceso de las comunidades autónomas a los registros, el artículo 10 de esta misma norma, recoge que *"sin perjuicio de lo dispuesto en el artículo 8.3, la información disociada fruto de la explotación estadística del registro estará a disposición de las administraciones públicas sanitarias, los gestores, los profesionales de la sanidad y los ciudadanos en los términos que se acuerden en el CISNS, de conformidad con lo dispuesto en el artículo 53.4 de la Ley 16/2003, de 28 de mayo".*

Aberasturi Gorriño también se manifiesta respecto a la cesión de los datos y lo hace de la siguiente forma, *"la cesión supone que unos datos de carácter personal salen de la inicial esfera de control de su titular, quien los había transmitido directamente a otra persona, para incorporarse a otro ámbito en el que actúa un tercer sujeto ajeno a la relación entre el titular de los datos y el primer responsable del fichero"*[387]*.* Afirmando además que *"la posibilidad de*

PIDEVAL BORRELL, Ignasi, VILLAR ABAD, Gloria, GONZÁLEZ PÉREZ, Jesús: *"Autonomía del paciente, información e historia clínica"*. Editorial Aranzadi, Madrid 2004. Pág. 219.

[387] ABERASTURI GORRIÑO, Unai: *"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 186.

que unos datos que están siendo tratados en un ámbito determinado sean trasladados a otro, en el que una tercera persona pueda acceder a ellos y manipularlos con una finalidad que será distinta, y la posibilidad de que dicha información sea puesta en relación con otros datos que este tercero pueda ya poseer, hace que sea necesaria toda la cautela posible a la hora de llevar a cabo la cesión. Es necesario encontrar el equilibrio entre la necesidad de un flujo ágil de información y el requerimiento de respetar el derecho a la autodeterminación informativa. Mucho más en campos como el sanitario donde los datos que se manipulan exigen, cuando menos de inicio, de una especial protección"[388]*.*

La Ley del aborto establece en este sentido en su artículo 22.1, respecto del acceso y cesión de datos de carácter personal que *"Únicamente será posible el acceso a los datos de la historia clínica asociados a los que identifican a la paciente, sin su consentimiento, en los casos previstos en las disposiciones legales reguladoras de los derechos y obligaciones en materia de documentación clínica. Cuando el acceso fuera solicitado por otro profesional sanitario a fin de prestar la adecuada asistencia sanitaria de la paciente, aquél se limitará a los datos estricta y exclusivamente necesarios para la adecuada asistencia, quedando constancia de la realización del acceso. En los demás supuestos amparados por la ley, el acceso se realizará mediante autorización expresa del órgano competente en la que se motivarán de forma detallada las causas que la justifican, quedando en todo caso limitado a los datos estricta y exclusivamente necesarios".* Su punto 2 puntualiza por su parte que *"el informe de alta, las certificaciones médicas y cualquier otra documentación relacionada con la práctica de la interrupción voluntaria del embarazo que sea necesaria a cualquier efecto, será entregada exclusivamente a la paciente o persona autorizada por ella. Esta documentación respetará el derecho de la paciente a la intimidad y*

[388] Ibídem.

confidencialidad en el tratamiento de los datos de carácter personal recogido en este Capítulo". Y el punto tercero dice que *"No será posible el tratamiento de la información por el centro sanitario para actividades de publicidad o prospección comercial. No podrá recabarse el consentimiento de la paciente para el tratamiento de los datos para estas actividades"*.

Como se ha examinado, la transmisión de datos a personas distintas del paciente una práctica más o menos habitual, que, personas distintas del interesado, accedan a los datos de los pacientes, cuando por alguna circunstancia, estos no pueden, por ejemplo, ir a recoger recetas médicas, unos análisis, u otro tipo de resultados. Pero pocas veces nos paramos a pensar, que en la mayoría de ocasiones, no nos piden la autorización del paciente para estas acciones, probablemente porque casi siempre, el médico conoce nuestra relación con el paciente porque ha acudido alguna vez a verle en nuestra compañía, por lo que deduce y asocia, que si el paciente una vez que ha consentido que otras personas de la familia o allegados conozcan la historia y resultados, en adelante no le importará que se siga conociendo por esas personas, que alguna vez conocieron esos datos.

En este sentido, parece lógico pensar que si el paciente entra acompañado de alguien a una consulta, consiente en que escuche o acceda a toda la información que en ese momento se le va a dar al paciente, pero, ¿Por qué sistema se puede asociar, que por enfermedad u otra circunstancia de ausencia del paciente, se pueda dar en adelante información del paciente a ese acompañante? ¿debería consentir el paciente en cada ocasión para esa cesión de información, o una vez consentida la cesión se entiende que a partir de entonces la persona acompañante puede conocer cualquier tipo de información del paciente?

La realidad, es que ese consentimiento no queda plasmado en ningún sitio, y podría plantear problemas respeto a la protección de

los datos personales. Y este tema puede plantear graves problemas, porque yo puedo consentir en que, por ejemplo, mi madre o pareja, conozca que tengo determinada afección, pero eso no significa, que quizás yo no quiera que conozca determinadas otras situaciones médicas, por diversas circunstancias.

Esta cesión de los datos del paciente, que en ocasiones se hace en mano, habitualmente en soporte papel, y otras de viva voz, nos puede llevar a pensar, que sobre todo en los traslados de datos de tú a tú, pueden existir grandes riesgos sobre la confidencialidad de la información que reina en la relación médico-paciente.

Cuando los datos se comunican de palabra, puede ser, como se acaba de mencionar, puede hacerse, en persona, a un individuo, presuntamente autorizado por el paciente, por asociación de otras situaciones que se han producido anteriormente, por teléfono a alguien que nosotros creemos que es el paciente, o esa persona autorizada por él, o incluso, puede llegar a hacerse , por ejemplo en salas de espera, donde además del paciente y la persona supuestamente autorizada por este, se encuentran al alcance de escuchar tal información otras personas. El teléfono sin duda, plantea grandes problemas en este sentido, ya que no podemos asegurar la identidad de la persona con la que hablamos, por mucho que a través de la voz podamos identificar el sexo de la persona con la que hablamos, y el timbre de voz, por mucho que se le parezca. En cambio, el tema de preservar la información que se da en una sala de espera en la que hay otras personas, parece más sencillo, desde el punto de vista del espacio y el sonido, ya que podemos buscar, dentro de las posibilidades, un lugar más apartado, y bajar el tono de voz, pero aún así, sigue siendo arriesga proporcionar información por este medio.

Asegurar la confidencialidad de los datos dados verbalmente es claramente complicado, porque a partir de esa comunicación, existe un riesgo grande de difusión descontrolada de la información del

paciente a otras personas sin vuelta atrás, una vez trasladada la información, esas otras personas ya la conocen y no la pueden borrar de su conocimiento, no es como una información plasmada en soporte papel que puede destruirse, aquí la única opción que queda, es que quienes la hayan conocido, guarden la debida confidencialidad**.**

Cabe referir aquí rocambolesco caso es el publicado por el periódico El País en el artículo titulado *"Jordi, el detective y falso doctor"*, en el que un detective encubierto como médico que sustraía datos de los pacientes con gran astucia, y que llegó a montar un gran negocio. Asegura este diario: *"La trama logró decenas de historiales clínicos en hospitales y centros de salud de toda España.La trama penetró también en hospitales de Girona, Hospitalet de Llobregat, Arbúcies y Vitoria. Los detectives vendían las historias clínicas a empresas y aseguradoras interesadas en investigar a sus trabajadores y clientes"*[389].

El tema de la cesión de los datos de salud, constituye uno de los pilares básicos de este estudio, así como de la protección de datos y de la propia relación del médico con el paciente, ya que, que ese hábitat se mantenga intacto es fundamental para el buen desarrollo del proceso médico. La falta de confianza, lleva en la mayoría de las ocasiones a un cambio radical, en casi todos los ámbitos de la vida, cuanto más en el médico, donde lo que está en juego es la salud de las personas, aunque hoy en día no parezca importar como antes.

[389] IRUJO, José María: *"Jordi, el detective y falso doctor"*. El País, domingo 15 de julio de 2012, Madrid. España. Pág 13.

IV.7.a. Comunicaciones de datos entre administraciones:

Establece en este sentido la LOPD en su artículo 21.1 que *"los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos".* Y puntualiza el segundo apartado de este artículo que *"podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra".* No obstante lo dicho el apartado cuarto establece a este respecto una limitación, *"en los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley".*

E igualmente el RLOPD, en su artículo 10.4 c), recoge al respecto que *"la cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos: Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando: c) Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos. Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra. La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias".*

El tema del copago sanitario instaurado en nuestro país, supone sin duda una cesión de datos entre las administraciones, en cuyo caso *"el cruce de los datos sanitarios con los económicos debería hacerse con un encapsulamiento integral, de forma automática y oculta para el profesional médico o farmacéutico. Esto*

es, sin que estos colectivos puedan conocer los datos específicos de la renta de los pacientes, para lo que debería bastar con un simple procesamiento informático. Si no fuera así, se podrían producir dos problemas. El primero que se contaminase el proceso médico al prescribir o dispensarse el tratamiento influenciado de la riqueza o pobreza del paciente. El segundo tiene que ver con un atentado contra la intimidad de las personas"[390]*.* De este modo *"el éxito del copago basado en la renta de los ciudadanos, podría encontrarse en que esa asociación de los datos sanitarios con los de renta, necesaria para el funcionamiento de dicho sistema, se haga siguiendo un procedimiento que los mantenga en la más estricta confidencialidad"*[391]*.* Cosa que no ocurre absolutamente, ya que el farmacéutico conoce al obrar el producto entre los niveles de renta que se encuentra el paciente. Entonces *"…habría que pararse a pensar detenidamente los criterios y conceptos del copago, así como los grupos de personas o niveles sanitarios a los que afectaría, teniendo en cuenta que el personal sanitario que tengamos delante, además de nuestras afecciones, que muchas veces resultan de por sí intimidatorias, va a conocer los datos de nuestra renta, lo cual puede resultar excesivo para intentar regular el gasto sanitario"*[392]*.*

Este sistema de contribución a la sanidad no fue apoyado por todas las comunidades, según asegura el periódico Expansión: *"El Consejo Interterritorial de Sanidad acordó ayer, con el rechazo de Andalucía Y País Vasco, la implantación de un copago de*

[390] VIDAL RASO, Marta, *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

[391] Ibídem.

[392] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

medicamentos según el nivel de renta que incluye a pensionistas y enfermos crónicos"[393].

Aún así, somos los que menos pagamos del continente europeo, según publica el diario Expansión Bajo el título *"España, a la cola de Europa en el copago"*, que asegura que: *"Aunque el gobierno ha decidido incrementar el copago de los medicamentos, los españoles seguirán contribuyendo a los fármacos que consumen en una proporción inferior a la de sus vecinos europeos"*[394].

"Otro problema que se plantea, fruto de la fragmentación normativa de nuestro país, tiene que ver con la comunicación de datos entre las Administraciones, prevista en el artículo 21 de la LOPD. La sentencia 292/2000 del Tribunal Constitucional declaró inconstitucional la cesión de datos entre Administraciones si no existía una norma habilitante con suficiente rango normativo. La situación actual con vientos a favor de la transparencia –presumiblemente con una nueva ley a finales de año- exige una coordinación de las Administraciones Públicas en materia de información, algo que ya se preveía en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y disposiciones legales de aplicación, que tiene como objeto "posibilitar la creación de una red de comunicaciones que interconecte los sistemas de información de las Administraciones públicas españolas y permita el intercambio de información y servicios entre las mismas". Esto juega sin duda, a favor de ese intercambio de datos entre administraciones, que en cualquier caso debe hacerse con todas las garantías que exige la ley"[395].

[393] SERRAILLER, Mercedes: "Todos los pensionistas pagarán entre 8 y 18 euros al mes por los fármacos". Expansión, jueves 19 de abril de 2012. Economía/política. Madrid. Pag 22.

[394] SAINZ, S: "España, a la cola de Europa en el copago". Expansión, jueves 19 de abril de 2012, economía/política, Madrid. Pág 23.

[395] VIDAL RASO, Marta: *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

Según establece el Real Decreto sobre receta médica, en el caso de las recetas que se emitan de forma electrónica, se requerirá el intercambio de datos entre la Administración central y las locales en las que se lleve a cabo la dispensación; para ello el Ministerio de Sanidad deberá facilitar tanto el código de identificación de cada usuario dentro del Sistema Nacional de Salud como el Nomenclator oficial de los productos farmacéuticos. Igualmente en estas recetas las Administraciones facilitarán el grupo al que pertenezca el paciente, para el cobro de los medicamentos a los pacientes, de acuerdo a la Real Decreto-Ley sobre sostenibilidad, que modifica las de calidad de este sistema, la de garantía y uso racional de los medicamentos, así como los Reales Decretos sobre receta médica, sobre los márgenes de los medicamentos dispensados, y sobre células y tejidos de uso humano, además de otras normas que afectan directamente a los profesionales sanitarios.

Serán las Administraciones sanitarias públicas las encargadas de gestionar esos sistemas electrónicos, garantizando la custodia, tanto de los datos de los prescriptores como de sus códigos de acceso a las bases de datos a las que tengan que acceder; para el acceso a este sistema el farmacéutico utilizará un equipo, que registrará siempre los datos de su acceso, ubicado en la oficina de farmacia que esté integrado en el sistema de receta electrónica debidamente autentificado, que garantice el cifrado de las comunicaciones, debiendo acreditar su identidad y firma electrónica, debiendo además solicitar la tarjeta sanitaria al paciente para introducir su código de identificación personal, siendo devuelta de forma inmediata al mismo.

De hecho, en el sistema de receta médica electrónica, se deberán aplicar las medidas de seguridad de nivel alto, no pudiendo tratarse los datos desde terminales distintos a los gestionados por la Administración Sanitaria, siendo accesible dicha información exclusivamente desde la oficina de farmacia para su dispensación y

almacenados en los equipos establecidos en ellas a efectos de facturación. Todas estas medidas de nivel alto se encuentran referidas en el apartado correspondiente de este estudio.

Así el artículo 7.1 establece en su primer párrafo que *"los tratamientos prescritos al paciente en receta médica electrónica podrán ser dispensados en cualquier oficina de farmacia del territorio nacional o en botiquines dependientes de las mismas, así como en los servicios de farmacia de los centros de salud y de las estructuras de atención primaria, según lo previsto en el artículo 2.6 de la Ley sobre el uso de los medicamentos. Para garantizar este derecho a los pacientes, el Ministerio de Sanidad, Política Social e Igualdad, como nodo nacional de intercambio electrónico de información sanitaria, actuará entre la Administración sanitaria de procedencia de la receta electrónica y la Administración sanitaria competente en la localidad donde se efectúe la dispensación correspondiente".*

Estableciendo en el segundo que *"a estos efectos, el Ministerio de Sanidad, Política Social e Igualdad facilitará el acceso al resto de Administraciones sanitarias, incluidas las mutualidades de funcionarios, a sus sistemas electrónicos provisores del código identificador unívoco del usuario del Sistema Nacional de Salud y del Nomenclátor oficial de productos farmacéuticos de dicho Sistema en el que figuran los códigos de identificación inequívoca de los medicamentos y productos sanitarios, sus formas farmacéuticas, vías y unidades de dosificación, así como el contenido de los envases comerciales y sus condiciones de financiación en el Sistema Nacional de Salud y además su posible dispensación en unidades concretas. Asimismo, se facilitará el acceso a otras bases de datos del Ministerio de Sanidad, Política Social e Igualdad que ofrecen información sobre los medicamentos y productos sanitarios autorizados en España".*

Del mismo modo el punto tercero recoge que *"el sistema de receta médica electrónica de cada una de las Administraciones*

sanitarias del Sistema Nacional de Salud posibilitará la identificación del régimen de pertenencia del paciente, a efectos de cobro de la aportación que en cada caso corresponda, y la realización de la facturación de las oficinas de farmacia a la correspondiente Administración sanitaria por medios telemáticos, con las necesarias medidas de seguridad y control que garanticen su correspondencia con las dispensaciones realizadas. Por las autoridades sanitarias competentes se determinarán los datos necesarios a los que podrán acceder los farmacéuticos para la facturación de la receta médica electrónica y el desarrollo de programas de calidad de la prestación farmacéutica. En cualquier caso, se facilitará el acceso de los farmacéuticos que posibilite el desarrollo de las funciones contempladas en el artículo 84.1 de la Ley sobre el uso de los medicamentos, en las condiciones que se establezcan por las autoridades sanitarias competentes".

Y por su parte el punto cuarto dice que *"las Administraciones sanitarias públicas son las responsables de la gestión de los sistemas de receta electrónica, por lo que garantizarán la custodia de las bases de datos de prescripción y dispensación y establecerán los criterios de autorización y control de acceso a dichas bases de datos. Todo ello sin perjuicio de los criterios generales de acceso que se establecen en este real decreto".*

Unai Aberasturi Gorriño manifiesta al respecto que *"se justifica, en definitiva, la cesión de datos entre administraciones, que a pesar de contar con competencias diferentes actúan sobre la misma materia. De esta manera, y siendo coherentes con la relevancia que se ha dado al principio de finalidad, en el ámbito estrictamente sanitario es admisible que la finalidad de salvaguardar la salud de las personas justifique las comunicaciones entre las administraciones que actúan en el sector sanitario"*[396].

[396] ABERASTURI GORRIÑO: Unai:*"La protección de datos en la salud"*. Editorial Aranzadi, S.A., Navarra, 2013. Pág. 221.

IV.7.b. Comunicaciones internacionales de datos :

El Convenio 108, recogía ya en su artículo 12 la regulación para los flujos transfronterizos de datos, estableciendo en su punto primero que *"las disposiciones que siguen se aplicaran a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento".* Y en el punto segundo que *"una parte no podrá, con el único fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra parte".* Y en referencia a este último punto, el tercero dispone que *"sin embargo, cualquier parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo 2: a) en la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra parte establezca una protección equivalente; b) cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un estado no contratante por intermedio del territorio de otra parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la parte a que se refiere el comienzo del presente párrafo"*.

La cesión de datos entre países se encuentra regulada en la LOPD, que en su artículo 30 recoge la norma general al respecto, así el punto primero del referido artículo establece que *"no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países*

que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas". El punto segundo se encarga de puntualizar que *"el carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".*

Pero como toda norma general tiene excepciones, que vienen recogidas en el en el artículo siguiente. El artículo 34 c) establece respecto al tema que nos ocupa, que no será aplicable lo dispuesto en el anterior artículo mencionad *"…cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios"*.

Regulado en el título VI bajo la rúbrica *"transferencias internacionales de datos"*, el RLOPD, contempla este movimiento de información en sus artículos 65 a 70, de entre los que cabe destacar el primero de ellos que establece que *"la transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento".* A este respecto establece el 66.1 que *"para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999,*

de 13 de diciembre, y en el presente Reglamento será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del presente reglamento". Hay que decir que el artículo 70.1 recoge en este aspecto que *"cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos".*

No obstante lo dicho, marca el punto segundo que *"la autorización no será necesaria: a) Cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección conforme a lo previsto en el capítulo II de este título. b) Cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a) a j) del artículo 34 de la Ley Orgánica 15/1999, de 13 de diciembre".* Atendiendo al punto b), hay que recordar que el recientemente comentado artículo 34 c) de la LOPD se encuentra entre los mencionados, de modo que en de materia sanitaria no será necesaria la autorización del director de la AEPD.

En este punto debo avanzar algunos artículos, para comentar otra excepción importante a la autorización del director de la AEPD que viene regulada en el 67.1, según el cual *"no será precisa autorización del Director de la Agencia Española de Protección de Datos a una transferencia internacional de datos cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de protección a juicio del Director de la Agencia Española de Protección de Datos. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se*

tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países. Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se acordase que un determinado país proporciona un nivel adecuado de protección de datos serán publicadas en el «Boletín Oficial del Estado»".

Y el artículo 68 por su parte establece que *"no será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección".*

Pero además el punto tercero del artículo 66, establece en relación a la inscripción y modificación de ficheros comentada, tanto en el apartado referido al documento de seguridad, como en el de la creación de las bases de datos, que como modificación de los datos del fichero que supone, debe ser notificada a la AEPD. Así dice literalmente este artículo que *"en todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento".*

La Recomendación sobre protección de datos médicos, habla de forma bastante extensa, de los flujos transfronterizos de datos médicos en el punto 11 de su apéndice, estableciendo en su punto primero que *"los principios de esta recomendación son aplicables al flujo transfronterizo de datos médicos".* Y da libertad a la circulación

de este tipo de datos, ya que es su punto segundo establece que *"no debe someterse a condiciones especiales de protección de la intimidad el flujo transfronterizo de datos médicos a un Estado que ha ratificado la Convención para la Protección de los Individuos en relación al Tratamiento Automatizado de Datos Personales, y que dispone de legislación que proporciona al menos una protección equivalente de los datos"*.

Es decir, que si se ha ratificado este convenio y se dispone de legislación aplicable equiparable, no hay razón para vetar la circulación internacional de estos datos. Pero además el punto tercero establece en cierta contradicción con lo ahora dicho que *"donde la protección de los datos médicos pueda considerarse en línea con el principio de protección equivalente sentado por la convención, no se debe aplicar restricción alguna al flujo transfronterizo de datos médicos a un Estado que no haya ratificado la Convención, pero que disponga de normas legales que aseguren una protección acorde con los principios de tal Convención y de esta recomendación".*

Así pues, con que haya legislación interna con principios similares a los establecidos por la Recomendación, se puede realizar esa transmisión de datos, no siendo necesario haber ratificado el texto que nos ocupa. Es más, el punto cuarto de esta norma, permite la transmisión de datos médicos a nivel internacional, incluso si el estado al que se transmiten los datos no asegura un nivel de protección equiparable al de la convención, en determinadas circunstancias *"salvo que la ley nacional disponga otra cosa, el flujo transfronterizo de datos médicos a un Estado que no asegura la protección de acuerdo con la Convención y con esta recomendación, el flujo no debe tener lugar a menos que: a. se hayan tomado las medidas necesarias, incluidas aquellas de naturaleza contractual, para que se respeten los principios de la Convención y de esta*

recomendación, y el afectado haya tenido la posibilidad de oponerse a la transferencia; o b. el afectado haya dado su consentimiento".

Y todavía el punto quinto del apéndice de la Recomendación abre la puerta en situaciones de emergencia o consentimiento para tomar esas medidas protectoras que viene a concretar *"salvo en caso de emergencia o de una transferencia a la que el titular de los datos haya dado su consentimiento informado, se deben tomar medidas apropiadas para asegurar la protección de los datos médicos transferidos de un país a otro, y en particular: a. la persona responsable de la transferencia debe indicar al destinatario los fines específicos y legítimos para los que se recogieron los datos, así como las personas u organismos a los que éstos pueden comunicarse; b. salvo que la legislación nacional disponga otra cosa, el destinatario debe comprometerse ante la persona responsable de la transferencia a respetar los fines específicos y legítimos que éste último ha aceptado, y a no comunicar los datos a personas u organismos distintos de los indicados por la persona responsable de la transferencia".*

La Ley General de Sanidad establece en este sentido, en su artículo 39 que *"mediante las relaciones y acuerdos sanitarios internacionales, España colaborará con otros países y Organismos internacionales: En el control epidemiológico; en la lucha contra las enfermedades transmisibles; en la conservación de un medio ambiente saludable; en la elaboración, perfeccionamiento y puesta en práctica de normativas internacionales; en la investigación biomédica y en todas aquellas acciones que se acuerden por estimarse beneficiosas para las partes en el campo de la salud. Prestará especial atención a la cooperación con las naciones con las que tiene mayores lazos por razones históricas, culturales, geográficas y de relaciones en otras áreas, así como a las acciones de cooperación sanitaria que tengan como finalidad el desarrollo de los pueblos. En el ejercicio de estas funciones, las autoridades*

sanitarias actuarán en colaboración con el Ministerio de Asuntos Exteriores".

La Directiva sobre protección en el tratamiento de datos regula en el artículo 25 los principios relativos a la transferencia de datos personales a países terceros y en el artículo 26 las excepciones. El artículo 25.1 establece en este sentido que *"los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado."* Y respecto del nivel de protección adecuado, recoge el 25.2 lo siguiente, *"el carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".*

Y respecto a las excepciones marca el 26.1 que *"no obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando: a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el*

responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta". Y el 26.2 establece una excepción, recogiendo que *"sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas".*

Hay que estar muy pendiente en esta materia sobre los países que tienen un nivel de protección suficiente para hacer la transferencia. En este sentido conviene citar el artículo que publica El País bajo el título *"La justicia europea falla que EEUU no garantiza la protección de datos"*, el periódico El País, publica en sus páginas de la sección internacional, que una sentencia del Tribunal de Justicia de la UE según la cual EEUU no cuenta con un suficiente nivel de protección de los datos personales y así dice: *"La decisión*

del interrumpir el almacenamiento de información en EEUU corresponde ahora a las agencias nacionales de protección de datos. Su criterio prevalecerá sobre el de Bruselas, que desde hace 15 años consideraba el territorio estadounidense como destino seguro para estos"[397].

El Real Decreto sobre atención especializada, recoge en su artículo 11 que *"El intercambio de datos con las instituciones de la Unión Europea se realizará de acuerdo con lo dispuesto en el Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo".*

IV.8. ACCESO A LOS DATOS POR CUENTA DE TERCEROS:

Hay que aclarar antes de comenzar este capítulo que la comunicación o cesión de datos y el acceso a los datos por cuenta de terceros, son cuestiones distintas.

En la primera de ellas, según se acaba de ver, los datos se entregan a otro distinto del responsable del fichero, que los tratará por su cuenta y riesgo y en su propio beneficio; esta acción requiere el consentimiento del interesado, ya que los datos pasan de una entidad a otra completamente distinta, con distinta finalidad, y el titular de los datos tiene que saber en todo momento donde están los mismos.

La segunda acción, el acceso a los datos por cuenta de terceros, conlleva la prestación de un servicio o encargo de tratamiento de los datos que justifica el traslado de los mismos a otra entidad diferente del responsable del fichero; esta acción debe

[397] DOMÍNGUEZ, Belén, ABAD LIÑÁN, José Manuel: *"La justicia europea falla que EEUU no garantiza la protección de datos".* El País, miércoles 7 de octubre de 2015, internacional, Bruselas/Madrid. Pág 3.

quedar plasmada en un contrato de prestación de servicios del tercero tratador que tratará los datos por orden del responsable del fichero. Así el 12.1 LOPD establece que *"no se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento".*

El informe jurídico de la AEPD 0162/2010 señala que *"…si los obligados a la custodia y conservación de las historias clínicas no se encontrasen en condiciones de hacerla efectiva, la solución podría ser contratar la prestación de un servicio para tales fines suscribiendo el contrato del artículo 12 de la LOPD que regula el tratamiento de datos por cuenta de terceros, con el Colegio Oficial de Médicos. El artículo 12 número 1 dispone que "No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento." En tal caso, no existiría cesión de datos y se cumplirían las previsiones de la Ley 41/2002 y de la LOPD por parte de los responsables directos de la custodia de las historias clínicas".* Aquí se ve claramente la diferencia entre cesión y prestación de servicios.

Hay otro informe jurídico de la AEPD que es necesario citar aquí, el 0360/2013, que resuelve en relación a si los centros privados que conciertan con una mutua de accidentes asume la condición de responsable o encargado del fichero, se resuelve que *" … si bien el contrato de prestación de servicios que ha de suscribir la Mutua de Accidentes de Trabajo y Enfermedades Profesionales con los centros sanitarios privados para la prestación de la asistencia sanitaria a los trabajadores es el referido en el artículo 8.1 en relación con el artículo 275.1 del Real Decreto Legislativo 3/2011, y que su disposición adicional vigésimo sexta atribuye al contratista que accede a datos de carácter personal de cuyo tratamiento es responsable la entidad contratante, la condición de encargado del*

tratamiento, es preciso tener en cuenta que, tratándose de datos de salud contenidos en historias clínicas por imperativo de la Ley 41/2002, de 14 de noviembre, el contratista no podrá tener la condición de encargado del tratamiento".

Respecto del acceso a los datos personales por terceras personas, expresa Lucas Murillo de la Cueva que *"…lo significativo no es sólo el que haya quien disponga de información acerca de nuestras personas y la ofrezca a terceros sino también y sobre todo que esto ocurra sin que dispongamos de medios para conocer esa circunstancia y, por tanto, para defendernos de los riesgos que puede depararnos…"*[398]*.* Y en este sentido sigue reflexionando que *"…más que datos personales, se almacenan y distribuyen informáticamente valoraciones. Es decir, se recoge y facilita a terceros un determinado perfil de un individuo. Si acaso puede ser suficiente recordar que una de las primeras leyes de protección de datos, la Datalag sueca, ya se ocupaba del procesamiento de juicios de valor sobre las personas…"*[399]*.*

Nuria Terribas manifiesta en este sentido que del acceso por terceros a la información tiene que ser siempre autorizada por el propio paciente cuando manifiesta que *"…también plantea dificultades en determinados contextos en que el paciente no se encuentra en condiciones de autorizar a un tercero, y en cambio sus familiares o cuidadores necesariamente deben acceder a esos datos para una correcta atención"*[400]. Sería este un acceso a los datos por terceros pero en el plano familiar, no institucional, y obviamente no requeriría de la existencia de ningún contrato, sino que se trasladaría más al plano de la confidencialidad, difícil de gestionar en estas situaciones.

[398] LUCAS MURILLO DE LA CUEVA, Pablo: "*Informática y Protección de Datos Personales"*, Centro de Estudios Constitucionales, Madrid 1993. Pág. 18.

[399] Ibídem.

[400] TERRIBAS SALA, Núria: "*Los avances del derecho ante los avances de la medicina. Confidencialidad de los datos sanitarios: de la norma a la práctica médica*". In Salomé Adroher Biosca- Thomson Aranzadi, 2008. Pags 796-802.

Cabe hacer aquí una referencia jurisprudencial cuya demanda se funda en que *"…la "ENTIDAD A", que ostenta la condición de entidad colaboradora de la Seguridad Social, dispone de una base de datos informática común a su acceso para los facultativos de la Seguridad Social y los servicios médicos propios de la empresa, denominada de "....."", en la que constan los resultados de las revisiones periódicas realizadas a los trabajadores de "ENTIDAD A" por los servicios médicos de la empresa y empresas médicas subcontratadas, así como los diagnósticos de las enfermedades que dieron lugar a una situación de baja laboral de los trabajadores y las fechas de baja y alta, todo ello sin consentimiento de los afectados y sin que el fichero médico estuviese dado de alta como tal en la Agencia de Protección de Datos".* Y según se expresa en los antecedentes, *"de permitirle la empresa el acceso, resultaría infringido el tenor de los artículos 8, 9, 10 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal"* [401]. El fallo es a favor del amparo solicitado, reconociéndose la tutela judicial efectiva del 24.1 de la CE el cual establece que *"todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión".*

IV.8.a. El encargado del tratamiento: contrato de encargo de prestación de servicios :

Este concepto ha sido ya muy comentado en la introducción de este estudio, por la importancia que tiene dentro de la normativa de protección de datos. Y recordemos que la definición del artículo 3g) donde se encuentra, fue ya mencionada en la introducción de este estudio, no obstante lo vemos ahora de nuevo para recordar que el

[401] Sentencia 153/2004, de 20 de septiembre de 2004 del Tribunal Constitucional. Recurso de Amparo núm. 6411/2002. Vulneración del derecho a la tutela judicial efectiva: reparación insuficiente del derecho a la intimidad del trabajador cuyos datos médicos obran en archivo informático de su empresa, en ejecución de la STC 202/1999.

encargado del tratamiento es la *"… persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".* Cabe también mencionar aquí el concepto de comunicación o cesión de datos que hace la LOPD en su artículo 3i) para ver claramente la diferencia entre ambos conceptos, definiendo como cesión o comunicación de datos *"…toda revelación de datos realizada a una persona distinta del interesado".*

Igualmente se hace necesario en este momento, recordar el artículo 12 de la LOPD sobre el acceso a los datos por cuenta de terceros para entender bien los apartados precedentes y al hilo de la anterior aclaración. El 12.2 de la LOPD recoge que *"la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar".* Medidas ya comentadas en el apartado de la seguridad de los datos.

El 12.3 por su parte establece que *"una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".*

Pero además, aclara el 12.4 que, *"en el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato,*

será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente".

Si se diese la circunstancia de que el encargo del tratamiento es llevado a cabo en los locales del propio responsable del fichero, hay que atender a lo establecido por el artículo 82.1 del RLOP. Este precepto establece que: *"Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento"*. Y como establece el segundo párrafo de este artículo: *"Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento"*.

También el 82.2 del RLOPD recoge la otra situación posible sobre la forma de prestar el servicio: *"Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento*".

De manera, que se acceda en los lugares que se haga, esto debería constar en el contrato de prestación de servicios firmado

entre las partes interesadas con tal cometido, para que se tomen las medidas oportunas al respecto.

Dentro de lo variado que puede ser el acceso a los datos de los pacientes, cabe citar también que, según publica el diario El País: *"La Agencia Española de Protección de Datos ha "exigido", según la expresión que usa en su nota informativa, a la Comunidad de Madrid que limite el acceso de los representantes religiosos en los hospitales a los datos de los pacientes. Esa exigencia se basa en un informe, solicitado por el Ministerio de Justicia, que la Agencia ha remitido ya al Gobierno regional para que lo traslade a todos los hospitales. El informe se refiere a la adecuación de la Ley de Protección de Datos del convenio, renovado el pasado enero, entre la Consejería de Sanidad y la Providencia Eclesiástica de Madrid, concluye que el acceso de los sacerdotes a los datos de los pacientes debe limitarse a aquellos que "efectivamente requieran la asistencia religiosa". El texto se refiere tanto a los religiosos de los comités de bioética- aconsejan sobre cuestiones como órdenes de no reanimar, qué hacer con bebés que tienen minusvalías graves o cuando desconectar aparatos de soporte vital-, como a los equipos de cuidados paliativos (que administran tratamientos para atajar el dolor en pacientes terminales) de los hospitales"*[402].

Respecto de la obligación de la existencia de un contrato de prestación de servicios, el Real Decreto-Ley sobre Células y Tejidos, recoge en su artículo 24.8, a propósito de regula en este artículo las relaciones entre los establecimientos de tejidos y terceros que *"cuando la contratación del tercero implique el acceso por parte de éste a datos de carácter personal, el contrato deberá cumplir lo establecido en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre".*

[402] SEVILLANO.G. Elena: "Los curas, lejos de la información ". El País, miércoles 16 de julio de 2008, Madrid. Pág. 5.

A este respecto, Samprón López se manifiesta en este sentido *"la custodia de la historia clínica por empresas privadas que no sean Centros Sanitarios o Consultas Privadas, deberán realizarse con las mismas garantías de protección que las exigidas para los Centros Sanitarios y Consultas Privadas"*[403]*.* Y sobre lo establecido en el ya citado artículo 12 de la LOPD, este mismo autor comenta que *"…deberá contratarse el servicio con una empresa especializada, debiendo quedar acreditado que dispone de las instalaciones y medios materiales y personales suficientes para asegurar la conservación y custodia en los términos exigidos por la normativa específica".*[404]

Por otro la es una realidad que el soporte informático está sustituyendo al soporte papel, aunque no por completo, pero lo cierto es que la problemática del espacio está latente en una sociedad que genera millones de datos al día, como ya se comentó en la introducción del capítulo sobre la regulación (artículo), y así refleja que *"…se trataría de encomendar el almacenamiento de historia clínica por cuestiones de espacio y gestión administrativa"*[405]*.* Pero según el autor esto podría tener ciertas trabas ya que *"…esto puede suponer un problema cuando se trata de historia clínica pertenecientes al INSALUD, ya que el RD 63/1995, de 20 de enero, sobre ordenación de prestaciones sanitarias del Sistema Nacional de Salud, dispone de manera clara, en su anexo I, apartado 5.6º la obligación de conservar la historia clínica en el Centro Sanitario. No ocurriría lo mismo cuando se trate de Centros Sanitarios o Consultas Privadas que no forman parte del Sistema Nacional de Salud, de acuerdo con el título III de la Ley General de Sanidad"*[406]*.* Incluso hace este autor referencia al procedimiento manifestando que

[403] SAMPRÓN LÓPEZ, David: "*Los derechos del paciente a través de la información de la historia clínica*". Edisofer, Madrid, 2002. Pág. 91.

[404] Ibídem.

[405] Ibídem.

[406] SAMPRÓN LÓPEZ, David. "*Los derechos del paciente a través de la información de la historia clínica*". Edisofer, Madrid, 2002. Pág. 91.

"…deberá hacerlo a través de procedimientos administrativos regulados en el Texto Refundido de la Ley de Contratos de las Administraciones Públicas, articulando a tal fin un Pliego de Cláusulas Administrativas Particulares y otro de Bases Técnicas en donde se establezcan todas las condiciones que han de regir el contrato, incluyendo los medios materiales, técnicos y personales, exigibles a la empresa de Servicio, así como los controles que puede hacer la administración"[407].

No obstante matiza Samprón López que *"…en cualquier caso, la custodia se debe limitar únicamente a conservar el soporte documental, y a impedir el acceso a las historia clínica a otras personas distintas a las autorizadas expresamente por el Centro Sanitario"*[408]. Y sugiere que *"…para ello sería conveniente guardar por bloques en archivos sellados un nº de historias, para ser facilitado al centro sanitario cuando lo solicite que devolverá el bloque para su nueva custodia a la empresa de servicios que procederá de nuevo al sellado"* [409].

Respecto de la falta de espacio y digitalización de los documentos, se manifiesta otro sector doctrinal *"dado que un problema importante de gestión documental clínico es el almacenamiento permanente, se describen a continuación las fases de almacenamiento de la HC para pasar a papel a digitalización y custodiar permanentemente la HC. Las fases del proceso son: preparación de la historia y archivación electrónica, preparación de documentos depurando aquellos que de destruirán sin pasar a la fase siguiente, captura del documento en el sistema informático, memorización del mismo, visualización e impresión"*[410].

[407] Ibídem.

[408] Ibídem.

[409] Ibídem.

[410] CURRIEL HERRERO, J y ESTÉVEZ LUCAS, J: "*Manual para la gestión sanitaria y de la historia clínica hospitalaria*". Editores Médicos, Madrid, 2000. Pág. 92.

"El tema de la gran acumulación de soporte papel que hay en los centros sanitarios, de décadas de años atrás, nos obliga a afrontar la problemática del expurgo documental, cual debe ser destruido, cual debe conservarse disociándose de los datos nominativos, cual debería emplearse para fines históricos, estadísticos o científicos, cual podría informatizarse y destruir el papel. Para este propósito han surgido en relación con el desarrollo de las nuevas tecnologías, terceras empresas que prestan servicios para todo ello; unas informatizan los datos, destruyendo posteriormente el soporte papel, lo cual está amparado por el RLOPD, según se ha comentado; otras en cambio se dedican a destruirlos. En estos casos el responsable del fichero debe mediante contrato - según marca el art. 12 de la LOPD- encargar a un tercero la prestación de un servicio, recogiendo expresamente las funciones encomendadas, así como la obligación del tercero de cumplir la normativa de protección de datos"[411].

Yo creo que habría que dejar un registro de entrada y salida de soportes. Posibilidad de escanearlas y tenerlas en dos soportes, lo que daría fluidez en el envío y riesgo de ponerlas en la red.

IV.8.b. Relaciones entre el responsable y el encargado del tratamiento:

Aunque ya se ha dicho que la relación entre ambos debe estar regulada en contrato, y las limitaciones que este debe contener, el artículo 20 del RLOPD, dedicado expresamente a las relaciones entre responsable y encargado, establece en su punto primero que *"el acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en*

[411] VIDAL RASO, Marta, *"Los datos sobre la salud de los ciudadanos".* Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012. Págs 29 a 36.

el presente capítulo. El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido. No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado". Ya vemos que este precepto es una mezcla de dos apartados analizados anteriormente, ya que se dedica a delimitar también los conceptos de cesión o comunicación de datos y acceso a los datos por cuenta de terceros.

El 20.2, por su parte, le hace una exigencia al responsable del tratamiento instando a que *"cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento".*

Y el 20.3 una advertencia al encargado del tratamiento *"en el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente. No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo".* Al igual que acaba de hacer el 12.2 de la LOPD.

IV.8.c. Posibilidad de subcontratación de servicios:

La subcontratación, de servicios, es decir, el que los datos pasen de unas manos a otras, debe hacerse con toda las cautelas

debidas, para que en el ir y venir de esos datos no se produzca menoscabo en los datos personales de loa pacientes.

El artículo 21 del RLOPD contempla esta posibilidad, estableciendo como premisa en su punto primero que *"el encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento".*

Pero a continuación el punto segundo de este mismo artículo, da otra posibilidad, *"no obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos: a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar. Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación. b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero. c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior. En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento".*

Aclarando el 21.3 que *"si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior"*.

Hay que recordar que este estudio se encuentra encuadrado dentro del ámbito sanitario, por lo que será necesario que quien trate los datos, sea el responsable, un encargado o un subcontratista, deben cumplir con las medidas de nivel alto de seguridad. Cabe pensar que cuantas más veces se trasladen los datos, ya sea a un encargado o a un subcontratista, más riesgos existen para los datos, por lo que habrá que poner especial atención en este punto.

IV.8.d. Conservación de los datos por el encargado del tratamiento:

El RLOPD contempla esta acción en su artículo 22 del RLOPD que atribuye esta obligación al encargado del tratamiento, estableciendo en su punto primero que *"una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación".* Y especificando en su punto segundo que *"el encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento".*

La conservación y custodia de la receta médica, tanto si es manual, como informatizada, será responsabilidad del prescriptor, así como de la oficina de farmacia, una vez dispensadas, que las conservará por un plazo de tres meses, en caso del soporte papel, transcurrido el cual serán destruidas por métodos que garanticen su no reconstrucción, y requerirán comunicación a la Administración sanitaria las pérdidas o accesos indebidos, previa denuncia policial, guardándose el justificante de la comunicación; en el caso del soporte informático, quedarán a disposición de la Administración

Sanitaria los datos relativos a la facturación, de acuerdo a su legislación.

El artículo 18.1 establece a este respecto que *"el prescriptor se responsabilizará de la conservación y custodia de los impresos y talonarios de recetas médicas, así como del acceso y utilización de datos para la prescripción electrónica. Las instituciones en las que los prescriptores presten sus servicios pondrán los medios necesarios para que puedan cumplirse estas obligaciones…".*

El punto segundo, por su parte, regula que *"en los supuestos de pérdida o sustracción de los impresos y talonarios de recetas médicas, así como de acceso no autorizado al sistema de receta médica electrónica, se presentará la correspondiente denuncia policial y se comunicará de inmediato al organismo o entidad que los hubiere facilitado, recabándose en dicho acto el justificante de haber realizado la comunicación".*

Y el punto tercero que *"una vez dispensadas y diligenciadas, las recetas médicas en soporte papel serán conservadas en la oficina de farmacia durante tres meses. El farmacéutico garantizará su seguridad, correcta conservación y confidencialidad. Finalizado el plazo de conservación, procederá a su destrucción, utilizando métodos que garanticen la imposibilidad de la reconstrucción del documento. No obstante, las recetas médicas de medicamentos estupefacientes o psicotrópicos y aquellas otras que deban ser sometidas a procedimientos de ulterior gestión o control, serán tramitadas por el farmacéutico de acuerdo con las normas e instrucciones específicas aplicables en cada caso".*

Para el formato electrónico en concreto, establece el punto cuarto que *"en las recetas médicas electrónicas del Sistema Nacional de Salud el farmacéutico se responsabilizará del acceso a los datos disponibles para la dispensación desde su oficina de farmacia. Una vez dispensados los productos prescritos y firmada y validada dicha dispensación, la oficina de farmacia solo podrá*

conservar la información y / o registros informáticos necesarios para la facturación, de acuerdo con lo dispuesto en el artículo 9.4 de este real decreto. En las recetas médicas electrónicas privadas, estas recetas serán conservadas el mismo período que las recetas médicas en papel, debiendo anular los registros informáticos finalizado el plazo de conservación".

En este sentido establece el artículo 19.1 respecto de ambos documentos en formato electrónico (recetas médicas y órdenes de dispensación que *"en los trámites a que sean sometidas las recetas médicas y órdenes de dispensación hospitalaria, y especialmente en su tratamiento informático así como en su proceso electrónico, deberá quedar garantizada, conforme previene la normativa específica de aplicación, la confidencialidad de la asistencia médica y farmacéutica, la intimidad personal y familiar de los ciudadanos y la protección de sus datos de carácter personal. A tal efecto, se implantarán en el tratamiento de los datos las medidas de seguridad previstas en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y en su normativa de desarrollo"*.

Puntualizando el punto segundo que *"no será necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica en soporte papel o electrónico, de conformidad con lo dispuesto en los artículos 7, apartados 3 y 6; 8; y 11, apartado 2.a), de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Las citadas actuaciones deberán tener por finalidad facilitar la asistencia médica y farmacéutica al paciente y permitir el control de la prestación farmacéutica del Sistema Nacional de Salud, incluidos los distintos regímenes especiales de las Mutualidades de Funcionarios".*

Por último, la disposición adicional séptima de este texto establece respecto del tratamiento de la información que *"en las actuaciones previstas en este real decreto que tengan relación con el tratamiento, cesión y custodia de datos de carácter personal se estará a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal".*

Las órdenes de dispensación hospitalarias, tanto en el ámbito público, como en el privado, se harán igualmente tanto en soporte papel, para ser cumplimentadas manual o informáticamente, como en soporte informático, y su conservación será durante un plazo mínimo de seis meses, según marca la ley del paciente. Así el artículo 17.1 establece que *"las órdenes de dispensación hospitalaria, extendidas en los hospitales públicos y privados, pueden emitirse en soporte papel, para cumplimentación manual o informatizada, y en soporte electrónico, y se editarán conforme a los criterios generales especificados en el anexo de este real decreto y los requisitos que las Administraciones sanitarias competentes o, en su caso, la Administración competente de las Fuerzas Armadas, introduzcan en el marco de sus competencias".* Y el 17.2 continúa diciendo que *"la orden de dispensación hospitalaria será dispensada por el servicio de farmacia o por el farmacéutico responsable del depósito de medicamentos del hospital en la que ha sido prescrita. En los Regímenes Especiales de las Mutualidades de Funcionarios y en el Sistema Nacional de Salud para los pacientes derivados a hospitales de referencia, podrán establecerse mecanismos que posibiliten la dispensación de la orden hospitalaria por los servicios de farmacia de los hospitales que las Administraciones competentes determinen".*

La Ley de Investigación Biomédica recoge, por su parte, en el Artículo 52 la Conservación de los datos, estableciendo en su punto primero que: "*Los datos genéticos de carácter personal se conservarán durante un período mínimo de cinco años desde la fecha en que fueron obtenidos, transcurrido el cual el interesado podrá solicitar su cancelación"*. Aunque su punto tercero estipula que *"si no mediase solicitud del interesado, los datos se conservarán durante el plazo que sea necesario para preservar la salud de la persona de quien proceden o de terceros relacionados con ella".* Pero además el punto tres de este artículo contempla que *"fuera de estos supuestos, los datos únicamente podrán conservarse, con fines de investigación, de forma anonimizada, sin que sea posible la identificación del sujeto fuente".*

IV.8.e. Externalización y Privatización: Particularidades de cada centro.

La externalización de los servicios de custodia de las historias clínicas, se hace cada vez más a menudo, sobre todo desde que hemos entrado en la era digital, ya que es mucho más sencillo que hacerlo con el soporte papel, ya que una gestión es virtual y la otra sería física.

Cada centro se organizará de acuerdo a lo que él mismo establezca. En el sector público se hará dentro de cada centro por comunidades autónomas, y en el sector privado de manera individualizada. De lo que no cabe duda, es que, respecto al sector público, estas actividades tienden a la privatización de la sanidad pública, como ya se ha comentado en la introducción de este estudio.

A este respecto un sector de la doctrina opina que *"…en la actualidad, se está extendiendo entre los centros sanitarios la práctica consistente en externalizar el tratamiento de las historias clínicas, a través de los llamados contratos de «outsourcing». Por*

medio de los mismos son entidades privadas, con personalidad jurídica distinta de la propietaria de las historias clínicas, quienes crean y gestionan los archivos. Estas entidades no pueden subcontratar el almacenamiento de las historias clínicas…"[412]*.* No obstante, sostiene este mismo sector que *"Estamos ante situaciones permitidas por la LOPD –que no recogía la derogada LORTAD- siempre que se cumplan una serie de requisitos. El artículo 12 exige que el encargo de tratamiento se realice por escrito y que la entidad externa que trate los datos contenidos en la HC quede sometida a las mismas obligaciones que el centro sanitario en cuanto responsable del tratamiento y que destruya o devuelva toda la información una vez finalizada la relación contractual…"* [413]. De modo que este capítulo de la externalización de los servicios hay que ponerlo en directa relación con el del tratamiento de datos por cuenta de terceros, ya que los datos pasan de un titular a otro.

Relacionado directamente con el tratamiento de datos por cuenta de terceros, es hoy en día cada vez más habitual que las bases de datos se encuentren fuera de los locales en los que se ubica el responsable del fichero. Unas veces por falta de espacio, y otras por buscar una mayor seguridad, la realidad es que la externalización del alojamiento de las bases de datos se está convirtiendo en una práctica habitual. Son los contratos de «*outsourcing*», ya comentados por parte de la doctrina, y que "*es un término inglés muy utilizado en el idioma español, pero que no forma parte del diccionario de la Real Academia Española (RAE). Su vocablo equivalente es subcontratación, el contrato que una empresa realiza a otra para que ésta lleve a cabo determinadas tareas que, originalmente, estaban en manos de la primera*." *"El*

[412] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso. *"La protección de datos personales en el ámbito sanitario"*, Editorial Aranzadi, Navarra 2002. Pág. 80.

[413] Ibídem.

outsourcing, en otras palabras, consiste en movilizar recursos hacia una empresa externa a través de un contrato. De esta forma, la compañía subcontratada desarrolla actividades en nombre de la primera. Por ejemplo: una firma que ofrece servicios de acceso a Internet puede subcontratar a otra para que realice las instalaciones. La empresa principal cuenta con la infraestructura de redes necesaria y el plantel para vender el servicio; la segunda, en cambio, se limita a llegar hasta el domicilio del usuario para efectuar la instalación pertinente. Cabe señalar que para el cliente final no existe diferencia alguna entre la empresa contratante y la subcontratada". "*Se habla de outsourcing offshore cuando la transferencia de los recursos se realiza hacia otros países, ya sea con la participación de empresas extranjeras o con la instalación de una sede en la nación foránea. Ejemplos de este tipo de subcontratación suelen darse en el ámbito de la informática, cuando empresas estadounidenses o europeas tercerizan ciertos servicios (como el diseño web o la programación) en compañías latinoamericanas o asiáticas. El tipo de cambio hace que las empresas subcontratadas resulten baratas para la compañía contratante, lo que le permite ahorrar costos (contratar en el extranjero es una opción más rentable que hacerlo en su propio país)*".

Pero la realidad, es que esta práctica, cada vez más habitual, puede suponer ventajas para la entidad que las externaliza, a nivel de gestión, e incluso que las medidas tomadas por el tercero sean mucho mayores que las que se hubiesen tomado internamente, pero no olvidemos que el transporte siempre tiene un riesgo. Sin olvidar que aunque se trate del un encargado del tratamiento que tomar las mismas medidas que el responsable del fichero.

V. CREACIÓN DE BASES DE DATOS MÉDICAS.

La creación de bases de datos es algo que sucede todos los días, cada minuto se generan millones de datos en el mundo. Este fenómeno ha sido provocado por el ya mencionado avance tecnológico que ha supuesto la implantación de la tecnología en todo el mundo.

En el sector médico ocurre lo mismo, ya sea en centros grandes o pequeños, el volumen de información que se genera es cada día mayor, requiriéndose de nuevos recursos para gestionarlas, casi todos ellos relacionados con la informática, pero también otros más tradicionales, como pueda ser la destrucción de documentos por empresas especializadas, debido al volumen manejado.

V.1. DESDE EL PUNTO DE VISTA MÉDICO:

Es obvio pensar que para la medicina lo importante es curar, y para la protección de datos proteger la información de sus titulares, sin embargo, es necesario encontrar un equilibrio entre ambos valores, para que ninguno de los bienes en juego quede desprotegido. Como objeto de este estudio, la protección de datos sanitarios cuenta con legislación en ambas materias al respecto, la protección de datos y la medicina, que ya han sido ampliamente descritas. Y por otro lado, existe además de la legislación que se aplica para el tratamiento de datos, otras normas que obligan igualmente a la generación de bases de datos, pero en las que el afectado no decide sobre la inclusión de sus datos en las mismas, me refiero a los registros nacionales que serán comentados a continuación.

En cualquiera de los casos, tanto si decidimos que nuestros datos de salud formen parte de un fichero de datos como si no, es de vital importancia que quienes traten la información, tengan además

unos valores morales que les lleven al correcto tratamiento de los datos personales.

V.1.a. Códigos deontológicos y valor moral:

Este punto referido, se encuentra respaldado en el sector sanitario por el Código de Deontología Médica, que en el plano de la protección de datos se puede equiparar con el apartado de la formación del personal, ya que ambos tratan normas de comportamiento respecto al tratamiento de datos personales. La principal diferencia, es que las normas relativas para el tratamiento de datos personales las impone una Ley Orgánica, y el CDM tiene un valor sectorial sobre la conducta de quienes a él pertenecen. No en vano, el artículo primero de este último texto citado, recoge como definición de deontología médica *"… el conjunto de principios y reglas éticas que han de inspirar y guiar la conducta profesional del médico".* Estableciendo además el 2.1 que *"los deberes que impone este Código, en tanto que sancionados por una Entidad de Derecho Público, obligan a todos los médicos en el ejercicio de su profesión, cualquiera que sea la modalidad en la que la practiquen".* Y además el 2.2 puntualiza que *"el incumplimiento de algunas de las normas de este Código supone incurrir en falta disciplinaria tipificada en los Estatutos Generales de la Organización Médica Colegial, cuya corrección se hará a través del procedimiento normativo en ellos establecido".*

Respecto del contenido del artículo primero, comenta una parte de la doctrina que *"lo que no dice es que en el CDM se incluyen artículos que obligan tanto desde el punto de vista legal como ético y normas con connotaciones exclusivamente éticas y que su incumplimiento supondría una sanción disciplinaria del Colegio. Hay así mismo artículos que tan solo son recomendaciones al médico para un comportamiento ético de excelencia"*[414]*.* Y respecto a lo que

[414] BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA

dice el artículo 2, comenta este mismo sector que *"debe quedar claro que las Juntas Directivas de los Colegios, antes de plantearse si una posible falta cometida por un colegiado es presumiblemente sancionable, pueden y deben solicitar el asesoramiento de las Comisiones de Deontología, cuyo informe no es vinculante"*[415].

Mantiene un sector doctrinal en este aspecto que "*es por ello muy pertinente el énfasis que el CDM hace en el artículo 3 al decir que «la Organización Médica Colegial asume como uno de sus objetivos primordiales la promoción y desarrollo de la Deontología profesional. Dedicará atención preferente a difundir los preceptos de este Código...». Este artículo tiene un valor extraordinario, siempre y cuando los médicos lo hagan suyo. No sólo la OMC como ente representativo de los médicos, sino también cada uno de los profesionales debe buscar en la autorregulación de sus acciones y criterios lo mejor para la sociedad y la profesión. Esta regulación, es decir la capacidad que se tiene de regular la conducta y actividad profesional médica es la que asegurará la autonomía para tomar decisiones respecto a la atención y tratamiento de los pacientes". Hay que tener en cuenta que según esta tendencia doctrinal "habitualmente cuando los médicos abordan cuestiones de índole ética en sus lugares de trabajo lo hacen en equipo con otros profesionales sanitarios y por ello en general se hace referencia a los principios y valores desarrollados por la Bioética, que no son otros que los que contiene el CDM"*[416]. Y sostiene que "*quizá por esto, es decir por la aparición de los equipos multidisciplinarios y por el*

GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: *"Manual de ética y deontología médica".* Organización Médica Colegial de España, 2012. Pág. 22.

[415] Ibídem. Pág. 24.

[416] BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: *"Manual de ética y deontología médica".* Organización Médica Colegial de España, 2012. Pág. 26.

desarrollo científico y tecnológico, lo que antes era una ética médica, se ha convertido en una ética "multidisciplinar", es decir que trasciende el propio campo de la actuación del médico, salvo cuando la relación se establece exclusivamente en el plano dual, médico-paciente"[417]*.*

Otra parte de la doctrina manifiesta a este respecto que *"los protocolos de ética clínica (PECs) son documentos cada vez más elaborados en los centros sanitarios. Se crean cuando existe, además de un problema clínico, un conflicto ético frecuente. Han sido elaborados a diferentes instancias (institucional, extrainstitucional...) y son documentos todavía poco conocidos, por su reciente aparición y más aún por su escasa difusión y aplicación"*[418]*.* Y especifican estos autores a continuación que *"los PECs son instrumentos que ayudan en la toma de decisiones cuando existen conflictos éticos. Un conflicto ético se produce porque al menos dos valores se enfrentan o entran en contradicción y es imposible que todos los valores se lleven a la práctica…"* [419]*.* A este respecto nos desvelan que *"los Comités de Ética multidisciplinares son órganos de deliberación que en la mayoría de situaciones no son vinculantes para el profesional que plantea la consulta. Dicho profesional, una vez asesorado, deberá tomar la decisión que considere oportuna, siguiendo las normas del vigente CDM"*[420]*.*

Otro sector doctrinal ha manifestado que *"el Código de Deontología Médica (CDM) vigente desde Julio del 2011, vuelve a retomar el título que tuvieron sus predecesores, a excepción del*

[417] Ibídem.

[418] BANDRÉS MOYÁ, Fernando Y DELGADO BUENO, Santiago: "*Biomedicina y derecho sanitario*". Ademas Comunicación, S.L., 2009. Pág. 377.

[419] Ibídem. Pág. 378.

[420] BÁTIZ CANTERA, Jacinto, CASADO BLANCO, Mariano, CASADO GÓMEZ, Tomás, CASTELLANO ARROYO, María, CIPRÉS CASASNOVAS, Luís, COLLAZO CHAO, Eliseo, GARCÍA GUERRERO, Julio, GÓMEZ SANCHO, Marcos, LABAD ALQUÉZAR, Antonio, LUNA MALDONADO, Aurelio, MÁRQUEZ GALLEGO, L. Fernando, MONÉSXIOL, Loan, MURILLO SOLÍS, Diego, SOLLA CAMINO, José Manuel, VILLANUEVA CAÑADAS, Enrique: "*Manual de ética y deontología médica*". Organización Médica Colegial de España, 2012. Pág. 27.

*último. El anterior incluía en el título dos conceptos diferentes: Ética Médica y Deontología Médica. En esta ocasión se ha preferido poner como subtítulo y por tanto de forma diferenciada, la Ética Médica y con la expresión: «Guía de Ética Médica»"*421*.* A este respecto *"quizá convenga intentar clarificar los conceptos que subyacen sobre los términos ética y moral, que en ocasiones se utilizan como sinónimos cuando no lo son, aunque efectivamente tienen muchos aspectos relacionados, lo que hace que sus límites para muchos médicos -y otras personas- sean ambiguos y de ahí la confusión"*422*.* Así *"…la ética a partir de ahora entendida como "éthos" constituye una reflexión consciente mediante la cual el ser humano valora si un acto es (éticamente) bueno o malo. La moral está estrechamente vinculada a las costumbres y cada época y cultura tiene las suyas. Costumbres cambiantes a lo largo de la historia y de las latitudes".* Y por otro lado *"la ética tiene una base de reflexión personal, individual, aunque pueda estar compartida por muchos, sobre actos realizados de forma individual o colectiva. Los actos colectivos pueden ser asumidos como costumbre moral aceptada por una sociedad dominante y ser éticamente rechazables"*[423]*.*

Karla Cantoral ha manifestado respecto a la ética que *"…los juristas tenemos una gran responsabilidad; el arma privilegiada para la igualdad y la intimidad es la eticidad indisponible en el derecho, sea bajo el nombre de derecho natural, justicia, derechos humanos, principios o cualquier otro…"*[424]*.* Defendiendo que *"si bien la inusitada evolución de la medicina y la ciencia producen cambios en el mundo de la política y el derecho, no debemos perder de vista que hay un mínimo ético que no se debe conculcar y que constituye uno de los pilares irrenunciables de las actuales sociedades*

[421] Ibídem. Pág. 19.

[422] Ibídem.

[423] Ibídem. Pág. 20.

[424] CANTORAL DOMÍNGUEZ, Karla: "*Derecho de protección de datos personales en la salud*". Editorial Novum, MEXICO D.F., 2012. Pág. 137.

democráticas; ese mínimo ético no es otro que el constituido por los derechos fundamentales y las libertades públicas…"[425].

En este sentido y en relación a la presentación del Comité de Ética para la Asistencia Sanitaria, publica el boletín de comunicación interna de la Consejería de Sanidad, que: *"Los CEAS son equipos interdisciplinares creados con la misión de asesorar a profesionales que trabajan en el ámbito de las organizaciones sanitarias, así como a los pacientes, en la solución de problemas éticos. Su objetivo no es otro que contribuir a mejorar la calidad de la atención sanitaria afrontando las cuestiones éticas asistenciales que han surgido en los últimos años, relacionadas con el desarrollo tecnológico, con el valor dado en nuestra sociedad a la autonomía de las personas y con la asignación de los recursos…"*[426].

Este apartado se encuentra muy relacionado con el deber de secreto establecido por la normativa de protección de datos analizado.

V.1.b. Leyes médicas:

La legislación médica, según se ha visto en la introducción de este estudio es muy extensa a lo largo del tiempo, con regulación vigente tanto muy antigua como muy reciente. Por esa razón y para no romper la perspectiva general del apartado de la introducción histórica, en el que se recoge normativa tanto sanitaria como no sanitaria, en este punto no conviene trasladar aquí esta última, sino hacer una referencia a lo ya desarrollado.

[425] Ibídem. Pág. 141.

[426] "Presentación del Comité de Ética para la Asistencia Sanitaria". Salud. Madrid, julio-septiembre 2007, Año IV- Número 48, Pág. 16.

V.1.c. Imposiciones legislativas: licitud sobre la creación de estas bases de datos y creación de registros nacionales.

Igualmente, en este apartado es necesario referir que a lo largo del estudio, serán constantemente nombradas situaciones en que los datos personales de los pacientes deban constar, o se trasladen sin su consentimiento, dando lugar a tratamientos por imperativo legislativo. Esto supone la creación de bases de datos obligatorias, es decir, en las que el paciente no decide si se incluye o no su información, como es el caso de los registros nacionales. Estos son creados en casi todos los sectores de actividad que hay en la sociedad, y por supuesto también en el sector sanitario.

En el año 2000, es llevado a cabo por la AEPD un plan de inspección de oficio al Registro Nacional de Sida, que se encuadra en el Centro Nacional de Epidemiología, y del que surgieron las siguientes conclusiones. Se recogen los datos de nombre, apellidos y fecha de nacimiento, así como sexo, edad, país de residencia y de origen, para la realización del estudio y que se incluyen en el registro que se nutre de hospitales públicos y privados, existiendo el compromiso para las comunidades autónomas de remitir esta información periódicamente al Centro Nacional de Epidemiología, que igualmente comparte con estas los casos detectados. Por otro lado este conjunto de datos se disocia de la persona y es enviado al Centro Europeo de la Organización Mundial de la Salud en París y al Instituto Nacional de Estadística, para que el control sea tanto interno, a nivel estatal, como externo a nivel internacional. Existe también la posibilidad de que se utilicen para investigación motivadamente y disociados.

Se observa además durante la realización del estudio, sobre la aplicación de las medidas de seguridad que *“el Registro Nacional del SIDA únicamente es gestionado por tres personas, siendo una de ellas el responsable de dicha gestión*”. Que *“el ordenador que contiene el fichero está ubicado en un despacho que se cierra con*

llave cuando no se encuentran en él los responsables de la gestión". Que *"existe una contraseña de "setup" para acceder al ordenador. La contraseña de acceso a la aplicación se cambia cuando hay alguna incidencia (v.gr.: cambio de personas responsables)". Que "no se guardan registros de auditorías de las operaciones que pueden afectar a los usuarios sobre los datos del fichero a través de la aplicación ó desde el propio Dbase".* Que *"la base de datos está comprimida y cifrada y el ordenador que la contiene está encendido en tanto se utiliza, permaneciendo apagado el resto del tiempo".* Que *"el mantenimiento del sistema se lleva a cabo por los propios profesionales que trabajan en el Registro Nacional del SIDA. Ocasionalmente se ha recurrido a personal del Área de Informática del Instituto de Salud Carlos III, siendo aplicadas las soluciones por los responsables del registro".* Que *"ninguna empresa informática de mantenimiento tiene acceso al ordenador donde se encuentra la base de datos del Registro Nacional del SIDA". Que "el Centro Nacional de epidemiología tiene inscrito en el Registro de Protección de Datos de la Agencia de Protección de Datos el fichero denominado "registro Nacional del Sida…"* Aportándose recomendaciones al respecto.

A la vista de lo expuesto, la AEPD redacta unas recomendaciones relativas a la recogida y tratamiento de los datos especialmente protegidos, al derecho de información en la recogida de los datos, a las cesiones de datos, al ejercicio de los derechos, al movimiento internacional de datos y a las medidas de seguridad que vienen a paliar las deficiencias encontradas.

Pero este no es el único registro nacional existente en materia sanitaria, por el contrario son muy numerosos, a saber, Registro Nacional de enfermos renales, de trasplante cardíaco, de pacientes con lupus, de pacientes con espina bífida, de enfermedades raras, de enfermos de alzheimer, de enfermos de parkinson, de enfermos de sarcoidosis, etc.

V.2. DESDE EL PUNTO DE VISTA DE LA PROTECCIÓN DE DATOS:

Del mismo modo, desde la perspectiva de la protección de datos, existe una extensa normativa que afecta al tema que nos ocupa, y que al igual que la sanitaria, ha sido descrita en el apartado correspondiente, por lo que nos remitiremos a él en este punto.

En la protección de datos, y por supuesto también en la de los datos sanitarios, la primera operación que debe efectuarse es la inscripción de los ficheros que vayan a contener los datos personales objeto de tratamiento, y que deberá hacerse de forma previa al cualquier otra acción en primera instancia e introduciendo las vicisitudes que se vayan produciendo.

Debe quedar claro que *"…tanto los ficheros de titularidad pública como los de titularidad privada están sujetos a esta normativa, pero con algunas diferencias en cuanto a su creación, modificación y extinción, órganos ante los que responden, y también respecto a las excepciones en el ejercicio de los derechos"*[427]*.* Y es que, sean recogidos los datos por una entidad pública o privada, la verdad es que deben ser igualmente protegidos, con independencia de quien sea el titular del fichero en el que se incluyen los datos.

Unos y otros, los de titularidad pública y los de titularidad privada, tienen una parte común y otra específica, a la hora de su creación. En el ámbito sanitario conviven ambos, e incluso llegan a entremezclarse, ya que hoy en día una misma persona acude para una misma cuestión a centros públicos y privados, incluso, con el tema de la privatización de la sanidad, el propio centro público nos envía al privado para la realización de determinada prueba, para evitar listas de espera. Dentro de este contexto hay que analizar los siguientes apartados.

[427] VIDAL RASO, Marta: "*El mundo empresarial se ve directamente afectado por la Ley de Protección de Datos de Carácter Personal*". Revista ejecutivos nº 179, Madrid, 2007.Págs. 140-141.

V.2.a. Generalidades y particularidades de los ficheros de titularidad pública y titularidad privada:

Ya el artículo 1 de la LOPD establece como su objeto que *"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".* Sirva esto como premisa para analizar el artículo segundo de esta norma, que aunque ya ha sido citado en la introducción, se hace necesario hacerlo ahora de nuevo, ya que en su punto primero establece que *"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…."*. De modo que hay que garantizar la intimidad de las personas tanto en el tratamiento de datos en los centros públicos como en los privados.

Igualmente el RLOPD, en su artículo primero, en el que también regula el objeto del mismo, establece que *"el presente reglamento tiene por objeto el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal".* Y en su artículo segundo, punto primero, regula el ámbito objetivo de aplicación, estableciendo que *"el presente reglamento 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".* Incluyendo el punto cuarto de este artículo las exclusiones que *"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 óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los*

datos". Cuestión esta última poco apetecible, pero que requiere igualmente el tratamiento de los datos personales en la faceta menos amable, dentro de lo poco amables que resultan casi todos los tratamientos de datos que se realizan dentro de los centros sanitarios.

Un sector doctrinal ha manifestado que *"la actuación de las Administraciones Públicas, como la de cualquier particular, es susceptible de incidir sobre el derecho a la protección de datos. La diferencia estriba en que la peculiar posición de la Administración en nuestro modelo de Estado constitucional, como sujeto cuya función es la satisfacción de los intereses generales (art. 103.1 CE), para lo que se le atribuyen potestades exorbitantes del Derecho privado, implica la existencia de limitaciones al derecho fundamental que no juegan en los casos en que la afección proviene de un particular"*[428]*.*

Dicho esto, la creación de ficheros, ya sean de titularidad pública o privada, genera una serie de obligaciones, la primera de ellas la notificación de los mismos al organismo correspondiente el Registro General de Protección de Datos (en adelante RGPD).

Respecto a la notificación de los ficheros en el RGPD, el artículo 26.1 de la LOPD contempla que *"toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos".* La regulación de su contenido la marca el 26.2 de la LOPD *"por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico,*

[428] ARRIBAS LEÓN, Mónica, CARRIZOSA PRIETO, Esther, CARRUSO FONTÁN, Viviana, GALAÁN MUÑOZ, Alfonso, HOLGADO GONZÁLEZ, María, LUCENA CID, Isabel Victoria, TOSCANO GIL, Francisco. "La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación". Tirant Lo Blanch, Valencia, 2014. Pág. 120.

medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros". Estos extremos se encuentran regulados en el título V del RLOPD, referido a las obligaciones previas al tratamiento de datos, en sus artículos 55 a 64, de los que se destacarán los aspectos más relevantes a continuación.

La notificación de ficheros de titularidad pública y privada, ya empieza con una diferencia recogida en el artículo 55, ya que su punto primero regula, e este aspecto, los ficheros de titularidad pública, estableciendo que *"todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente".* Y su punto segundo los de titularidad privada, recogiendo a su vez que *"los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos".* El punto cuarto de este artículo requiere lo siguiente *"la notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento"*. Relativa a los procedimientos tramitados por

al AEPD, en relación con los procedimiento para la inscripción de ficheros, en el que no procede ahondar en estos momentos.

Una vez tramitados estos procedimientos, establece el artículo 60.2 que *"la inscripción contendrá el código asignado por el Registro, la identificación del responsable del fichero, la identificación del fichero o tratamiento, la descripción de su finalidad y usos previstos, el sistema de tratamiento empleado en su organización, en su caso, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, y la indicación del nivel de medidas de seguridad exigible conforme a lo dispuesto en el artículo 81. Asimismo, se incluirán, en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales. En el caso de ficheros de titularidad pública también se hará constar la referencia de la disposición general por la que ha sido creado, y en su caso, modificado".* Cuestión, la modificación, abordada a continuación.

Y como último requisito, respecto de las obligaciones relativas a la inscripción de ficheros, en su punto tres marca el 26.3 de la LOPD que *"deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación." De modo que no solo habrá que notificar la creación del fichero, sino también las eventuales variaciones que vaya sufriendo, para con ellos mantener un registro actual y fiel a la situación de cada entidad".*

A este respecto, y en relación a la modificación, el artículo 58.1 establece que *"la inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la Agencia Española de Protección de Datos o a las autoridades de control autonómicas competentes, a fin de proceder a*

su inscripción en el registro correspondiente, conforme a lo dispuesto en el artículo 55".

Y sobre la supresión de ficheros, como variación que es, el 55.2 recoge que *"cuando el responsable del fichero decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el registro correspondiente"*. Lo dicho sobre la modificación y supresión de ficheros, para los ficheros de titularidad privada, ya que para los de titularidad pública el 58.3 establece que *"tratándose de ficheros de titularidad pública, cuando se pretenda la modificación que afecte a alguno de los requisitos previstos en el artículo 55 o la supresión del fichero deberá haberse adoptado, con carácter previo a la notificación la correspondiente norma o acuerdo en los términos previstos en el capítulo I de este título".* Este capítulo contempla en su artículo 52.1 que *"la creación, modificación o supresión de los ficheros de titularidad pública sólo podrá hacerse por medio de disposición general o acuerdo publicados en el «Boletín Oficial del Estado» o diario oficial correspondiente".* Concretando el punto segundo que *"en todo caso, la disposición o acuerdo deberá dictarse y publicarse con carácter previo a la creación, modificación o supresión del fichero".*

Respecto de la notificación e inscripción de ficheros, aun algunas especialidades que no se han comentado. Una de ellas viene marcada en el artículo 56, y se refiere a la posibilidad de realizar tratamientos de datos en distintos soportes, así se establece en su punto segundo que *"cuando los datos de carácter personal objeto de un tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado sólo será precisa una sola notificación, referida a dicho fichero".* Ya que según marca el punto primero *"la notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento*

de los datos". La segunda especialidad se refiere a aquellos ficheros en los que existan varios responsables, a este respecto marca el artículo 57 del RLOPD que *"cuando se tenga previsto crear un fichero del que resulten responsables varias personas o entidades simultáneamente, cada una de ellas deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las comunidades autónomas, la creación del correspondiente fichero".*

Y existen otras dos situaciones en las que las distintas autoridades podrán proceder en esta materia por su propia cuenta. La marcada en el artículo 63.1 del RLOPD, según el que *"en supuestos excepcionales con el fin de garantizar el derecho a la protección de datos de los afectados, y sin perjuicio de la obligación de notificación, se podrá proceder a la inscripción de oficio de un determinado fichero en el Registro General de Protección de Datos"* .Pero con la condición del 63.2: *"Para que lo dispuesto en el apartado anterior resulte de aplicación, será requisito indispensable que la correspondiente norma o acuerdo regulador de los ficheros que contengan datos de carácter personal haya sido publicado en el correspondiente diario oficial y cumpla los requisitos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento"*. Por último, el artículo 64 establece que: *"El Director de la Agencia Española de Protección de Datos podrá celebrar con los directores de las autoridades de control de las comunidades autónomas los convenios de colaboración o acuerdos que estime pertinentes, a fin de garantizar la inscripción en el Registro General de Protección de Datos de los ficheros sometidos a la competencia de dichas autoridades autonómicas".*

Conviene citar aquí una referencia jurisprudencial que establece que: *"El solicitante de amparo sostiene que los hechos declarados probados en ambas decisiones resultan concluyentes al*

respecto, pues la entidad había procedido a crear una base de datos en la que figuran, al menos, los diagnósticos de las enfermedades que originaron una situación de baja laboral por incapacidad temporal, sin requerir para ello la previa autorización del interesado, ni invocar interés contractual alguno; de igual modo, tampoco se aduce dicho interés para motivar la negativa a la cancelación de los datos obrantes en el archivo automatizado. Dicho archivo no está dado de alta en la Agencia de Protección de Datos, por lo que no existe responsable oficial del mismo, y a él tienen acceso, por un lado, los cuatro médicos contratados por la entidad crediticia como médicos de empresa y, por otro, un empleado de "ENTIDAD A" adscrito al área de personal, que no ostenta la condición de facultativo y que facilita la clave de acceso al sistema. Finalmente, el recurrente pone de manifiesto una situación de pluriempleo de los médicos al servicio de la entidad, dado que son también facultativos de la Seguridad Social:*"finalmente Se declara vulnerado el derecho a la intimidad del recurrente de los artículos 18.1 y 4 de la CE. Esto nos muestra que es una realidad la no inscripción de los ficheros en la AEPD, así como otras que subyacen de esta sentencia, como el acceso por personal indebido de acuerdo al desarrollo de sus funciones"*[429]*.*

V.2.b. Especialidades: los códigos tipo.

Podría decirse que los códigos tipo son unas normas de conducta especiales, que basadas en la generalidad de lo establecido por la normativa de protección de datos que marca los mínimos, vienen a complementarlos de forma sectorial, obligando a su cumplimiento a todos los que se adhieren a ellos.

El artículo 32 de la LOPD, regula esta materia, y establece en su punto primero que *"mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de*

[429] Sentencia 202/1999, de 08 de noviembre de 1999 del Tribunal Constitucional. Recurso de Amparo núm. 4138/1996.

tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo".

Matizando en su punto segundo que *"los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación. En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél".*

Finalmente en el punto tercero hace referencia a la función que cumplirán estos documentos dentro de la organización *"los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas".*

Así mismo, el RLOPD, en su artículo 71.1 establece que *"los códigos tipo a los que se refiere el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, tienen por objeto adecuar lo establecido en la citada Ley Orgánica y en el presente reglamento a*

las peculiaridades de los tratamientos efectuados por quienes se adhieren a los mismos. A tal efecto, contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento". Y el punto segundo de este artículo recoge que *"los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional y serán vinculantes para quienes se adhieran a los mismos".* Lo cual podemos poner en relación con lo dicho sobre el CDM en anteriores apartados.

Estos documentos no son obligatorios, así lo marca el 72.1 del citado reglamento *"los códigos tipo tendrán carácter voluntario."* Pero la entidad que se adhiera a ellos debe acatarlos según el 72.3: *"Los códigos tipo promovidos por una empresa deberán referirse a la totalidad de los tratamientos llevados a cabo por la misma".* Y además tienen otras características que vienen marcadas por el 72.2, estableciendo que *"los códigos tipo de carácter sectorial podrán referirse a la totalidad o a parte de los tratamientos llevados a cabo por entidades pertenecientes a un mismo sector, debiendo ser formulados por organizaciones representativas de dicho sector, al menos en su ámbito territorial de aplicación, y sin perjuicio de la potestad de dichas entidades de ajustar el código tipo a sus peculiaridades".* Existe una última especificación al respecto de su aplicación que afecta a los centros sanitarios públicos, en el caso de este estudio, y es que *"las Administraciones públicas y las corporaciones de Derecho Público podrán adoptar códigos tipo de acuerdo con lo establecido en las normas que les sean aplicables".*

Respecto del contenido de los mismos, viene regulado en el artículo 73 RLOPD, que recoge en su primer punto que *"los códigos tipo deberán estar redactados en términos claros y accesibles".* Y a continuación en el punto segundo regula el contenido mínimo de los

mismos, estableciendo que *“los códigos tipo deben respetar la normativa vigente e incluir, como mínimo, con suficiente grado de precisión: a) La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo. b) Las previsiones específicas para la aplicación de los principios de protección de datos. c) El establecimiento de estándares homogéneos para el cumplimiento por los adheridos al código de las obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre. d) El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición. e) La determinación de las cesiones y transferencias internacionales de datos que, en su caso, se prevean, con indicación de las garantías que deban adoptarse. f) Las acciones formativas en materia de protección de datos dirigidas a quienes los traten, especialmente en cuanto a su relación con los afectados. g) Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código tipo, en los términos previstos en el artículo 74 de este reglamento”.* Especificando el punto tercero de este artículo que *“en particular, deberán contenerse en el código: a) Cláusulas tipo para la obtención del consentimiento de los afectados al tratamiento o cesión de sus datos. b) Cláusulas tipo para informar a los afectados del tratamiento, cuando los datos no sean obtenidos de los mismos. c) Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición. d) Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso”.*

El artículo 74.1del reglamento por su parte establece también en este sentido que *“los códigos tipo podrán incluir cualquier otro compromiso adicional que asuman los adheridos para un mejor cumplimiento de la legislación vigente en materia de protección de datos”* .Y en cualquier caso, sean las reglas que establezcan

mínimas o mejoradas, los códigos tipo, según marca el artículo 75.1 que *"…deberán incluir procedimientos de supervisión independientes para garantizar el cumplimiento de las obligaciones asumidas por los adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio".* Es decir, que los compromisos adoptados deberán cumplirlos estando bajo la supervisión de alguien que haga cumplir las normas las normas en ellos establecidas.

Una vez adoptado el código tipo, deberá darse traslado de él a la AEPD, de acuerdo al artículo 77.1 *"para que los códigos tipo puedan ser considerados como tales a los efectos previstos en el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento, deberán ser depositados e inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos o, cuando corresponda, en el registro que fuera creado por las comunidades autónomas, que darán traslado para su inclusión al Registro General de Protección de Datos".* Una vez hecho esto, la AEPD procederá a su publicación de acuerdo al punto segundo del artículo 77, que marca que *"en todo caso, la Agencia Española de Protección de Datos dará publicidad a los códigos tipo inscritos, preferentemente a través de medios informáticos o telemáticos".* Y posteriormente, los adheridos constarán en un lista, según marca el artículo 76 RLOPD *"el código tipo deberá incorporar como anexo una relación de adheridos, que deberá mantenerse actualizada, a disposición de la Agencia Española de Protección de Datos".*

Y por último, existen una serie de obligaciones posteriores a la inscripción de los mismos, que consta en el artículo 78 y que obligan a *"las entidades promotoras o los órganos, personas o entidades que al efecto se designen en el propio código tipo tendrán, una vez el mismo haya sido publicado, las siguientes obligaciones: a) Mantener accesible al público la información actualizada sobre las entidades promotoras, el contenido del código tipo, los procedimientos de*

adhesión y de garantía de su cumplimiento y la relación de adheridos a la que se refiere el artículo anterior. Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos. b) Remitir a la Agencia Española de Protección de Datos una memoria anual sobre las actividades realizadas para difundir el código tipo y promover la adhesión a éste, las actuaciones de verificación del cumplimiento del código y sus resultados, las quejas y reclamaciones tramitadas y el curso que se les hubiera dado y cualquier otro aspecto que las entidades promotoras consideren adecuado destacar. Cuando se trate de códigos tipo inscritos en el registro de una autoridad de control de una comunidad autónoma, la remisión se realizará a dicha autoridad, que dará traslado al registro General de Protección de Datos. c) Evaluar periódicamente la eficacia del código tipo, midiendo el grado de satisfacción de los afectados y, en su caso, actualizar su contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento. Esta evaluación deberá tener lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor. d) Favorecer la accesibilidad de todas las personas, con especial atención a las que tengan alguna discapacidad o de edad avanzada a toda la información disponible sobre el código tipo".

Por su parte, la Directiva sobre protección en el tratamiento de datos, regula en su artículo 27 los llamados códigos de conducta. El punto primero del citado artículo establece que *"los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva".*

Especifica en su punto segundo que *"los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales. Los Estados miembros establecerán que dicha autoridad vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, la autoridad recogerá las observaciones de los interesados o de sus representantes".*

Y abre esta norma el abanico aún más al ámbito comunitario, recogiendo en su punto tercero que *"los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del grupo contemplado en el artículo 29. Éste se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del grupo".*

Actualmente hay cinco códigos tipo inscritos en la AEPD relacionados con el sector sanitario, que se comentarán a continuación.

En el año 2001 se inscribió el primero de ellos por parte de la Agrupación catalana de establecimientos sanitarios, viniendo a regular principalmente los derechos y garantías de los afectados, las garantías de cumplimiento de los códigos tipo, los principios de calidad, las obligaciones del responsable del fichero respecto de la información a los usuarios, el consentimiento de los mismos, las

medidas de seguridad, el deber de secreto, la cesión de los datos, el deber de indemnizar, el tratamiento por cuenta del responsable del fichero y la cooperación con la AEPD.

En el año 2002, también en la comunidad catalana, se inscribió el código tipo de la unió catalana d'hospitals, que fue modificado posteriormente en el año 2004, y que establece en el primer párrafo de su introducción que *"con la entrada en vigor de la Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal (LOPD) se recondujo el desarrollo legislativo iniciado con la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD). Efectivamente esta última, desarrollo legislativo del Artículo 18.4 de la Constitución Española, pronto se vio superada por la legislación europea, y en concreto por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de Europa del 24 de Octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos".* Pasando a regular en su contenido principalmente las materias relativas a la calidad de los datos, sus garantías en cuanto al ejercicio de derechos, así como los derechos de los mismos en relación a la información, consentimiento, seguridad de los datos, la cesión de los mismos, el acceso por cuenta de terceros, la obligación de secreto y las auditorías.

En el año 2004, pero modificado en 2006, se inscribió el código tipo de odontólogos y estomatólogos de España, promovido por el Consejo General del Colegios de odontólogos y estomatólogos de España, y que recoge mejoras principalmente en lo relativo a los principios de la protección de datos, medidas de seguridad para ficheros manuales y automatizados incluyendo las auditorías, derechos de los afectados en relación al ejercicio de los mismos, y a las obligaciones del responsable del fichero en relación a la recogida de datos, consentimiento de los afectados, cesión, transferencias

internacionales, datos de menores e incapaces, deber de secreto y tratamiento por cuenta del responsable del fichero.

En el año 2009 se inscribió el de farmaindustria, centrándose fundamentalmente en concretar una larga lista de definiciones, el ámbito de aplicación y los Protocolos de actuación en materia de Investigaciones clínicas, Farmacovigilancia, Derechos ARCO y Sistema de autorregulación.

Y por último, en el año 2011, se suma a los ya citados, el código tipo de tratamiento de datos de carácter personal para establecimientos sanitarios privados de la provincia de Sevilla, regulando básicamente lo relativo a las obligaciones principales de los sujetos que intervienen en el tratamiento de los datos, los principios de la protección de datos, los sujetos legitimados para el ejercicio de los derechos, la publicidad y prospección comercial, las obligaciones previas al tratamiento de los datos, las acciones encaminadas a mejorar el cumplimiento, la responsabilidad social con los derechos de los ciudadanos y el marco normativo, incluyendo además, unos protocolos de actuación en el tratamiento de datos de carácter personal en los establecimientos sanitarios privados adheridos al código tipo, lo cual debería ser una pauta a seguir por cualquier entidad que proceda al tratamiento de datos personales de cualquier tipo, cuestión que se abordará debidamente en el apartado de formación del personal.

V.3. UTILIDAD DE LOS DATOS DE LA HISTORIA CLÍNICA DENTRO Y FUERA DE LOS CENTROS SANITARIOS QUE LAS CONFIGURAN:

Las utilidades de los datos contenidos en los historiales clínicos de los pacientes son infinitas, sanitarias, docentes, judiciales, etc. Los usos de la historia clínica radican fundamentalmente en la adecuada asistencia al paciente, según se establece en el artículo

16.1: *"La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia"*.

Deberá garantizarse siempre el derecho de acceso, ya que, según establece el 16.2 *"cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten".*

Aunque el artículo 16.3 establece especialidades para fines específicos, al recoger que *"el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en la Ley General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos".* El segundo párrafo de este artículo establece en cambio las excepciones a la norma establecida anteriormente, estableciendo que *"se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso".* Y el último párrafo del 16.3 establece un uso especial por el interés general *"cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, General de Salud Pública, podrán*

acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos".

No obstante, y como excepción a lo establecido en el artículo 16 de la Ley de atención al paciente, según recoge el informe jurídico 0400 de la AEPD, sería posible que un médico funcionario público, accediese a la historia clínica para defenderse si se le hubiese abierto un procedimiento disciplinario, siempre que los datos que aportase fuese concluyentes para su defensión *"…sería posible su incorporación al expediente en caso de que el expedientado solicite dicha inclusión como medio de prueba, pudiendo en ese caso, dentro del trámite de audiencia que al interesado concede la legislación de procedimiento administrativo, acceder a la información incluida en las historias clínicas y efectuar las alegaciones que convengan a su derecho".*

También a este propósito, el informe 0611/2008 de la AEPD establece que *"… en el ámbito de la regulación de las historias clínicas, el artículo 16.3 de 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, dispone que "el acceso a la historia clínica con fines judiciales (…) se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de*

investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso".

Respecto a los usos de la historia clínica, una parte de la doctrina ha manifestado que *"…la historia clínica a nivel jurídico es considerada como un medio de prueba para valorar la existencia o inexistencia de responsabilidad médica"*[430]*.* Matizando a continuación que *"…este criterio tan genérico no se puede aplicar a todo tipo de historia, porque hay que diferenciar de la historia en papel y la historia clínica informatizada. El valor probatorio de la historia clínica con soporte papel y no a la informatizada de fácil manipulación"*[431]*.*

Este mismo sector, a propósito de la publicación del Real Decreto-Ley 14/1999 de 17 de septiembre, que regula el uso de la firma electrónica, manifiesta que *"…las HC informatizadas que tengan firma electrónica avanzada tiene el mismo valor jurídico que la historia clínica en soporte papel…"*[432]*.* Pero además sigue diciendo *"…que a las que únicamente se incorpore la firma electrónica no se les negarán los efectos jurídicos, ni serán excluidas como prueba, por el mero hecho de presentarse en forma electrónica"*[433]*.* De modo que, utilizando una forma segura en su procesamiento y custodia, tendrían ambas el mismo valor jurídico.

Otra parte de la doctrina manifiesta en cambio que *"dado que la historia clínica va a ser utilizada para múltiples usos, esta debe tener unas característica para que la utilización sea eficiente: única, una*

[430] CRIADO DEL RÍO, María Teresa y SEOANE PRADO, Javier: "*Aspectos médico-legales de la historia clínica"*. Colex, Madrid, 1999. Pág. 32.

[431] CRIADO DEL RÍO, María Teresa y SEOANE PRADO, Javier: *"Aspectos médico-legales de la historia clínica"*. Colex, Madrid, 1999. Pág. 32.

[432] Ibídem.

[433] Ibídem.

por cada persona física y jurídica, acumulativa de la información de todos los procesos asistenciales en un solo dosier, e integrada, por cada proceso asistencial debe contener un resumen"[434]*.* Y acotan aún más especificando que *"la HC debe tener unas características físicas, referidas a el soporte físico del documento, y otras intelectuales, relativos a los usuarios y forma de tratamiento"*[435]*.*

Juan Mejía ha manifestado sobre este tema que *"aunque el acceso a la HC debe tener una función asistencial, concurren a la postre una complejidad de intereses y fines, entre los que se encuentra la docencia e investigación, el uso de la información con fines estadísticos, como documento probatorio en procesos judiciales"*[436]*.* Además establece este autor que *"el uso de la HC sin disociación de los datos debe quedar mayoritariamente restringido en el ámbito sanitario"*[437]*.* Porque en opinión de este autor *"ciertamente las HC pueden tener un interés científico, pero no tiene ningún interés el identificar quien es el paciente"*[438]*.*

Respecto a este tema publica la Revista Española de Cardiología que: "Los hospitales generan cantidades ingentes de información clínica que tiene usos múltiples, con el asistencial como primordial. Para su correcta explotación, la información clínica, que habitualmente está en las historias clínicas, se almacena en bases de datos informatizadas"[439]. De lo que se puede deducir, y según ya se ha comentado anteriormente, no toda la información médica se encuentra dentro de las historias clínicas, ni tampoco todas las informaciones hoy en día están informatizadas.

---

[434] CURRIEL HERRERO, J y ESTÉVEZ LUCAS, J: "*Manual para la gestión sanitaria y de la historia clínica hospitalaria*", Editores Médicos, Madrid, 2000. Pág. 33.

[435] Ibídem.

[436] MEJÍA, Juan: "*Hacia un estatuto jurídico desarrollado de la Historia Clínica*". Diario La Ley 5638 de octubre de 2002.

[437] Ibídem.

[438] Ibídem.

[439] YETANO LAGUNA, Javier , LARAUDOGOITIA ZALDUMBIDE, Eva: *"Documentación clínica. Aspectos legales y fuente de información para las bases de datos hospitalarias".* Revista Española de Cardiología, Vol 7. Núm. Supl.C. Junio 2007.

V.3.a. Gestión interna de la información de la historia clínica, tanto manual como informatizada, desde las perspectivas médica y de la protección de datos:

Dentro de los centros sanitarios, hay una amplia gama de personal que maneja los datos personales y los destina a diferentes utilidades. Esto, multiplica sin duda los riesgos para los datos de carácter personal de los pacientes que se hacen más vulnerables, por lo que es preciso que las normas sean conocidas por todos ellos y se cumplan a rajatabla.

Un sector de la doctrina manifiesta en este sentido que *"…uno de los problemas más importantes que se producen en relación con los datos de salud es el de multiplicidad de usos que pueden darse de los mismos y, en consecuencia, de sus potenciales usuarios. Existe una utilización clara de estos datos en los que puede denominarse atención directa al enfermo. Aquí la información está protegida, en principio, por la deontología médica y por las normas jurídicas positivas que protegen el secreto médico…"*[440].Pero por otro lado aseguran que, *"…otro ámbito por el que es frecuente que circulen datos relativos a la salud de los pacientes es el administrativo, entendiendo como tal, las actividades instrumentales o de apoyo de la atención médica. Estamos ante el supuesto del uso de la información sanitaria para el control de la calidad de la asistencia médica por vía de reclamaciones, cuestiones relacionadas con la facturación, estudios de estadística, etc. El número de potenciales cesionarios de los datos se dispara: pagos de prestaciones a los que tendrán que hacer frente aseguradoras privadas y para cuya tramitación se exigirá una puntual justificación del tratamiento médico recibido por el asegurado"*[441].

[440] JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan, GONZÁLEZ GARCÍA, Celso: "*La protección de datos personales en el ámbito sanitario*". Editorial Aranzadi, Navarra 2002. Pág. 103.

[441] Ibídem. Pág. 104.

También con respecto a las utilidades de la historia clínica, publica Diario Médico: *"El uso de historias clínicas con fines no asistenciales ha reabierto la polémica sobre la protección de datos personales. En un debate organizado por Diario Médico sobre la materia, diversos expertos coincidieron en que el Sistema Nacional de Salud no garantiza a sus usuarios la debida confidencialidad (ver DM del 30-1-2006). En opinión de Nuria Terribas, del Instituto Borja de Bioética, "La Ley de Protección de Datos va bien para unas cosas, pero es necesario un apartado especial para la sanidad". Otro aspecto que deben mejorar es la concienciación de los profesionales y gestores"*[442].

Un uso muy particular y poco apropiado es el que se da a las historias clínicas en el caso publicado por el diario ABC: "La Agencia Catalana de Protección de Datos (ACPD) ha abierto un proceso sancionador a nueve hospitales públicos barceloneses por facilitar a la Generalitat historiales clínicos de pacientes para la elaboración de una encuesta sobre el uso del catalán en el ámbito sanitario, según afirmó a ABC un portavoz de la Agencia"[443].

V.3.b. Requisitos para la configuración de registros que permitan la externalización de las bases de datos configuradas:

Las bases de datos en el sector sanitario tienen muchas utilidades, según se ha visto, sobre todo asistenciales. Y como también se ha expuesto, tanto si se van a tratar interna como externamente, deben cumplir con lo establecido en la legislación sanitaria y de protección de datos personales.

[442] ARBÓS, Daniel: "Expediente por usa historias clínicas con fines no asistenciales". Diario Médico, viernes, 19 de enero de 2007. Europa Press. Pág 10.

[443] GUIL,J: "Expedientan a varios hospitales por dar historiales para una encuesta sobre el catalán". ABC, viernes 19 de enero de 2007. España. Pág 18.

Pero fuera de los centros sanitarios esa información puede tener un valor incalculable puesta en relación con otras bases de datos, habrá que extremar la vigilancia, en lo relativo sobre todo a la disociación de los mismos, tema ya expuesto en anteriores apartados. Esta es la idea, que después de todo lo expuesto, se terminará de perfilar en el siguiente apartado a la vista de las conclusiones.

VI. CONCLUSIONES Y PROPUESTAS BASADAS EN LA TEORÍA Y EN LA PRÁCTICA, PARA UN MEJOR APROVECHAMIENTO DE LA INFORMACIÓN MÉDICA, RESPETANDO LA NORMATIVA DE LA PROTECCIÓN DE DATOS.

VI.1. CONCLUSIONES:

Existe una tensión entre la protección de datos personales y la existencia de un sistema informático que permita a los profesionales de la sanidad obtener información actualizada y en tipo real de las experiencias de otros profesionales. En todo caso, esa información debería de estar disociada de los pacientes que dieron lugar a la experiencia que se comparte. En materia sanitaria es necesario y beneficioso para el paciente que fluya la información, pero esto debe ocurrir con las cautelas necesarias para evitar que la información médica de una persona sea divulgada de forma perjudicial para el mismo.

Las tecnologías de la información constituyen una gran ayuda para la medicina, pero presentan un gran riesgo para el paciente, pues el conocimiento de su enfermedad por personas ajenas al ámbito sanitario pueden suponer graves perjuicios. Las TICS constituyen un arma de doble filo que es necesario vigilar.

La historia clínica de un paciente debería abarcar toda la información médica de un paciente, independientemente de dónde se generó o se almacenó. Es un elemento clave para el tratamiento del paciente. Integrar toda la información sanitaria en misma historia clínica ofrece también un riesgo notable a la hora de proteger a la persona en su honor, intimidad y otros derechos frente a las TICS.

Las historias clínicas en sus diferentes utilidades constituyen también una fuente de información de primer orden para ser empleada como experiencia en casos similares, desarrollar

investigaciones, conocer estadísticamente la salud de la sociedad o servir como ejemplos en la docencia.

Pese a que el derecho a la protección de datos personales es relativamente reciente en nuestro país, ha calado de forma importante y hoy en día casi siempre se solicita a los pacientes la conformidad para el tratamiento de sus datos personales. Pese a ello existen muchas situaciones en las que Ley o por circunstancias de premura se exime del consentimiento del paciente. Por ejemplo cuando hay que tratar a un enfermo que no tiene consciencia.

En el ámbito sanitario para los médicos concurre el deber de secreto médico con el deber de secreto derivado de la protección de datos personales. Para el resto del personal sanitario ese deber de secreto procede del derecho a la protección de datos.

La propia actividad diaria en los centros sanitarios, en muchos casos motivados por la urgencia, hacen difícil cumplir todas las especificaciones de la protección de datos personales. Por ello, la normativa en esta materia debe de tener presente estas circunstancias propias del ámbito sanitario.

La protección de datos personales en el ámbito sanitario es manifiestamente mejorable. La mayor carencia en la protección de datos personales es la falta de formación y concienciación de quienes tratan los datos personales de los pacientes.

Es esencial la existencia un correcto documento de seguridad en donde se determinen las medidas necesarias. Dicho documento de seguridad debe ser conocido por personal en la medida de sus funciones y obligaciones en el ámbito de la protección de datos personales.

Existe una sobreabundancia de normas en materia sanitaria que afectan a la protección de datos personales y que no mejoran el sistema de protección y, que por el contrario, crean confusión y complejidad innecesaria. Cada norma trata de redefinir los conceptos

y a veces para un mismo concepto encontramos definiciones diferentes.

Aunque se ha invertido en sistemas informáticos, la inversión se ha realizado por las Comunidades Autónomas y falta una integración que permita un servicio global de sanidad. Es necesaria una gran base de datos a nivel de toda España que permita compartirse a nivel internacional. Lo esencial es permitir una interconexión en favor de la salud. La fragmentación del sistema sanitario español es injusto y disfuncional. En definitiva, debe existir un sistema común de intercambio de información sanitaria que permita aprovechar los recursos que existen.

La cesión datos personales en ámbito sanitario se ha contaminado por la mercantilización de la sanidad. Hemos podido comprobar que después de ser diagnosticada una enfermedad que precisa de determinados servicios, el paciente recibe ofertas de empresas que se dedican a ello. Debería establecerse claramente en los formularios de recogida de datos y de forma diferencial, por ejemplo con la necesidad de marcar una casilla, la autorización para ceder los datos.

Pese a que la protección de datos concede innumerables ventajas a favor de los pacientes, sin embargo, supone en algunos casos un freno a la investigación médica, ya que en muchas ocasiones, en este campo de la medicina, es necesario conocer la identidad del paciente al completo, para poder así concluir los estudios que se les estén realizado y proteger con ello en mayor medida la salud de los mismos.

VI.2. PROPUESTAS BASADAS EN LA TEORÍA Y EN LA PRÁCTICA, PARA UN MEJOR APROVECHAMIENTO DE LA INFORMACIÓN MÉDICA, RESPETANDO LA NORMATIVA DE LA PROTECCIÓN DE DATOS:

El modelo que propongo de puesta en común de historias clínicas es evidentemente informático. Sería interesante que existiese esta herramienta a nivel provincial, nacional e internacional, que rompiendo las barreras del espacio y el tiempo, que suele apremiar en medicina, fuese superado con la ayuda de la tecnología para, respectando siempre la confidencialidad de los datos, compartir esa información con el resto de la comunidad médica.

Tanto para el presente como para el futuro, el pasado, es decir, la experiencia ya vivida, supone un avance en el saber cómo obrar. Si se tiene un conocimiento previo sobre algo se va más rápido y seguro, y esto en el sector sanitario sería un gran logro.

La gestión de la sanidad a nivel autonómico, podría suponer sin embargo, un freno para esta propuesta, ya que, con el deber de respetar una normativa estatal, las diferencias de gestión entre unas comunidades y otras, podría plantear problemas a la hora de compartir la información, ya que se utilizan programas distintos creados por empresas distintas y configurados de forma distinta.

Desde luego habría que empezar desde abajo e intentar crear un sistema para compartir los datos personales en una misma comunidad, para luego compartirlos con otras comunidades, quizás a través del almacenamiento en unos servidores que contuviesen historias clínicas de forma disociada.

A primera vista podrían plantearse dos problemas, por un lado el enfrentamiento entre la legislación nacional y la autonómica que tendrían que conciliarse, ya que sin ir más lejos, en materia de protección de datos existe una legislación a nivel de comunidades autónomas y otra a nivel estatal. Y el otro gran problema sería el del

contenido de las historias clínicas, formada por datos objetivos de las pruebas realizadas y subjetivos de los profesionales que las crean, ya que para este sistema de puesta en común sería imprescindible la perspectiva de quien escribe la historia clínica a la vista de los resultados objetivos de las pruebas realizadas a los pacientes. En este sentido ¿Se podría “obligar” a los profesionales médicos a entregar esa parte de su opinión acerca de los datos subjetivos de un paciente? Ya hemos visto que no.

El concepto de esta propuesta sería una especie de sesión clínica multitudinaria y constante, todo ello gestionado informativamente, ya que de otro modo sería imposible reunir a tal número de profesionales, para que, compartiendo sus casos, pudiesen sacar provecho en beneficio de otros pacientes.

Probablemente la solución estaría en establecer los criterios a nivel internacional. Por nuestra parte, que a nivel europeo se crease un sistema de reporte de información, al igual que ya existe en determinados ámbitos esa cesión internacional de datos, en el que con un programa compartido para todos los países de un continente, se plasmasen una serie de datos fijos, ya que el dar la opción de ponerlo o no, probablemente empobrecería el proyecto.

Vista la realidad existente de esta puesta en común de datos a nivel autonómico, al igual que a nivel nacional e internacional, Podría darse la hipótesis de una gran base de datos para compartir información médica intercontinental a través de los organismos oportunos y con las debidas medidas de seguridad. Yo creo que estamos en el camino.

VII. FUENTES.

VII.1. BIBLIOGRAFÍA:

LUCAS MURILLO DE LA CUEVA, Pablo: *"La protección de los datos personales frente al uso de la informática"*. Editorial Tecnos, Madrid, 1990.

LUCAS MURILLO DE LA CUEVA, Pablo: "*Informática y Protección de Datos Personales"*. Centro de Estudios Constitucionales, Madrid 1993.

SANCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA, Manuel: *"Sobre la intimidad".* Fundación Universitaria San Pablo C.E.U., Valencia, 1.996.

FERNÁNDEZ BAJÓN, María Teresa: *"La profesión del documentalista: Apuntes para una reflexión"*. Boletín de la ANABAD, ISSN 0210-4164, Tomo 48, Nº 2, 1998.

HERRÁN ORTIZ, Ana Isabel: "*La violación de la intimidad en la protección de datos personales".* Dykinson, Madrid 1.999.

CRIADO DEL RÍO, María Teresa y SEOANE PRADO, Javier: "*Aspectos médico-legales de la historia clínica"*. Colex, Madrid, 1999.

CURRIEL HERRERO, J y ESTÉVEZ LUCAS, J: *"Manual para la gestión sanitaria y de la historia clínica hospitalaria"*. Editores Médicos, Madrid, 2000.

SAMPRÓN LÓPEZ, David: *"Los derechos del paciente a través de la información de la historia clínica"*. Edisofer, Madrid, 2002.

JAÑEZ RAMOS, Fernando Mª, ZAPATERO GÓMEZ-PALLATE, Juan, RAMOS SUÁREZ, Fernando, PUENTE SERRANO, Natalia, MUÑIZ CASANOVA, Natalia, SÁNCHEZ CRESPO LÓPEZ, Antonio, CARRASCO LINARES, Juan,

GONZÁLEZ GARCÍA, Celso: *"La protección de datos personales en el ámbito sanitario"*. Editorial Aranzadi, Navarra 2002.

ATELA BILBAO, Alfonso, BENAC URROZ, Mariano, CODÓN HERRERA, Alfonso, GARAY ISASI, Josu, GONZÁLEZ SALINAS, Pedro, HERNÁNDEZ-MARTÍNEZ CAMPELLO, Carlos, LIZARRAGA BONELLI, Emilio, MARTÍ MONTESINOS, Cristina, PELLEJERO GARCÍA, Carlos, PIDEVAL BORRELL, Ignasi, VILLAR ABAD, Gloria, GONZÁLEZ PÉREZ, Jesús: *"Autonomía del paciente, información e historia clínica"*. Editorial Aranzadi, Madrid 2004.

MEJÍA, Juan*. "Hacia un estatuto jurídico desarrollado de la Historia Clínica"*. Diario La Ley 5638 de octubre de 2002.

VIDAL RASO, Marta: *"Entorno de la Ley de Protección de Datos de Carácter Personal"*. Revista Top Franquicias Nº 7, Madrid, 2003.

DE MIGUEL SÁNCHEZ, Noelia: *"Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público"*. Tirant lo Blanch, Valencia, 2004.

BELL MALLÉN, José Ignacio (Coord.): "Comunicar para crear valor. La dirección de comunicación en las organizaciones." EUNSA, Navarra, 2004.

VIDAL RASO, Marta: *"¿Todavía no se ha adaptado a la Ley de Protección de Datos Personales?"*. Boletín Informativo nº57-Consulting Empresarial, Madrid 2005.

VIDAL RASO, Marta: *"El mundo empresarial se ve directamente afectado por la Ley de Protección de Datos de Carácter Personal"*. Revista ejecutivos nº 179, Madrid, 2007.

YETANO LAGUNA, Javier , LARAUDOGOITIA ZALDUMBIDE, Eva: "Documentación clínica. Aspectos legales y fuente de

información para las bases de datos hospitalarias." Revista Española de Cardiología, Vol 7. Núm. Supl.C. Junio 2007.

CENTENO SORIANO, Cristina: *"Operaciones administrativas y documentación sanitaria"*. Formación Alcalá, Jaén, 2007.

TERRIBAS I SALA, Núria: *"Aspectos legales de la atención a los menores de edad"*. Institut Borja de Bioética. Universitat Ramon Llull. FMC. 2008. Barcelona. España. Pags 367-73.

TERRIBAS I SALA, Núria: *"Los avances del derecho ante los avances de la medicina. Confidencialidad de los datos sanitarios: de la norma a la práctica médica"*. In Salomé Adroher Biosca-Thomson Aranzadi, 2008. Pags 796-802.

URSO, Elena, traducción Torre, E: *"Infancia, adolescencia y derecho a la salud en el hospital: el papel clave de los derechos fundamentales"*. Revista europea de derechos fundamentales. ISSN 1699-1524. Núm. 14/2ºsemestre 2009. Páginas 183-229.

PÉREZ FUENTES, Gisela María (coordinadora): *"Temas selectos de derecho a la información, derecho a la intimidad, transparencia y datos personales"*. Editorial Sista, S.A. Tabasco, 2010.

ARZOZ SANTIESTEBAN, Xavier, CALONGE CRESPO, Iñaki, ESPARZA LEIBAR, Iñaki, ETXEBERRIA GURIDI, José Francisco, GONZÁLEZ LÓPEZ, Juan José, ORDEÑANA GEZURAGA, Ixusco, PECHARROMÁN FERRER, Begoña, PÉREZ GIL, Julio, SUBIJANA ZUNZUMEGUI, Ignacio José: *"Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de datos personales"*. Tirant Lo Blanch, Valencia, 2011.

DIEZ-HOCHLEITNER, Javier, MARTÍNEZ CAPDEVILLA, Carmen, BLÁZQUEZ NAVARRO, Irene, FRUTOS MIRANDA, Javier: *"Últimas tendencias de la jurisprudencia del Tribunal de Justicia de la Unión Europea"*. La Ley, Madrid, 2012.

TERRIBAS I SALA, Núria: *"La confidencialidad en la relación terapéutica"*. Revista de psiquiatría infanto-juvenil número 2/2012 especia congreso, sábado 12 de mayo. Barcelona, 2012.

VIDAL RASO, Marta, *"Los datos sobre la salud de los ciudadanos"*. Encuentros Multidisciplinares, nº41, volumen XIX, mayo-agosto 2012. Fundación General de la Universidad Autónoma de Madrid, Madrid, 2012.

CANTORAL DOMÍNGUEZ, Karla: *"Derecho de protección de datos personales en la salud"*. Editorial Novum, MEXICO D.F., 2012.

RODOTA, Stefano, DUPRAT, Jean-Pierre, PIÑAR MAÑAS, José Luis, NIETO GARRIDO, Eva, HERNÁNDEZ CORCHETE, Juan Antonio: *"Transparencia, acceso a la información y protección de datos"*. Editorial Reus, S.A., Madrid, 2014.

SÁNCHEZ GONZÁLEZ, Santiago (coord.): *"Dogmática y práctica de los derechos fundamentales*". Tirant lo Blanch, Valencia 2015.

VII.2. RECURSOS ELECTRÓNICOS:

www.agpd.es

www.boe.es

www.rae.es

www.elpais.com

www.abc.es

www.elmundo.es

www.diariomedico.com

ww.expansión.com

www.eladelantado.com

http://definicion.de/outsourcing/

VIII. ANEXO LEGISLATIVO.

Carta de las Naciones Unidas, San Francisco, 26 de junio de 1945.

Declaración Universal de Derechos Humanos de la Unesco, 1948.

Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente.

Versión consolidada del Tratado de Funcionamiento de la Unión Europea, 25 de marzo de 1957.

Instrumento de Ratificación de España del Pacto Internacional de Derechos Civiles y Políticos, hecho en Nueva York el 19 de diciembre de 1966.

Constitución Española, 1978.

Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.

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.

Ley 14/1986, de 25 de abril, General de Sanidad.

Tratado de la Unión Europea, hecho en Maastrich el 7 de febrero de 1992.

Declaración para la promoción de los derechos de los pacientes en Europa, Amsterdam, 28-30 de marzo de 1994.

Real Decreto Legislativo 1/1994, de 20 de junio, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social.

Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales.

Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 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.

Real Decreto 1907/1996, de 2 de agosto, sobre publicidad y promoción comercial de productos, actividades o servicios con pretendida finalidad sanitaria.

Recomendación nº R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre Protección de Datos Médicos.

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, hecho en Oviedo el 4 de abril de 1997.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

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.

Carta Europea de los derechos de los pacientes, Roma, noviembre 2002.

Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la agencia vasca de protección de datos.

Declaración universal sobre Bioética y Derechos Humanos, 2005.

Ley 14/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida.

Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios.

Ley 14/2007, de 3 de julio, de Investigación biomédica.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Ley Orgánica 2/2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo.

Carta de los Derechos Fundamentales de la Unión Europea, 2010.

Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación.

Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.

Ley 33/2011, de 4 de octubre, General de Salud Pública.

Real Decreto-ley 16/2012, de 20 de abril, de medidas urgentes para garantizar la sostenibilidad del Sistema Nacional de Salud y mejorar la calidad y seguridad de sus prestaciones.

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Orden SSI/321/2014, de 26 de febrero, por la que se aprueba la política de seguridad de la información en el ámbito de la

administración electrónica del Ministerio de Sanidad, Servicios Sociales e Igualdad.

Real Decreto 81/2014, de 7 de febrero, por el que se establecen normas para garantizar la asistencia sanitaria transfronteriza, y por el que se modifica el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación.

Ley 9/2014, de 9 de mayo, de Telecomunicaciones.

Real Decreto-ley 9/2014, de 4 de julio, por el que se establecen las normas de calidad y seguridad para la donación, la obtención, la evaluación, el procesamiento, la preservación, el almacenamiento y la distribución de células y tejidos humanos y se aprueban las normas de coordinación y funcionamiento para su uso en humanos.

Orden SSI/1687/2014, de 9 de septiembre, por la que se modifica la Orden de 21 de julio de 1994, por la que se regulan los ficheros con datos de carácter personal.

Real Decreto 640/2014, de 25 de julio, por el que se regula el Registro Estatal de Profesionales Sanitarios.

Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.

Orden SSI/1885/2015, de 8 de septiembre, por la que se modifica la Orden de 21 de julio de 1994, por la que se regulan los ficheros con datos de carácter personal gestionados por el Ministerio de Sanidad y Consumo.

Real Decreto 69/2015, de 6 de febrero, por el que se regula el Registro de Actividad de Atención Sanitaria Especializada.

IX. GLOSARIO DE ABREVIATURAS.

CNU	Carta de las Naciones Unidas
DUDH	Declaración Universal de Derechos Humanos
CDHLF	Convenio de Derechos Humanos y Libertades Fundamentales
PIDCP	Pacto Internacional de Derechos Civiles y Políticos
CE	Constitución Española
CCEPP	Convenio 108
LODHIP	Ley del Derecho al Honor
LGS	Ley de Sanidad
TUE	Tratado de la UE
DPDPE	Declaración sobre Derechos de los pacientes
LGSS	Ley General de la Seguridad Social
LPRL	Ley de Prevención de Riesgos Laborales
DPECE	Directiva 95/46
RDPPS	Real Decreto sobre Publicidad Sanitaria
RCMCE	Recomendación sobre Protección de Datos Médicos
CDHB	Convenio de Derechos Humanos y Biología
LOPD	Ley de Protección de Datos Personales
LSSI	Ley de Sociedad de la Información y Comercio Electrónico
LAP	Ley del Paciente
CEDP	Carta de los derechos de los pacientes
LCS	Ley de calidad sanitaria
LFAV	Ley de ficheros públicos vasca
DUBDH	Declaración sobre Bioética y Derechos Humanos

LRA	Ley de reproducción asistida
LGM	Ley sobre uso de los medicamentos
LIB	Ley de Investigación Biomédica
RDPPS	Real Decreto de la Ley de protección de datos
LOA	Ley del aborto
CDF	Carta de Derechos Fundamentales de la UE
RDRM	Real Decreto sobre Receta Médica
LACPD	Ley de la Autoridad catalana de protección de datos
TFUE	Tratado de funcionamiento de la UE
LGSP	Ley General de Salud Pública
RD-LS	Real Decreto-Ley de sostenibilidad
LTAB	Ley de Transparencia
OSI	Orden de Seguridad Electrónica
RDAST	Real Decreto de asistencia sanitaria transfronteriza
LT	Ley de Telecomunicaciones
RD-LCT	Real Decreto-Ley de Células y Tejidos
OFDP	Orden sobre ficheros de datos personales
RDPS	Real Decreto de profesiones sanitarias
LTPA	Ley de Transparencia andaluza
OFMS	Orden sobre ficheros Ministerio de Sanidad y Consumo
RDASE	Real Decreto sobre atención especializada