Lucia Nicole CRISTEA UIVARU

LA PROTECCIÓN DE DATOS DE CARÁCTER SENSIBLE EN EL ÁMBITO EUROPEO.
Historia Clínica Digital y Big Data en Salud.

Tesis doctoral

dirigida por

Dra. Carmen PARRA RODRÍGUEZ

Universitat Abat Oliba CEU
Facultad de Ciencias Sociales
Programa de doctorado en Humanidades y Ciencias Sociales
Departamento de Derecho

2017

El secreto del éxito radica en la prontitud de las decisiones.

Resumen

El presente trabajo tiene por objeto el análisis de los problemas jurídicos vinculados y derivados de la incorporación de la historia clínica digital en el entorno sanitario, así como el análisis del cambio de paradigma que se vislumbra en el contexto del Big Data en el ámbito sanitario, que entra en colisión con la protección al derecho de intimidad y la confidencialidad de los datos de salud. Las bases que rigen los ordenamientos normativos vigentes, y el Reglamento General de Protección de Datos que entrará en vigor en el año 2018, no han resuelto aún la dicotomía entre el derecho a la protección de datos de carácter personal y los avances tecnológicos.

Resum

Aquest treball té per objecte l'anàlisi dels problemes jurídics vinculats i derivats de la incorporació de la història clínica digital a l'entorn sanitari, així com l'anàlisi del canvi de paradigma que s'albira en el context del Big Data a l'àmbit sanitari, que entra en col·lisió amb la protecció al dret de intimitat i confidencialitat de les dades de salut. Les bases que regeixen els ordenaments normatius vigents, i el Reglament General de Protecció de Dades que entrarà en vigor l'any 2018, no ha resolt encara la dicotomia entre el dret a la protecció de dades de caràcter personal i els avenços tecnològics.

Abstract

This work has for objective to analyze the juridical implications of incorporating digital clinical history in the healthcare environment, as well as to analyze the paradigm change enabled by big data, which challenges the right to privacy and confidentiality of healthcare data. The current regulatory environment, as well as the General Data Protection Regulation which will be adopted in 2018, have not yet solved the challenge between the right to data protection and the technological advances.

Palabras claves / *Keywords*

Protección de datos – Datos de salud – Historia clínica digital – Big Data – Intimidad y confidencialidad de los datos de salud – Receta electrónica – Reglamento General de Protección de Datos

Sumario

Introducción

El presente trabajo tiene por objeto el análisis de los problemas jurídicos vinculados y derivados de la incorporación de la historia clínica digital en el entorno sanitario, así como el análisis del cambio de paradigma que se vislumbra en el contexto del Big Data en el ámbito sanitario, que entra en colisión con la protección al derecho de intimidad y la confidencialidad de los datos de salud. El interés de dicho trabajo, viene motivado por la necesidad del reconocimiento del derecho a la protección de datos como un nuevo derecho fundamental en el ámbito normativo, tanto en el ámbito nacional como europeo, carente en la actualidad de una regulación específica, uniforme, consolidada y actualizada.

Para llevar a cabo el análisis de la situación actual, se ha partido inicialmente del estudio de las fuentes normativas referentes a la protección de los datos de salud, tanto en el ámbito de la Unión Europea, como en el ámbito nacional y autonómico, trazando un recorrido legislativo y jurisprudencial que a lo largo de estos últimos 50 años ha venido a configurar a la protección de datos como un nuevo derecho fundamental. Tras el análisis de los diversos ordenamientos sostenemos que es cada vez más notorio el requerimiento de independizar al derecho sanitario y convertirlo en una nueva rama del derecho, por lo que uno de los objetivos de este trabajo será el de ofrecer argumentos que sirvan para acercarnos a esta nueva disciplina jurídica.

Para alcanzar el objetivo de ésta Tesis, la investigación se ha desarrollado utilizando diferentes técnicas propias de la investigación jurídica. En primer lugar, desde la observación pragmática y descriptiva del uso de datos, mecanismos de recogida, del tratamiento y acerca de su utilización. En segundo lugar, y desde un punto de vista de investigación, nos centramos en la recopilación y el análisis de la legislación existente en la materia, tanto a nivel europeo como nacional, en el análisis de las diversas opiniones doctrinarias de referencia, en la jurisprudencia, en los informes del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE, y en los informes y resoluciones de las Agencias de Protección de Datos. En tercer lugar, y desde un punto de vista analítico, hemos interpretado si la legislación existente en materia de protección de datos, brinda o no respuesta a la utilización y al tratamiento de los mismos, y, en consecuencia, si salvaguarda nuestros datos personales.

Para obtener resultados el trabajo se ha estructurado en dos partes. La Primera Parte, se divide en cuatro Capítulos. En el primero de ellos, de carácter más introductorio, se parte de la definición de los conceptos objeto del análisis de la Tesis Doctoral, identificando cuál es el bien jurídico protegido por el derecho, a fin de poder analizar en profundidad qué es un dato, diferenciándolo de otras imprecisiones terminológicas, acotando el objeto de estudio para centrarnos en el contenido de los datos sensibles poniendo especial énfasis en los datos de salud.

En el segundo Capítulo de la Primera Parte, se realiza un análisis de los elementos jurídicos que vinculan a los datos de salud, analizando los principios jurídicos y éticos, que deben observarse a la hora del tratamiento de ésta categoría de datos, por parte del facultativo médico y del personal sanitario, para explicar los derechos que le asisten al interesado en relación con sus datos de salud y las sanciones que el ordenamiento legal establece en caso de su incumplimiento. Hemos considerado relevante analizar qué se entiende por tratamiento de los datos personales y cuáles son sus límites normativos, porque los datos por sí mismos no constituyen ningún riesgo. Lo que sí goza de amparo normativo es su tratamiento, según tendremos oportunidad de analizar, el hecho de que nuestros datos personales sean tratados por terceras personas conlleva un peligro, y este denominado “tratamiento” es lo que encuentra un paraguas legal y ético que profundizaremos en éste Capítulo.

El tercer Capítulo de la Primera Parte de este trabajo, es el núcleo del mismo, y en él se analizará la integración de los datos de salud, que se encuentran comprendidos en la historia clínica del paciente. En éste Capítulo profundizaremos desde el punto de vista legal, los requisitos que deben observarse en torno a la historia clínica, haremos un breve repaso a su origen, a su definición y a los aspectos que debe reunir, a su contenido, intentando delimitar los parámetros jurídicos que la historia clínica debe respetar, como factor fundamental en la relación médico-paciente. Finalmente, nos centraremos en analizar las diferentes corrientes doctrinarias en torno a la propiedad de la historia clínica, y la relevancia de ésta cuestión.

El Capítulo cuarto de la Primera Parte, resulta de esencial relevancia para el objeto de estudio de éste trabajo académico, y en él nos centraremos en profundizar y analizar desde el punto de vista jurídico y social, a través de la incorporación de las nuevas tecnologías, la evolución que se ha vislumbrado en las últimas décadas en lo referente a las especificidades que la digitalización incorpora en la historia clínica digital, su funcionalidad, los datos que debe contener, las medidas de seguridad que debe

respetar y las responsabilidades de los intervinientes en su consulta y redacción. Así mismo haremos referencia a otros documentos digitales, como son la receta digital y la tarjeta sanitaria digital.

En la Segunda Parte del trabajo, en el Capítulo primero, hacemos referencia al cambio de modelo económico y social con respecto al incremento del intercambio transfronterizo de datos personales entre los operadores públicos y privados, incluidas las personas físicas, las asociaciones y las empresas, como resultado de la vertiginosa evolución tecnológica y la globalización, siendo éstos elementos los que plantean nuevos retos para la protección de los datos personales tanto a nivel europeo como a nivel nacional.

La Protección de Datos ha surgido como respuesta al desarrollo de la sociedad y frente a la necesidad de la protección legal ante un ámbito absolutamente innovador hace tan solo unos treinta y cinco años. Estos avances requieren un marco más sólido y coherente para la protección de datos en la UE, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Por ello, si la información se refiere a datos de carácter personal, ésta ha de someterse a los principios y a las reglas establecidas, y controlarse de manera eficaz para evitar así una lesión en los derechos de los individuos. Si esa información incorpora además revelaciones sobre datos de salud, las garantías deben ampliarse.

Estas circunstancias llevan a plantearse la necesidad en la uniformización normativa, al menos, en la UE de la que formamos parte, a fin de que dichos avances no resulten vulneradores de un derecho fundamental, como lo es, la protección de datos. En base a ello, y con el fin de avalar un nivel análogo y elevado de protección de las personas físicas por lo que se refiere al tratamiento de los datos personales, debe ser equivalente en todos los Estados miembros, a la vez que se deben superar los obstáculos relacionados con la circulación de datos personales dentro de la UE, el nivel de protección de los derechos y la libertad de las personas físicas, sobre los que tendremos ocasión de profundizar en éste Capítulo.

Asimismo, nos centraremos en el estudio de las circunstancias que han dado lugar a la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al

tratamiento de datos personales y a la libre circulación de estos datos, y a su análisis. Esta nueva ordenación legal, entrará en vigor el 25 de mayo del año 2018 y derogará la Directiva 95/46/CE. El Reglamento General de Protección de Datos, introduce varias novedades englobadas en un nuevo modelo de protección de datos para Europa. Entre sus previsiones, destaca desde el cambio en la gestión de los datos, al uso responsable de la información. Esto conllevará dar un mayor protagonismo a una figura de nueva creación que es el Delegado de Protección de Datos, en el que recaerá la responsabilidad de determinar y adoptar las medidas que sean necesarias para garantizar la adecuada protección de los datos. Además, el Reglamento introduce en el marco de los datos de salud, dos nuevas categorías, como son los datos biométricos y los datos genéticos. También reformula algunos de los principios que inspiran la protección de datos e introduce otros nuevos, y realiza otras aportaciones novedosas que estudiaremos en éste Capítulo. Sin embargo, como tendremos oportunidad de exponer, las bases que rigen los ordenamientos normativos vigentes, y el Reglamento General de Protección de Datos, no han resuelto aún la dicotomía entre el derecho a la protección de datos de carácter personal y los avances tecnológicos.

Finalmente, en el Capítulo II de la Segunda Parte, estudiaremos el fenómeno incipiente denominado “Big Data” en el ámbito sanitario, analizando las ventajas que ofrece aunar la información sanitaria dispersa que se dispone de cada paciente y en diversos formatos, agrupándola y organizándola de forma tal, que redunde en el beneficio del paciente, pero también para el sector médico, para la organización hospitalaria, y para las farmacéuticas. Sin embargo, pondremos de manifiesto los inconvenientes que se intuyen en la implementación del Big Data en salud, entre los que destacan la anonimización de los datos que se muestra ajena y no es garantía de la no re-identificación de las personas, creando vulnerabilidad en torno a la información, y la necesidad de que la recopilación, el almacenamiento, el tratamiento y la confidencialidad de los datos sensibles quede garantizada, dotando de mayores garantías jurídicas a la protección de los datos de salud en este novedoso, incipiente pero inevitable entorno tecnológico.

Ciertamente, la información es un bien en sí mismo. Si añadimos a ese “bien” la peculiaridad de que se compone de información personal y sensible de las personas, cobra aún más magnitud. Y si sumamos que la forma de recopilar esos datos sensibles resulta extremadamente sencilla actualmente a través de la utilización de medios electrónicos, entonces es cuando debemos poner el énfasis en conocer con certeza quién recopila esos datos, quién dispone de ellos, para qué fin, y cómo nosotros

podemos impedir su utilización para fines que no han sido otorgados a dichos datos. Es en este punto donde la seguridad, el contenido y la manipulación o tratamiento de nuestros datos sensibles cobra máxima importancia tanto en el ámbito legal como social. Y a esta creciente preocupación se añade el factor transfronterizo. Nuestros datos ya no son objeto de las fichas en papel que antiguamente gestionaba la secretaria de un doctor, sino que han pasado a formar parte de bases de datos de grandes servidores que almacenan información, y todo este tráfico de datos trasciende nuestras fronteras y escapa a un control jurídico en la materia. Si bien la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el Real Decreto de la Ley Orgánica de Protección de Datos 1720/2007, de 21 de diciembre, la Ley 41/2002, de 14 de noviembre, básica reguladora de la Autonomía del Paciente, y el Reglamento General de Protección de Datos pretenden poner solución a ello, aún sin lograrlo plenamente, el fenómeno denominado Big Data se escapa a la legislación específica existente a nivel nacional y europeo.

PRIMERA PARTE

EL MARCO TEÓRICO DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER SENSIBLE

CAPÍTULO I

El marco teórico en torno a los datos de salud

SUMARIO: 1. El derecho a la protección de datos. 1.1. El bien jurídico protegido: la intimidad como derecho fundamental. 1.2. Límites normativos marcados por la Protección de Datos en el ámbito sanitario. 2. Definición jurídica: la búsqueda de la esencia del dato de salud. 2.1. Conjunto de definiciones actuales. 2.1.1. El dato de carácter personal. a) Breves consideraciones sobre la expresión "cualquier información". b) Breves consideraciones sobre la expresión "identificadas o identificables". 2.2. Datos sensibles o especialmente protegidos. 2.2.1. Los datos sensibles. 2.2.2. Los datos relativos a la salud. 2.2.3. Definiciones legales. a) Marco normativo español. b) Marco normativo internacional y europeo. b) 1. Marco jurídico internacional. b) 2. Marco jurídico español.

Introducción.

A lo largo de ésta primera parte de la investigación doctoral, y a fin de comprender adecuadamente lo que engloba el dato sanitario, resulta esencial una primera aproximación teórica en la que nos encargaremos de definir los conceptos que van a ser objeto de análisis a lo largo de este trabajo.

Para ello, iniciaremos el estudio del presente apartado analizando brevemente el derecho a la protección de datos y lo que abarca la protección de datos, identificando cuál es el bien jurídico protegido por el derecho, a fin de poder analizar en profundidad qué es un dato, diferenciándolo de otras imprecisiones terminológicas, acotando el objeto de estudio para centrarnos en el contenido de los datos sensibles, poniendo especial énfasis en los datos de salud.

A continuación, expondremos someramente el origen y posterior desarrollo normativo del derecho a la protección de datos, poniendo el acento, en la regulación normativa referente a los datos de salud, tanto en el ámbito internacional como en el ámbito español, trazando un recorrido legislativo y jurisprudencial que a lo largo de estos últimos 50 años ha venido a configurar a la protección de datos como un nuevo derecho

fundamental.

1. El derecho a la protección de datos.

La protección de datos es una materia de creación relativamente reciente. Podemos situar como punto de partida legislativo, la década del '60, coincidiendo con el desarrollo de la informática. Es en aquél momento cuando se vislumbra por parte del legislador una preocupación en torno a la protección de la intimidad de las personas.

El derecho a la protección de datos personales se configura en nuestro ordenamiento jurídico como un derecho fundamental en la Constitución Española[1] (en adelante, CE). En el Capítulo Segundo de la CE, donde se asientan los derechos fundamentales y las libertades públicas, tiene especial relevancia el Artículo 18.1 que garantiza el derecho a la intimidad personal. Esto conlleva una protección especial que el legislador asigna a los datos personales de los individuos, que ha servido como punto de partida de la legislación vigente al respecto y de las cada vez más frecuentes sentencias judiciales que los Tribunales se ven obligados a promulgar a fin de preservar este derecho contenido en nuestra Carta Magna, como analizaremos posteriormente.

Los datos personales que ampara el precepto constitucional, son datos absolutamente personalísimos, que sólo pueden pertenecer a un individuo en concreto y por ello podemos definirlo desde dos pilares: por un lado, el derecho a la protección de datos otorga la potestad a la persona cuyos datos pertenezcan a conocer quién tiene información sobre ella, cuál es dicha información, de dónde proviene y para qué finalidad se van a tratar sus datos; y por otro lado, este derecho se configura como el control sobre el uso que se hace de sus datos personales. Este control es lo que nos permite conocer qué datos nuestros se tratan y de qué manera, y ello conlleva a la necesidad de protección jurídica sobre los datos personales.

La terminología utilizada por la protección de datos se refiere de manera amplia al conjunto de normas y principios que regula el tratamiento de datos personales en todas sus etapas, es decir, desde su recolección, almacenamiento, circulación, publicación

[1] Artículo 18.1, de la Constitución Española de 27 de diciembre de 1978, modificada por reforma de 27 de agosto de 1992 (BOE núm. 207, 28.08.1992).

hasta su transferencia, tanto nacional como internacional[2]. Si bien existen diferencias terminológicas a la hora de la denominación. Así, por ejemplo, MURILLO DE LA CUEVA[3], cuando se refiere a la protección de datos habla del "derecho a la autodeterminación informática", por su parte BAZÁN[4] la denomina "habeas data" y sostiene que:

> Puede conceptuarse al hábeas data como una acción, una garantía constitucional, un procedimiento jurisdiccional de trámite especial y sumarísimo, un proceso constitucional o un recurso protectorio del derecho de autodeterminación informativa o derecho a la protección de los datos personales, frente a los posibles excesos del poder de registración precisamente de la información de carácter personal[5].

En otras palabras, a través del "hábeas data" el legitimado puede acceder al conocimiento de sus datos personales y al destino de tal información que se encuentre en archivos, registros, bancos de datos u otros medios técnicos, electrónicos, de carácter público o privado, de soporte, y, en determinadas hipótesis (por ejemplo, falsedad o uso discriminatorio de tales datos), se puede solicitar la supresión, rectificación, actualización o el sometimiento a confidencialidad de los mismos[6].

Por su parte la autodeterminación informativa[7] hace referencia, según SUÑÉ LLINÁS[8], a la decisión personal e intransferible de determinar qué es lo que cada uno de nosotros quiere que los demás sepan de nuestra persona, posibilidad que alcanza también al

---

[2] REMOLINA, N. *Recolección internacional de datos: un reto del mundo post-internet.* AEPD, Madrid, 2015, pp. 96 y ss.

[3] MURILLO DE LA CUEVA, P. L. *La construcción del derecho a la autodeterminación informática y las garantías para su efectividad.* Fundación Coloquio Jurídico Europeo, Madrid, 2009, pp. 11-12.

[4] BAZÁN, V. "El Hábeas Data y el Derecho de Autodeterminación Informativa en Perspectiva de Derecho Comparado". *Estudios Constitucionales*. Año 3, núm. 2, Chile, 2005, pp. 85-139. Disponible en Internet: <http://studylib.es/doc/7019100/el-h%C3%A1beas-data-yelderechodeautodeterminaci%C3%B3ninformat> [Consulta: 10 de septiembre de 2016].

[5] BAZÁN, V., op. cit., p. 90.

[6] Ibídem.

[7] Para profundizar más sobre la conceptualización de "autodeterminación informativa" véase: MURILLO DE LA CUEVA, P. L., op. cit., pp. 11-12.; MARTÍNEZ MARTÍNEZ, R. *Una aproximación crítica a la autodeterminación informativa. Civitas*, Madrid, 2004, pp. 61 y sig.

[8] SUÑÉ LLINÁS, E. La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina. Tesis presentada en la Universidad Complutense de Madrid, Madrid, 2013, p. 132. Disponible en Internet: <http://eprints.ucm.es/22832/1/T34731.pdf> [Consulta: 17 de septiembre de 2016].

derecho a conocer los datos propios que obran en archivos ajenos y en este punto se relaciona directamente con la protección de los datos de carácter personal, lo que no deriva únicamente en la visión que los demás puedan tener de nuestra persona, sino, yendo más lejos, en la definición de nuestra propia identidad a partir de datos nuestros, que no obstante y por circunstancias de la vida, pudieran ser desconocidos para nosotros. Según refiere, como la protección de nuestro propio ser, de nuestra identidad, de nuestra personalidad[9].

A través de su jurisprudencia[10], el Tribunal Constitucional (en adelante, TC) ha evolucionado desde la concepción del derecho a la intimidad como un límite a la informática, a un nuevo y distinto derecho a la libertad informática, entendido como el derecho a la protección de los datos personales y a la autodeterminación informativa.

El TC, al abordar un asunto vinculado a la protección de datos, sostuvo en la STC 254/93 que:

> Nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales[11].

Asimismo, ya en el año 2000, el TC pondera la protección de datos como un derecho fundamental, diciendo que:

> El objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza

[9] Ibídem.

[10] Entre las más destacadas: STC 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad planteado respecto de los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, Fundamento Jurídico 7 (BOE núm. 4, 4.01.2001, Suplemento, pp. 104-117); STC 53/1985 de 11 de abril (BOE núm. 119, 18.05.1985); y STC 290/2000, de 30 de noviembre de 2000. Recursos de inconstitucionalidad contra diversos artículos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (BOE núm. 4, 4.01.2001, 70-93).

[11] STC 254/1993, de 20 de julio de 1993 del Tribunal Constitucional. Recurso de Amparo núm. 1827/1990 (BOE núm. 197, 18.8.1993).

> a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo[12].

Con oportunidad de la STC 292/2000, el TC diferencia, el derecho a la libertad informática del derecho a la intimidad otorgándole una finalidad, un objeto y un contenido propio. Además, saca conclusiones sobre el significado y el contenido del derecho a la protección de datos personales, haciendo un análisis acertado desde nuestro punto de vista, y manifestando que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporciona a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, al mismo tiempo que permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular.

Ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos. Concretamente, determinó la STC 292/2000 que el derecho fundamental a la protección de datos protege cualquier tipo de dato personal, sea o no íntimo manifestando que:

> El objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art.

[12] STC 290/2000, op. cit.

> 18.1 CE otorga, sino los datos de carácter personal". Asimismo, añade que: "Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que, a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido[13].

Pareciera ser que tanto la doctrina, como la jurisprudencia, y las normas, han cambiado las denominaciones, pero, en realidad, cuando se habla de protección de datos o lo que es lo mismo, de "habeas data", hay que entender la referencia a la autodeterminación informativa y viceversa[14].

1.1. El bien jurídico protegido: la intimidad como derecho fundamental.

Es imposible hablar de los datos personales sin hacer referencia a su fundamento legal, que, en definitiva, es el bien jurídico que la normativa protege. Su génesis se encuentra en el *derecho a la intimidad*, derecho fundamental reconocido por nuestra CE, como adelantamos. En España, el Derecho a la Protección de Datos es un derecho fundamental, que se articula sobre la dignidad de la persona reconocido en el Artículo 10 de la CE[15], sobre su honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, reconocidos en el Artículo 18[16] de la CE, además de disponer que la ley limitará el uso de la informática para garantizar el honor y a la intimidad.

Con objeto de desarrollar el párrafo 4 del citado artículo 18.4, fue aprobada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[17] (en adelante, LOPD), que a día de hoy es el eje de la protección de datos en España,

---

[13] STC 292/2000, op. cit.

[14] SUÑÉ LLINÁS, E., op. cit., pp. 132-133.

[15] El Artículo 10, de la CE establece que: *"La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social".*

[16] El Artículo 18, de la CE establece que: *"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 4. 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".*

[17] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE núm. 298, 14.12.1999).

estando a la espera de la entrada en vigor en mayo del año 2018 del Reglamento General de Protección de Datos, pero que a la fecha de redacción de la presente Tesis Doctoral aún no es vigente[18].

El concepto jurídico de intimidad, tuvo su origen en un artículo de los juristas WARREN y BRANDEIS[19] en el que se reclamó la necesidad de reconocimiento de un nuevo derecho, denominado derecho a la intimidad. En ese primer momento, éste derecho se configuró como necesario para proteger a la persona frente a las intromisiones de los medios de comunicación. Surgió como la búsqueda de un límite jurídico que vedase las intromisiones de la prensa en la vida privada, para evitar las lesiones que la difusión generalizada de hechos relativos a la vida privada podía provocar. Sin embargo, el derecho a la intimidad debía a su vez limitarse para convivir con otros bienes y derechos fundamentales, como la libertad de expresión y el derecho a la información.

A partir del momento de este reconocimiento legal, el derecho a la intimidad pierde su vertiente más patrimonial para consagrarse como el derecho que posee toda persona para protegerse de las intrusiones ajenas respecto a su vida privada. De éste modo, la libertad individual pasa a ser el fundamento del derecho a la intimidad, que deja de ser un derecho de propiedad, para convertirse en un derecho por sí mismo, el derecho a la protección de datos[20].

Entiende PIÑAR MAÑAS[21] que, el reconocimiento pleno de la protección de datos estriba en que los datos personales son sometidos a tratamiento, lo cual implica que se tratan datos ajenos, y que los mismos deben utilizarse con estricto respecto a los

---

[18] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DOUE L 119, 4.05.2016, pp. 1-88).

[19] Vid. WARREN, S. D.; BRANDEIS, L. D. "The right to privacy". *Harvard Law Review*. Vol. IV, núm. 5, 1890, pp. 193 y ss.; PENDÁS, B.; BASELGA, P. *Derecho a la intimidad / SAMUEL WARREN, LOUIS BRANDEIS*. (Traducción). Civitas, Madrid, 1995.; WESTIN, A. *Privacy and Freedom.* Athebeum, New York, 1967, p. 7.

[20] La primera Constitución que recoge este derecho fundamental fue la portuguesa en el año 1976, donde en su Artículo 35 hacía referencia a "dato" para luego ser modificada en el año 1982 y ampliar el concepto a "datos personales", y finalmente en el año 1989 dotar de más protección al derecho. Para profundizar más sobre el tema, véase: TRONCOSO REIGADA, A. *La protección de los datos personales. En busca del equilibrio.* Tirant lo Blanch, Vol. 1, Valencia, 2010, pp. 49-50.

[21] PIÑAR MAÑAS, J. L. *Legislación de Protección de Datos.* Iustel, Madrid 2011, pp. 34-35.

derechos del interesado. Es por ello, que, el legislador le otorga la máxima protección porque, en definitiva, estamos hablando de la dignidad humana. En el mismo sentido, SUÑÉ LLINÁS[22] entiende que el carácter primordial reside, en realidad, en la autodeterminación informativa, verdadero derecho fundamental que enlaza en la esencia misma de la dignidad humana. Por su parte, GARRIGA DOMÍNGUEZ[23] sostiene que la Ley de Protección de datos pretende proteger la propia personalidad del individuo, de forma mediata a través de la posibilidad inmediata que el individuo tiene sobre la información que le concierne, posibilitando su control.

Recientemente, el Magistrado SALCEDO[24], Presidente de la Sección 9ª de la Audiencia Provincial de Barcelona, ha manifestado en el marco del 1r Congrés de l'Advocacia de Barcelona que: *"El derecho a la intimidad es una derivación del derecho a la dignidad. Y por ello, el referido derecho a la intimidad ha venido a construirse como un derecho propio y que es necesario para mantener una calidad de la vida humana".* Prosiguió el Magistrado haciendo una reflexión muy importante: *"la intimidad es un derecho a ser desconocido, lo cual constituye las lindes de nuestra vida privada"*. Por lo tanto, y consecuentemente con lo esgrimido por SALCEDO[25], se genera un doble deber, por un lado, el deber jurídico de abstención, y, por otro lado, el deber jurídico de no hacer uso de lo conocido.

Sostiene al respecto, HERRÁN ORTIZ[26] que:

> Si bien es cierto que el derecho a la protección de datos nace vinculado a la idea de intimidad, ha de superarse esta concepción y avanzar en el reconocimiento de un nuevo derecho fundamental, que en la actualidad se configura a partir de la atribución de un haz de facultades de actuación y control que permiten a la persona decidir sobre la información que le concierne.

Por tanto, podemos definir el derecho a la intimidad desde dos perspectivas. Una

[22] SUÑÉ LLINÁS, E., op. cit., p. 134.

[23] GARRIGA DOMÍNGUEZ, A. *Tratamiento de datos personales y derechos fundamentales.* 2ª Edición, Dykinson, Madrid, 2009, p. 53.

[24] SALCEDO, A. (30.06.2016) El delicte de revelació de secrets: especial menció a l'aportació de documents en procediments judicials. Ponencia celebrada en el marco del 1r Congrés de l'Advocacia de Barcelona, celebrado el 30 de junio de 2016, ICAB, Barcelona. Disponible en Internet: <www.congresadvocaciabcn.cat> [Consulta: 1 julio 2016].

[25] Ibídem.

[26] HERRÁN ORTIZ, A. I. *El derecho a la protección de datos personales en la sociedad de información.* Universidad de Deusto, Instituto de Derechos Humanos, Bilbao, 2003, p. 21.

perspectiva con efecto restrictivo, en la que se define como el espacio reservado a los asuntos de la persona frente a interferencias ajenas, es decir, en cuanto reserva, supone que hay un espacio de actividad que es exclusivo del individuo y que no puede ser conocido por otros sujetos. Y desde otra perspectiva, un efecto de control, como la oposición al conocimiento y manejo de la información del titular, especialmente en bases de datos, sin su consentimiento.

La nota característica de ser un derecho fundamental, le otorga tres diferencias sustanciales, Por un lado, es un derecho irrenunciable, por otro lado, prevalece sobre otros derechos fundamentales y, finalmente, es un derecho personalísimo. Es por ello, que se protege el derecho a la intimidad no sólo frente a las injerencias, sino también frente a los riesgos potenciales[27].

Por tanto, el bien jurídico protegido es la intimidad. La intimidad de la persona no sólo entendida como relativa a su vida sexual, la salud, sino que también se extiende esa protección jurídica incluso a datos relativos al estado económico, al contenido de una agenda, a la reseña de una fotografía, datos que antes de la reforma del Código Penal (en adelante, CP), no contaban con un nivel de protección tan alto como lo es ahora, equiparable a los datos sensibles. Por ello, el concepto de la intimidad se ha vinculado con el concepto de privacidad para reforzar el derecho a la protección de datos[28].

1.2. Límites normativos marcados por la Protección de Datos en el ámbito sanitario.

El derecho a la protección de datos no es ilimitado, y es la CE la que permite que se pongan límites legislativos a éste derecho fundamental. Al respecto, la CE establece 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"*[29]. Además,

---

[27] SALCEDO, A., op. cit.

[28] El concepto de privacidad o *privacy* en inglés, ha sido interpretado por la doctrina de muchas maneras y no se ha logrado un consenso sobre su alcance y definición. Para profundizar más el tema, véase: SOLOVE, D. J. "Understanding Privacy". *USA Hardvard University Press*. Estados Unidos, 2008, p. 2.; WESTIN puntualizó que *privacy* es el derecho de las personas, grupos o instituciones para determinar por sí mismos cuándo, cómo y en qué medida la información sobre ellos se comunica a otros. WESTIN, A. op. cit., p. 7.; FRIED sostiene que *privacy* abarca el control que los individuos tienen sobre su información. FRIED, C. "Privacy". *Yale Law Jurnal*, Estados Unidos, 1968, p. 483.

[29] Artículo 18.4, de la CE.

estos límites han de estar constitucionalmente previstos y sólo se justificará recogerlos, almacenarlos y tratarlos por parte de un poder público, si ello responde a la protección de otros derechos o bienes que también estén tutelados por la Constitución[30].

Los límites normativos a la protección de los datos de carácter personal, vienen dados por las garantías que han de observarse por parte de las personas que los recogen, los tratan y los usan. En este sentido se ha pronunciado el TC con ocasión de la STC 254/1993[31] con carácter general, como anteriormente hacíamos referencia. Éste pronunciamiento tiene su origen en el Recurso de Amparo presentado contra la denegación por parte del Gobernador Civil de Guipúzcoa y del Ministro de Interior, de la comunicación de la información que había solicitado el actor acerca de sus datos de carácter personal que obraban en ficheros automatizados de la Administración del Estado.

El TC estima el recurso de amparo, considerándose que:

> Se ha vulnerado el derecho a la intimidad, basándose en que las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración Pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el art. 18 C.E., y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos, y ha de ser salvaguardado por este Tribunal, haya sido o no desarrollado legislativamente[32].

Asimismo, la Jurisprudencia se manifestó a través de la STC 143/1994[33], sosteniendo que un régimen normativo que autorizase la recogida de datos personales, incluso con fines legítimos, vulneraría el derecho a la intimidad si no incluyese garantías adecuadas frente al uso potencialmente invasor de la vida privada del ciudadano a través de su tratamiento informático, al igual que lo harían las intromisiones directas en el contenido nuclear de ésta. Éste veredicto tiene su origen en el Recurso contencioso-administrativo que el Consejo General de Colegios de Economistas interpuso contra las disposiciones reglamentarias que regularon la composición y la forma de utilización del Número de

[30] Vid. LESMES SERRANO, C. (Coordinador). *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia.* Lex Nova, Valladolid, 2008, p. 58.

[31] STC 254/1993, op. cit.

[32] Ibídem.

[33] STC 143/1994, de 9 de mayo de 1994 (BOE núm. 140, 13.05.1994).

Identificación Fiscal (N.I.F.), por considerar que vulneraban el derecho fundamental a la intimidad consagrado en el Artículo 18 CE, y que adolecían de defectos procedimentales y formales que acarreaban su nulidad de pleno Derecho, por la ausencia de garantías sobre el uso de la información obtenida a través de las operaciones identificadas con el N.I.F. El TC desestima el Recurso, porque entiende que la norma impugnada no legítima por sí misma la manipulación o difusión de datos que no esté estrechamente conectada con la finalidad que autoriza su recogida, y entiende que, de producirse infracciones, existen mecanismos legales para poder denunciarlos en concreto. Sostiene el TC al respecto, que:

> No puede afirmarse que las disposiciones reglamentarias desconozcan por sí mismas de estas garantías. El Real Decreto 338/1990, lo mismo que su orden de desarrollo, forman parte de un conjunto normativo que introduce garantías suficientes frente al eventual uso desviado de la información que aquellas normas permiten recabar. En este marco destaca, en desarrollo del art. 18.4 C.E., la Ley Orgánica de 29 de octubre de 1992, de regulación del tratamiento automatizado de los datos de carácter personal, que aparte, de las reglas generales sobre tratamiento de datos […], establece normas específicas para restringir el defecto que la parte imputa a la norma reglamentaria impugnada. En concreto, garantizándose la seguridad de los archivos (art. 9), imponiéndose un deber específico de secreto profesional, incluso después de finalizadas sus tareas al respecto, al "responsable del fichero automatizado y (a) quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal" (art. 10) e impidiendo la transmisión de datos de carácter personal almacenados, con la excepción de que concurra el consentimiento del interesado, la autorización legal específica o la conexión y reconocida necesidad de la transmisión de datos para el logro de finalidades constitucionalmente relevantes (art. 11) en las condiciones dispuestas en la norma[34].

2. Definición jurídica: la búsqueda de la esencia del dato de salud.

2.1. Conjunto de definiciones actuales.

Es frecuente referirse a los datos de salud como datos personales o datos sensibles. De hecho, en la práctica cotidiana, se hace referencia a los datos de salud de forma amplia y poco precisa, tratándolo indistintamente como dato de carácter personal,

[34] Ibídem.

información personal, datos sensibles, etc. No obstante, el "dato sanitario" es independiente de las otras expresiones y, por tanto, su conceptualización resulta esencial, desde la perspectiva jurídica a la que se va a dedicar esta investigación.

Tanto la legislación como la doctrina han puesto de relieve la necesidad de definir con rigurosidad y certeza el concepto de "dato sanitario" para evitar las confusiones que su uso terminológico incorrecto puede acarrear en relación con el nivel de seguridad y protección jurídica que el "dato" debe ofrecer en virtud de tratarse de un "dato de carácter personal", un "dato sensible" o un "dato de salud".

Sostiene REMOLINA[35], que el tratamiento jurídico sobre la información personal no es uniforme y depende de la naturaleza o de los riesgos o efectos que pueda ocasionar cada tipo de información. Por eso, la clasificación jurídica de dato personal, es relevante en la medida en que define los parámetros que deben observarse en su tratamiento por parte de terceros. Las pautas, procesos o protocolos que debe observar el tratamiento de determinada información personal, dependen de la naturaleza del dato, siendo por ello de vital importancia tener presente la calificación (jurisprudencial o legal) de los datos personales para que, a partir de ella, el Responsable o Encargado adopte las medidas concretas que debe impregnar el tratamiento de determinado dato personal.

A raíz de la promulgación de diferentes normas al respecto de los datos personales[36], es menester en este punto llevar a cabo una aproximación terminológica de lo que jurídicamente debe entenderse por "dato de carácter personal", "dato sensible" y finalmente "dato sanitario".

2.1.1. El dato de carácter personal.

Nos parece adecuado iniciar precisando a qué nos referimos como dato personal y diferenciarlo del dato sensible, porque se trata de expresiones que comúnmente se

[35] REMOLINA, N., op. cit., p. 72.

[36] LOPD, op. cit.; 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 (BOE núm. 17, 19.01.2008); Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN (BOE núm. 242, 9.10.2007); Ley 14/2007, de 3 de julio, de Investigación Biomédica (BOE núm. 159, 4.07.2007).

utilizan de forma indistinta, pero que, sin embargo, jurídicamente tienen una connotación diferente y específica, lo cual resulta determinante en ésta investigación doctoral, como hemos hecho referencia anteriormente.

Los datos de carácter personal, son la referencia que nos hace individualizables. Consiste en toda aquella información relevante concerniente a una persona que nos hace identificables. Se considera que una información hace referencia a una persona física[37], cuando la misma es suficiente para que podamos reconocer al individuo cuyos datos se suministran.

Podemos delimitar dos características significativas, por un lado, que el concepto de dato personal es muy amplio, puesto que abarca cualquier tipo de información[38] respecto de una persona física (edad, nombre y apellido, DNI, datos de carácter cultural, aficiones, correo electrónico, estado civil, número de cuenta bancaria, etc.), y, por otro lado, que no es necesario que la persona se encuentre totalmente identificada, sino que basta que resulte identificable[39].

Por tanto, podemos definir el dato personal como aquel que se ocupa de la información acerca de las personas, independientemente del medio que se utilice para recogerla, guardarla, tratarla, utilizarla, elaborar registros o transferirla a otros terceros. El elemento fundamental para determinar que se trata de un dato de carácter personal es que la información, por sí misma o combinada, permita conocer datos de una persona concreta, bien por estar directamente identificada a través de algún dato, o bien porque pueda llegar a ser identificada por otro medio.

[37] Los datos personales hacen referencia únicamente a personas físicas, no jurídicas. El hecho de que los datos personales se contemplen con relación al honor, la dignidad, la intimidad y la imagen es lo que ha excluido de su ámbito aquellos datos relativos a personas jurídicas, que, en principio, se entiende que no tienen datos personales.

[38] Esta información puede manifestarse de diferente manera (alfabética, numérica, fotográfica, gráfica, y acústica), pero debe referirse siempre a una persona física identificada o identificable para tener la consideración de dato de carácter personal.

[39] Sobre la definición de dato personal, véase: Dictamen 4/2007 del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE, 4/2007, sobre el concepto de datos personales, 20.06.2007 (WP 136). Disponible en Internet: <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm> [Consulta: 11 de septiembre de 2016].

Sostiene SANTAMARÍA RAMOS[40] que: *"La información consiste ni más ni menos en un conjunto organizado de datos que permiten obtener el conocimiento necesario para la toma de decisiones"*. El autor advierte sobre los peligros futuros que los datos y su posterior tratamiento y recolección pueden conllevar, manifestando que: *"El dato se ha convertido en la unidad básica de la sociedad de la información, y por tanto cualquier organización se encuentra en la necesidad de recolectar datos de carácter personal como forma de maximizar sus beneficios"*[41].

Como punto de partida, las diferentes normativas que legislan sobre datos personales[42], coinciden en la conceptualización del dato de carácter personal, recogiéndolo como "cualquier información relativa a una persona física identificada o identificable". A pesar de esta aparente uniformidad, la utilización de esta definición resulta demasiado amplia e imprecisa[43]. En este sentido se ha pronunciado el Grupo de Trabajo del Artículo 29[44], manteniendo que: *"ésta definición refleja la intención del legislador europeo de mantener un concepto amplio de datos personales"*[45].

---

[40] SANTAMARÍA RAMOS, F. J. *El encargado independiente. Figura clave para un nuevo Derecho de protección de datos.* La Ley grupo Wolters Kluwer, Madrid, 2011, pp. 512-513.

[41] Ibídem.

[42] A nivel español, el Artículo 3.a) de la LOPD, el Artículo 5.1.f) del RD 1720/2007; a nivel de Comunidades Autónomas, el Artículo 3.a) de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid (BOE núm. 245, 12.10. 2001); y Artículo 3.a) de 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 (BOPV núm. 44, 4.03.2004); a nivel del Consejo de Europa, el Artículo 2.a) del Convenio Nº 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 el 27 de enero de 1984 (BOE núm. 274, 15.12.1985, pp. 36000-36004); y, finalmente, a nivel de la UE, el Artículo 2.a) 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 (DOUE L 281, 23.11.1995, pp. 31-50); Artículo 2.a) del Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DOUE L 8, 12.01.2001, pp. 1-22).

[43] PIÑAR MAÑAS, J. L. "Concepto de datos de carácter personal", en TRONCOSO REIGADA, A. *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Civitas, Madrid, 2010, p. 193.; DEL CASTILLO VÁZQUEZ, I. C. *Protección de datos: cuestiones constitucionales y administrativas: (el derecho a saber y la obligación de callar).* Thomson-Civitas, Navarra, 2007, p. 329.

[44] El Grupo de Trabajo del Artículo 29, se creó en 1996 (en virtud del Artículo 29, de la Directiva 95/46/CE), con carácter consultivo y está compuesto por representantes de las autoridades nacionales de control de la protección de datos (ACPD) de cada Estado miembro, el Supervisor Europeo de

Probablemente el legislador europeo ha querido esta extensión en la definición jurídica del concepto de dato de carácter personal, para que perdurara en el tiempo sin que fueran necesarias reformas al respecto, y, de hecho, ahora se están planteando reformas desde el ámbito europeo, veinte años después, tal y como profundizaremos en la última parte de éste trabajo. Sin embargo, ésta amplitud terminológica ha sido objeto de numerosas consultas a la Agencia Española de Protección de Datos (en adelante, AEPD), para que clarificara si diversos conceptos estaban o no alcanzados por la normativa de protección de datos[46].

Protección de Datos (SEPD) y la Comisión Europea. Las funciones del Grupo de Trabajo reconocidas por la Directiva incluyen estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la Directiva 95/46/CE, emitir dictámenes sobre el nivel de protección existente dentro de la Comunidad y en países terceros, asesorar a la Comisión sobre cualquier proyecto de modificación de la Directiva 95/46/CE, y formular recomendaciones sobre cualquier asunto relacionado con la protección de datos en la Unión Europea. El Grupo de Trabajo se pronuncia a través de Dictámenes, Documentos de Trabajo, Informes o Recomendaciones, aunque también manifiesta su posición en cartas o comunicados de prensa. Las decisiones del Grupo no son jurídicamente vinculantes, pero tienen un importante valor doctrinal y son frecuentemente utilizados y citados por los legisladores y los tribunales nacionales y europeos. <http://ec.europa.eu/justice/data-protection/index_es.htm> [Consulta: 19 septiembre 2015].

[45] Dictamen 4/2007, del Grupo de Trabajo del Artículo 29, op. cit.

[46] Vid. Informe jurídico de la AEPD, 0034/2010 en el que se plantea la cuestión de considerar si el número de una finca registral constituye un dato personal, conforme a la LOPD y en que la AEPD concluye que: *"el número de una finca registral, es el que se otorga a la inscripción de la finca, por lo que conociendo dicho número podemos conocer el contenido de la inscripción en el que aparecerá entre otro tipo de información; "la persona natural o jurídica a cuyo favor se haga la inscripción y la persona de quien procedan inmediatamente los bienes o derechos que deban inscribirse". Por tanto enlazando este concepto con las definiciones previstas tanto en la Ley Orgánica 15/1999 y su reglamento de desarrollo, habrá de concluirse que el número de finca registral es un dato identificable".* Informe jurídico de la AEPD 0034/2010, Disponible en Internet: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2010-0034_El-n-uu-mero-de-finca-registral-es-un-dato-identificable.pdf> [Consulta: 18 septiembre 2016]; Informe jurídico de la AEPD 0153/2014 que plantea si las imágenes captadas por cámaras panorámicas de diversas ciudades españolas constituyen datos de carácter personal, entendiendo la Agencia que en la medida de que esas personas no resulten identificables a raíz de dichas imágenes, por carecer de un zoom las cámaras u otras herramientas que permitan aproximar la imagen de forma que los transeúntes resulten identificados, no es objeto de aplicación de la LOPD. Informe jurídico de la AEPD 0153/2014. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdf_destacados/2014-0153_C-aa-maras-panor-aa-micas._Inexistencia-de-datos.pdf> [Consulta: 18 septiembre 2016].

En este punto, cabe matizar que ésta definición que brinda la legislación en materia de datos personales, hace referencia a "cualquier información" y también se refiere a una persona "identificada o identificable". Pero, ¿a qué se refiere exactamente con dichas expresiones? A continuación, esbozaremos unas breves consideraciones a tener en cuenta sobre estos conceptos.

a) Breves consideraciones sobre la expresión "cualquier información".

Tal y como se ha hecho referencia anteriormente, con la finalidad de dotar de una extensa protección a los datos personales, el legislador emplea la fórmula "cualquier información" para incluir información de carácter variable relacionada con la información numérica, alfabética, gráfica, fotográfica[47], acústica, o de cualquier otro tipo concerniente a personas físicas identificadas o identificables[48]. Es evidente la intención de dotar de amplitud esta expresión y la palabra "cualquier" es la que permite ese abanico tan extenso de "información" que al fin y al cabo permitirían identificar a una persona, o a raíz de la información de la que se disponga, determinada persona resulte claramente identificable.

[47] Respecto a la información fotográfica, la AEPD se ha pronunciado entendiendo que la publicación de una fotografía de una festividad de moros y cristianos no necesita recabar el consentimiento informado de las personas que en ella aparecen por ser de interés público. Informe jurídico 0624/2009 de la AEPD. Disponible en Internet: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2009-0624_Publicaci-oo-n-en-revista-de-foto-ganadora-de-concurso-con-im-aa-genes-de-personas.-No-necesidad-de-consentimiento.pdf> [Consulta: 18 septiembre 2016].

[48] En este sentido regula el Artículo 5.1.f) del Real Decreto 1720/2007, op. cit. Con anterioridad, Ley Orgánica 5/1992, de 29 de octubre (LORTAD), establecía la necesidad de proteger 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".* Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (BOE núm. 262, 31.10.1992, derogada). Vid. HEREDERO HIGUERAS, M. "La Protección de datos de salud informatizados en la Ley Orgánica 5/1992, de 29 de octubre". *Derecho y Salud*. Núm. 1, enero-junio 1994, pp. 17-28.; SÁNCHEZ BRAVO, A. "La regulación de los datos sensibles en la LORTAD". *ID*. Núm. 6-7, UNED, 1994, pp. 117-132.

Esta redacción amplia de conceptos viene transpuesta 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[49] (en adelante, Directiva 95/46/CE), y al respecto DAVARA RODRÍGUEZ[50] afirma que la Directiva 95/46/CE pretende que la protección se extienda a toda persona que, de una forma u otra, por asociación de conceptos o contenidos, aunque no se haga referencia directa a ella pueda ser identificada o identificable.

Por lo tanto, se pone de manifiesto que la normativa actual de protección de datos intenta dar cobijo a una serie amplia de situaciones, no limitándose estrictamente a la intimidad o a "lo íntimo" de una persona en concreto, sino a toda información relativa a un individuo por muy intrascendente que al principio pueda parecer, resultando de poca importancia el medio a través del cual se recopila dicha información. En este sentido se ha pronunciado la Jurisprudencia sentando como base que el derecho a la protección de datos protege cualquier tipo de dato personal, sea o no íntimo y que además de ello, que se trata de un derecho que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de su persona y la prohibición de hacer uso de lo así conocido[51].

De manera muy somera es necesario puntualizar en este momento que el empleo de la expresión "dato" es diferente de la expresión "información". Aunque en la práctica resultan términos que se usan de forma indistinta, al objeto de estudio de ésta Tesis resulta necesario establecer la diferencia que entre estos conceptos existe.

---

[49] Directiva 95/46/CE, op cit.

[50] DAVARA RODRÍGUEZ, M. A. *La Protección de datos en Europa: principios, derechos y procedimiento.* Grupo Asnef Equifax, Madrid, 1998, p. 47.

[51] Entre las más destacadas, la STC 292, op. cit., y la STC 290/2000, op. cit. Si bien éstas dos sentencias son las que revisten mayor notoriedad sobre el particular, también hubo otros pronunciamientos jurisprudenciales en el mismo sentido, tales como la STC 73/1982, de 2 de diciembre, Fundamento Jurídico 5 (BOE núm. 312, 29.12.1882); STC 110/1984, de 26 de noviembre, Fundamento Jurídico 3 (BOE núm. 305, Suplemento, 21.12.1984); STC 89/1987, de 3 de junio, Fundamento Jurídico 3 (BOE núm. 151, 25.06.1987); STC 231/1988, de 2 de diciembre, Fundamento Jurídico 3 (BOE núm. 307, 23.12.1988); STC 197/1991, de 17 de octubre, Fundamento Jurídico 3 (BOE núm. 274, 15.12.1991); y en general las STC 134/1999, de 15 de julio (BOE núm. 197, Suplemento, 18.08.1999); STC 144/1999, de 22 de julio (BOE núm. 204, Suplemento, 26.08.1999); y STC 115/2000, de 10 de mayo (BOE núm. 136, 7.06.2000).

Por “dato” se debe entender aquella recopilación en bruto que puede ser de forma numérica, cualitativa, cuantitativa, en forma de letra, caracteres, etc. Se trata de una representación simbólica de un hecho o un conocimiento, pero que por sí mismo el dato no aporta una referencia concreta de una persona.

Contrariamente a lo que se ha explicado que debe interpretarse por “dato”, la “información” consiste en un conjunto de datos, es decir, datos que ya se encuentran procesados y que pueden ser interpretados o asociados a una persona determinada o determinable. En el ámbito sanitario, un valor numérico en la historia clínica (en adelante, HC) de un paciente, de por sí no indica nada, sin embargo, si dicho valor numérico está contenido en un análisis clínico y viene acompañado de otros datos que revelan que dicho valor numérico se corresponde a la medición en sangre del colesterol, y además, se completa con otros datos que valoran los niveles recomendados como mínimos y máximos, ya estamos en presencia de lo que denominamos información y la misma puede ser interpretada, conocida y valorada con fines médicos en este ejemplo.

b) Breves consideraciones sobre la expresión “identificadas o identificables”.

Con la inclusión de esta terminología en el Artículo 3 de la LOPD[52] (en adelante, LOPD), donde se define el dato personal como *“cualquier información concerniente a personas físicas identificadas o identificables”,* se ha generado confusión al respecto. Esta expresión jurídica que el legislador ha empleado planteó dudas a la hora de considerar determinados datos personales como identificadores o no de una persona en concreto. Frente a las cuantiosas consultas que fueron planteadas a la AEPD, por parte de los responsables de los ficheros, a la hora de incluir dichas consideraciones, la AEPD se ha pronunciado en este sentido, manteniendo que:

> Para que exista dato de carácter personal no es necesario que exista una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados […], y […], para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente

[52] Artículo 3, de la LOPD, op. cit.

utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona[53].

En cuanto a ésta expresión se pretende delimitar la aplicación de la normativa de protección de datos, solamente a aquellos datos que resulten relevantes o determinantes a la hora de hacer posible la identificación de una persona. En este sentido se ha pronunciado la Audiencia Nacional (en adelante, AN), entendiendo que si de un dato que *a priori* tiene la consideración de dato de carácter personal como lo es una fotografía, no puede identificarse a la persona que en la misma aparece, no se puede considerar dato personal[54].

Por tanto, consideramos que un dato es identificador si contiene información de la cual se identifica plenamente a la persona a la que hace referencia, sin necesidad de recurrir a más información sobre la misma[55]. Por el contrario, un dato tendrá la consideración de identificable, si la información no hace referencia directa a la persona a la que se

[53] Véase al respecto: Conclusiones y recomendaciones efectuadas por la AEPD en la Inspección Sectorial de Oficio relativa a "Concursos, juegos y sorteos de televisión", punto 3.1. Conclusiones y recomendaciones de la AEPD, 18.10.2002. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/recomendaciones_concursos_tv.pdf> [Consulta: 11 de septiembre de 2016]. En el mismo sentido, Informe jurídico 327/2002 de la AEPD, sobre el carácter de dato personal de la dirección IP. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP.pdf> [Consulta: 11 de septiembre de 2016]; Informe jurídico 285/2006 de la AEPD, sobre número de teléfono y concepto de dato personal. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2006-0285_N-uu-mero-de-tel-ee-fono-y-concepto-de-dato-personal.pdf> [Consulta: 18 septiembre 2016].

[54] En éste caso, la recurrente había denunciado la publicación en una red social de una fotografía de pequeñas dimensiones que la mostraba de perfil, caminando, imagen que la denunciante reconocía como propia, si bien no iba acompañada de ningún otro dato que permitiera la identificación de la denunciante, considerando en su resolución la Sala que no se puede predicar la condición expuesta del carácter identificable de la denunciante, desestimando el recurso planteado. SAN de 11 de marzo de 2013, Recurso 510/2011 (Roj: SAN 1133/2013 ECLI: ES:AN:2013:1133) Disponible en Internet: <http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=6668869&links=%22510%2F2011%22&optimize=20130403&publicinterface=true> [Consulta: 10 septiembre 2016].

[55] Un ejemplo, es el DNI que hace plenamente identificable a la persona física a la que pertenece.

refiere, pero aporta información suficiente para poder llegar a averiguar su identidad[56]. En base a ello, una *"persona identificable"* será *"toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social"*[57]. No obstante, *"una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados"*[58].

Según lo manifestado, no basta con que la información haga referencia a una persona, sino que de dicha información ha de resultar plausible la identificación de una persona. En este sentido, existe una doble barrera: por un lado, la información para ser considerada dato de carácter personal ha de hacer referencia a un aspecto íntimo de la persona cuya referencia se trate, y, por otro lado, esta información debe ser por sí misma suficiente para poder lograr la identificación de la persona de cuya información se hace referencia.

En consecuencia, la identidad hace referencia a los atributos de una persona que la diferencian de otras[59]. Así, por ejemplo, los rasgos que caracterizan a un ser humano como pueden ser su nombre y apellido, ADN, DNI, entre otros, atendiendo a tipologías fisiológicas, económicas, sociales o culturales, que forman parte del carácter personal protegido como tal por la normativa de protección de datos[60].

---

[56] Las direcciones de correo electrónico, en la medida en que nos proporcionan información que llegue a determinar la identidad de una persona, son considerados datos identificables. En el mismo sentido el ADN a priori contiene información genética de una persona, sin embargo, hasta que no se realice un determinado estudio no podremos asociarlo a una persona en particular.

[57] Artículo 5.o), del Real Decreto 1720/2007, op. cit.

[58] Ibídem.

[59] ROMEO CASABONA, C. M. "Persona identificada o identificable, el afectado o interesado y el procedimiento de disociación en la protección de datos de carácter personal", en TRONCOSO REIGADA, A. *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Thomson-Civitas, Pamplona, 2010, p. 227.

[60] El Artículo 13.2, de la Ley 12/1989, de 9 de mayo de la Función Estadística Pública viene a dar respuesta a cuándo los datos personales hacen identificable a una persona, consagrando que: *"Son datos personales los referentes a personas físicas o jurídicas que o bien permiten la identificación inmediata de los interesados o bien conduzca por su estructura, contenido, o grado de desagregación a la identificación"*. Si bien esta Ley recoge a las personas jurídicas, consideramos que ello carece de trascendencia toda vez que las personas jurídicas no son titulares de derechos relativos a la protección de datos de carácter personal, salvo las últimas inclusiones de la Jurisprudencia que ha venido a incorporar el derecho a la imagen y al honor como un derecho personal a ser protegido por

2.2. Datos sensibles o especialmente protegidos.

2.2.1. Los datos sensibles.

Dentro de los datos de carácter personal, situamos los datos que por su importancia son considerados sensibles. Asimismo, reciben la denominación de "datos especialmente protegidos" y ello es así en virtud de la especial atención que le brinda el legislador desde el punto de vista de su protección.

Los datos sensibles pueden categorizarse desde un prisma material y un prisma formal. Desde un punto de vista material, son datos sensibles los que revelan o son susceptibles de poner de manifiesto datos que hacen referencia a las cualidades de la persona relacionadas con su dignidad, con aspectos que afectan a su personalidad, que dibujan su forma de ser y de comportarse. Y desde un punto de vista formal, los datos que requieren unas especiales y reforzadas garantías de uso que alcanzan su recogida y tratamiento y que sopesan, en estas fases concretas del tratamiento, la voluntad de la persona.

HERRÁN ORTIZ[61] hace una diferenciación entre los datos sensibles, distinguiendo entre un criterio referido al contenido de los datos y otro criterio referido al mayor o menor nivel de protección que ampara a los mismos. Agrupa así, a las informaciones referidas a la libertad ideológica o creencias religiosas en un primer grupo, y en un segundo grupo que involucra, según HERRÁN ORTIZ[62], datos de origen racial, comportamiento sexual y salud.

En el mismo sentido, CORTÉS[63], comenta que los datos sensibles pueden dividirse en tres bloques. En primer lugar, sitúa la autora a los datos que revelen la ideología, afiliación sindical, religión y creencias. Cuando se proceda a su recogida será preciso

---

los Tribunales. Ley 12/1989, de 9 de mayo de la Función Estadística Pública (BOE núm. 112, 11.05.1989).

[61] HERRÁN ORTIZ, A. I. *La violación de la intimidad en la protección de datos personales.* Dykinson, Madrid, 1998, pp. 263-273.

[62] Ibídem.

[63] CORTÉS, E. (6.10.2015) Los tres candados que una empresa debe poner sobre los dados especialmente protegidos. [Blog post]. Blog Sage. Disponible en Internet: <http://blog.sage.es/economia-empresa/que-son-los-datos-especialmente-protegidos-en-proteccion-de-datos/> [Consulta: 18 septiembre 2016].

que se advierta sobre el derecho que se tiene a no facilitar este tipo de datos y, además, solo será posible con consentimiento expreso y por escrito del afectado. En un segundo bloque, coloca los datos que hagan referencia al origen racial, la salud y la vida sexual. En cuanto a estos datos, solo podrán ser recogidos, tratados y cedidos cuando exista una finalidad de interés general, lo disponga una ley o lo consienta el protagonista de forma expresa. También existen excepciones. Por ejemplo, cuando exista una razón de prevención, prestación de asistencia sanitaria o tratamiento médico no hará falta el consentimiento siempre que el sujeto que trata los datos sea un profesional sanitario u otro sujeto al secreto profesional. Por último, sitúa a los datos relativos a las infracciones penales o administrativas. Aunque éstos datos sólo pueden ser incluidos en ficheros que posean las Administraciones Públicas en determinados supuestos.

Ahora bien, *¿por qué es trascendente conceptualizar y diferenciar el concepto de dato personal del dato sensible?* Porque, no todos los datos personales tienen la categoría de sensibles. Serán considerados datos personales si revelan aspectos de nuestra *vida privada*, pero serán considerados datos sensibles si son datos que revelan aspectos *íntimos* de las personas[64].

Por lo tanto, los datos sensibles son datos que nos identifican y que hacen referencia a la ideología, origen racial o étnico, afiliación sindical, la situación patrimonial, la situación financiera, las opiniones políticas, color de pelo, filosóficas, religiosas, las condenas penales, la salud o vida sexual, ente los más significativos, aspectos absolutamente personales e intrínsecos de cada individuo. En base a ello, podemos sostener que tendrán la consideración de datos sensible, aquellos que, en caso de divulgarse de manera indebida, perturbarían la esfera más íntima del ser humano.

2.2.2. Los datos relativos a la salud.

Dentro de los considerados datos sensibles o especialmente protegidos, tiene un lugar especial el dato de salud que será la unidad mínima de referencia para este trabajo. Los datos de salud consisten en las informaciones que se refieren a la salud pasada,

[64] Para clarificar y ejemplificar el concepto, basta con pensar en la declaración de renta que hacemos, claramente es un dato personal que forma parte de nuestra vida privada, pero si padezco una enfermedad como puede ser el cáncer, eso es un dato personal sensible.

presente o futura, en personas sanas o enfermas, con enfermedades de carácter físico o psicológico, y que incluye la adicción al alcohol o a las drogas. También forma parte de los datos sobre la salud, la información de datos genéticos[65]. En este sentido, DIETRICH PLAZA[66] entiende que, desde la perspectiva de la protección de datos, los datos genéticos y las muestras biológicas, en cuanto permiten la identificación de la persona física, van a tener la consideración de dato personal especialmente protegido, ya que pueden dar información sobre la salud de las personas, así como revelar su origen racial o étnico.

Los datos personales, referidos a la salud, contienen información de las personas que permite conocer las dolencias o enfermedades que han padecido, padecen o incluso podrán padecer o tendrán tendencia a padecer en el futuro. Se trata, en definitiva, de datos personales que forman parte de la esfera más íntima de la persona, que pueden estar revelando situaciones críticas relativas a determinadas enfermedades a la aplicación de técnicas de reproducción asistida o relativa a información genética, cuyo potencial vulnerador de la intimidad personal nadie se atreve a poner en duda[67].

Esta versión amplia sobre los datos de salud, permite incluir todas aquellas informaciones sobre el cuerpo humano, la sexualidad, la raza, el código genético, los antecedentes familiares, los hábitos de vida, de alimentación y consumo[68].

El profesor que más aportaciones destacadas ha realizado sobre la materia es MURILLO DE LA CUEVA[69]. Sostiene el autor sobre los datos de salud, que:

---

[65] Ésta definición ha sido sustentada por la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM) en la redacción de la *Guía de protección de datos personales para Servicios Sanitarios Públicos.* Thomson Civitas, Madrid, 2004, p. 69.

[66] DIETRICH PLAZA, C. "Datos genéticos y protección de datos personales", en BUISÁN, L.; SÁNCHEZ URRUTIA, A. (coordinadoras). *Intimidad, confidencialidad y protección de datos de salud.* Thomson Reuters, Navarra, 2011, pp. 109 y ss.

[67] PIÑAR MAÑAS, J. L. "La Protección de Datos en el ámbito Sanitario". *El Médico.* Anuario 2004, pp. 42-44.

[68] SÁNCHEZ-CARO, J.; ABELLÁN, F. *Datos sobre la salud y datos genéticos. Su protección en la Unión Europea y en España.* Comares, Granada, 2004, p. 15.

[69] MURILLO DE LA CUEVA, P. L. "El derecho a la autodeterminación informativa y la protección de datos personales". *Cuadernos de Derecho*. Núm. 20, 2008, pp.43-58.; Ídem. "La protección de los datos de carácter personal en el horizonte de 2010". *Anuario de la Facultad de Derecho*. Núm. 2, 2009, pp.131-142.; Ídem. "Perspectivas del derecho a la autodeterminación informativa". *Revista de Internet, Derecho y Política*. Núm. 5, 2007, pp. 18-32.

> Son aquéllos que, por afectar a los aspectos más íntimos de la personalidad, reciben el más alto nivel de protección establecido. Y eso se debe a que se sitúan en un plano en el que confluyen dos derechos fundamentales al menos: el derecho a la intimidad y el derecho a la autodeterminación informativa. E, incluso, pueden proyectarse sobre otros estrechamente relacionados con los anteriores, como la libertad ideológica reconocida en el artículo 16 de la Constitución o con el propio derecho a la protección de la salud. Contienen, por tanto, una información personal especialmente cualificada y esencialmente ligada a la dignidad y libertad de aquél a quien pertenecen[70].

Por su parte, la doctrina mayoritaria[71], entiende que la definición de los datos referidos a la salud abarca tanto a los datos de carácter médico como a aquellos otros que guarden relación con la salud. Quedarían comprendidos, por tanto, todos aquellos datos que tiene que ver con el cuerpo humano, como la sexualidad, la raza, el código genético, pero, además, los antecedentes familiares, los hábitos de vida, de alimentación, de consumo, así como las enfermedades actuales, pasadas o futuras previsibles, bien sean de tipo físico o psíquico; y las informaciones relativas al abuso de alcohol o al consumo de drogas. En definitiva, abarcaría todos los datos que de alguna forma se refieran a la salud tanto de individuos con buena salud, enfermos o fallecidos[72].

GÓMEZ RIVERO[73], completa estas definiciones doctrinarias, y entiende que el conocimiento de los datos propios de salud por parte de terceros, afectaría no sólo a la

---

[70] MURILLO DE LA CUEVA, P. L. "El derecho a la autodeterminación informativa y la protección de datos personales", op. cit., pp. 43-58.

[71] En este sentido se han pronunciado académicos de reconocido prestigio como MURILLO DE LA CUEVA, P. L., *"La publicidad de los archivos judiciales y la confidencialidad de los datos sanitarios".* VII Congreso Nacional de Derecho Sanitario, octubre, 2000. Editorial Fundación Mapfre Medicina, Madrid, 2001.; RIPOL CARULLA, S.(ed.); BACARIA MARTRUS, J.(coord.). *Estudios de protección de datos de carácter personal en el ámbito de la salud.* APDCAT Agencia Catalana de Protección de Datos. Marcial Pons, 2006.; DE LORENZO Y MONTERO, R. "¿Qué se entiende por dato de salud?". *Revista Redacción Médica*. 21.06.2007, núm. 585, Año III.; GÓMEZ RIVERO, Mª C. *La protección penal de los datos sanitarios. Especial referencia al secreto profesional médico.* Comares, Granada, 2007, pp. 35 y ss.; GÓMEZ NAVAJAS, J. *La protección de datos personales.* Thomson-Civitas, Navarra, 2005, pp. 425-430.; LEÓN ALONSO, M. *La Protección constitucional de la salud.* La Ley, Madrid, 2010, pp. 135 y ss.

[72] Vid. ANTÓN BOIX, Mª C. "La Protección de Datos". *Revista de la Salud Mental, Sección Salud Mental, Implicaciones Legales y Forenses*. Disponible en Internet: <http://www.saludmental.info/Secciones/Juridica/2008/proteccion-datos-feb08.html> [Consulta: 18 septiembre 2016].

[73] GÓMEZ RIVERO, Mª C., op. cit., pp. 35 y ss.

parcela íntima y personal del individuo, sino que proporcionaría información sobre nuestras dolencias, rutinas diarias, etc. Al respecto, afirma que:

> Los datos relativos a la salud afectan de forma indiscutida a la esfera más íntima y personal del individuo, en cuanto que proporciona una información que, como pocas, permite acceder a su esfera privada y llegar a conocer no sólo su reducto más personal, como es el estado de su cuerpo o de su mente sino, a partir de ahí, obtener detalles sobre su padecimiento, hábitos de vida, tratamiento, etc.[74].

Por su parte, DE LORENZO[75], señala que la referencia a datos de salud, no ha de limitarse sólo a aquéllos datos que se refieran a enfermedades o a problemas de salud, sino también a aquéllos datos que indiquen un buen nivel de salud.

2.2.3. La regulación de los datos sensibles o especialmente protegidos.

a) Marco normativo español.

Los datos personales relativos a la salud no están tratados de manera unitaria en el ordenamiento jurídico nacional. Por el contrario, la regulación normativa es tanto de carácter estatal[76] como de carácter autonómico[77]. La CE[78], es la clave del Derecho

[74] Ibídem.

[75] DE LORENZO Y MONTERO, R., op. cit.

[76] LOPD, op. cit. y el correspondiente RD 1720/2007, op. cit.; Ley 14/1986, de 25 de abril, General de Sanidad (BOE núm. 102, 29.04.1986); 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 (BOE núm. 274, 15.11.2002).

[77] En el caso de Catalunya, destaca la Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y a la autonomía del paciente, y a la documentación clínica. En la Comunidad Autónoma de Andalucía cuentan con la Ley 1/2014, de 24 de junio, de Transparencia Pública (BOE núm. 172, 16.07.2014). En el País Vasco, 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 (BOPV núm. 44, 4.03.2004); Decreto 272/1986 de 25 de noviembre por el que se regula el uso de la Historia Clínica de los Centros Hospitalarios de la Comunidad Autónoma del País Vasco (BOPV núm. 242, 6.12.1986); Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica (BOPV núm. 65, 29.03.2012); la Ley 8/1997, de 26 de junio, de Ordenación sanitaria de Euskadi (BOE núm. 9,

Sanitario que en su Artículo 43 marca el inicio del reconocimiento del derecho a la salud. Asimismo, otorga las competencias necesarias a los poderes públicos para que estructure, organice y administre un sistema sanitario que comprenda a todos los ciudadanos, para prestarles una atención sanitaria adecuada. Por su parte, el Artículo 51 de la CE, insta a los poderes públicos a garantizar el derecho a la salud[79]. En

---

11.01.2012); y el Decreto 45/1998, de 17 de marzo, por el que se establece el contenido y se regula la valoración, conservación y expurgo de los documentos del Registro de Actividades Clínicas de los Servicios de Urgencias de los Hospitales y de las Historias Clínicas Hospitalarias (BOPV núm. 67, 8.04.1998). En Aragón, la Ley 6/2002, de 15 de abril, de Salud de Aragón (BOE núm. 121, 21.05.2002); Decreto 19/2015, de 24 de febrero, del Gobierno de Aragón, por el que se crea el Registro de solicitudes de acceso a la información pública y el fichero de datos de carácter personal "Solicitantes de acceso a la información pública" (BOA núm. 43, 4.03.2015). En Galicia, Ley 3/2001, de 28 de mayo, reguladora del consentimiento informado y de la historia clínica de los pacientes (BOE núm. 158, 3.07.2001). En La Rioja, Ley 2/2002, de 17 de abril, de Salud (BOR núm. 49, 23.04.2002). En la Comunidad Valenciana, disponen del Decreto 56/1988, de 25 de abril, del Consell de la Generalitat Valenciana (DOGV núm. 817, 4.05.1988); la Ley 3/2003, de 6 de febrero, de Ordenación Sanitaria de la Comunidad Valenciana (BOE núm. 55, 5.03.2003); Orden de 17 de febrero de 1994, de la Conselleria de Sanitat i Consum, por la que se regula la confidencialidad y custodia de los datos médicos de los servicios médicos de empresa (DOCV núm. 2227, 13.03.1994); y la Orden de 14 de septiembre de 2001, de la Conselleria de Sanidad, por la que se normalizan los documentos básicos de la historia clínica hospitalaria de la Comunidad Valenciana y se regula su conservación (DOGV núm. 4111, 22.10.2001). En la Comunidad Autónoma de Castilla y León, cuentan con el Decreto 101/2005 de 22 de diciembre, por el que se regula la historia clínica (BOCyL núm. 249, 28.12.2005); Ley 8/2003, de 8 de abril, sobre derechos y deberes de las personas en relación con la salud, Comunidad Autónoma de Castilla y León (BOE núm. 103, 30.04.2003). La Comunidad Extremeña cuenta con la Ley 10/2001, de 28 de junio, de Salud de Extremadura (DOE núm. 76, 3.07.2001); Ley 7/2011, de 23 de marzo, de salud pública de Extremadura (DOE núm. 59, 25.03.2011); Ley 3/2005, de 8 de julio, de información sanitaria y autonomía del paciente, Comunidad Autónoma de Extremadura (BOE núm. 186, 5.08.2005). En Navarra, disponen de la Ley Foral 11/2002, de 6 de mayo, sobre los derechos del paciente a las voluntades anticipadas, a la información y a la documentación clínica de Navarra (BON núm. 58, 13.05.2002). En Madrid, la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid (BOE núm. 245, 12.10. 2001); Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid (BOCM núm. 306, 26.12.2001). En Murcia cuentan con la Ley 4/1994, de 26 de julio, de Salud de Murcia (BOE núm. 243, 11.10.1994). Finalmente, en Asturias disponen de la Ley 1/1992, de 2 de julio, del Servicio de Salud del Principado de Asturias (BOE núm. 211, 2.09.1992).

[78] Artículo 43, de la CE.

[79] Al respecto, mantuvo el TC que: *"De la interpretación sistemática de todos esos preceptos se infiere la exigencia constitucional de que exista un sistema normativo de la sanidad nacional, puesto que los derechos que en tal sentido reconoce la Constitución en los artículos 43 y 51 o, complementariamente, en otros como el 45.1, que reconoce el derecho que todos tienen a disfrutar de un medio ambiente*

cumplimiento del mandato constitucional, se promulga la Ley 14/1986, de 25 de abril, General de Sanidad (en adelante, LGS), que establece y garantiza un sistema sanitario para toda la población, sienta las bases de la intervención pública en dicha materia y confiere una estructura básica y organizativa del sistema de salud.

En el ámbito de la protección de datos de carácter sanitario debemos focalizarnos principalmente en dos normas. Por un lado, en la LOPD, y, por otro lado, para completar la legislación de aquél momento en la materia, se promulgó la Ley 41/2002, de 14 de noviembre, ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (en adelante, LAP), que completa las previsiones que la LGS enuncia como principios generales. Si bien la LAP tiene su origen en la LGS, ha venido a legislar el vacío que imperaba en nuestro cuerpo normativo al respecto a la tutela específica sobre la HC.

Finalmente, la citada normativa se conjuga necesariamente con la LOPD, que califica a los datos relativos a la salud de los ciudadanos como datos especialmente protegidos, estableciendo un régimen especialmente riguroso para su obtención, custodia y eventual cesión. En su Artículo 3 define a los datos de carácter personal, diciendo que se trata de *"cualquier información concerniente a personas físicas identificadas o identificables"*. Sin embargo, la norma no define expresamente al dato de salud como tal. En el Artículo 7.3, la LOPD alude a los datos de salud como *"datos de carácter personal que hagan referencia a la salud"*. Por su parte, el Artículo 8 de la LOPD, limita el tratamiento que los profesionales de los centros de salud respecto a los datos de salud recopilados[80].

Podemos apreciar la generalidad que el legislador le otorga a tal definición. Quizás, desde nuestro punto de vista, ambigua, porque entendemos que ha sido intención del legislador, tal y como se explicó anteriormente, que la Ley perdurara más en el tiempo, hecho que sólo podía alcanzarse si el objeto de protección no estaba estrictamente

---

adecuado para el desarrollo de la persona, pertenecen a todos los españoles y a todos se les garantiza por el Estado la igualdad en las condiciones básicas para el ejercicio de los mismos". STC 32/1983, de 28 de abril (BOE núm. 117, 17.05.1983).

[80] El Artículo 8, de la LOPD, 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".*

limitado, sino que englobaba una serie de datos que podían hacer referencia a la salud y por tanto contar con la protección más alta de la normativa.

Sin embargo, esta norma, si bien se refiere explícitamente a los datos de salud, considerándolos expresamente protegidos y limitando la posibilidad de su recopilación y cesión, no establece un concepto concreto de este tipo de datos.

Por tanto, realizada esta apreciación, a fin de definir a los datos de salud desde el punto de vista legal, se deberá partir del concepto que las normas nacionales e internacionales, vigentes en España dan al mismo[81], labor que realizaremos en el siguiente apartado.

[81] Destacan la Declaración de Helsinki de la Asociación Médica Mundial de 1964 (Adoptada por la 18ª Asamblea Médica Mundial, Helsinki, Finlandia, junio de 1964 y enmendada por la 29 Asamblea Médica Mundial, Tokio, Japón, octubre de 1975, la 35ª Asamblea Médica Mundial, Venecia, Italia, octubre de 1983 y la 41ª Asamblea Médica Mundial, Hong Kong, septiembre de 1989), como una propuesta de principios éticos para investigación médica en seres humanos, incluida la investigación del material humano y de información identificables. Disponible en Internet: <http://www.wma.net/es/30publications/10policies/b3/17c_es.pdf> [Consulta: 2 septiembre 2016]; Recomendación (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. Disponible en Internet: <http://www.bioeticaweb.com/recomendaciasn-nao-r-97-5-de-13-de-febrero-de-1997-del-comitac-de-ministros-del-consejo-de-europa-a-los-estados-miembros-sobre-protecciasn-de-datos-macdicos/> [Consulta: 2 septiembre 2016]; la Declaración Universal sobre el Genoma Humano y los Derechos Humanos, 28 de abril de 1977. Disponible en Internet: <http://portal.unesco.org/es/ev.php-URL_ID=13177&URL_DO=DO_TOPIC&URL_SECTION=201.html> [Consulta: 18 septiembre 2016]; la Declaración Internacional sobre los datos genéticos humanos, adoptada por unanimidad en la Conferencia General de la UNESCO el 16 de octubre de 2003. Disponible en Internet: <http://portal.unesco.org/es/ev.php-URL_ID=17720&URL_DO=DO_TOPIC&URL_SECTION=201.html> [Consulta: 18 septiembre 2016]; el Convenio para la Protección de los Derechos Humanos y de la Dignidad del Ser Humano con Respecto a las Aplicaciones de la Biología y de la Medicina, hecho en Oviedo el 4 de abril de 1997. Instrumento de Ratificación del Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina), hecho en Oviedo el 4 de abril de 1997 (BOE núm. 251, 20.10.1999, pp. 36825-36830); y la Carta de Derechos Fundamentales de la Unión Europea, de 18 de diciembre de 2000 (DOCE C 364, 18.12.2000, pp.1-22).

Por su parte, la CE refiriéndose a los derechos fundamentales y a las libertades públicas, recoge en el Artículo 10 el derecho a la dignidad de la persona[82], y el derecho a la intimidad personal según el en el Artículo 18. Aunque es en su artículo 43.1 donde la CE reconoce expresamente el derecho a la salud estableciendo en su apartado primero que*: "Se reconoce el derecho a la protección de la salud".*

La LOPD, consagra en su Artículo 7, referido a los datos especialmente protegidos 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.

Por su parte, Convenio relativo a los derechos humanos y la biomedicina[83] (en adelante, Convenio de Oviedo), también establece que *"Toda persona tendrá derecho a que se respete su vida privada cuando se trate de informaciones relativas a su salud".*

b) Marco jurídico internacional y europeo.

b) 1. Marco jurídico internacional.

La protección de datos tiene origen europeo y se incorpora como primera formulación del ordenamiento jurídico como el reconocimiento y la profundización en el derecho a la intimidad personal y familiar de la persona.

[82] El Artículo 10, de la CE establece que: *"La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social. 2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España".* Al respecto, varios autores entienden que el origen de la protección de datos está en la intimidad y ésta a su vez viene contenida en la dignidad humana. Vid. MURILLO DE LA CUEVA, P. L. *La construcción del derecho a la autodeterminación informática y las garantías para su efectividad*., op. cit., pp. 11-12.; BAZÁN, V., op. cit. pp. 85-139.

[83] Artículo 10, sobre la vida privada y el derecho a la información, del Convenio de Oviedo, op. cit.

Sin ánimo de hacer un estudio pormenorizado de la normativa internacional y europea al respecto porque excede del objeto de estudio de ésta Tesis, sí que resulta necesario enmarcar a los datos de salud en el contexto jurídico que traspasa nuestras fronteras, dando una breve aproximación al lector en la normativa existente en la materia.

El marco jurídico internacional de la protección de datos se edifica a partir del Artículo 12 de la Declaración Universal de los Derechos del Hombre, que protege a toda persona en su vida privada frente a injerencias o ataques[84].

Posteriormente, en la década del '50 se aprobó el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales[85], (en adelante, CEDH), que en su Artículo 8 hace referencia expresa a la vida privada y familiar. Y también ha supuesto un avance el Convenio en lo que respecta a la extensión a los extranjeros la protección que se concede a la vida familiar en éste Artículo 8[86].

---

[84] La Declaración Universal de los Derechos Humanos, establece que: *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".* Declaración Universal de los Derechos del Hombre, declaración adoptada en París por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), de 10 de diciembre de 1948. Disponible en Internet: <http://www.un.org/es/universal-declaration-human-rights/> [Consulta: 2 septiembre 2016].

[85] En el Artículo 8 del CEDH, se establece que: *"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".* Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, de 4 de noviembre de 1950, ratificado por España el 26.09.1979 (BOE núm. 243, 10.10.1979).

[86] En el Caso Abdulaziz, Cabales y Balkandali, se trata de tres residentes legales en el Reino Unido que contraen matrimonio en su país de origen, y a cuyos maridos se les niega la residencia en el Reino Unido como consecuencia de las leyes inmigratorias del Reino Unido. Las recurrentes alegaron que esa negativa, implicaba necesariamente una injerencia ilícita por parte de las autoridades británicas en su vida familiar, al impedir la misma. El TEDH consideró que el Convenio puede generar obligaciones positivas de los Estados inherentes a un efectivo respeto a la vida familiar que no excluyen de por sí su adopción en el campo de la inmigración y determinó en su sentencia el TEDH que el legítimo control de los estados sobre la inmigración debe ejercerse de forma compatible con el Convenio (Sentencia TEDH, 28.05.1985, Abdulaziz, Cabales y Balkandali contra Reino Unido (Serie A nº 94) apartados 60-69). En el mismo sentido, en el Caso Berrehab contra Países Bajos, el TEDH ha

Este Artículo ha sido ampliado en su aplicación por la Jurisprudencia que el Tribunal Europeo de Derechos Humanos (en adelante, TEDH) ha dictado en la materia. En este sentido, afirma el TEDH que a esta obligación negativa de no injerencia pueden añadirse obligaciones positivas inherentes al respeto a la vida privada y familiar, entre las cuales pueden encontrarse la adopción de medidas tendentes a asegurar el respeto de la vida privada, incluso en las relaciones entre los individuos[87].

FREIXES SANJUÁN[88] sostiene que este posicionamiento del TEDH abre nuevas vías de interpretación del Convenio, postulando no únicamente una acción de protección de los derechos contra los poderes públicos, sino incluyendo la protección frente a violaciones realizadas por particulares, lo cual rompe con la función clásica de los tratados internacionales (creación de obligaciones interestatales) para dotarlos de una eficacia objetiva, que comporta la vinculación de los particulares a las disposiciones del Convenio.

Ya en el año 1966, el Pacto Internacional de Derechos Civiles y Políticos[89], siguió el mismo criterio que el mantenido en su predecesor, y se refiere a la protección de la vida privada, otorgándole protección frente a las injerencias arbitrales o ilegales.

---

considerado que la negativa a conceder un permiso de residencia a un extranjero que pretende visitar con frecuencia a un hijo de corta edad constituye un límite desproporcionado al derecho al respeto a la vida familiar y, por lo tanto, es incompatible con el Convenio (Sentencia TEDH, 21.06.1988, Caso Berrehab contra Países Bajos).

[87] La pretensión del Convenio de asegurar el goce de los derechos protegidos, partiendo de que su finalidad consiste no en proclamar derechos ilusorios sino en garantizar la efectividad de los mismos, En este sentido, el TEDH afirma que a esta obligación negativa de no injerencia pueden añadirse obligaciones positivas inherentes al respeto a la vida privada y familiar, entre las cuales pueden encontrarse la adopción de medidas tendentes a asegurar el respeto de la vida privada, incluso en las relaciones entre los individuos. Para profundizar más el tema, véase al respecto: FREIXES SANJUÁN, T. "Las principales construcciones jurisprudenciales del Tribunal Europeo de Derechos Humanos. El standard mínimo exigible a los sistemas internos de derechos en Europa". *Proyecto DGICYT.* "Integración europea y derechos fundamentales: Integración de la jurisprudencia del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea en las sentencias del Tribunal Constitucional" (PB93-0851). Disponible en Internet: <http://personal.us.es/juanbonilla/contenido/CM/TRIBUNAL%20EUROPEO%20DE%20DERECHOS%20HUMANOS/JURISPRUDENCIA%20TEDH/PRINCIPALES%20CRITERIOS%20JURISPRUDENCIALES%20DEL%20TEDH.pdf> [Consulta: 18 septiembre 2016].

[88] FREIXES SANJUÁN, T., op. cit.

[89] El Pacto Internacional de Derechos Civiles y Políticos, en su Artículo 17, establece que: *"1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su*

TELLES[90] y NAVALPOTRO[91] consideran que los primeros pasos en la materia se han visto dados a través de la Resolución 22/1973, de 20 de noviembre, del Consejo de Europa, sobre regulación jurídica de los ficheros electrónicos en el sector privado y con la Resolución 29/1974, de 29 de noviembre de 1974, del Consejo de Europa, para establecer las pautas ordenadoras del sector público de la informática.

Con posterioridad, el Convenio 108, del Consejo de Europa, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, de 28 de enero de 1981[92], (en adelante, el Convenio 108), advierte sobre la necesidad de llevar a cabo una unión más íntima entre los miembros del Consejo de Europa, basada en el respeto particularmente de la preeminencia del derecho así como de los derechos humanos y de las libertades fundamentales y se reconoce 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. Asimismo, esta norma destaca la importancia de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos[93].

El Convenio 108 vino a ser el primer instrumento a nivel europeo en el cual los países firmantes reconocen de forma unánime la necesidad de legislar sobre el intercambio de

---

correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques". Pacto Internacional de Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966, en vigor desde 3.01.1976 (BOE núm. 103, 30.04.1977). Disponible en Internet: <http://www.ohchr.org/SP/ProfessionalInterest/Pages/CESCR.aspx> [Consulta: 2 septiembre 2016].

[90] TÉLLEZ AGUILERA, A. *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores.* Edisofer, Madrid, 2002, pp. 29 y ss.

[91] NAVALPOTRO NAVALPOTRO, Y. "Antecedentes de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)", en ALMUZARA ALAMAIDA, C. (Coordinadora). Estudio práctico sobre la protección de datos de carácter personal. Lex Nova, 2ª Edición, Valladolid, 2007, p. 34.

[92] Convenio Nº 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 el 27 de enero de 1984 (BOE núm. 274, 15.12.1985, pp. 36000-36004).

[93] Según se recoge en las consideraciones previas del Convenio 108.

datos personales que la sociedad estaba experimentando en aquellos tiempos[94]. Como consecuencia de la posición común de los Estados miembros del Consejo Europeo, sobre la necesidad de establecer un marco de criterios a seguir por todos ellos, al objeto de tutelar de forma amplia la protección de los derechos y libertades fundamentales de los individuos en un momento en el que el flujo de los datos de carácter personal trasfronterizo había incrementado, como consecuencia de los avances tecnológicos, persiguiendo establecer un adecuado equilibrio entre el respeto a la vida privada y la libre circulación de la información en los distintos países.

El aspecto más destacable al objeto de análisis en esta Tesis es que el Convenio 108, enuncia las categorías especiales de datos, es decir los datos sensibles, a los que hacemos referencia en la primera parte de éste trabajo, estipulando que el tratamiento de los datos de salud no podrá tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas[95].

El apartado 45 de la Memoria Explicativa del Convenio 108, se refiere a los datos de carácter personal relativos a la salud, considerando que su concepto abarca *"las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo",* pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido[96]. Añade el apartado 45 que: *"debe entenderse que estos datos*

---

[94] Ibídem.

[95] El Artículo 1, del Convenio 108, establece 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»).* En su Artículo 2, define el concepto de "Datos de carácter personal", diciendo que significa cualquier información relativa a una persona física identificada o identificable «persona concernida» Referido a las categorías de datos en particular, estipula en el 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".* Para profundizar más al respecto, véase: BAYO DELGADO, J. "Derecho comunitario sobre protección de datos", en GÓMEZ MARTÍNEZ, C. (Director). *Derecho a la intimidad y nuevas tecnologías.* Consejo General del Poder Judicial, Madrid, 2004, pp. 45-76.

[96] En la Memoria Explicativa del Convenio 108, se considera que el concepto de datos de salud abarca "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo", pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido.

comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas"[97].

Ya más aproximados a la definición de los datos de salud que en ésta Tesis nos ocupa, la Recomendación nº R (97) 5, del Comité de Ministros del Consejo de Europa, referente a la protección de datos médicos, afirma que: *"la expresión datos médicos hace referencia a todos los datos de carácter personal relativos a la salud de una persona. Afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas"*[98]*.* Según COUDERT[99], éste concepto de dato de salud es el más conveniente para su delimitación.

Por su parte, la Organización Mundial de la Salud (en adelante, OMS) también elabora una definición, destacando que se trata de información referida al bienestar físico, mental o social, y no solo a la ausencia de enfermedades o dolencias. Hasta el presente, podemos sostener que aquí encontramos la definición más exacta sobre el dato de salud en sí. La OMS concluye diciendo que: *"La salud es un estado de completo bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades"*[100]*.* Ésta definición no ha sido modificada desde 1948.

b) 2. Marco jurídico español.

Recuerdan FERNÁNDEZ CONTE y LEÓN BRUGOS[101] que por los años '70, los Estados miembros de la UE comenzaron a desarrollar en sus ordenamientos jurídicos

[97] Ibídem.

[98] 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.

[99] COUDERT, F. "Tratamiento de datos especialmente protegidos", en ALMUZARA ALAMAIDA, C. (Coordinadora). *Estudio práctico sobre la protección de datos de carácter personal.* Lex Nova, 2ª Edición, Valladolid, 2007, pp. 340 y ss.

[100] Preámbulo de la Constitución de la Organización Mundial de la Salud, que fue adoptada por la Conferencia Sanitaria Internacional, celebrada en Nueva York del 19 de junio al 22 de julio de 1946, firmada el 22 de julio de 1946 por los representantes de 61 Estados (Official Records of the World Health Organization, Nº 2, p. 100), y entró en vigor el 7 de abril de 1948.

[101] Vid. FERNÁNDEZ CONTE, J.; LEÓN BRUGOS, D. "Antecedentes y proceso de reforma sobre protección de Datos en la Unión Europea", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016, p. 37.

internos, el derecho a la protección de datos. Alemania siendo el primer país en abordar el tema del derecho a la protección de datos codificando su contenido y regulación[102].

Posteriormente, en la UE se adoptó 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[103], cuyo objetivo primordial es la tutela sobre el derecho a la intimidad en el tratamiento de los datos de carácter personal, y cuya trasposición a nuestro ordenamiento jurídico dio como resultado la LOPD[104], Ley desarrollada por el Real Decreto 1720/2007, de 21 de diciembre[105], (en adelante, RD 1720/2007).

La Directiva 95/46/CE persigue especialmente que los Estados miembros apliquen unas medidas equivalentes para tutelar el respeto a la intimidad en el tratamiento automatizado de datos de carácter personal. En la actualidad, la Directiva 95/46/CE es la piedra angular de la legislación vigente de la UE en materia de protección de datos, que fue adoptada hace dos décadas con un doble objetivo: por un lado, defender el derecho fundamental a la protección de datos protegiendo el derecho a la intimidad en el tratamiento de los datos de carácter persona y, por otro lado, garantizar la libre circulación de estos datos entre los Estados miembros. Se complementó mediante la Decisión Marco 2008/977/JAI, en su calidad de instrumento general a escala de la Unión para la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal[106].

Uno de los instrumentos normativos más recientes e importantes desde el punto de vista de su carácter vinculante y supranacional, es el Convenio sobre Derechos Humanos y la Biomedicina del Consejo de Europa[107] (en adelante, Convenio de Asturias), que consagra la necesidad de informar al paciente sobre su estado de salud y

---

[102] En el Estado Alemán de Hesse se codificó por primera vez una norma de protección de datos Datenschutzgesetz Gesetz vom: 07.10.1970 (GVBI.I Nr. 41 S.625-627, 12.10.1970).

[103] Directiva 95/46/CE, op. cit.

[104] LOPD, op. cit.

[105] RD 1720/2007, op. cit.

[106] Para profundizar más el tema, véase: NAVALPOTRO NAVALPOTRO, Y., op. cit., pp. 34 y ss.

[107] Conocido también como Convenio de Asturias de Bioética, firmado por España el 4 de abril de 1997, en Oviedo. Entró en vigor el 1 de enero de 2000 (BOE núm. 251, 20.10.1999). El ministro de Sanidad en aquel momento, José Manuel Romay Beccaría, equiparó la relevancia de Convenio con la Declaración Universal de Derechos Humanos.

sobre las terapias posibles y también la obligación de obtener el libre consentimiento del enfermo de forma previa a cualquier intervención médica[108].

Por último, con la firma de del Convenio de Oviedo[109], que ha sido objeto de elaboración y discusión durante una década en el seno del Consejo de Europa, éste instrumento legal se convirtió en el primer texto jurídico internacional sobre este asunto y, según SANCHEZ-CARO[110], viene a marcar la senda en el desarrollo científico en los ámbitos de la biología y la medicina que, a partir de su aprobación, quedó supeditado siempre el respeto de los derechos y la dignidad de la persona, requiriéndose el consentimiento expreso del individuo al tratar sus datos.

Conclusión.

En consecuencia, podemos advertir que la legislación nacional se ha visto directamente influida por el marco internacional. Conjugando las opiniones de los diversos autores citados, podríamos decir que los datos referidos a la salud no sólo se refieren a los datos médicos en sentido estricto, sino que engloban todos aquellos datos referidos al cuerpo humano, enfermedades presentes y futuras tanto físicas como psíquicas, o datos sobre el fallecimiento.

Consideramos que la normativa legal presente carece de una definición concreta de datos de salud, lo que conlleva a una cierta inseguridad jurídica en el sector del derecho sanitario. Debemos resaltar que tratar los datos de salud, datos especialmente protegidos por la ley, requiere de unas garantías mayores. Por tanto, si la legislación no contiene una conceptualización más concreta, estaremos frente a una ambigüedad de lo que implica un dato de salud y si ha de considerarse como tal o no, y en ese caso saber qué garantías han de aplicarse.

[108] Artículo 6, del Convenio de Oviedo, op. cit.

[109] Ibídem.

[110] SANCHEZ-CARO, J. "El consentimiento previo a la intervención y la protección de los incapaces", en ROMEO CASABONA, C. M. *El Convenio de derechos Humanos y Biomedicina. Su entrada en vigor en el ordenamiento jurídico español.* Comares, Granada, 2002, pp. 123-127.

CAPÍTULO II

Elementos jurídicos que vinculan el dato de salud.

SUMARIO: 1. Tratamiento y cesión de los datos de salud. 1.1. El papel normativo y su protección. 1.1.1 Normativa Comunitaria. 1.1.2. Normativa interna. 1.1.3. Ética sanitaria y carácter vinculante de los Códigos Deontológicos. 2. Principios que se aplican al tratamiento de los datos personales. 2.1. Principio de calidad de datos. a) Adecuación de los datos. b) Finalidad de los datos. c) Certeza de los datos. d) Cancelación de los datos. e) Almacenamiento de los datos. f) Fraude en la recopilación de los datos. 2.2. Principio de información. 2.3. Principio de consentimiento del afectado. 2.4. Consentimiento informado. a) Excepciones al consentimiento. b) Vicios del consentimiento. c) Revocación del consentimiento. 2.5. Conocimiento informado. 2.6. Principio de seguridad. 2.7. Principio de confidencialidad y secreto médico. a) Sanciones en el ámbito Penal respecto a la revelación de secretos. 2.8. Transparencia o publicidad en el tratamiento. 3. Derechos del paciente respecto a su historia clínica. 3.1. Acceso. 3.2. Derecho a la rectificación o cancelación de los datos erróneos. 3.3. Derecho de oposición de los interesados.

Introducción.

Los datos personales referidos a la salud de las personas, son datos sensibles y especialmente protegidos que la Ley consagra como tales, y por ello, la normativa vigente establece de manera taxativa la forma en que esta categoría espacial de datos ha de ser tratada por los profesionales que recopilan y habitualmente trabajan con estos datos. Así también, se ha de comprobar que esos datos sean adecuados a la finalidad asistencial que se brinde y en su caso, cómo ha de tratarse a este especial grupo de datos sensibles y si los mismos han de ser comunicados a terceras personas para la realización de los fines para los cuales han sido recabados.

Es importante analizar qué se entiende por tratamiento de los datos personales y cuáles son sus límites normativos, porque los datos por sí mismos no constituyen ningún riesgo. Lo que sí goza de amparo normativo es su tratamiento; el hecho de que nuestros datos personales sean tratados por terceras personas conlleva un peligro, y

este denominado “tratamiento” es lo que encuentra un paraguas legal que profundizaremos a continuación.

En éste Capítulo nos centraremos en analizar los principios jurídicos y éticos, que deben observarse a la hora del tratamiento de los datos de salud, por parte del facultativo médico y el personal sanitario, y finalmente explicaremos los derechos que le asisten al interesado en relación con sus datos de salud.

1. Tratamiento y cesión de los datos de salud.

No cabe duda de que los datos de salud se sitúan en la esfera más íntima de la persona, particularmente, aquellos datos que su conocimiento por parte de otros puede menoscabar el desarrollo de la personalidad. Nos referimos a datos tan delicados como, por ejemplo, la orientación sexual, el padecimiento de enfermedades psiquiátricas o de transmisión sexual, embarazos interrumpidos, fertilidad, ser alcohólico o ex alcohólico, etc. Como se ha explicado en la primera parte de ésa Tesis, los datos de salud disfrutan de un *status* jurídico particular dada su calificación de datos especialmente protegidos y es por ello, que, su tratamiento inadecuado puede vulnerar derechos fundamentales[111] y la normativa establece de forma contundente cómo ha de llevarse a cabo el tratamiento de éste grupo de datos.

El tratamiento de datos debe entenderse como el conjunto de operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y

[111] Pueden verse involucrados y por tanto afectados, el derecho a la intimidad, a la igualdad, a la no discriminación, etc., es por ello que, el Artículo 7, de la LOPD califica los datos de salud como especialmente protegidos y, al respecto, precisa en su apartado 3, que los datos de carácter personal que hagan referencia 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 lo consienta expresamente. Vid. BELTRÁN AGUIRRE, J. L. (27.06.2012). La Protección de los datos personales relacionados con la salud. Ponencia presentada en el Defensor del Pueblo de Navarra, junio de 2012, Navarra. Disponible en Internet: <http://www.navarra.es/NR/rdonlyres/517A4434-9C3B-442E-8651-61A7AE0490AD/226320/pdps.pdf> [Consulta: 7 julio 2015].

transferencias[112]. Por lo tanto, nuestros datos pueden ser recabados por cualquier medio, ya sea en formato papel tradicional o a través de cualquier variante informática, como ordenador, tablet, teléfono, etc. y los mismos pueden ser tratados para los fines que han sido recabados, tal y como analizaremos más adelante.

Según ÁLVAREZ CIVANTOS[113], *"el concepto de tratamiento de datos se asienta en un concepto superior que no es otro que el de conservación o utilización activa o pasiva de los datos personales en continuo"*. Se refiere el autor, a que existe tratamiento de los datos, a pesar de que los mismos no sean utilizados de forma constante, sino por el contrario, los datos siguen almacenados y serán utilizados en la medida de que el responsable los necesite para la finalidad que fueren recogidos. En el mismo sentido, concluye ÁLVAREZ HERNANDO[114], quien sostiene que el tratamiento de datos permite prácticamente todo. El autor afirma que, se entiende que existe tratamiento de datos por el mero hecho de poseerlos, conservarlos o visualizarlos, aunque, no exista dolo o intención de usarlos, ya sea de forma lícita o ilícita.

Éste tratamiento de nuestros datos de salud puede llevarse a cabo de dos maneras muy diferentes: con nuestro consentimiento o sin nuestro consentimiento. Estos temas se abordarán más en profundidad en los siguientes epígrafes. Evidentemente, la relación jurídica que vinculará a la persona responsable del tratamiento de nuestros datos con el individuo, será desigual según medie o no el consentimiento de éste último, y como consecuencia de ello, la protección legal y las obligaciones que la Ley impone serán distintas y sólo puede darse en determinados supuestos que la Ley establece de forma taxativa[115]. En este sentido, manifiesta APARICIO SALOM[116] que:

---

[112] Artículo 3. c), de la LOPD.

[113] ÁLVAREZ CIVANTOS, O. *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades.* 3ª edición, Auren, Granada, 2008, p.16.

[114] ÁLVAREZ HERNANDO, J. *Guía Práctica sobre Protección de Datos. Cuestiones y Formularios.* Lex Nova, Valladolid, 2011, p. 64.

[115] 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. Asimismo, 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. Finalmente, también podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del

> El tratamiento sin consentimiento se engloba en el concepto de relación jurídica ajena a la voluntad, ya que nace a consecuencia del acto jurídico que, conforme a la Ley, el interesado se ve obligado a aceptar el tratamiento de datos por parte de un tercero, que lo lleva a cabo habilitado o por imperativo de la Ley, y provoca, desde su inicio y mientras se mantiene, una pluralidad de obligaciones para dicho responsable así como el derecho de mantener el tratamiento de los datos mientras concurran las circunstancias que justifican la autorización legal para el mismo, y paralelamente, la obligación del interesado de soportarlo.

1.1. El papel normativo y su protección.

A continuación, haremos referencia al marco europeo, al marco español y a los Códigos Deontológicos relevantes, que regulan el tratamiento de los datos de salud.

1.1.1. Normativa Comunitaria.

El derecho comunitario tiene como función aproximar las legislaciones entre los Estados miembros de la Unión Europea (en adelante, UE), y en este sentido, las directivas son los instrumentos legislativos que consiguen dicha aproximación. Esta es la razón por la cual en los años 90 se optó por esta fuente normativa para tratar la protección de datos en Europa. Hoy en día, los avances en la unificación han conseguido que la regulación de esta materia se realice a través de un Reglamento comunitario que será de obligado cumplimiento para todos los Estados miembros a partir de 2018.

A continuación, vamos a analizar la Directiva que ha servido de base para inspirar la legislación española en materia de protección de datos

La Directiva 95/46/CE tiene como objetivo proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento. Estos principios han de entenderse vinculados tanto a la calidad de los datos, como a su legitimación.

---

afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento, según preceptúa el Artículo 7.3 y 7.6, de la LOPD.

[116] APARICIO SALOM, J. *Estudio sobre la Protección de Datos.* 4ª Edición, Thomson Reuters Aranzadi, Pamplona, 2013, pp. 62-63.

Los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, serán exactos y, cuando sea necesario, actualizados. En cuanto a la legitimación, ésta sólo podrá efectuarse si el interesado ha dado su consentimiento de forma inequívoca o si el tratamiento es necesario para proteger el interés vital del interesado, en el caso que nos ocupa.

En este sentido, la Directiva 95/46/CE, establece como regla general a este tipo de datos: la prohibición de su tratamiento respecto a una categoría especial de datos relacionados con la información personal relativa a los aspectos más esenciales de la persona. Se refiere a esta categoría en su Considerando 33, manifestando 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[117].

En efecto, su Artículo 8, sobre tratamiento de categorías especiales de datos indica que: *"Los Estados 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"*[118]. Sin embargo, a ésta regla genérica caben algunas excepciones que la misma Directiva 95/46/CE anuncia en el apartado 2, del Artículo 8:

> 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 […], 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[119].

---

[117] Considerando (33), de la Directiva 95/46/CE.

[118] Artículo 8.1, de la Directiva 95/46/CE.

[119] Artículos 8.1 y 8.2 a) y c), de la Directiva 95/46/CE. Éste último inciso citado de la Directiva 95/46/CE, ha sido incorporado a nuestra legislación nacional, casi sin modificación alguna, en el Artículo 7.6 segundo párrafo, de la LOPD.

Asimismo, se exceptúa de la regla general de prohibición del tratamiento de los datos relativos a la salud, cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria, 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[120].

Finalmente, la Directiva 95/46/CE da carta verde a los Estados miembros para que dispongan las garantías adecuadas, con la finalidad de establecer otras excepciones siempre que se trate de motivos de interés público importantes[121]. Es evidente que, la Directiva 95/46/CE sigue en éste sentido, la pauta establecida por el Convenio 108[122].

En consecuencia, advertimos, que el legislador ha puesto especial énfasis en la regulación normativa sobre el tratamiento de los datos de salud, puesto que forma parte del aspecto más personal e íntimo de la persona y, por tanto, debe salvaguardarse como derecho fundamental de la persona. Sin embargo, ésta protección no resultó ser suficiente, y así se pone de manifiesto con la aprobación del nuevo Reglamento General de Protección de Datos, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016[123], relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, Reglamento que analizaremos en la Segunda Parte de ésta Tesis.

[120] Artículo 8.3, de la Directiva 95/46/CE.

[121] Artículo 8.4, de la Directiva 95/46/CE.

[122] El Artículo 6, del Convenio 108 sostiene 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 regla regirá en el caso de datos de carácter personal referentes a condenas penales".*

[123] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, op. cit.

1.1.2. Normativa interna.

En éste apartado expondremos las diversas fuentes normativas de derecho interno que rigen el tratamiento y la cesión de los datos de salud, explicando también los casos en los que se puede realizar el tratamiento de los datos sin necesitar del consentimiento del interesado.

SANTOS GARCÍA[124] define de manera genérica y con un amplio espectro a la cesión de datos diciendo que:

> Teniendo en cuenta los avances de la informática y los numerosos tipos de soportes que existen cada vez más reducidos en los que se puede almacenar cada vez más información y transmitirla sin dejar rastro, resulta difícil a veces interceptar una comunicación de datos personales. Es cesión grabar los datos en un soporte y entregarlos a otra persona, enviarlos por correo electrónico, cualquier otro tipo de transferencia de datos personales incluso por correo postal en soporte de papel, una consulta de datos o la comunicación verbal a otra persona.

Vemos que el autor pone de relieve que la transmisión y cesión de datos puede realizarse en diferentes soportes y, además, de forma casi involuntaria por su cedente. Es por ello, que entendemos ha de ponerse el acento en la regulación normativa a fin de que la protección de nuestros datos personales quede absolutamente blindada de injerencias no deseadas.

Por ello, nuestra legislación contiene varias referencias al tratamiento y cesión de los datos especialmente protegidos. En efecto, el RD 1720/2007 establece como norma general 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"*[125]*.*

Por su parte, la Ley 16/2003 de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud[126], en su Artículo 53.6 menciona que la cesión de los datos, incluidos

---

[124] SANTOS GARCÍA, D. *Nociones generales de La Ley Orgánica de Protección de Datos.* Tecnos, Madrid, 2005, p. 79.

[125] Artículo 10.5, del RD 1720/2007.

[126] Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud (BOE núm. 128, 29.05.2003).

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.

Si bien el Artículo 10.1 del RD 1720/2007 requiere el consentimiento previo del interesado para que sus datos puedan ser tratados, estableciendo que: *"Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello",* en el apartado 5 del mismo Artículo, exculpa esa necesidad del consentimiento, en los casos en los que la cesión de los datos se realice para brindar asistencia sanitaria al afectado[127].

Advertimos que los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando en el terreno que nos ocupa, los mismos se recogen 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, o en el caso de que 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 LOPD[128] y del apartado 3 del Artículo 10 del RD 1720/2007[129]. Sobre este particular vemos que será la Ley la encargada de definir expresamente los casos en los cuales no será necesario el consentimiento del afectado. En el mismo sentido, PUENTE ESCOBAR[130] se refiere a la "habilitación legal" diciendo que: *"Se consagra así el principio de reserva de Ley en la determinación de posibles límites al ejercicio por los*

[127] El Artículo 10.5, del RD 1720/2007 en su segundo párrafo establece 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".*

[128] El Artículo 7.6, de la LOPD, establece que: "*No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento 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".*

[129] Artículo 10.3 apartados a) y c), del RD 1720/2007.

[130] PUENTE ESCOBAR, A. "Legitimación para el tratamiento", en MARTÍNEZ MARTÍNEZ, R. (coordinador). *Protección de Datos. Comentarios al Reglamento de desarrollo de la LOPD.* Tirant lo Blanch, Valencia, 2009, pp. 23 y ss.

ciudadanos de un derecho fundamental, de modo que sólo la Ley podrá establecer tales límites, tal y como consagra el artículo 53.1 CE".

Así, el Artículo 7 de la LOPD, circunscribe los supuestos en que cabe tratamiento lícito de los datos especialmente protegidos, lo que, por tanto, significa excluir todos los demás. Obsérvese, en este sentido las fórmulas que emplea: *"2. 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".* En el siguiente apartado del Artículo 7, la LOPD, hace referencia expresa a los datos sobre la salud, manifestando que: *"3. 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 ésta manera, y según el tema que nos ocupa, la información concerniente al ámbito más personal del ser humano, sólo puede ser recabada y tratada si se cuenta con el consentimiento expreso del afectado[131] - en este sentido, como es lógico, el interesado ha de estar debidamente informado y de forma inequívoca y no fraudulenta[132] acerca de la finalidad que la revelación de sus datos tendrá -, como así también de la posibilidad de ejercer sus derechos legales de acceso, rectificación, cancelación y por supuesto, la oposición[133]. Por tanto, podemos señalar que existe una regla genérica y una regla restrictiva para el tratamiento de los datos de carácter sanitario.

Como norma genérica, la Ley sólo autoriza que se traten los datos de carácter personal referidos a la salud en tres supuestos[134]:

---

[131] El Artículo 6.1, de la LOPD, se refiere al consentimiento del afectado estableciendo que: *"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado".*

[132] Expresamente se prohíbe en la LOPD, la recogida de datos a través de la utilización de medios fraudulentos, desleales o ilícitos (Artículo 4.7, sobre calidad de los datos).

[133] El Artículo 5.1, de la LOPD, sobre el derecho de información en la recogida de datos, consagra que: *"1. 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".*

[134] Artículo 7.3, de la LOPD.

(i) En el caso de que el afectado lo consienta expresamente.

(ii) Cuando así lo disponga una Ley[135].

(iii) Por razones de interés general[136].

Sin embargo, existen algunas excepciones en las que la normativa vigente autoriza al personal sanitario perteneciente a Centros de Salud públicos o privados a tener acceso a nuestra historia clínica, contemplando algunas particularidades[137] a la regla general comentada *ut supra*.

Estos supuestos excepcionales son los siguientes:

- Cuando resulte necesario para la prevención o para el diagnóstico médico, 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

[135] Por citar algún ejemplo del supuesto, Ley 14/1986, de 25 de abril, General de Sanidad establece en su Capítulo V sobre la intervención pública en relación con la salud individual y colectiva, en el Artículo 23 que: *"Para la consecución de los objetivos que se desarrollan en el presente Capítulo, las Administraciones sanitarias, de acuerdo con sus competencias, crearán los registros y elaborarán los análisis de información necesarios para el conocimiento de las distintas situaciones de las que puedan derivarse acciones de intervención de la autoridad sanitaria".*

[136] Razón de interés general definida e interpretada por la Jurisprudencia del Tribunal de Justicia de las Comunidades Europeas como el orden público, la seguridad pública, la protección civil, la salud pública, la preservación del equilibrio financiero del régimen de seguridad social, la protección de los derechos, la seguridad y la salud de los consumidores, de los destinatarios de servicios y de los trabajadores, las exigencias de la buena fe en las transacciones comerciales, la lucha contra el fraude, la protección del medio ambiente y del entorno urbano, la sanidad animal, la propiedad intelectual e industrial, la conservación del patrimonio histórico y artístico nacional y los objetivos de la política social y cultural. Asimismo, en la Sentencia del Tribunal de Justicia Europeo (STJE) en el asunto Comisión / Italia C-531/06, y en los asuntos acumulados C-171/07 y C-172/07, el STJE estableció que: *"hay que tener presente que la salud y la vida de las personas ocupan el primer puesto entre los bienes e intereses protegidos por el Tratado y que el Estado miembro puede decidir qué nivel de protección de la salud pública pretende asegurar y de qué manera debe alcanzarse ese nivel".* STJUE, 19 de mayo de 2009 (Asunto Comisión / Italia C-531/06 Nº 44/2009). ECLI:EU:C:2009:316. Disponible en Internet: <http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d696860d54c3404d8dbe76bbbba61bc4d1.e34KaxiLc3eQc40LaxqMbN4PahuPe0?text=&docid=78517&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=8024> [Consulta: 7 julio 2015]; STJUE, 19 de mayo de 2009 (Asuntos acumulados C-171/07 y C-172/07). ECLI:EU:C:2009:315 Disponible en Internet: <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62007CJ0171> [Consulta: 7 julio 2015].

[137] Artículo 7.6, de la LOPD.

sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto[138].

Vemos aquí que el legislador incorpora garantías estrictas para el tratamiento de este tipo de datos especialmente protegidos, puesto que únicamente podrán ser tratados por profesionales sanitarios y guardando el secreto profesional los datos de carácter personal[139]. Aunque, y coincidiendo con la opinión de SANCHEZ-CARO y ABELLÁN[140], la expresión "*otra persona sujeta asimismo a una obligación equivalente de secreto"* puede resultar ambigua, ya que el Derecho español no es unánime la cuestión relativa a cuáles son las actividades respecto de las que cabe afirmar un deber de secreto profesional en sentido estricto.

- También pueden ser objeto de tratamiento los datos de salud, cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento. Se destaca muy especialmente que el paciente -el afectado- no pueda dar su consentimiento por hallarse impedido[141].

- Finalmente, los datos relativos a la salud, pueden ser comunicados a terceros vinculados con el afectado, siempre que medie una urgencia o se tenga que realizar algún estudio de carácter epidemiológico[142].

---

[138] Ibídem.

[139] Recordamos que la referencia "datos personales" engloba aquellos datos que se refieren a la ideología, afiliación sindical, religión y creencias, origen racial, y especialmente a los datos que en esta Tesis nos ocupan que son los vinculados a la salud.

[140] Vid. SÁNCHEZ-CARO, J.; ABELLÁN, F. *Datos de salud y datos genéticos.* Comares, Granada, 2004, p. 32.

[141] La LOPD dice expresamente en su Artículo 7.6, segundo párrafo que: *"También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento".*

[142] El Artículo 11.1, de la LOPD establece 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. 2. El consentimiento exigido en el apartado anterior no será preciso: 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".*

Por su parte, el Artículo 8, de la LOPD establece y regula a propósito del tratamientos de los datos relativos a la salud señalando que sin perjuicio de lo que se dispone en el Artículo 11 de la LOPD 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. Fuera de estos casos, es preciso el consentimiento expreso de los titulares de los datos, o la existencia de una Ley que permita el tratamiento de dichos datos.

Sin embargo, y según la AEPD[143], estas dos últimas especialidades al régimen general, tanto la del Artículo 8 como la del Artículo 7.6 de la LOPD, no pueden interpretarse de forma genérica o extensiva, (por ejemplo, en el sentido de que baste para el tratamiento de los datos la simple expresión de la opinión de un facultativo en tal sentido), sino que debe restringirse a los dos supuestos en que únicamente será de aplicación, esto es: que una disposición normativa establezca y disponga con carácter específico un tratamiento de tales datos, o bien que el mismo resulte efectivamente necesario e imprescindible, y ello se justifique debidamente en cada caso concreto. Fuera de estos dos supuestos excepcionales, el régimen aplicable con carácter general es el del Artículo 7.3 de la LOPD, como recalca la AEPD, que establece que *"Los datos de carácter personal que hagan referencia al origen racial, la salud y a la vida sexual solo podrán ser recabados, tratados y cedidos cuando*, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente".

No sólo la LOPD regula el tratamiento de datos sanitarios, la Ley 14/1986, de 25 de abril, General de Sanidad (LGS), establece en su Artículo 10.3 el derecho del ciudadano a la confidencialidad de sus datos y en el Artículo 23 de la citada Ley, se recoge la potestad de la Administración sanitaria para crear registros y elaborar los análisis de información necesarios para el conocimiento de las distintas situaciones de las que puedan derivarse acciones de intervención de la autoridad sanitaria.

Por su parte, la LAP, establece en su Artículo 9, sobre el respeto a la autonomía del paciente, que:

[143] Informe jurídico 2001/0000 de la AEPD, sobre el Tratamiento de los Datos de Salud. Disponible en Internet: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/index-ides-idphp.phpf> [Consulta: 13 agosto 2016].

> 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 permitan, a sus familiares o a las personas vinculadas de hecho a él[144].

Aquí, observamos que, si bien el consentimiento del paciente es necesario, la Ley prevé una serie de acontecimientos dentro de los cuales, los profesionales de la salud pueden actuar y llevar a cabo su labor, siempre y cuando se haga dentro de los límites que la misma Ley establece. Sobre la citada Ley, BERROCAL LANZAROT[145] mantiene que la LAP ha innovado en su momento puesto que:

> No sólo porque amplía y regula los derechos de los pacientes en materias tan vitales como la información relativa a la salud o el consentimiento del paciente, sino también porque se configura como instrumento de delimitación de los deberes u obligaciones del colectivo sanitario y les exime de responsabilidad dentro del marco establecido en la norma.

1.1.3. Ética sanitaria y el carácter vinculante de los Códigos Deontológicos.

Antiguamente, *el arte de curar*[146] estaba regulado de forma escueta, aunque podemos apreciar varias normas referidas a las profesiones sanitarias, hasta el momento actual,

---

[144] Artículo 9, de la LAP.

[145] BERROCAL LANZAOT, A. I. "El valor de la autonomía del paciente en la Ley 41/2002, de 14 de noviembre, reguladora de los derechos y deberes de los pacientes", en CIENFUEGOS SALGADO, D. (Coord.). *Estudios en homenaje a Marcia Muñoz de Alba Medrano. Bioderecho, tecnología, salud y derecho genómico.* Universidad Nacional Autónoma de México, 2006, pp. 69-142.

[146] La expresión "arte de curar" viene de la previsión que antiguamente contenía la Ley de 1855 y la Instrucción General de 12 de enero de 1904, referidas a la práctica de la medicina. La primera regulación de las profesiones sanitarias en España data de 1848 a través del Reglamento para las Subdelegaciones de Sanidad Interior del Reino, de 24 de julio, que determinaba que el ejercicio de las profesiones de Medicina, Farmacia y Veterinaria estaba comprendido dentro del ramo de la Sanidad. Posteriormente se instituyeron los Jurados Médicos Provinciales de Calificación, a través de la Ley de 28 de noviembre de 1855, sobre el Servicio General de Sanidad, y tenían por cometido la prevención,

en el que nos encontramos, frente a una regulación genérica que requiere una especificidad dada la complejidad que los temas de salud requieren. Frente a ésta necesitad que la sociedad va desarrollando, los Códigos éticos vienen a dar una respuesta adecuada cuando los profesionales se ven desprotegidos y frente a lagunas jurídicas. Por ello, coincidimos con GONZÁLEZ VARAS-IBÁÑEZ[147], al decir que, las regulaciones contenidas en los Códigos éticos son más acertadas porque existe una clara proximidad entre el autor de la norma deontológica y su destinatario, y, por tanto, las disposiciones contenidas en el Código deontológico, regulan la materia con claro conocimiento de causa. Esto importa una buena influencia para el legislador al momento de buscar soluciones normativas.

Tal como se pretende poner de manifiesto en ésta Tesis, las normas que regulan los datos de salud y la historia clínica, no están adaptados a los requerimientos reales. Estamos frente a unos acontecimientos nuevos para la sociedad, que poco a poco comienza a tomar conciencia de la importancia que reviste proteger sus datos, datos tan especiales y sensibles como lo son los datos de salud, contenidos en la HC y en otros soportes que hoy en día resultan posibles, como ordenadores, tablets, teléfonos inteligentes, etc.

---

amonestación y la calificación de las faltas que cometieran los profesionales en el ejercicio de sus facultades, así como regularizar sus honorarios, reprimir los abusos y establecer una severa moral médica. Ya en los años 1855 y 1904, la normativa se preocupó por reglamentar el ejercicio profesional con el establecimiento de un registro de profesionales que pusieron a cargo de los Subdelegados de Sanidad. A partir del año 1944, se promulgaron diversas leyes sanitarias, entre las que la Ley de Bases de la Sanidad Nacional, de 25 de noviembre de 1944, que incorpora la existencia de corporaciones profesionales. Por su parte, la Ley 14/1986, de 25 de abril, General de Sanidad, únicamente se refiere al ejercicio libre de las profesiones sanitarias, pero sin afrontar su regulación, se trata de una norma de naturaleza predominantemente organizativa, cuyo objetivo primordial es establecer la estructura y el funcionamiento del sistema sanitario público en el nuevo modelo político y territorial del Estado que deriva de la Constitución de 1978. En consecuencia, sostenemos que la normativa española carece de una regulación específica y por ello, ha de observarse a las disposiciones diversas contenidas en la regulación del sistema sanitario, las relaciones con los pacientes, y las relativas a los derechos y deberes de los profesionales en cuanto tales o a las que regulan las relaciones de servicio de los profesionales con los centros o las instituciones y corporaciones públicas y privadas, y los Códigos éticos y deontológicos que los vinculan a los profesionales.

[147] GONZÁLEZ-VARAS IBÁÑEZ, A. *Derecho y conciencia en las profesiones sanitarias.* Dykinson, Madrid, 2009, pp. 169 y ss.

Cabe resaltar que la situación de inexistencia de normativa específica y actualizada, unida a la íntima conexión que el ejercicio de las profesiones sanitarias tiene con el derecho a la protección de la salud, con el derecho a la vida y a la integridad física, con el derecho a la intimidad personal y familiar, con el derecho a la dignidad humana y con el derecho al libre desarrollo de la personalidad, aconseja el tratamiento legislativo específico y diferenciado de las profesiones sanitarias[148].

Ante los vacíos legales, que nuestro ordenamiento jurídico presenta al respecto de los temas que aquí se tratan, los Códigos éticos suelen dar respuesta y a la vez sirven de "refugio moral" para los profesionales de la salud. En el mismo sentido, GONZÁLEZ VARAS-IBÁÑEZ[149] sostiene que: *"En un ámbito de constante innovación e implicaciones éticas como el sanitario, los contenidos deontológicos adquieren una particular relevancia".*

Señala, MARTÍNEZ-CALCERRADA[150] que, en el ejercicio profesional del sanitario, un fallo puede tener consecuencias irremediables, porque la vida que se pierde es irrecuperable. En virtud de ello, el autor destaca, acertadamente desde nuestro punto de vista, la responsabilidad moral del médico o de aquellos que cooperan con él. Por respecto a la dignidad del cuerpo humano, sobre el que tiene que actuar el sanitario, los deberes de justicia nunca podrán medirse sólo por los términos estrictos del contrato por lo que quedan ligados el enfermo y el profesional, sino que en atención a esta singular relación humana hacia el semejante y a los valores espirituales que encierra. En esta dirección la función médica es, más que un acto de justicia social, un deber que impone la fraternidad universal con el fin de hacer más llevadero el dolor y la muerte, según entiende el autor.

Las reglas que contienen el Código Deontológico de la Organización Médica Colegial de España (en adelante, CDOMCE)[151] y el Código de Enfermería[152], no deben ser

[148] Exposición de motivos I, de la Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias (BOE núm. 280, 22.11.2003).

[149] GONZÁLEZ-VARAS IBÁÑEZ, A., op. cit., pp. 149 y ss.

[150] MARTÍNEZ-CALCERRADA, L. *Derecho Médico. Volumen I. Derecho Médico General y Especial.* Tecnos, Madrid, 1986, p. 139.

[151] En España está vigente el denominado Código de Deontología Médica y Guía de Ética Médica de 1999 y actualizado por la Organización Médica Colegial en 2011 (CDOMCE). Su contenido se puede dividir en tres grandes apartados: la relación con el paciente, la relación interprofesional y la relación con la sociedad. Código de Deontología Médica. Guía de ética médica. Organización Colegial Médica de España. Disponible en Internet:

miradas como meras normas éticas a tener en cuenta. Los códigos éticos y deontológicos, se aprueban por el respectivo colegio profesional, y sus disposiciones tienen plena eficacia jurídica respecto a sus colegiados.

Cuando el profesional médico ejerce su profesión, está sujeto tanto a las leyes como a las normas contenidas en el Código ético que rige su profesión. Para poder desarrollarse profesionalmente, es requisito en España pertenecer a un Colegio Profesional. Por ello, el Colegio obliga al acatamiento de las prácticas contenidas en el Código de ética y deontología. Es más, de hacer caso omiso a las disposiciones deontológicas, el profesional incurrirá en una falta. La falta puede calificarse como menos leve, leve y grave. Resulta importante la observancia de éstas disposiciones mientras el sanitario ejerce su profesión, porque la falta le puede acarrear, según la gravedad de la misma, la suspensión del Colegio profesional o, incluso en casos graves, se puede llegar a apartar al profesional sanitario de su profesión.

MARTÍN MATEO[153] sostiene que los Códigos deontológicos adquieren un doble carácter vinculante para el destinatario. Considerado como miembro del colectivo profesional, debe atenerse a su contenido en cuanto que informa la *lex artis* de su profesión. En cuanto ciudadano, debe respetarlo del mismo modo que se deben observar las demás normas del ordenamiento jurídico. También CASADO[154], entiende del mismo modo, que el profesional de la medicina ha de estar vinculado al Código deontológico de su profesión y en constante observancia de las leyes en la materia.

<http://www.cgcom.es/sites/default/files/codigo_deontologia_medica_1.pdf> [Consulta: 15 julio 2015]. El CDOMCE no es el único que existe en España, ya que el Consell de Col·legis de Metges de Catalunya, tiene su propio Codi de Deontologia (CDC), aprobado en 1997 y actualizado en 2005, donde hay que señalar, con respecto al nacional, que introdujo como novedad el derecho a la huelga en los artículos 92 y 93. También fue novedoso el artículo 54 sobre la relación con la industria farmacéutica, un aspecto que el CDM español no incluía en su versión de 1999, aunque el CDOMCE lo incorporó en la vigente actualización del CDM desde 2011. Codi de Deontologia. 1997. Consell de Col·legis de Metges de Catalunya. Disponible en Internet: <https://www.comb.cat/cat/colegi/docs/codi_deontologic.pdf> [Consulta: 16 julio 2015].

[152] Código Deontológico de la Enfermería Española, de 14 de julio de 1989, aprobado por la Resolución Nº 32/1989 del Consejo General de Enfermería Disponible en Internet: <http://www.codem.es/codigo-deontologico> [Consulta: 16 julio 2015].

[153] MARTÍN MATEO, R. *Bioética y derecho.* Ariel, Barcelona, 1987, p. 57.

[154] CASADO, M. "Ética, Derecho y deontología profesional*". Derecho y Salud*. Vol. 6, núm. 1, 1998, p. 34.

Y todo ello, reviste especial trascendencia a la hora de proteger los datos de salud que el personal sanitario trata diariamente y que toma conocimiento de ello en base a su profesión, porque donde la normativa vigente sobre protección de datos no alcance, el Código ético será el encargado de suplir tal laguna. En este sentido, 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[155]. Asimismo, la enfermera o enfermero, debe guardar en secreto toda la información sobre el paciente que haya llegado a su conocimiento en el ejercicio de su trabajo[156].

2. Principios que se aplican al tratamiento de los datos personales.

Los datos personales únicamente pueden ser recabados[157] atendiendo a las limitaciones legales existentes. Estas limitaciones vienen a jugar el papel de las garantías que de ellas se desprenden a los afectados. Es por ello, que estas limitaciones o principios han de ser observados por quienes recopilan datos sensibles o los tratan. La legislación de protección de datos en nuestro país se asienta sobre ésta serie de principios que constituyen una garantía para la protección de datos personales.

En referencia a los principios a los que deben observarse y respetarse para poder tratar datos de salud, sostiene GUZMÁN GARCÍA[158] que:

---

[155] Artículo 27, del CDOMCE.

[156] Artículo 19, Código Deontológico de la Enfermería Española, op. cit.

[157] La recogida de datos hace referencia a cualquier procedimiento en virtud del cual los datos del paciente llegan al conocimiento y disponibilidad del responsable del fichero, siendo, por tanto, la comunicación de los datos personales por el interesado al responsable del fichero o la obtención de dichos datos por otros medios distintos del propio afectado. Sostiene LESMES SERRANO que los procedimientos de recogida de datos pueden ser diversos: declaraciones o formularios, encuestas o entrevistas, transmisión electrónica de datos, directorios electrónicos o comerciales, páginas Web, etc. Vid. LESMES SERRANO, C. (Coordinador). *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia.* Lex Nova, Valladolid, 2008, pp. 142 y ss.

[158] GUZMÁN GARCÍA, M. Á. *El derecho fundamental a la protección de datos personales en México: Análisis desde la influencia del ordenamiento jurídico español.* Tesis doctoral inédita. Universidad Complutense de Madrid. Facultad de Derecho. Madrid, 2013, p. 208. Disponible en Internet:

> Estos principios sirven para delimitar el marco en el que debe desenvolverse cualquier uso o cesión de los datos de carácter personal y para integrar la definición de los tipos de infracción definidos en el Artículo 44 LOPD, pues este precepto aborda la tipificación de las distintas infracciones mediante una remisión a los principios definidos en la propia Ley.

La Agencia de Protección de Datos de la Comunidad de Madrid[159] (en adelante, APDCM), define a los principios entendiendo que:

> Estos principios constituyen la base mediante la cual se articula el derecho fundamental a la Protección de Datos de Carácter Personal, siendo de obligado cumplimiento desde el momento en que se produce la recogida de datos de un afectado o interesado (ciudadano), siempre y cuando dichos datos sean almacenados en un fichero, ya sea informatizado, manual o parcialmente automatizado.

La LOPD regula los principios de la protección de datos, abocándose a ellos en el Título II[160]. Así también el RD 1720/2007, de 21 de diciembre, se ocupa de legislar estos principios[161].

Desde el ámbito comunitario, la Directiva 95/46/CE, otorga la pauta que los Estados miembros han de tener en cuenta a la hora de legislar en sus propios ordenamientos jurídicos con la finalidad de garantizar el proceso del tratamiento de datos y establece de manera expresa una serie de principios relativos a la legitimación de tratamiento de datos[162].

<http://eprints.ucm.es/22817/1/T34727.pdf> [Consulta: 10 julio 2016].

[159] APDCM. *Protección de datos personales para Servicios Sanitarios Públicos.* Thomson-Civitas, Madrid, 2008, pp. 531 y ss.

[160] Título II, Artículos 4 a 12, de la LOPD.

[161] RD 1720/2007, Título II, Artículos 8 a 11.

[162] En su Artículo 7, la Directiva 95/46/CE, establece 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, o 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*

Por su parte, la Carta de los Derechos Fundamentales de la Unión Europea[163], refiere expresamente al derecho de la protección de datos en su Artículo 8, reconociéndolo como un derecho que tiene toda persona a los datos que le conciernen, como así también que sus datos han de tratarse de manera leal y para fines concretos, y ello con el consentimiento de la persona afectada, o en virtud de un fundamento legal y establece que el control sobre estas normas ha de ser ejecutado por una autoridad independiente[164].

A continuación, explicaremos brevemente en qué consiste cada uno de éstos principios que deben considerarse a la hora de tratar datos personales, con especial atención a los datos de salud.

2.1. Principio de calidad de datos.

Este principio descansa en la premisa de la proporcionalidad de los datos, es decir, es necesario que los datos sean adecuados a la finalidad que motiva su recogida[165]. El principio de calidad de los datos viene recogido en el Artículo 4, de LOPD.

Asimismo, la APDCM entiende que el principio de calidad de los datos está basado, además del criterio de proporcionalidad, en un criterio de racionalidad[166]. En esta Tesis

---

libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del Artículo 1 de la presente Directiva".

[163] Carta de los Derechos Fundamentales de la Unión Europea (DOCE C 364, 18.12.2000, pp. 1-22).

[164] El Artículo 8, de la Carta Europea de Derechos Fundamentales de la Unión Europea, de diciembre de 2000, recoge expresamente el derecho a la protección de datos de carácter personal, estableciendo que: *"1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. 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 la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".*

[165] Para profundizar más al respecto, véase: SANZ CALVO, L. *Artículo 4. Calidad de los datos. La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia.* Lex Nova, Valladolid, 2007, pp. 137 y ss.; AGÚNDEZ LERÍA, I. *Artículo 8. Principios relativos a la calidad de los datos. Protección de datos. Comentarios al Reglamento.* Lex Nova, Valladolid, 2008, pp. 140 y ss.

[166] APDCM, op. cit., pp. 531 y ss.

se sustenta idéntica premisa. En el mismo sentido, SANCHEZ-CARO y ABELLÁN[167], entienden que la recogida y el proceso debe estar presidido por el principio del uso legítimo, en el sentido de que la recogida y el manejo de los datos sobre la salud, debe obedecer estrictamente al propósito legítimo que justifique su utilización (que será normalmente la protección de la salud), sin que en ningún caso terceras personas puedan tener acceso directo a los mismos.

El Artículo 5, del Convenio 108[168], consagra el principio de calidad de los datos y en él se engloban los principios de lealtad, licitud, finalidad, pertinencia, proporcionalidad, exactitud o veracidad y conservación de los datos. Asimismo, el Artículo 6 del Convenio 108[169], refiere expresamente a los datos especialmente protegidos, haciendo mención expresa a los datos de salud, promulgando que sólo pueden tratarse si los ordenamientos internos de los Estados miembros prevén garantías para ello.

Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos al mismo, 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[170]. Asimismo, resulta necesario para determinar la calidad de los datos, que los mismos sean exactos y que se encuentren actualizados[171]. Lo que, evidentemente, en el ámbito de los datos de salud es absolutamente necesario, puesto que las patologías, enfermedades y tratamientos siempre tienen unas consecuencias que, de no estar debidamente acreditado y actualizado, podría dar lugar a una

[167] SÁNCHEZ-CARO, J.; ABELLÁN, F., op. cit., p. 19.

[168] El Artículo 5, del Convenio 108, en relación con la calidad de los datos establece que: *"Los datos de carácter personal que sean objeto de un tratamiento automatizado: a) Se obtendrán y tratarán leal y legítimamente; b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán 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 conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado".*

[169] El Artículo 6, del Convenio 108, hace referencia a las categorías particulares de datos, estableciendo 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".*

[170] Artículo 4.1, de la LOPD.

[171] Artículo 4.3, de la LOPD.

actuación médica equivocada, a un mal diagnóstico o incluso a que no se prescriba un determinado tratamiento.

En virtud de ello, los datos deben recogerse con un objetivo determinado y fijo. Además, cabe destacar, que, si los datos son transferidos con posterioridad, se debe tener en cuenta y ha de mirarse al objetivo inicial para el cual fueron recopilados. De lo contrario, es necesario el consentimiento expreso del interesado[172].

La Directiva 95/46/CE consagra en su Artículo 6, que el tratamiento de los datos, ha de hacerse de manera leal y lícita; con fines determinados, explícitos y legítimos, y que los datos no sean tratados posteriormente de manera incompatible con dichos fines. Aunque, destaca la norma, que 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. También menciona que los datos recopilados han de ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente; 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; y finalmente, destaca que los datos han de ser 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[173].

Sin embargo, y a la postre de lo analizado, se evidencia que la Directiva 95/46/CE y el Convenio 108, no son homogéneos en la regulación de los principios de tratamiento de

---

[172] Al respecto, el Informe jurídico de la AEPD 0488/2008, sostuvo que: *"la ausencia de una Ley que legitime la recogida, tratamiento y comunicación de los datos de salud, determina que para ello se deba obtener el consentimiento expreso del afectado".* Informe jurídico 0488/2008 de la AEPD. Disponible en Internet: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/common/pdfs/2008-0488_Tratamiento-y-Cesi-oo-n-de-datos-de-salud-con-finalidad-desconocida.pdf> [Consulta: 18 septiembre 2016].

[173] Artículo 6.1, de la Directiva 95/46/CE. Para profundizar más al respecto, véase: PRIETO ANDRÉS, A. "La nueva Directiva europea sobre el tratamiento de los datos personales y la protección de la intimidad en el sector de las telecomunicaciones". *La Ley*. Año XXIII, núm. 5620, 26 de septiembre de 2002, pp. 1-3.

los datos personales. ARENAS RAMIRO[174] entiende que el amplio margen de actuación deja en manos de los Estados miembros la posibilidad de dotar de más garantías a la protección de datos, no existiendo por dicha razón un criterio unánime de los países, opinión que compartimos y que la UE ha intentado dar solución a través del recientemente aprobado Reglamento General de Protección de Datos, que analizaremos en la Segunda Parte de este trabajo.

Por tanto, dentro del principio de calidad de los datos, podríamos diferencias algunos pilares que el mismo Artículo 4 de la LOPD establece, sobre el que se asienta, y a continuación desarrollaremos.

a) Adecuación de los datos.

El principio de adecuación de los datos, o lo que es lo mismo, según lo denominan SÁNCHEZ-CARO y ABELLÁN[175], principio de pertinencia y proporcionalidad, viene a establecer que los datos médicos que se recojan, siempre han de ser los necesarios para los fines que han de ser tratados[176]. Asimismo, se añade otra exigencia y es que

[174] Vid. ARENAS RAMIRO, M. *El derecho fundamental a la protección de datos personales en Europa.* Tirant lo Blanch, Valencia, 2006, pp. 317.

[175] SÁNCHEZ-CARO, J.; ABELLÁN, F., op. cit., p. 19.

[176] En este sentido se ha pronunciado la doctrina, véase al respecto: TRONCOSO REIGADA, A., "Título II. Principios de la Protección de Datos. Artículo 4", en TRONCOSO REIGADA, A. *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Civitas, Madrid, 2010, pp. 340-394.; APARICIO SALOM, J. "Título II. Principios de la Protección de Datos. Artículo 4", en TRONCOSO REIGADA, A. *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Civitas, Madrid, 2010, pp. 323-340.; GUTIÉRREZ CALVO, M., "Problemas jurídicos derivados de la aplicación del principio de calidad del dato por parte de las Administraciones Públicas". *REDUR.* Núm. II, diciembre 2013, pp. 169-198. Disponible en Internet: <http://www.unirioja.es/dptos/dd/redur/numero11/gutierrez.pdf> [Consulta: 10 julio 2016]; ARIAS POU, M. "Cumplir la normativa sobre protección de datos en el entorno laboral". *Revista de Estudios Locales.* Núm. 113, septiembre, 2008, pp. 1-19. Disponible en internet: http://www.navarra.es/NR/rdonlyres/DCF7A5483551481C8CE46CBD251352BC/162689/3CumplimientoNormativaEntornoLaboral.pdf [Consulta: 10 julio 2016]. Asimismo, el principio de adecuación de datos, es tratado por algunos Códigos éticos profesionales, al entenderse que, para la realización de determinada práctica médica, intervención o tratamiento, es menester recabar exclusivamente datos que guarden estricta relación con dicha intervención, no pudiendo exceder de los rigurosamente necesarios. Al respecto, el Código Tipo de Tratamiento de Datos de Carácter Personal para Odontólogos y Estomatólogos de España, establece en su Artículo 5 que: *"Los datos de carácter personal recabados a los pacientes o usuarios de los servicios de salud bucodental por parte de los*

los mismos se encuentren actualizados para que el paciente pueda recibir la correcta atención[177].

En este sentido, la LOPD[178] deja claro que los datos de carácter personal sólo pueden ser recogidos para su tratamiento, así como sometidos 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 obtenidos[179].

La legislación sanitaria añade a la pertinencia y adecuación de los datos, el calificativo de "trascendental" que refuerza la relación y la conservación de los datos personales con las finalidades que motivan su recogida y su almacenamiento, particularidad que será valorada por el profesional sanitario. Según CRIADO DEL RIO[180], el contenido de la historia clínica debe ser completo, ordenado y actualizado, inteligible, respetuoso, rectificado y aclarado, veraz y en el soporte documental adecuado, en relación con el principio en cuestión.

Adheridos al Código, deberán ser adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. En este sentido únicamente se recabarán los datos necesarios para la prestación de los servicios de salud bucodental que resulten necesarios para la correcta atención del paciente o usuario de estos servicios y no podrán recabarse otros datos personales que no sean completamente necesarios para su atención, salvo consentimiento expreso". Disponible en Internet: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/common/pdfs/codigo_tipo_consejo_estomat_odont_dic_2009.pdf> [Consulta: 15 julio 2015]

[177] Ésta exigencia guarda estrecha relación con el principio de certeza de los datos, por el cual se exige que los datos de los pacientes se encuentren al día para brindar una atención óptima al afectado.

[178] El Artículo 4.1, de la LOPD exige que los datos sean adecuados, pertinentes y no excesivos en relación con las finalidades para las que se hayan recabado. La recogida y el tratamiento de datos sanitarios persiguen una finalidad principal intrínsecamente ligada a la finalidad de la historia clínica que es según el Artículo 16.1 de la Ley 41/2002 *"garantizar una asistencia adecuada al paciente"*. Esta finalidad determina a su vez la pertinencia y adecuación de los datos que recoja. Así lo recoge el Artículo 15.2 al señalar que el fin principal de la historia clínica es facilitar la asistencia sanitaria para lo cual según el apartado primero incorporará *"la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente"*.

[179] Ibídem.

[180] Vid. CRIADO DEL RIO, Mª T. *Aspectos médico-legales de la historia clínica.* Colex, 1999, pp. 51 y ss.

b) Finalidad de los datos.

Cuando se recaben datos médicos del paciente, los mismos han de servir a una necesidad específica y concreta, que responda a la atención médica que deba recibir el afectado. En relación con ésta finalidad se requerirán unos determinados datos[181] y ésta finalidad tiene un doble límite. Por un lado, los datos recogidos no pueden no guardar relación con el proceso asistencial que deba llevarse a cabo. Así, por ejemplo, si consultamos a un odontólogo para un tratamiento dental, no es necesario que en el formulario que se nos presenta antes de la consulta informemos si hemos sido sometidos a una cirugía estética, el estado civil, etc. Por otro lado, estos datos que el paciente suministra única y exclusivamente pueden ser utilizados para el fin asistencial, por ejemplo, si he acudido al odontólogo para que se me practique una limpieza dental, no pueden enviarme publicidad de productos para mantener una higiene bucal, salvo que hayamos dado nuestro consentimiento expreso para recibir esa información o publicidad.

La LOPD 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"*[182]*.*

En el mismo sentido, la Directiva 95/46/CE contempla lo siguiente:

> 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

[181] Resulta interesante el Artículo 6, del Código Tipo de Tratamiento de Datos de Carácter Personal para Odontólogos y Estomatólogos de España que regula expresamente ésta circunstancia, prohibiendo usos comerciales de los datos: *"Los datos de carácter personal recabados por parte de los Adheridos al Código únicamente podrán utilizarse para la prestación de los servicios solicitados por el paciente o usuario de los servicios de salud bucodental. En ningún caso, podrán utilizarse dichos datos para otras finalidades. En este sentido queda expresamente prohibida la utilización de datos recabados de pacientes para fines comerciales o publicitarios, salvo en aquellos casos en que previamente se haya informado y recabado el consentimiento de la forma establecida en el presente Código Tipo para estos fines".*

[182] Artículo 4.2, de la LOPD.

objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados[183].

Cabe destacar aquí, la previsión legal que hace la legislación del País Vasco al respecto, porque resulta muy clarificadora del principio que nos ocupa, estableciendo que: "[…] *sólo podrán utilizarse para las finalidades determinadas, explícitas y legítimas para las que se hubieran obtenido, sin perjuicio de su posible tratamiento posterior para fines históricos, estadísticos o científicos, de acuerdo con la legislación aplicable"*[184].

c) Certeza de los datos.

Este principio consiste en que los datos que se recopilen deben guardar relación con la realidad del paciente. Si es el mismo afectado el que declara sobre sus datos personales, éstos se tienen por veraces ante la Ley. De esta manera, LOPD 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"*[185]. Este deber que pesa sobre el paciente, en el ámbito de la sanidad resulta especialmente relevante en méritos al interés vital que tiene el interesado en adecuar los datos incluidos en su historia clínica, con su realidad. Y a la vez, la LOPD señala la obligación que corresponde al responsable del fichero acerca de la rectificación, cancelación y sustitución de los datos incompletos o inexactos por los correctos, tema que analizaremos más adelante.

De la misma manera lo recoge la LAP[186] al disponer que la historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. También dispone en su Artículo 15.2 que la historia clínica tendrá como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud. Corresponderá a las Administraciones Sanitarias, según el Artículo 14.3, establecer los mecanismos que garanticen la autenticidad del contenido de la historia clínica y los cambios operados en ella. Por otro lado, el Artículo

[183] Considerando (28), de la Directiva 95/46/CE.

[184] Artículo 5, de 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.

[185] Artículo 4.3, de la LOPD.

[186] Artículo 15.1, de la LAP.

17.3 habla de la responsabilidad de los profesionales sanitarios en orden a la creación y mantenimiento de una documentación clínica ordenada y secuencial del proceso asistencial de los pacientes, mientras que el Artículo 17.5 responsabiliza de todo ello, a los profesionales sanitarios que trabajen de manera individual.

Resulta relevante éste principio en el terreno sanitario, porque el hecho de "tener al día" nuestra historia clínica, facilitará cualquier intervención médica que deba practicarse en nuestro beneficio. Por el contrario, no tener los datos de salud al día puede suponer un grave perjuicio para el paciente.

d) Cancelación de los datos.

El Artículo 4.5 de la LOPD, recoge la cancelación de los datos cuando hayan dejado de ser necesarios o pertinentes en relación con la finalidad para la que fueron recopilados. La vinculación entre el almacenamiento de los datos y su finalidad presenta en el ámbito sanitario alguna singularidad puesto que es factible que sea necesario mantener los datos sanitarios en caso de tratamientos médicos prolongados o enfermedades crónicas en las que probablemente nunca llega a romperse la conexión entre la finalidad y el mantenimiento del dato.

En relación con ello, el Artículo 17 de la LAP, señala la obligación de los centros sanitarios de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque, aclara, que no resulta necesario que tal almacenamiento se efectúe en soporte original, y deja a criterio del médico el período necesario en cada caso, para mantener dicha información, sin embargo, establece un tiempo mínimo de 5 años desde el momento del alta del paciente.

La excepción a la cancelación de los datos sanitarios la constituye su conservación a efectos judiciales, por razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. En estos casos y dentro de lo posible, se evita la relación de los datos con las personas afectadas[187], utilizando procesos de anonimización, según se explicará más adelante.

[187] Artículo 17.2, de la LAP.

La posibilidad de que el paciente cancele sus datos sanitarios, contenidos en su historial clínico, ha suscitado dudas desde el punto de vista legal y doctrinal[188]. Se trata de un derecho con un alcance controvertido. Sostiene al respecto RODRIGO DE LARRUCEA[189] que nos encontraríamos en un vacío legal, si un paciente decide cancelar sus datos contenidos en la historia clínica, y como consecuencia de una intervención médica, se produce el fallecimiento del mismo. En este caso, si por parte de sus herederos se pretende iniciar la vía judicial para despejar posibles responsabilidades médicas, se carecerían de los datos necesarios para poder establecer el nexo de causalidad entre el fallecimiento, la intervención médica y los antecedentes médicos del paciente, que a la postre podrían indicarnos de forma evidente, por ejemplo, que el difunto era alérgico a determinado medicamente y éste le fue suministrado durante la intervención.

También la LOPD es la encargada de señalar al responsable del tratamiento como el obligado de hacer efectivo el derecho de rectificación o cancelación del interesado y para ello, se le concede un plazo legal de tan sólo diez días[190]. Los datos de carácter personal que deberán ser rectificados o cancelados, cuando tales datos resulten inexactos o incompletos, serán los indicados por el interesado. 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, según indica el precepto legal.

Sin embargo, aquí advertimos un inconveniente que consiste en la falta de preparación por parte del facultativo sanitario en el ámbito jurídico. Entendemos que es una carga excesivamente onerosa que se añade al profesional médico, que no tiene por qué conocer los plazos de prescripción que conlleva un procedimiento judicial por responsabilidad médica[191], que según sea el caso, no es el mismo.

---

[188] Ver al respecto MÉJICA, J. DÍEZ, J. R. *El Estatuto del Paciente. A través de la nueva legislación sanitaria estatal.* Thomson-Civitas, Navarra, 2006, pp. 201 y ss.

[189] RODRIGO DE LARRUCEA, C. Conversaciones informales en el marco de las reuniones de los miembros de la Comisión de Derecho Sanitario del ICAB, Barcelona 2016.

[190] Artículo 16, de la LOPD.

[191] Vid. RODA GARCÍA, L.; GALÁN CORTÉS, J. L. "Las historias clínicas y su incorporación a los expedientes judiciales". *Actualidad del Derecho Sanitario.* Núm. 33, 1997.

Al respecto, también el CDOMCE[192] tiene una previsión en la que se señala 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, sostiene el CDOMCE. Nos resulta curiosa ésta previsión deontológica, puesto que al mencionar que la documentación clínica ha de mantenerse mientras resulte favorable para el paciente, adolece de una ambigüedad manifiesta. No se especifica de manera alguna cómo ha de interpretar el médico si los datos contenidos en la historia clínica de un paciente le pueden resultar más o menos favorables, o que tengan alguna incidencia en futuras posibles patologías. Así también, deja la puerta abierta a mantener los datos por el tiempo que la legislación lo estipule. Porque, como hemos puesto de manifiesto ut supra, la normativa remite a las posibles responsabilidades médicas y a sus plazos de prescripción. Por tanto, si conjugamos la Ley y el CDOMCE apreciamos una clara incongruencia que lo único que haría es remitir de un ordenamiento a otro sin ofrecer solución alguna.

e) Almacenamiento de los datos.

Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados. En este punto vemos que los datos sanitarios han de almacenarse, sin importar el soporte, y con las peculiaridades que pusimos de manifiesto *ut supra*, pero no queda claro si el paciente decide cancelar sus datos, si en ese supuesto los datos sanitarios deben mantenerse, únicamente a disposición de la Administración o de Jueces y Tribunales para poder, en su caso, dirimir posibles responsabilidades, tal y como prescribe el Artículo 16, de la LOPD. Porque, a tenor de lo planteado, la LOPD establece que no serán conservados los datos personales 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[193], existiendo desde nuestro punto de vista, una incoherencia entre los preceptos citados.

[192] Artículo 19.3, del CDOMCE.

[193] Artículo 4.5, de la LOPD.

f) Fraude en la recopilación de los datos.

La recogida de datos personales por medios fraudulentos, desleales o ilícitos está absolutamente prohibida. Se trata de una prohibición que lleva aparejada una infracción y puede incluso derivar en responsabilidad penal. Concretamente la LOPD, tipifica como infracción muy grave en su Artículo 44.4.a), la recogida de datos en forma engañosa o fraudulenta.

De la misma manera, la Directiva 95/46/CE consagra en su Artículo 6, que el tratamiento de los datos ha de hacerse de manera leal y lícita[194].

2.2. Principio de información.

Este principio implica el deber y el derecho de información. Supone que antes de tratar los datos personales habrá que informar al paciente sobre quién los tratará y para qué, también se debe informar sobre la identidad y dirección del responsable del tratamiento. Al respecto, SANCHEZ-CARO y ABELLÁN[195], definen al principio de información, diciendo que el afectado ha de estar informado sobre los datos que se recaban sobre él, conociendo esencialmente quién, cómo y para qué se tratan sus datos.

La LAP regula de forma separada dos conceptos que se encuentran vinculados estrechamente entre sí. Por un lado, la información clínica o asistencial[196] y, por otro lado, el consentimiento informado. La distinción tiene su razón de ser en que el derecho de información establece quién ha de informar y tiene el deber de hacerlo, a quién debe informar y de qué exactamente[197]. Por su parte, el derecho al consentimiento informado viene a formar parte de la faceta de quién debe consentir, cómo y en qué casos el consentimiento no es necesario[198].

---

[194] Artículo 6.1, de la Directiva 95/46/CE.

[195] SÁNCHEZ-CARO, J.; ABELLÁN, F. *Datos de salud y datos genéticos.* Comares, Granada, 2004, p. 30.

[196] El Artículo 3, de la LAP, define al concepto "Información clínica" como: "*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*".

[197] La LAP regula principalmente en sus Artículos 4 y 5 el derecho de información.

[198] La LAP se ocupa de las bases legales principalmente en sus Artículos 8, 9 y 10 del consentimiento informado, de sus límites y de las condiciones para otorgarlo.

La LAP[199] responsabiliza al médico del deber de información y a los profesionales que atienden a la persona afectada. En este sentido el CDOMCE sostiene que, un elemento esencial de la información debida al paciente es darle a conocer la identidad del médico que en cada momento le está atendiendo. Y también entiende que el hecho de que la atención medica recaiga en un equipo de trabajo, esto no puede ser óbice de que el paciente conozca cual es el médico responsable de la atención que se le presta y que será su interlocutor principal ante el equipo asistencial[200].

La LAP vislumbra algunas condiciones por parte del médico para que brinde la información al paciente, con la finalidad de obtener su consentimiento. En su Artículo, 10 establece que:

> El facultativo proporcionará al paciente, antes de recabar su consentimiento escrito, la información básica siguiente: Las consecuencias relevantes o de importancia que la intervención origina con seguridad. Los riesgos relacionados con las circunstancias personales o profesionales del paciente. Los riesgos probables en condiciones normales, conforme a la experiencia y al estado de la ciencia o directamente relacionados con el tipo de intervención. Las contraindicaciones.

Es decir, que ésta información, ha de ser clara, desde el punto de vista de la comprensión del paciente, atendiendo a su edad y sus posibles conocimientos, para que comprenda exactamente cuáles son las ventajas y cuáles podrían ser los inconvenientes que se podrían derivar de determinado tratamiento[201].

---

[199] El Artículo 4.3, de la LAP establece que: *"El médico responsable del paciente le garantiza el cumplimiento de su derecho a la información. Los profesionales que le atiendan durante el proceso asistencial o le apliquen una técnica o un procedimiento concreto también serán responsables de informarle".*

[200] Artículo 10, apartados 2 y 3, del CDOMCE.

[201] Especifica el TS, que en cumplimiento del Artículo 10 (5) de la Ley General Sanitaria, la información debe ser completa, comprendiendo los pros y contras de la actuación sanitaria y las opciones posibles al respecto, con inclusión de los riesgos, que la literatura científica conoce y describe como anudados al tipo de intervención de que se trata, y desde luego, personalizados en función de las características del paciente (edad, padecimientos anteriores, etc.), (STS de 17 de Octubre de 2001, RJ 2001\8741). Para profundizar más sobre el análisis de ésta Sentencia, véase: DOMÍNGUEZ LUELMO, A. *Derecho sanitario y responsabilidad médica. Comentarios a la Ley 41/2002 de 14 de noviembre, sobre derechos del paciente, información y documentación clínica.* 2ª Edición, Lex Nova, Valladolid, 2007, pp. 226 y ss.; GARRIDO CORDOBERA, L. M.; BUSTO LAGO, J. M. *Los riesgos del desarrollo en una visión comparada. Derecho argentino y Derecho español.* Reus, Madrid, 2010, pp. 260 y ss.

A nivel europeo, y en relación con el principio de información que nos ocupa, la Directiva 95/46/CE[202], establece para el caso en que los datos sean recabados del propio interesado, que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, al menos la siguiente información:

> 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:
> - 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.

Asimismo, es obligación del titular del fichero, informar a la persona sobre su posibilidad de ejercer los derechos legales de acceso, rectificación, cancelación y oposición, si así lo estimase conveniente[203]. La LOPD[204], ampliando las garantías establecidas por la Directiva 95/46/CE, consagra que:

> 1. 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.

Respecto al principio de información en el ámbito autonómico, fue recogido de la siguiente manera. Por ejemplo, en Cataluña[205] se ha establecido que:

---

[202] Artículo 10, de la Directiva 95/46/CE.

[203] Artículo 5. 1, 15, 16 y 17, de la LOPD.

[204] Artículo 5. 1, de la LOPD

[205] Artículo 23.3, del Estatuto de Autonomía de Cataluña (BOE núm. 172, 20.07.2006).

> Todas las personas, con relación a los servicios sanitarios públicos y privados, tienen derecho a ser informadas sobre los servicios a que pueden acceder y los requisitos necesarios para su uso; sobre los tratamientos médicos y sus riesgos, antes de que les sean aplicados; a dar el consentimiento para cualquier intervención; a acceder a la historia clínica propia, y a la confidencialidad de los datos relativos a la salud propia, en los términos que se establecen por ley.

En la Comunidad Autónoma de Cataluña, es competencia de la Agencia Catalana de Protección de Datos, la encargada de mediar en los asuntos relativos a los datos de carácter personal. El Decreto que aprueba el Estatuto Catalán[206], sostiene que: *"6.1 la agencia Catalana de Protección de datos informará a las personas de los derechos que la ley les reconoce en relación con el tratamiento de datos personales. a estos efectos podrá realizar campañas de difusión. 6.2 la agencia atenderá y dará respuesta a las peticiones que le dirijan las personas afectadas, sin perjuicio de los recursos que puedan interponer"*[207].

En la Comunidad de Madrid, se dispone a través de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal, en relación con el derecho de información en la recogida de datos de carácter personal, que: *"Los interesados cuyos datos personales sean objeto de tratamiento deberán ser previamente informados de modo expreso, preciso e inequívoco de los extremos señalados en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, en la forma y condiciones establecidas en ese mismo artículo".*

Por su parte, la legislación del País Vasco[208] introduce una diferencia sustancial al respecto. Concibe su normativa que, queda en manos del Director de la Agencia Vasca

---

[206] Artículo 6, de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal de la Comunidad de Madrid (BOE núm. 245/2001, 12.10. 2001).

[207] Artículo 5, del Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos (DOGC núm. 3835, 4.03.2003).

[208] El Artículo 6, de 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, op. cit., consagra que: *"Los interesados a los que se soliciten datos de carácter personal serán previamente informados, de conformidad con la legislación sobre protección de dichos datos. No obstante, cuando los datos no hayan sido recabados del propio interesado y la información a éste resulte imposible o exija esfuerzos desproporcionados, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias, el director de la Agencia Vasca de Protección de Datos, de acuerdo con la susodicha legislación, podrá dispensar al responsable del fichero de la obligación de informar a los interesados".*

de Protección de Datos, dirimir si es menester o no informar al interesado o a los interesados, si fuese el caso, cuando ello resulte complicado o difícil de realizar conforme se haría normalmente, por parte del responsable del fichero.

El derecho de información que asiste a la persona, también se deberá observar, indistintamente de si los datos han sido recabados directamente por parte del mismo paciente o no, con la salvedad de que una disposición legal prevea lo contrario[209].

Asimismo, el CDOMCE[210] expone que el médico está obligado a brindarle toda la información al afectado, tanto información sobre los datos que se solicitan a fin de tratarle, como de hacerle conocer fehacientemente el diagnóstico, la enfermedad que padece y el tratamiento a seguir. Sin embargo, el afectado puede negarse a oír esta información por parte del médico o de la persona encargada. Por tanto, el principio de información es facultativo desde el punto de vista del paciente. En éste sentido se refirió la Organización Mundial de la Salud[211], al entender que, si el paciente lo solicita explícitamente, no debe ser informado. Es por ello que, sostenemos, que el derecho a la información, es un derecho que ha de considerarse como potencial, ya que es el mismo paciente el que puede decidir si quiere o no hacer uso del mismo.

En caso de no querer conocer la información sobre su salud, y tal como queda de manifiesto en la parte final del Artículo 10.1 del CDOMCE[212], el médico deberá notificar a los parientes o amistades cercanas del diagnóstico efectuado.

---

[209] El Artículo 5, de la LOPD establece que: *"Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: 4. 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".*

[210] El Artículo 10, del CDOMCE, manifiesta que: *"1. Los pacientes tienen derecho a recibir información sobre su enfermedad y el médico debe esforzarse en dársela con delicadeza y de manera que pueda comprenderla. Respetará la decisión del paciente de no ser informado y comunicará entonces los extremos oportunos al familiar o allegado que haya designado para tal fin".*

[211] Declaración para la promoción de los derechos de los pacientes en Europa. Consulta Europea sobre los Derechos de los pacientes. Ámsterdam, 28-30 de marzo de 1994. Organización Mundial de la Salud (OMS). EUR/ICP/HLE 121, 28.06.1994. Disponible en Internet: <https://www.ffis.es/ups/documentacion_ley_3_2009/Declaracion_promocion_derechos_pacientes_en_Europa.pdf> [Consulta: 18 septiembre 2016].

[212] Ibídem.

Aunque, en este punto podemos apreciar una incongruencia con la LOPD, que en su Artículo 7, sobre los datos espacialmente protegidos establece como norma general la necesidad del consentimiento expreso del afectado para que sus datos puedan ser tratados. Sin embargo, en el apartado 6, del mismo artículo acepta algunas excepciones, manifestando que los datos pueden ser tratados sin el consentimiento de la persona afectada 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. Pero si estamos ante un caso, por ejemplo, de una enfermedad que le es diagnosticada a un paciente, y él mismo se niega a someterse al tratamiento indicado, y si él mismo no quiere que su familia esté enterada del suceso a fin de evitarles el sufrimiento, consideramos que el médico no puede hacer prevalecer un derecho de información comunicándolo a los familiares para tratar al paciente y por tanto relevar el derecho a la salud en pro del derecho a la información.

En este sentido, la LAP dice en su Artículo 5 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".* Entendemos que la interpretación que ha de hacerse sobre este precepto, va en consonancia con lo manifestado anteriormente, es decir, si el paciente se niega a que sus allegados conozcan la realidad sobre su estado de salud, ésta voluntad del paciente debe prevalecer y debe respetarse por el profesional sanitario, que, en consecuencia, deberá abstenerse de brindar dicha información.

2.3. Principio de consentimiento del afectado.

El principio del consentimiento, se erige como el eje fundamental de la protección de datos en el ámbito de la salud. Constituye un presupuesto indispensable para el tratamiento de los datos del paciente, y a la vez, exigencia para la práctica de cualquier proceso asistencial al interesado[213].

[213] Vid. GRIMALT SERVERA, P. "Deberes y responsabilidad en materia de protección de datos", en CAVANILLAS MÚGICA, S. (Coordinador). *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar.* Editorial Comares, Granada, 2005, pp. 195 y ss.; GÓMEZ

El consentimiento consiste en la manifestación libre, voluntaria y consciente de un paciente, otorgado en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar una actuación que afecta a su salud[214]. La LOPD expresa que el consentimiento del interesado es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen[215].

Éstas características que debe reunir el consentimiento se materializan de la siguiente manera:

(i) Libre: para que sea considerado que el consentimiento se ha otorgado libremente, deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento, como explicaremos en los posteriores epígrafes.
(ii) Específico: referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del fichero. Por tanto, no cabe un consentimiento genérico, sino que debe ser consultado el paciente cada vez que sea sometido a un tratamiento diferente o una intervención distinta.
(iii) Informado: el usuario debe conocer, con anterioridad al tratamiento, la existencia y las finalidades para las que se recogen los datos. Éste tema lo desarrollaremos en el siguiente epígrafe.
(iv) Inequívoco: es preciso que exista expresamente una acción que implique la existencia del consentimiento, descartándose de la forma legal la posibilidad del consentimiento presunto. Por lo tanto, el tratamiento de los datos de carácter

---

PAVÓN, P. *Tratamientos médicos: su responsabilidad penal y civil.* 2da. Edición, Bosch, Barcelona, 2004, pp. 81 y ss.; PUENTE ESCOBAR, A. *Consentimiento del afectado y deber de información.* Tirant lo Blanch, Valencia, 2009, pp. 37 y ss.

[214] Artículo 3, de la LAP.

[215] Artículo 3. h), de la LOPD. Resulta interesante destacar la definición que realiza la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, en su Artículo 3, sobre el consentimiento, expresando que es: *"Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen",* repitiendo textualmente la definición de la LOPD. Para profundizar más al respecto, véase: PALOMAR OLMEDA, A.; GONZÁLEZ ESPEJO, P. (Directores). *Comentario al Reglamento de desarrollo de la Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal (aprobado por RD 1720/2007, de 21 de diciembre).* Thomson-Civitas, Navarra, 2008, pp. 157 y ss.

personal requerirá el consentimiento indudable del afectado, salvo que la Ley disponga lo contrario[216].

Como principio general, el RD 1720/2007[217] establece que habrá de ser el responsable del tratamiento el encargado de obtener el consentimiento para el tratamiento de sus datos de carácter personal, exceptuándose aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes. Los supuestos que legitiman el tratamiento o la cesión de los datos personales únicamente pueden ser tratados si el interesado hubiera prestado previamente su consentimiento para ello[218].

COUDERT[219] indica que la LOPD no exige que el consentimiento se recabe por escrito pero la forma expresa implica que las cláusulas de protección de datos destinadas a los formularios u otras formas de recogida de estas categorías de datos hagan mención específica al tratamiento o a la cesión prevista. De esta forma, cuando se recaben datos que hagan referencia a la salud, los formularios deberán contener una cláusula que mencione que, a través del cumplimiento del mismo, el interesado consiente de forma expresa el tratamiento de sus datos con la finalidad indicada.

El CDOMCE entiende que de requerirse un determinado tratamiento médico que suponga un riesgo significativo y grave para el paciente, el consentimiento ha de ser dado por escrito. Sin que medie el consentimiento inequívoco y específico para la realización de los tratamientos indicados, en principio[220], el médico no podrá practicar las intervenciones o prácticas diagnosticadas[221].

---

[216] Artículo 6.1, de la LOPD.

[217] Artículo 12.1, del RD 1720/2007.

[218] Artículo 10.1, del RD 1720/2007.

[219] COUDERT, F. op. cit., pp. 340 y ss.

[220] Recordemos que la LOPD pondera la salvaguarda del interés vital del afectado, si éste se encuentra impedido física o jurídicamente para dar su consentimiento, tal como queda reflejado en el Artículo 7.6, segundo párrafo.

[221] El Artículo 10.4, del CDOMCE, expresa que: *"Cuando las medidas propuestas supongan para el paciente un riesgo significativo el médico le proporcionará información suficiente y ponderada a fin de obtener, referentemente por escrito, el consentimiento especifico imprescindible para practicarlas".*

El principio del consentimiento está íntimamente vinculado al principio de información del paciente. Así lo recoge expresamente el Artículo 2 de la LAP[222], entendiendo que en algunos casos debe constar por escrito el referido consentimiento, como así también la negativa a someterse a un tratamiento determinado. Y completa éste precepto, el Artículo 8 de la LAP[223], entendiendo que, en principio, la regla general para proporcionar el consentimiento será verbal, lo cual evidentemente, puede suponer un problema a nivel probatorio si existe una reclamación judicial por responsabilidad médica. Sin embargo, la LAP deja asentado los supuestos en los que el consentimiento del paciente debe quedar recogido por escrito, y estos casos que son taxativos, como las intervenciones quirúrgicas, los procedimientos diagnósticos y terapéuticos invasores y, en aquellos procedimientos médicos que puedan suponer riesgos de notoria y previsible repercusión negativa sobre la salud del paciente"[224].

2.4. El consentimiento informado.

Actualmente el consentimiento del interesado reviste fundamental importancia para el médico a la hora de tratar a un paciente. Éste fenómeno, por un lado, es consecuencia del incremento de demandas en el ámbito de la responsabilidad civil de los médicos, y,

---

[222] El Artículo 2, de la LAP, consagra que: *"2. 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. 3. El paciente o usuario tiene derecho a decidir libremente, después de recibir la información adecuada, entre las opciones clínicas disponibles. 4. 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".*

[223] El Artículo 8, de la LAP, establece que: *"1. 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. 2. 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. 3. 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. 4. Todo paciente o usuario tiene derecho a ser advertido sobre 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 su salud".*

[224] Ibídem.

por otro lado, porque ahora el que realmente decide si se somete o no a un determinado tratamiento, intervención o proceso asistencial, es el mismo paciente, una vez que está debidamente informado de las características y riesgos de cada proceso médico, por el facultativo sanitario. En caso de tratamiento de esta tipología de datos, será necesario que el responsable del fichero acredite que ha obtenido el consentimiento del paciente, con todas las garantías establecidas por la Ley, es decir, que además de que el consentimiento sea libre, inequívoco, específico, informado, sea prestado de forma expresa, y por escrito en los casos que la Ley lo obliga[225].

El principio del consentimiento en el derecho de protección de datos representa, según HERRÁN ORTIZ[226], una condición indisponible sobre la que se fundamenta la licitud del tratamiento de datos y su legitimidad. Hasta tal punto reviste importancia que el paciente otorgue su consentimiento informado que, de no prestarse, ello da lugar a que se ejercite una acción indemnizatoria por parte del paciente, su representante o sus familiares más allegados, y será el médico y el Centro Sanitario el encargado de probar que medió el consentimiento del paciente[227].

Recordemos que el consentimiento informado se apoya en derechos fundamentales tales como la vida, a la integridad física y a la libertad de conciencia. En este sentido, el TS manifiesta al respecto que *"es una de las últimas aportaciones realizada en la teoría*

---

[225] Para profundizar más al respecto, véase: ALONSO OLEA, M.; FANEGO CASTILLO, F. *Comentario a la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.* Thomson Civitas, Madrid 2003, pp. 61 y ss.; ATELA BILBAO, A.; GARAY IASI, J. "Ley 41/2002 de derechos del paciente, avances, deficiencias y problemática", en GONZÁLEZ SALINAS, P.; LIZARRAGA BONELLI, E. (coordinadores). *Autonomía del paciente, información e historia clínica (estudios sobre la Ley 41/2002, de 14 de noviembre).* Thomson Civitas, Madrid, 2004, pp. 43-77.; PUENTE ESCOBAR, A., op. cit., pp. 37 y ss.

[226] HERRÁN ORTIZ, A. I., op. cit., p. 57.

[227] El TS ha expresado que: *"el consentimiento informado constituye un derecho humano fundamental",* en la medida en que es un *"el derecho a decidir por sí mismo en lo atinente a la propia persona y a la propia vida y… a la autodisposición sobre el propio cuerpo",* (STS 12 de enero de 2001, RJ 2001\3). Además, el TS sostuvo que la carga de la prueba recae sobre el profesional de la medicina por ser quién se halla en una posición más favorable para conseguir su prueba, (STS de 28 diciembre de 1998, RJ 1998\10155 y STS de 19 abril de 1999, RJ 1999\2588). Para profundizar más el tema, véase: VÁZQUEZ BARROS, S. *Responsabilidad Civil de los Médicos. Doctrina, Legislación básica, Jurisprudencia, Formularios y Bibliografía.* Tirant lo Blanch, Valencia, 2009, pp. 135 y ss.; AMAYA RICO, V. "El deber médico de información: un derecho humano fundamental*". Revista La Ley*. Tomo I, Año 2002, pp. 1831-1832.; BLAS ORBÁN, C. *El equilibrio en la relación médico – paciente.* Bosch, Barcelona, 2006, pp. 46 y ss., 116 y ss.

de los derechos humanos, consecuencia necesaria o explicitación de los clásicos derechos a la vida, a la integridad física y a la libertad de conciencia" (STS de 12 enero de 2001, y STS de 11 mayo de 2001)[228]. Por tanto, el fundamento del consentimiento informado, como procedimiento necesario para ejercer la libertad, es el exponente fundamental del principio de autodeterminación personal ante los tratamientos médicos. El respeto a la autonomía del paciente y el consentimiento informado son indispensables en la relación médico-paciente.

Para definir al consentimiento informado, coincidimos con MÉNDEZ BAIGES[229] que dice que: *"puede definirse al consentimiento informado como un acto mediante el cual el paciente, y después de que le hayan sido explicadas las principales características de una intervención, autoriza al médico a poner en práctica un tratamiento".* Se trata entonces del permiso que el paciente le otorga a su médico, una vez que éste o su equipo de sanitarios le hayan informado debidamente respecto al diagnóstico y al tratamiento que creen más conveniente aplicar en el caso. Sostiene, asimismo, MÉNDEZ BAIGES[230] que: *"puede definirse el derecho al consentimiento informado como el derecho del paciente a ser informado, y a dar o negar su autorización, antes de la puesta en práctica de cualquier tratamiento médico que le afecte".*

Debemos recalcar que el consentimiento informado, requiere siempre y previamente la información terapéutica. El término consentimiento "informado" hace justamente

[228] En idéntico sentido, el TC manifiesta que a través del reconocimiento del derecho fundamental a la integridad física y moral, se protege la inviolabilidad de la persona, no sólo contra ataques dirigidos a lesionar su cuerpo o espíritu, sino también contra toda clase de intervención en esos bienes que carezca del consentimiento de su titular (STC120/1990, de 27 de junio (BOE núm. 181, 30.06.1990); STC137/1990, de 19 de julio (BOE núm. 181, 30.07.1990); STC 215/1994, de 14 de julio (BOE núm. 197, 18.08.1994); STC 35/1996, de 11 de marzo (BOE núm. 93, 17.04.1996); y STC 207/1996, de 16 de diciembre (BOE núm. 19, 22.01.1997). Asimismo, el TC se ha pronunciado en distintas Sentencias al respecto del derecho a la intimidad personal, en cuanto derivación directa de la dignidad reconocida en el Artículo 10.1 CE, confiere a su titular el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima, incluso privada sin la debida autorización (STC 231/1998, de 1 de diciembre (BOE núm. 312, 30.12.1998); STC 197/1991, de 17 de octubre (BOE núm. 274, 15.11.1991), STC 57/1994, de 28 de febrero (BOE núm. 71, 24.03.1994), STC 143/1994, de 9 de mayo de 1994 (BOE núm. 140, 13.05.1994), STC 207/1996, de 16 de diciembre (BOE núm. 19, 22.01.1997), STC 156/2001, de 2 de julio (BOE núm. 178, 26.07.2001), STC 127/2003, de 30 de junio (BOE núm. 181, 30.07.2003), y STC 196/2004, de 15 de noviembre (BOE núm. 306, 21.12.2004).

[229] MÉNDEZ BAIGES, V.; SILVEIRA GORSKI, H. C. *Bioética y derecho.* Editorial UOC, Barcelona, 2007, pp. 76 y ss.

[230] Ibídem.

referencia a ello. Si el paciente conoce claramente cuál es su estado de salud, si el diagnóstico del médico es suficientemente claro y si el tratamiento que se le indica es plenamente comprendido por el paciente, tanto por conocer en qué consiste, qué riesgos ha de asumir y qué probabilidades de resultados entraña, es entonces cuando puede ser otorgado el "consentimiento", con plena certeza de que ha estado debidamente "informado".

No obstante, se pueden apreciar dos puntos de vista diferentes respecto al deber de informar, por parte del médico. Por un lado, tenemos el deber de información como presupuesto del consentimiento informado; y, por otro lado, el deber de información como presupuesto indispensable para llevar a cabo un tratamiento determinado[231].

Por su parte CORBELLA DUCH[232] es contrario a la expresión "consentimiento informado". Sostiene el autor, que la información y el consentimiento son inseparables, sin embargo, la expresión no es acertada, por un lado, aduce que la traducción que se ha hecho del derecho inglés "*informed consend*" es incorrecta puesto que significa consentir después de la información, y por otro lado dice que la misma locución "consentimiento informado" es contradictoria en tanto presupone que puede existir un consentimiento sin información previa, lo que por definición es imposible.

Dentro del derecho comparado en el derecho argentino[233], el consentimiento informado también es de carácter obligatorio, pero los requisitos para obtenerlo son aún más

[231] SÁNCHEZ-CARO, J. "El consentimiento informado ante el derecho: una nueva cultura". *Revista calidad asistencial*. Vol. 14, núm. 2, 1999, pp. 128-144.

[232] Vid. CORBELLA DUCH, J. *Manual de Derecho Sanitario.* Atelier, Barcelona, 2006, pp. 116 y ss.

[233] En la legislación argentina, se establece la obligación de informar al paciente y a sus familiares más cercanos de los riesgos del tratamiento indicado. Los contenidos mínimos que debe reunir el consentimiento son: 1) Nombre y apellido del paciente y médico que informa. 2) Explicar la naturaleza de la enfermedad y su evolución natural. 3) Nombre del procedimiento a realizar, especificando en que consiste y como se llevará a cabo. 4) Explicar los beneficios que razonablemente se puede esperar del tratamiento y consecuencia de la denegación. 5) Información sobre riesgos de la cirugía (si procede), probables complicaciones, mortalidad y secuelas. 6) Planteo de alternativas de tratamiento. 7) Explicación sobre el tipo de anestesia y sus riesgos (si conlleva). 8) Autorización para obtener fotografías, videos o registros gráficos en el pre, intra y postoperatorio y para difundir resultados o iconografía en Revistas Médicas y/o ámbitos científicos. 9) Posibilidad de revocar el consentimiento en cualquier momento antes del sometimiento al tratamiento. 10) Satisfacción del paciente por la información recibida y evacuación de sus dudas. 11) Fecha y firma aclarada del médico, paciente y testigos, si la hubiere. Para profundizar más el tema, véase: la Ley 17.132 en los Artículos 896, 897, 902, 904, 905 del Código Penal Argentino y a la Ley 21.541 Artículo 16 del Código Civil Argentino.

rigurosos que en España. Al enfermo le asiste el derecho de estar informado acerca de su padecimiento, sobre la propuesta de tratamiento y terapias alternativas, riesgos y probabilidad de resultados adversos, para poder tomar una decisión afirmativa. Al respecto, RODRÍGUEZ MARTÍN[234]. añade que:

> No basta como información que el paciente lea el consentimiento. Es el médico que va a realizar el procedimiento quien debe explicar convenientemente al paciente y familiares sobre los diferentes tópicos arriba indicados. Esta información no debe hacerse en una charla de pasillo, en lugares públicos o en encuentros casuales, sino con la debida privacidad, necesaria para tal fin.

En el Derecho Español, destaca la opinión de GALÁN CORTÉS[235], que defiende el uso de protocolos específicos de información y consentimiento, evitando así cualquier duda el respecto de si la información ha sido brindada correctamente y si el paciente ha comprendido todos los parámetros de la misma.

La Jurisprudencia se ha pronunciado respecto a esto, entendiendo que, si el médico o su equipo profesional ha brindado al paciente toda la información y le ha explicado de forma comprensible, no meramente protocolaria, las consecuencias y riesgos de la intervención, quedarán exonerados de responsabilidad civil, a pesar de que se produzca el resultado de muerte[236]. Contrariamente, la Jurisprudencia entiende que, si

---

[234] RODRÍGUEZ MARTÍN, J., et al. "Consentimiento Informado. ¿Un dilema ético o legal?" *Revista Argentina de Cirugía*. Núm. 77, 1999, pp. 229-241.

[235] Vid. GALÁN CORTÉS, J. C. *El Consentimiento informado del usuario de los servicios sanitarios.* Colex. Madrid, 1997, pp. 175 y ss.

[236] En éste caso, el TS desestimó la demanda interpuesta por los herederos de un paciente que fue intervenido de un quiste, con el fatídico resultado de muerte. En ésta Sentencia, el TS entendió que al paciente se le brindó toda la información necesaria, que el consentimiento otorgado revestía la característica de ser informado y que la operación fue correcta en términos médicos. A respecto sostuvo: *"El paciente recibió la información necesaria que le permitió consentir o rechazar intervención quirúrgica. Se le informó de los riesgos generales tanto del acto quirúrgico como de la anestesia; de sus riesgos personalizados relacionados con su estado de salud o patologías que le aquejaban y de la existencia de posibles complicaciones que pudieran aparecer en el curso de la intervención, inclusive la muerte, así como de la inexistencia de un tratamiento alternativo eficaz para dar solución al quiste pilonidal. Y ello tanto de forma escrita, suficientemente expresiva, como verbal y con antelación bastante a la intervención, sin que pueda estimarse que la suscripción de los documentos escritos integre en el caso litigioso mero acto protocolario. Como con reiteración ha dicho esta Sala, el consentimiento informado es presupuesto y elemento esencial de la lex artis y como tal forma parte de toda actuación asistencial (SSTS 29 de mayo; 23 de julio de 2003; 21 de diciembre 2005; 15 de noviembre de 2006; 13 y 27 de mayo de 2011), constituyendo una exigencia ética y legalmente*

bien cabe la buena praxis médica, la falta del consentimiento informado del paciente, genera la responsabilidad del facultativo médico, y, por tanto, da derecho a indemnización. Sostiene el TS que, si el médico no le informa al paciente de todos los posibles riesgos a que se somete en una intervención quirúrgica, teniendo en cuenta que no se trataba de una operación de urgencia sino programada, en un paciente de alto riesgo posquirúrgico, incurre en responsabilidad[237].

a) Excepciones al consentimiento.

Sin embargo, el consentimiento al que se refiere la Ley, y que hemos analizado anteriormente, no será preciso cuando los datos de carácter personal son recogidos en

---

exigible a los miembros de la profesión médica, antes con la Ley 14/1986, de 25 de abril, General de Sanidad, y ahora, con más precisión, con la ley 41/2002, de 14 de noviembre de la autonomía del paciente, en la que se contempla como derecho básico a la dignidad de la persona y autonomía de su voluntad. Es un acto que debe hacerse efectivo con tiempo y dedicación suficiente y que obliga tanto al médico responsable del paciente, como a los profesionales que le atiendan durante el proceso asistencial, como uno más de los que integran la actuación médica o asistencial, a fin de que pueda adoptar la solución que más interesa a su salud. Y hacerlo de una forma comprensible y adecuada a sus necesidades, para permitirle hacerse cargo o valorar las posibles consecuencias que pudieran derivarse de la intervención sobre su particular estado, y en su vista elegir, rechazar o demorar una determinada terapia por razón de sus riesgos e incluso acudir a un especialista o centro distinto, aún en aquellos supuestos en los que se actúa de forma necesaria sobre el enfermo para evitar ulteriores consecuencias (SSTS 4 de marzo de 2011 , 8 de septiembre de 2015)". STS 1624/2016, de 12 de abril de 2016. Recurso 618/2014 (Roj: STS 1624/2016 - ECLI:ES:TS:2016:1624).

[237] En ésta Sentencia, el TS condena al médico y a su aseguradora al pago de una indemnización, por no dar la información adecuada al paciente a fin de que reste su consentimiento informado. Concretamente entiende el TS que: *"No informó al paciente de la gravedad de esta intervención, ni de sus riesgos ni de las posibilidades alternativas. No se dieron por tanto los mínimos requisitos del consentimiento informado. La sentencia del juzgado de primera instancia, partiendo de la adecuada praxis del acto médico quirúrgico, hace descansar la responsabilidad civil del facultativo en la ausencia de información médica para conseguir del paciente el oportuno consentimiento. Atendiendo a la realidad de los hechos, y teniendo en cuenta que la operación provocó un agravamiento en el estado del paciente, valora tal agravación en función de la ausencia de la información debida sobre el riesgo inherente a la intervención o a la técnica operatoria empleada, y ponderando todas esas circunstancias fija el quantum indemnizatorio en 60.101,21€, por haberse aumentado el grado de invalidez y por el dolor sufrido. Consecuencia de lo anterior es que la responsabilidad del facultativo no nace del acto médico quirúrgico practicado, sino del hecho de no haber facilitado la adecuada información al paciente para que éste pudiese valorar someterse o no a la intervención quirúrgica, y hacerlo de forma consciente y libre, conociendo las posibles consecuencias de ella".* STS 1427/2016, de 8 de abril de 2016. Recurso 2050/2014 (Roj: STS 1427/2016 – ECLI:ES:TS:2016:1427).

previsión de un imperativo legal, o para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias o 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 LOPD[238], 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 tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado[239]. El RD 1720/2007, desarrolla este apartado de la Ley, en su Artículo 10, que contempla la posibilidad de que los datos sean tratados o cedidos sin el consentimiento del afectado, cuando:

> *i) 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.*
> *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.*
>
> *ii) Los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado.*
> *No obstante, las Administraciones públicas sólo podrán comunicar al amparo de este apartado los datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de ley*[240]*.*

Por lo tanto, ésta previsión normativa contenida en el primer supuesto - para que no se requiera el consentimiento del afectado – ha de estar así regulado por norma con rango de Ley[241]. Cualquier otro tipo de disposición que no tuviera esta jerarquía, no puede

[238] Artículo 7.6, segundo párrafo, de la LOPD. Asimismo, el RD 1720/2007, recoge el imperativo legal del Artículo 7.6, de la LOPD, y establece en su Artículo 10.3, que: *"Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando: 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".* Al respecto, ver también el Artículo 8.2, apartados a) y c) de la Directiva 95/46/CE.

[239] Artículo 6.2, de la LOPD.

[240] Artículo 10, RD 1720/2007.

[241] Véase al respecto: Informe jurídico 0488/2008 de la AEPD, op. cit.

mermar el consentimiento que la Ley exige de la persona interesada en lo que refiere a sus datos de carácter sensible.

Asimismo, si los datos son necesarios para salvaguardar la vida o integridad del paciente y éste no puede darlo porque se encuentra impedido física o jurídicamente incapacitado los datos sanitarios del mismo, serán tratados, aún sin que medie su consentimiento. El CDOMCE[242] deja en manos de la "conciencia profesional" del médico, la decisión del tratamiento, si el enfermo no estuviese en condiciones de dar su consentimiento por ser menor de edad, estar incapacitado o por la urgencia de la situación, y resultase imposible obtenerlo de su familia o representante legal, en estos casos, el médico deberá prestar los cuidados que le dicte su conciencia profesional.

Por su parte, la LAP establece taxativamente las circunstancias en las que se exceptúa de la necesidad de contar con el consentimiento del paciente[243], prescindiéndose, fundamentalmente, en caso de existir un riesgo para la salud pública a causa de razones sanitarias establecidas por la Ley, o un grave riesgo para la propia salud del paciente, en caso de no intervenir de forma inmediata.

---

[242] Artículo 10.5, del CDOMCE.

[243] El Artículo 9, de la LAP, dispensa el consentimiento del paciente cuando: *"2. 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: 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. 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 permitan, a sus familiares o a las personas vinculadas de hecho a él. 3. Se otorgará el consentimiento por representación en los siguientes supuestos: 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. Cuando el paciente esté incapacitado legalmente. 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. 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".*

Cabe resaltar que las excepciones al otorgamiento del consentimiento del afectado para el tratamiento de sus datos de salud, no exime de la obligación de informar a la persona de que sus datos van a ser tratados[244].

b) Vicios del consentimiento.

No obstante, como explicamos anteriormente, el consentimiento que la persona brinda para que sus datos de salud sean tratados, ha de ser una manifestación de voluntad, otorgada libremente, de forma inequívoca, específica y que responda a una información adecuada, veraz y certera sobre el tratamiento que se llevará a cabo con los datos sensibles que está facilitando[245]. Evidentemente, la información que se le otorga, debe ser comprensible para el paciente, evitando tecnicismos y el empleo de recursos propios del ámbito médico, que no resulten entendibles por un paciente, ajeno al mundo sanitario.

Coincidimos con APARICIO SALOM[246] cuando destaca entre los vicios del consentimiento, el error en la prestación del consentimiento, puesto que para que la manifestación de voluntad afirmativa sea dada conforme a la Ley, la comprensión del alcance de lo que se está autorizando es de suma importancia. Destaca APARICIO SALOM[247] que: *"cabe afirmar que, si la información no es completa, dicho defecto podrá afectar a la validez de la autorización obtenida y, por tanto, a la legitimidad del tratamiento que se realiza respecto de los datos de quien prestó su consentimiento sin la debida información".*

Por tanto, el consentimiento ha de estar estrechamente vinculado a la finalidad para la cual los datos de salud son recabados, siendo necesario que la misma, sea determinada. Y frente a esto, debemos añadir, que la finalidad ha de estar previamente fijada, y la recogida de datos debe siempre ser posterior, es decir, si no se sabe exactamente para qué se necesitan los datos, no sería congruente recogerlos, porque tampoco sabríamos con certeza qué datos son necesarios.

---

[244] Para profundizar más al respecto, véase: COUDERT, F., op. cit., p. 345.

[245] Artículo 3.h), de la LOPD.

[246] APARICIO SALOM, J. *Estudio sobre la Ley Orgánica de Protección de Datos de carácter personal.* 3ª Edición, Aranzadi-Thomson Reuters, Navarra, 2009, pp. 154-157.

[247] Ibídem.

Se deduce de ésta premisa, la importancia del 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".* De no ser así, estaríamos consintiendo el tratamiento de nuestros datos de carácter sanitario creyendo que lo hacemos para una acción médica específica y podría ocurrir que los mismos fuesen destinados a otra finalidad.

Frente a ésta posibilidad, el legislador, pone el punto de mira en la persona que trata los datos, para determinar su responsabilidad ante la eventualidad de la utilización de los datos recabados para propósitos diferentes. Por tanto, 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[248].

Asimismo, aún dado el consentimiento por parte del paciente, la Ley entiende que será nulo, cuando la información que se facilite al interesado no le permita conocer la finalidad a la que se destinarán los datos cuya comunicación se autoriza, o el tipo de actividad de aquel a quien se pretenden comunicar, en caso de que los datos personales recabados se cedan a un tercero[249]. Por lo tanto, cuando se comuniquen o transmitan datos de salud, sólo será legítima si el paciente la autoriza y si la finalidad es la misma para la cual se da brindado el consentimiento.

Vemos, en consecuencia, como la LOPD establece de forma imperativa que el consentimiento debe existir, y siempre en relación con una finalidad determinada de tratamiento del dato personal que se está revelando. En este sentido, incluso, prohíbe la recogida y almacenamiento de datos por el mero hecho de almacenarlos[250].

[248] Artículo 12.4, de la LOPD.

[249] Artículo 11.3, de la LOPD.

[250] Artículo 7.4, de la LOPD.

c) Revocación del consentimiento.

Asimismo, la LOPD prevé la posibilidad de que el consentimiento sea revocado siempre que exista causa justificada para ello y no se le atribuyan efectos retroactivos[251]. En el mismo sentido, la LAP requiere que la revocación se realice por escrito[252].

El consentimiento prestado válidamente, puede ser revocado en cualquier momento. Sorprende la estipulación que contiene el Artículo 7.4 de la LOPD, al referirse a la existencia de una "causa justificada", porque resulta un concepto absolutamente subjetivo. Si el paciente decide simplemente revocar su consentimiento, no debe haber obstáculo legal para ello, toda vez que la revocación del consentimiento, tiene sentido antes de una práctica médica determinada. Es decir, si el paciente ha otorgado su consentimiento para una intervención quirúrgica, y una vez operado decide revocar ese consentimiento, evidentemente carecería de sentido porque la actuación médica ya se materializó.

Asombra la estipulación que hace la LAP respecto a la forma en que debe realizarse la revocación, estableciendo que la misma debe hacerse por escrito, según el Artículo 8.5. Sin embargo, el Artículo 17 del RD 1720/2007, fija las condiciones y el procedimiento a través del cual se permite revocar el consentimiento prestado, ya sea de forma tácita o expresa. Para la materialización de dicha revocación, el responsable del tratamiento debe ofrecer al interesado un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. Considera el RD 1720/2007 que la revocación del consentimiento puede llevarse a acabo 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[253].

Sostiene DOMÍNGUEZ LUELMO[254] que, siendo la regla general para otorgar el consentimiento de forma verbal, a su juicio, el legislador ha tenido en cuenta los casos en los que el consentimiento se exige por escrito para establecer en el caso del Artículo

[251] Artículo 6.3, de la LOPD.

[252] El Artículo 8, de la LAP establece en su apartado 5 que: *"El paciente puede revocar libremente por escrito su consentimiento en cualquier momento".*

[253] Artículo 17, del RD 1720/2007. Para profundizar más el tema, véase: ÁLVAREZ HERNANDO, J. op. cit., p. 64 y ss.

[254] DOMÍNGUEZ LUELMO, A., op. cit., p. 309.

8.5 de la LAP, que la revocación se realice por escrito, evitando así dudas sobre si subsiste o no el consentimiento prestado.

Para proceder a la revocación, el responsable del tratamiento dispondrá de un plazo de diez días. Y, en caso de haber cedido los datos, también será el responsable del tratamiento el encargado de notificar a los cedentes para que procedan asimismo a revocar los datos.

2.5. Conocimiento informado.

La parte del conocimiento informado está directamente relacionada con el paciente. Es él el que tiene que otorgar su consentimiento para la aplicación de cualquier tratamiento o intervención que el médico le haya indicado como más adecuado. Sin embargo, para que el enfermo sea plenamente capaz de consentir, ha de estar debidamente informado, por tanto, el conocer exactamente y comprender todos los parámetros que el médico le informa sobre su diagnóstico, tratamiento más adecuado, alternativas, secuelas, etc., es lo que denominamos conocimiento informado y le permitirá al paciente dar su conformidad.

Por lo tanto, el conocimiento informado es la autorización que conlleva el consentimiento informado, que hace una persona con plenas facultades físicas y mentales para que los profesionales de la salud puedan realizar un tratamiento o procedimiento. Es el derecho que tienen los pacientes de recibir la información completa sobre los riesgos y posibles complicaciones de un tratamiento o intervención. Por tanto, el consentimiento es la justificación misma del acto médico, basado en el derecho del paciente a su autonomía y autodeterminación, fundamentado en el conocimiento informado.

Dentro del principio de autonomía de la voluntad, la persona puede aceptar o rechazar las indicaciones del acto médico, como un tratamiento, o tomar uno que él considere apropiado para su condición de salud, aunque no coincida con la indicación médica. Pero para que se presuponga que jurídicamente se ha tenido un conocimiento informado, el médico debe realizar un diagnóstico e informar al paciente del pronóstico, sobre sus circunstancias de salud, sobre las posibilidades terapéuticas o quirúrgicas, las ventajas y los resultados esperados, los efectos secundarios, adversos, inmediatos

o tardíos como consecuencia del tratamiento o intervención, y el riesgo previsto, de tal forma que el paciente pueda consentir en forma voluntaria y consciente.

Cabe añadir, que el conocimiento informado, implica que el paciente ha comprendido, ha entendido y ha interpretado de forma correcta la información médica de quién la recibe, no bastando con brindar datos de una manera fría y mecánica, instrumental o procedimental. Asimismo, el médico debe evaluar rigurosamente el grado de percepción de la persona que recibe la información, y eso solo es posible mediante una conversación abierta, sincera, con unos datos claros y precisos.

Por lo tanto, el paciente sabe de la existencia de los riesgos y otorga el consentimiento confiando en que el profesional actuará con la debida diligencia y con el cuidado que le impone su profesión. Al otorgarse el consentimiento, el paciente sólo acepta los riesgos propios del tratamiento o procedimiento, evidentemente no tiene cabida la mala praxis médica o complicaciones que puedan surgir en la intervención o durante un tratamiento médico[255].

Sostiene JIMENA QUESADA[256], que el conocimiento informado se compone de dos variantes, una subjetiva que implica la autonomía de la voluntad del paciente, y otra objetiva que implica el estado de progreso de la ciencia médica. Coincidimos con el autor al hacer ésta puntualización, y ello nos lleva a la siguiente reflexión: por un lado, el avance de la medicina, de la investigación y los tratamientos aplicados están cada vez más cerca de llegar a una precisión muy alta (aunque también es menester destacar que muchas veces los tratamientos probados y eficientes en algunos pacientes no obtienen el mismo resultado en otros enfermos o pueden tener consecuencias diferentes, secuelas, etc.); y, por otro lado, la medicina no es una profesión que implique la obligación de resultados, sino que se trata de una obligación de medios, es decir, el médico empleará su *lex artis*, sus conocimientos, habilidades y aptitudes para llegar al mejor resultado, pero esto no quiere decir que pueda o deba garantizar ese resultado buscado[257].

---

[255] Cfr. STS 1427/2016, de 8 de abril de 2016, op. cit.

[256] Vid. JIMENA QUESADA, L. "La tutela constitucional de la salud: Entre el consentimiento informado y la información consentida", en GARCÍA RUIZ, Y., et al. *La salud: intimidad y libertades informadas.* Tirant lo blanch, Valencia, 2006, pp. 41-82.

[257] TAJADURA TEJADA, J.: "La protección de la salud (art. 43 CE)", en TAJADURA TEJADA, J. (COORDINADOR). *Los principios rectores de la política social y económica.* Editorial Biblioteca Nueva, Madrid, 2004, pp. 222-223.

2.6. Principio de seguridad.

El responsable del fichero y, en su caso, el encargado del tratamiento, son los gestores que deben adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal, con el fin de evitar 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 los que puedan estar expuestos, ya provengan de la acción humana, del medio físico o natural[258].

Por su parte, la LAP, también establece que: *"Las Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental"*[259].

DEL PESO NAVARRO[260] define seguridad de la información como *"la técnica que permite que todas las personas autorizadas puedan acceder a la información, ésta se encuentre disponible para ellas, que estando autorizadas podrán modificarla o variarla, y que garantiza que quien está al otro lado de una red es quien dice ser".* Por supuesto que el autor se refiere a la seguridad informática, pero la primera parte de la definición que realiza, es plenamente adecuada a las medidas de seguridad que involucran la gestión de los datos de salud. Ello es así, porque, tanto el médico como los profesionales sanitarios son personas *autorizadas para acceder* a nuestra información sanitaria; asimismo es su cometido *modificarla o variarla* en función de las consultas, diagnóstico y tratamiento que se le realiza al paciente. Coincidimos con DEL PESO NAVARRO[261], al decir que la seguridad de la información se define también por sus características: confidencialidad, integridad, disponibilidad y autenticidad.

En éste sentido, a continuación, explicaremos los criterios que han de observarse a la hora de tratar datos de salud.

---

[258] Artículo 9.1, de la LOPD.

[259] Artículo 14.4, de la LAP. En el mismo sentido, ver el Artículo 23.3 del Estatuto de Autonomía de Cataluña (BOE núm. 172 de 20 de julio de 2006).

[260] DEL PESO NAVARRO, E., et al. *Nuevo Reglamento de Protección de Datos de carácter personal. Medidas de Seguridad.* Díaz de Santos, Madrid, 2008, pp. 291 y ss.

[261] Ibídem.

Las medidas de seguridad de los ficheros de datos se clasifican en tres niveles de seguridad, según establece el RD 1720/2007: nivel bajo, nivel medio y nivel alto[262]. Estos tres niveles son acumulativos atendiendo a la naturaleza de la información tratada y almacenada en los ficheros de datos, y en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información almacenada en dichos ficheros según la LOPD[263].

La aplicación acumulativa a la que hacíamos referencia *ut supra*, conlleva determinar a qué tipo de dato se le está dando tratamiento, y en función de ello, se va subiendo de nivel de protección. En este sentido, los tres niveles funcionan como a continuación expondremos.

El nivel básico de seguridad, se aplica a los ficheros que solo contienen datos identificativos y, en virtud de la acumulación, se aplica a todos los niveles, es decir al medio y al alto de seguridad. Podemos citar, por ejemplo, datos que hagan referencia al nombre, domicilio, teléfono, DNI, número de afiliación a la seguridad social, fotografía, firmas, correos electrónicos, datos bancarios, edad, fecha de nacimiento, sexo, nacionalidad, etc.

En el nivel medio de seguridad, se aplica, entre otros, a los ficheros que contienen datos relativos a solvencia patrimonial, operaciones financieras y de crédito. En éste nivel de seguridad, podemos citar, por ejemplo, los de personalidad, hábitos de consumo, hábitos de carácter, datos de seguridad social, solvencia patrimonial y crédito, antecedentes penales, sanciones administrativas, pruebas psicotécnicas, etc.

El nivel alto de seguridad es el que se aplica a los ficheros que contienen datos especialmente protegidos como los relativos a ideología, afiliación sindical y política, religión y creencias, origen racial, salud, alimentación, bajas laborales, historias clínicas, etc.

En el ámbito de la protección de los datos vinculados a la salud, tal y como acabamos de mencionar, ha de emplearse el nivel alto, los medios de seguridad deben extremarse

[262] Artículo 80, del RD 1720/2007.

[263] Para profundizar más al respecto, véase: DEL PESO NAVARRO, E.; RAMOS GONZÁLEZ, M. A.; DEL PESO RUIZ, M. *Documento de seguridad.* Díaz de Santos, Madrid, 2004, pp. 45-62.

a la hora de proteger estos datos especialmente sensibles. Es por ello, que se aplica el nivel máximo de seguridad[264].

Sin embargo, a éste principio general de aplicación del nivel alto de seguridad en caso de tratarse de datos de carácter personal, hay que añadirle las excepciones que nos plantea la misma normativa[265]. Si bien se trata de datos de salud, especialmente protegidos[266], hay circunstancias en las que su conocimiento no revela en sí una información altamente comprometida. El Artículo 81, del RD 1720/2007, consagra tres excepciones a la aplicación del nivel alto de seguridad, y estas excepciones se dan 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 no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.
> c) 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.

En estos casos, lo que se busca a través de la información recopilada es simplemente conocer si el afectado está sujeto a algún tipo de beneficio o está exento del mismo, la realización de una transferencia bancaria, etc., por citar algún ejemplo. Se trata de tres excepciones al nivel alto de seguridad, que vincula estrechamente el tratamiento de los datos recabados con la finalidad para los cuales son requeridos. En el mismo sentido, MARTÍNEZ MARTÍNEZ[267] sostiene que: *"los tres casos tienen en común un elemento esencial que relaciona el tratamiento con la finalidad del mismo".*

Consideramos por ello, que exigir un nivel alto de seguridad en estos casos sería excesivo, aunque, no hay que olvidarse que éste tipo de datos de carácter sensible lo

---

[264] El Artículo 83, del RD 1720/2007, establece lo siguiente: *"3. 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".*

[265] Artículo 81, del RD 1720/2007.

[266] Artículo 7.3, de la LOPD.

[267] MARTÍNEZ MARTÍNEZ, R. (coordinador). *Protección de Datos. Comentarios al Reglamento de desarrollo de la LOPD.* Tirant lo Blanch, Valencia, 2009, pp. 99 y ss.

requiere. En ésta línea se mantiene MARTÍNEZ MARTÍNEZ[268] que apunta que: *"Se trata de supuestos en los que el objeto que persigue el responsable no es el conocimiento del estado de salud sino la simple comprobación de un dato objetivo para el cumplimiento de un deber público".* Y cita el autor un ejemplo muy ilustrativo: "*Se trata de cuestiones como el cálculo y la práctica de las retenciones del IRPF o la atribución de beneficios y ayudas sociales como una matrícula gratuita".*

2.7. Principio de confidencialidad y secreto médico.

En el ámbito sanitario, la protección de datos y la confidencialidad de los mismos, va intrínsecamente relacionado con el secreto médico[269]. Su fundamento se encuentra en la relación de confidencialidad entre el médico y el paciente. SISO MARTÍN[270] explica que. el posicionamiento del secreto en la figura de la confidencialidad, introdujo un cambio conceptual y normativo. En un principio existía la obligación profesional y general del médico de guardar secreto (el Juramento Hipocrático[271] es el ejemplo evidente), pero sin el correlativo derecho del paciente. El secreto médico se asentaba en obligaciones deontológicas, no legales. Hoy con la obligación de confidencialidad, el secreto es exigible como un derecho del titular de la información, a que acceda sólo quien debe y a que se maneje bajo condiciones legales. De este modo, según explica SISO MARTÍN, la exigencia de confidencialidad del usuario se complementa, en un solapamiento absoluto, con la obligación de secreto de quien recibe la confidencia. Este es el modo de que sea eficaz la protección, porque, tal como explica el autor, un derecho no es nada sin un sistema de garantías que lo sustente.

---

[268] Ibídem.

[269] Vid. SÁNCHEZ JORDÁN, M. E. "Algunas cuestiones relativas al derecho de información y al deber de secreto profesional en un supuesto de responsabilidad médica". *Derecho y Salud*. Vol. 10, núm. 2, julio-diciembre 2002, pp. 162 y ss.; SÁNCHEZ CARAZO, C. *La intimidad y el secreto médico.* Díaz de Santos, Madrid 2000, pp. 191-222.; SÁNCHEZ GONZÁLEZ, M. A. *Intimidad y confidencialidad: su concepto e importancia.* I Jornadas de Protección de Datos sanitarios en la Comunidad de Madrid, Mapfre, Madrid, 2000, pp. 55 y ss.

[270] SISO MARTÍN, J. "Responsabilidad profesional en secreto médico", en Ponencia del Master en valoración médica de la incapacidad laboral y dependencia. Tema 2, Universidad de Alcalá, Disponible en Internet: <http://www.juansiso.es/Almacen/SECRETO%20MEDICO%20-%20RESPONSABILIDAD%20PROFESIONAL.pdf> [Consulta: 23 marzo 2017].

[271] Disponible en Internet: <http://www.bioeticanet.info/documentos/JURHIP.pdf> [Consulta: 23 marzo 2017].

Al respecto, la CE dentro del Título I referido a los Derechos y Libertades fundamentales, hace referencia a que la Ley regulará el secreto profesional[272]. Asimismo, la LOPD establece en su Artículo 10 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 aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Por su parte, la LAP entiende que: *"1. 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"*[273]*.* Asimismo, establece en su Artículo 1 apartado 7, que: *"La persona que elabore o tenga acceso a la información y la documentación clínica está obligada a guardar la reserva debida".*

También, se reconoce el derecho a la confidencialidad de toda la información relacionada con el proceso asistencial del paciente, y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público, según la LGS[274].

En el mismo sentido, es un imperativo médico y así queda recogido en el CDOMCE que promulga 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[275]. 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[276]. Incluso el CDOMC va más allá, y obliga al médico a preservar

---

[272] Artículo 20.1.d), de la CE.

[273] Artículo 7, de la LAP.

[274] Artículo 10.3, de la LGS. Resulta interesante y esclarecedor, el Artículo 6, de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal de la Comunidad de Madrid, que dispone 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".*

[275] Artículo 27.1, del CDOMCE.

[276] Artículo 27.2, del CDOMCE.

en su ámbito social, laboral y familiar, la confidencialidad de los pacientes[277]. Apreciamos por tanto la rigurosidad que emplea el CDOMC con respecto al secreto médico que se debe guardar, no ya sólo referido al contenido de la historia clínica, sino a las confidencias entre paciente y médico que frecuentemente ocurren en base a esa relación estrecha que nutre tal relación de confianza.

Además, el secreto médico constituye un deber no sólo del médico que interviene, sino que se extiende a todo el personal sanitario que tienen acceso al paciente, ya sea la enfermera en la misma consulta, el equipo médico en una intervención, o el personal administrativo que gestiona los datos de salud del paciente[278], poniéndose el énfasis en el médico principal la facultad de exigir esa discreción y observancia estricta del secreto profesional.

Así también, el secreto profesional, es una obligación que perdura en el tiempo. El médico debe guardar secreto de todo lo que el paciente le haya confiado y de lo que de él haya conocido en el ejercicio de la profesión y la muerte del paciente no exime al médico del deber del secreto[279]. Vemos, en ésta parte final, que tanto el CDOMCE como la LOPD, han querido dejar de manifiesto que el deber de confidencialidad ha de mantenerse y perpetuarse en el tiempo, con indiferencia de la extinción de la relación del paciente con el médico en cuestión o incluso la muerte del paciente, puesto que estamos ante una información especialmente sensible, tal como explicamos al principio de ésta tesis.

A nivel internacional, la Asociación Médica Mundial (WMA, en inglés)[280], ha publicado una serie de normas que resultan obligatorias en el ámbito ético del desarrollo de la profesión sanitaria. Al respecto, el Código Internacional de Ética Médica dispone que el médico debe guardar absoluto secreto de todo lo que se le haya confiado, incluso después de la muerte del paciente. Asimismo, establece que: *"El médico debe respetar*

[277] Artículo 27.7, del CDOMCE.

[278] Artículos 29.1 y 29.2., del CDOMCE.

[279] Artículo 28.5, del CDOMCE.

[280] Ver al respecto el apartado referido a los deberes de los médicos hacia los enfermos, del Código Internacional de Ética Médica, adoptado por la 3ª Asamblea General de la AMM, Londres, Inglaterra, octubre 1949 y enmendado por la 22ª Asamblea Médica Mundial, Sydney, Australia, agosto 1968 y la 35ª Asamblea Médica Mundial, Venecia, Italia, octubre 1983. Asociación Médica Mundial (WMA, en inglés). Disponible en Internet: <http://www.wma.net/es/30publications/10policies/c8/> [Consulta: 6 agosto 2016].

los derechos del paciente, de los colegas y de otros profesionales de la salud, y debe salvaguardar las confidencias de los pacientes". En igual sentido, promulgó la denominada Declaración de Ginebra[281], que contiene las promesas que los médicos han de realizar para ejercer la profesión, establece en una de sus disposiciones que el médico debe: *"Guardar y respetar los secretos confiados a mí, incluso después del fallecimiento del paciente".*

En este punto, ha de hacerse una breve referencia, acerca del acceso a los datos de un paciente fallecido. Debemos puntualizar en este sentido, que la LOPD no legisla sobre el particular, aunque cabe destacar que es la AEPD, así como las Agencias que algunas Comunidades Autónomas poseen, las encargadas de pronunciarse ante este tipo de cuestiones. Hasta el momento, la AEPD permite a los familiares de un paciente fallecido, acceder al historial clínico y solicitar al responsable del fichero, la cancelación de sus datos.

Sin embargo, y a pesar del deber de secreto que obliga a todos los profesionales de la medicina[282], el CDOMCE, admite la revelación del secreto médico, manteniendo que, con discreción, exclusivamente ante quien tenga que hacerlo, en sus justos y restringidos límites y, si lo estimara necesario, solicitando el asesoramiento del Colegio, el médico podrá revelar el secreto en los siguientes casos[283]:

(i) En las enfermedades de declaración obligatoria.
(ii) En las certificaciones de nacimiento y defunción.
(iii) Si con su silencio diera lugar a un perjuicio al propio paciente o a otras personas, o a un peligro colectivo.
(iv) Cuando se vea injustamente perjudicado por mantener el secreto del paciente y éste permita tal situación.

---

[281] Declaración de Ginebra, adoptada por la 2ª Asamblea General de la AMM, Ginebra, Suiza, septiembre 1948 y enmendada por la 22ª Asamblea Médica Mundial, Sydney, Australia, agosto 1968 y la 35ª Asamblea Médica Mundial, Venecia, Italia, octubre 1983 y la 46ª Asamblea General de la AMM, Estocolmo, Suecia, septiembre 1994. Asociación Médica Mundial. Disponible en Internet: <http://www.wma.net/es/30publications/10policies/g1/WMA_DECLARACION-DE-GINEBRA_A4_ESP.pdf> [Consulta: 6 agosto 2016].

[282] Artículo 14, del CDOMC, establece en su apartado 1 que: *"El secreto médico es inherente al ejercicio de la profesión y se establece como un derecho del paciente a salvaguardar su intimidad ante terceros". Y seguido, agrega que: "El secreto profesional obliga a todos los médicos cualquiera que sea la modalidad de su ejercicio".*

[283] Artículo 30, del CDOMCE.

(v) En caso de malos tratos, especialmente a niños, ancianos y discapacitados psíquicos o actos de agresión sexual.

(vi) Cuando el médico sea citado por el Colegio Profesional para testificar en materia disciplinaria.

(vii) 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.

(viii) Por imperativo legal:

a) En el parte de lesiones, que todo médico viene obligado a enviar al juez cuando asiste a un lesionado.

b) Cuando actúe como perito, inspector, médico forense, juez instructor o similar.

c) 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.

Al respecto, reconoce EGUISQUIZA BALMASEDA[284], la tutela de intereses colectivos, reconocidos socialmente, ha llevado a que se compela a los profesionales de la medicina a informar de lo conocido por su actividad profesional cuando se produzcan determinadas situaciones. Este deber está previsto legalmente para tres materias: la actuación ante los Tribunales de Justicia, las enfermedades de declaración obligatoria y las anotaciones registrales.

MARTÍ MERCADAL y BUISÁN ESPELETA[285], entienden que no hay un derecho absoluto del paciente a su confidencialidad, lo cual compartimos ampliamente. Nosotros entendemos que la realidad social obliga al médico a revelar en según qué circunstancias, informaciones concernientes a la salud de su paciente y ello hace que el derecho no pueda ser considerado absoluto. Podríamos decir que estamos ante un derecho absoluto de confidencialidad médico-paciente, si la Ley no prevé las excepciones a las cuales aludimos en este punto. Por tanto, el deber de secreto

[284] EGUSQUIZA BALMASEDA, Mª Á. *Protección de datos: Intimidad y salud.* Aranzadi, Navarra, 2009, pp. 36 y ss.

[285] MARTÍ MERCADAL, J. A.; BUISÁN ESPELETA, L. *El secreto profesional en la medicina.* Espasa Calpe, Madrid, 1988, p. 81.

legislado en el Artículo 10 de la LOPD, no es ni mucho menos que una premisa imperativa, sino que admite excepciones tal como se ha comentado *ut supra*.

a) Sanciones en el ámbito Penal respecto a la revelación de secretos.

El Código Penal (en adelante, CP), castiga con prisión la revelación de secretos. De manera general, el descubrimiento y la revelación de secretos[286], con penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. Y serán castigados con una pena de prisión de tres a cinco años cuando los hechos afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.

Y, en caso de tratarse de un médico en ejercicio de su profesión, la pena se agrava con la inhabilitación para el desempeño de su trabajo. Así, el CP establece que:

> 1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses. 2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años[287].

Sin embargo, ese deber de sigilo cede ante lo preceptuado por el Artículo 262, de la Ley de Enjuiciamiento Criminal, consagra que:

---

[286] Artículos 197, 197 bis, 197 ter y 197 quater, del Código Penal. Para profundizar más al respecto, véase: MORALES PRATS, F. "El Código Penal y la protección de datos personales". *Jornadas sobre el Derecho Español de la protección de datos personales.* Agencia de Protección de Datos, Madrid, 1996.; MARTÍNEZ-PEREDA RODRÍGUEZ, J. M. "La Protección penal del secreto médico en el derecho español". *Actualidad Laboral*. Núm. 20. Semana del 4 al 10 de marzo, 1996.

[287] Artículo 199, del Código Penal. La peculiaridad penal reside en que este tipo de delitos son perseguidos a instancia de una denuncia, salvo que se trate de casos que afecten a una pluralidad de personas o vulnere intereses generales, según el Artículo 201, del Código Penal. En Argentina, la Ley 25.326, inciso 1º del Artículo 10, obliga al encargado del tratamiento de los datos sensibles a mantener la confidencialidad de los datos cuyo conocimiento ha tenido en razón o con ocasión de su profesión, y la ley es más rigurosa aún que en España, y únicamente permite que estas personas puedan ser relevadas de este deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

> Los que por razón de sus cargos, profesiones u oficios tuvieren noticia de algún delito público, estarán obligados a denunciarlo inmediatamente al Ministerio fiscal, al Tribunal competente, al Juez de instrucción y, en su defecto, al municipal o al funcionario de policía más próximo al sitio, si se tratare de un delito flagrante.
> Los que no cumpliesen esta obligación incurrirán en la multa señalada en el artículo 259, que se impondrá disciplinariamente.
> Si la omisión en dar parte fuere de un profesor de Medicina, Cirugía o Farmacia y tuviese relación con el ejercicio de sus actividades profesionales, la multa no podrá ser inferior a 125 pesetas ni superior a 250.

Se aprecia en el caso de los facultativos médicos, que ellos sí tienen deber de informar de hechos delictivos de los que puedan tener conocimiento, contrariamente a lo que ocurre en nuestra esfera de Abogados, o a los Procuradores y Eclesiásticos. Pero entendemos que la diferencia estriba en que la Ley ampara el derecho de defensa y el derecho de libertad religiosa, de nuestros clientes, en el ámbito legal, y de los creyentes en el ámbito religioso, aun existiendo el deber de secreto, cosa que en el ámbito médico deja de prevalecer.

2.8. Transparencia o publicidad en el tratamiento.

SANCHEZ CARO y ABELLÁN[288] entienden que la transparencia en el tratamiento de los datos va relacionada con la obligatoriedad de que se informe al interesado sobre el objetivo del tratamiento de sus datos personales, sobre la identidad del responsable del mismo y, en su caso, de su representante, y sobre cualquier otro elemento preciso para garantizar un trato leal.

Este principio implica que el interesado conozca quién es el responsable del fichero, quién es el personal que interviene en el tratamiento, qué datos se poseen, y para qué serán utilizados. Además, comporta la garantía de que se lleven a cabo las revisiones pertinentes en los sistemas de tratamiento de datos, conforme a la normativa vigente.

Cabe resaltar que el principio de transparencia requiere que el interesado pueda ejercer sus derechos de información, además de los derechos de acceso, rectificación y oposición, como a continuación se desarrollará en relación con los derechos del paciente.

[288] SÁNCHEZ-CARO, J.; ABELLÁN, F. *Datos de salud y datos genéticos.* Comares, Granada, 2004, p. 4.

3. Derechos del paciente respecto a su historia clínica.

La LOPD[289] regula los derechos de acceso, rectificación, cancelación y oposición (denominados derechos ARCO), que poseen los pacientes para ejercer la observancia y control, sobre sus datos de salud[290]. La LAP[291] recoge sólo el derecho de acceso a la historia clínica y a la conservación de los datos. A continuación, analizaremos en qué consiste cada uno de éstos derechos en relación con los datos sanitarios del individuo contenidos en su historia clínica (en adelante, HC).

3.1. Acceso.

El derecho de acceso a los propios datos, consiste en que el interesado puede solicitar acceder a la información que sobre sus datos de salud existe en posesión del médico o del centro asistencial.

La persona afectada está facultada por la Ley para solicitar la información que existiere relacionada a su persona. El Artículo 15.1, de la LOPD permite al paciente conocer qué datos de salud obran en su HC. El interesado tendrá derecho a solicitar y obtener gratuitamente información acerca de sus datos de carácter personal sometidos a tratamiento, sobre el origen de dichos datos, así como sobre las comunicaciones realizadas o que se prevean hacer de los mismos.

Este derecho de acceso a los propios datos, evita que se mantengan datos erróneos, incompletos o falsos, de manera que el afectado pueda ejercer ante esto su derecho de rectificación, cancelación u oposición. Los centros sanitarios deben contemplar y regular un procedimiento, con el fin de garantizar la observancia del derecho de acceso a los propios datos del paciente, contenidos en su HC.

La LOPD al referirse a la calidad de los datos, establece que: *"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, sin perjuicio de las facultades que a los afectados reconoce el artículo*

[289] Artículos 15, 16 y 17, de la LOPD.

[290] Vid. CARDONA RUBERT, Mª B. *Derechos de acceso, rectificación, cancelación y oposición en el nuevo reglamento de desarrollo de LOPD.* Tirant lo Blanch, Valencia, 2008, pp. 201 y ss.

[291] Artículos 18 y 7.2, de la LAP.

16"[292]. El Artículo 16, de la LOPD consagra el derecho a la rectificación o cancelación si fuese necesario, en caso de que los datos de carácter personal tratados en la HC del paciente no se ajusten a lo dispuesto por la LOPD o cuando tales datos resulten inexactos o incompletos.

Así también, la Directiva 95/46/CE al tratar el acceso del interesado a sus datos[293], manifiesta fundamentalmente que los Estados miembros, tienen la obligación de garantizar a los interesados el derecho de conocer si existen datos sobre ellos, cuál es el origen de esos datos y para qué van a ser tratados. Y, mantiene la Directiva 95/46/CE, que éste derecho debe poder ejercerse libremente, sin restricciones y sin gastos excesivos. Observamos como se contempla la posibilidad de imponer algún tipo de coste, pero el legislador español ha preferido establecer este derecho de acceso a los propios datos, para el interesado, sin que ello le conlleve gasto alguno[294].

En Cataluña también se ha legislado en su Estatuto de Autonomía sobre el particular, estableciéndose que todas las personas, con relación a los servicios sanitarios públicos y privados, tienen derecho a ser informadas sobre los servicios a que pueden acceder y los requisitos necesarios para su uso; sobre los tratamientos médicos y sus riesgos, antes de que les sean aplicados; a dar el consentimiento para cualquier intervención; a acceder a la historia clínica propia, y a la confidencialidad de los datos relativos a la

[292] Artículo 4.4, de la LOPD.

[293] El Artículo 12, de la Directiva 95/46/CE, sostiene 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 automatizadas 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".

[294] Artículo 17.2, de la LOPD.

salud propia, en los términos que se establecen por Ley[295]. Por su parte, la Ley 2/2004, del País Vasco[296], reconoce en su Artículo 8, el procedimiento para el ejercicio de los derechos de los interesados, es decir, los derechos ARCO, sin que ello pueda dar lugar a ningún tipo de contraprestación.

Para poder ejercer el derecho de acceso que nos ocupa, el paciente puede solicitar la información 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[297].

Asimismo, el derecho de acceso del paciente a la HC puede ejercerse también a través de un representante, pero dicha representación, según exige la Ley, ha de estar debidamente acreditada[298]. Aquí cabe preguntarse si ésta representación tiene un plazo de duración, o, por el contrario, una vez otorgada por el paciente, no tiene "caducidad" alguna. Creemos que la solución frente a esto, es que el escrito de representación contemple, como requisito, una duración, o, que contenga la formula, hasta su revocación. Pero sí que vemos necesaria una consideración al respecto, porque, de lo contrario, puede hacerse un uno indebido de una representación otorgada para una circunstancia puntual, e incluso, pueden coexistir varias representaciones, con el consiguiente inconveniente del centro de salud al no saber a quién proporcionarle la información requerida.

---

[295] Artículo 23.3, del Estatuto de Autonomía de Cataluña. Asimismo, en el Artículo 31 del Estatuto de Autonomía de Cataluña, se consagra el derecho a la protección de los datos personales diciendo que: *"Todas las personas tienen derecho a la protección de los datos personales contenidos en los ficheros que son competencia de la Generalitat y el derecho a acceder a los mismos, a su examen y a obtener su corrección".*

[296] El Artículo 8, de 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, especifica que: *"1. Los interesados podrán ejercitar los derechos de oposición, acceso, rectificación, cancelación y cualesquiera otros que les reconozca la ley. El contenido material de los mismos será el determinado en la ley. 2. Cada administración, institución o corporación regulará reglamentariamente el procedimiento para el ejercicio de los derechos señalados en el número anterior, en relación con los ficheros de su titularidad a los que es de aplicación esta Ley. No se exigirá contraprestación alguna por ello".*

[297] Artículo 15.2, de la LOPD.

[298] Artículo 18.2, de la LAP.

También, según nuestro punto de vista, sorprende la previsión que hace el Artículo 15.3, limitando dicho acceso a un plazo de doce meses. Es decir, salvo que determinadas circunstancias relevantes hagan necesario un acceso más frecuente, la LOPD señala que dicho acceso no se podrá realizar en intervalos más cortos de doce meses. Entendemos que dicha previsión la tuvo en cuenta el legislador para evitar colapsos de gestión a la hora de pacientes que soliciten el acceso a sus datos de forma constante. Pero, ésta previsión legal nos parece desacertada y que carece de trascendencia jurídica, toda vez que, si un paciente necesita acceder a los datos de salud contenidos en su HC, es por alguna razón en concreto, es decir, porque, por ejemplo, porque ha de someterse a una segunda opinión de un médico privado, porque quiere conocer si los datos de salud son correctos, etc., pero una vez realizado esto, no necesitará nuevos accesos a los mismos, porque, salvo que se someta a más tratamientos o consultan, los datos contenidos no sufrirán modificación alguna. Es por ello, que entendemos que es una previsión legal vacía de relevancia.

No obstante, el derecho al acceso del paciente a la documentación contenida en su HC, 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 incluso, pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas, tema que desarrollaremos más adelante.

Finalmente, en caso de personas fallecidas, los centros sanitarios sólo facilitarán el acceso a la HC, a las personas vinculadas al difunto, por razones familiares o, de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así conste acreditado, por ejemplo, con un testamento vital. En cualquier caso, el acceso de un tercero a la HC motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido, ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros[299].

3.2. Derecho a rectificación o cancelación de los datos erróneos.

Una vez verificado el derecho de acceso por parte del paciente, si constata que la información contenida en su HC no es correcta, tiene el derecho de solicitar la

[299] Artículo 18.4, de la LAP.

rectificación de los datos erróneos, inexactos, incorrectos o incompletos, a fin de ser corregidos, o, incluso, su cancelación, si lo que prefiere es que no consten determinados datos. En éste caso, el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

Si lo que se solicita, es la cancelación, entonces ésta dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, de los Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas[300]. Una vez se cumpla dicho plazo, se deberá proceder a la supresión. Ante ésta previsión legal, detectamos un inconveniente, y ello es el desconocimiento por parte de los facultativos médicos o centros de salud de los plazos de prescripción para dirimir posibles responsabilidades, que varía significativamente según se trate de responsabilidad civil, y dentro de ella, en los amplios ámbitos que puedan generarse, y a su vez, los plazos de responsabilidad penal y que puedan originarse que no coinciden con el ámbito civil.

Por lo tanto, dicha estipulación en la LOPD, puede acarrear un problema, y es, a tenor de lo manifestado, que el centro de salud, prefiera mantener los datos, a pesar de obrar una solicitud de cancelación por parte del paciente, solamente a los fines de exonerarse de posibles responsabilidades, tal y como está legislado. Por tanto, el ejercicio del derecho que tiene atribuido el paciente, no se vería materializado, obstaculizado, en parte, por la misma previsión legal.

3.3. Derecho de oposición de los interesados.

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 determinados supuestos:

(i) 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[301].

[300] Articulo 16, de la LOPD.

[301] Artículo 34, del RD 1720/2007.

(ii) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial[302].

(iii) 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. Es decir, los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos 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, tales como su rendimiento laboral, crédito, fiabilidad o conducta[303].

Tanto la normativa comunitaria[304] como la nacional[305], contemplan la posibilidad de que la persona afectada pueda oponerse al tratamiento de sus datos.

La Directiva 95/46/CE delimita las razones que puedan dar lugar a una oposición en el tratamiento de los datos de carácter personal, estableciendo que el interesado puede realizar dicha oposición en cualquier momento, y por razones legítimas propias de su situación particular, a que los datos que le conciernan que sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa[306].

Por su parte, la LOPD prevé también la posibilidad del afectado a oponerse al tratamiento de sus datos, 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 afectado[307]. La normativa impone un plazo de diez días, muy breve desde nuestro punto de vista, para que el encargado del tratamiento de los datos haga efectiva la oposición solicitada por un interesado[308].

---

[302] Artículo 51, del RD 1720/2007.

[303] Artículo 36, del RD 1720/2007.

[304] Artículo 14, de la Directiva 95/46/CE.

[305] Artículos 34, 35 y 36, del RD 1720/2007; Artículo 17, de la LOPD.

[306] Artículo 14, de la Directiva 95/46/CE.

[307] Artículo 6.4, de la LOPD.

[308] Artículos 35.2, del RD 1720/2007.

Finalmente, y común a todos los derechos ARCO, es la circunstancia que no se puede exigir contraprestación alguna para ejercer los derechos de oposición, acceso, rectificación o cancelación[309].

Conclusión.

Según todo lo analizado anteriormente, queda plasmada la necesidad de que las personas conozcan fehacientemente si sus datos personales de salud son tratados, y en ese caso, se deberá conocer quién los trata y con qué finalidad. Ello facilitará ejercer los derechos que la normativa otorga a los interesados. También es menester que las personas tomen conciencia de la importancia que reviste que sus datos sanitarios puedan ser conocidos por terceros, y ello debe llevarlos a la conclusión de velar por su protección.

Creo fervientemente que las personas aún no han tomado conciencia de la magnitud de datos que se manejan diariamente, y lo sencillo que resulta que se recopilen, y que los mismos tarde o temprano, pueden afectar a nuestra esfera más íntima, personal y hacernos vulnerables.

Tan sólo pensemos que manejamos teléfonos móviles que podemos activar con nuestra huella dactilar, pero, ¿alguien se ha puesto a pensar que en verdad lo que estamos haciendo es proporcionar nuestros datos biométricos a una plataforma que los registra y almacena, que ni siquiera está en España, y por tanto escapa a nuestra normativa en materia de protección de datos? Sin embargo, son prácticas cotidianas, que nos facilitan el día a día, el estar conectados, poder trabajar, mantener una vida social, etc., pero que al día de hoy desconocemos el "precio" de suministrar tan ligeramente nuestros datos más personales.

[309] Artículo 17.2, de la LOPD.

CAPÍTULO III

La Historia Clínica

SUMARIO: 1. La Historia Clínica: origen. 1.1. Concepto y delimitaciones doctrinales. 1.2. Relevancia de la Historia Clínica. 1.3. Aspectos éticos de la historia clínica. 2. Tratamiento normativo de la Historia Clínica en el derecho español. 2.1. Marco normativo nacional. 2.2. Breve referencia al marco normativo autonómico. a) Comunidad Autónoma de Cataluña. b) Otras Comunidades Autónomas. 3. Características de la historia clínica. 4. Contenido de la historia clínica. 4.1. Datos de inclusión obligatoria. 4.2. Mecanismos para garantizar la autenticidad y uniformidad de los datos contenidos en la historia clínica. 4.3. Derecho de acceso a la historia clínica. Anotaciones subjetivas. 5. Propiedad de la historia clínica. 5.1. Consideración de la historia clínica como propiedad del centro sanitario. 5.2. Consideración de la historia clínica como propiedad del médico. 5.3. Consideración de la historia clínica como propiedad del paciente. 5.4. Teoría mixta sobre la propiedad de la historia clínica. 5.5. Nuestra postura en torno a la historia clínica.

Introducción.

Tal y como se ha explicado en los capítulos precedentes, la salud es un dato de carácter sensible, especialmente protegido y que requiere de un alto nivel de protección. La información sobre nuestro estado de salud, diagnósticos, pruebas médicas, tratamientos, etc., se encuentra almacenada en lo que nombramos "historia clínica". Centros sanitarios y hospitales, clínicas privadas y laboratorios son los que tratan este tipo de datos y en consecuencia los que deben garantizar al paciente los derechos que la LOPD otorga al interesado[310] y donde ha de ponerse el énfasis normativo para proteger a la persona.

En éste Capítulo analizaremos desde el punto de vista legal, los requisitos que deben observarse en torno a la HC, haremos un breve repaso a su origen, a su definición y a

[310] Véase al respecto PIÑAR MAÑAS, J. L. "La Protección de Datos en el ámbito Sanitario", op. cit., pp. 42-44.

los aspectos que debe reunir, a su contenido, intentando delimitar los parámetros jurídicos que la HC debe respetar, como factor fundamental en la relación médico-paciente.

Finalmente, nos centraremos en analizar las diferentes corrientes doctrinarias en torno a la propiedad de la HC, y la relevancia de ésta cuestión.

1. La Historia Clínica: origen.

Las primeras historias clínicas completas están contenidas en los libros Las Epidemias I y III del *Corpus Hipocraticum*[311]. Su elaboración se remonta a la Edad Media con Los Consilea y se mantiene a lo largo del renacimiento denominándose Observatio. Sydenham[312] perfecciona su contenido completándose a lo largo del siglo XVIII con el método anatomoclínico[313] y del XIX con el desarrollo de técnicas fisiopatológicas.

Sydenham reinterpretó las enseñanzas del *Corpus Hipocraticum*, lo que le llevó a exponer con claridad los fenómenos de cada enfermedad sin fundarlos en hipótesis ni agruparlos de manera forzada. Redactó meticulosamente las historias individuales de sus pacientes y reunió su amplia experiencia clínica en el "*Observationes medicae*"[314]

[311] Lo que se conoce como "*Corpus Hipocraticum",* está constituido por unos cincuenta libros, cuya autoría se desconoce. Es una recopilación heterogénea en estilo, doctrina y época. Está escrita en dialecto jónico y se sabe que una parte importante estuvo en la biblioteca de la escuela de Cos. Los principales tratados fueron escritos entre los años -420 y -350, probablemente algunos por el propio Hipócrates, pero no se sabe con certeza cuáles. Los tratados teóricos más importantes que podemos mencionar, son: "Sobre la medicina antigua" que es una obra filosófica, "Sobre la dieta en enfermedades agudas", "Sobre fracturas", "Sobre articulaciones", esta última tiene la peculiaridad de que está ilustrada. En "Sobre aires, aguas y lugares" se expone la influencia del medio ambiente en las enfermedades. También revisten especial relevancia los tratados cuya autoría es atribuida a Hipócrates: Pronóstico, Epidemias I y III, Aires, aguas y lugares, Sobre la enfermedad sagrada y la mayor parte de los tratados quirúrgicos.

[312] Thomas Sydenham fue un médico inglés (1624-1689). Siendo apreciado como el representante más destacado de la medicina inglesa, fue apodado el "Hipócrates inglés".

[313] El método anatomoclínico es una forma de observación médica, cuyo objeto es reconocer, en el individuo vivo, con la ayuda de signos precisos extraídos de la exploración física, las modificaciones patológicas de los órganos profundos.

[314] Puede consultarse en: <https://global.britannica.com/topic/Observationes-Medicae> [Consulta: 29 octubre 2016].

en cuyo prólogo expuso un programa para construir una nueva patología basada en la descripción de todas las enfermedades "tan gráfica y natural como sea posible" ordenando los casos de la experiencia clínica en especies, igual que hacían los botánicos de la época. Su trabajo se caracterizó por ser siempre de estrecho contacto con el paciente, consagrándose más al estudio de los síntomas que al de las teorías médicas[315].

Sydenham describe y nombra con precisión los síntomas y signos, los clasifica en patognomónicos o peculiares (propios de la enfermedad), constantes (aparecen siempre pero no son propios) y accidentales (añadidos por la naturaleza del enfermo, edad, sexo, temperamento, otras enfermedades, etc.). Define los grandes Síndromes. Ordena los síntomas en el tiempo por la velocidad de instauración: agudo y crónico y por el momento en que aparecen (curso clínico). La minuciosa observación de muchos casos individuales y su comparación hace reunirlos de forma abstracta definiendo lo que es propio de cada enfermedad. Proscribe los casos raros a los que considera aberraciones de la naturaleza debidas a causas circunstanciales. Aspira a tratamientos específicos[316].

En el siglo XX se vislumbra un rápido crecimiento de pruebas complementarias con aumento de la complejidad de la HC que se convierte en multidisciplinar y de obligado cumplimiento. La informatización de la HC conllevará cambios radicales en el siglo XXI.

1.1. Concepto y delimitaciones doctrinales.

Cabe comenzar este apartado explicando que en nuestro país la regulación específica en relación a la HC en concreto, es realmente escueta. Contamos a nivel nacional con la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y

---

[315] Para profundizar más al respecto, véase: FOMBELLA POSADA, Mª. J.; CEREIJO QUINTEIRO, Mª. J. "Historia de la Historia Clínica". *Galicia Clínica, Sociedade Galega de Medicina Interna*. Núm. 73, 2012, pp. 21-26. Disponible en Internet: <https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=0ahUKEwiA04TkktvRAhVGPRQKHS5XBa0QFgg3MAQ&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F4056927.pdf&usg=AFQjCNHnSXyVWkqJ61TH75IJErfg63tcVQ&sig2=_fDnnOGKIMwGBxj2E8Ek3g> [Consulta: 29 octubre 2016].

[316] Ibídem.

de derechos y obligaciones en materia de información y documentación clínica[317] (LAP), y en el ámbito autonómico, algunas autonomías en el ámbito de sus competencias, han dictado normas sobre HC que en posteriores epígrafes analizaremos.

En la misma línea de pensamiento que DE LORENZO[318] sostenemos que la regulación española en la materia es escasa, prácticamente nula en lo que a HC específicamente se refiere. De esta manera, DE LORENZO[319] explica el desacuerdo entre diferentes autores sobre cuestiones centrales de la HC, como son su contenido, sobre la propiedad de la misma, su eficacia, su naturaleza jurídica, etc.[320].

Las HC, pueden definirse como el conjunto de documentos sanitarios relativos a la evolución médica del paciente, que podemos considerar un documento esencial del aprendizaje y la práctica clínica, según FOMBELLA POSADA y CEREIJO QUINTEIRO[321]. En la misma línea, SUÁREZ RUBIO[322] entiende que la HC es el documento fundamental en la relación médico-paciente.

En sus orígenes, Ley 14/1986, de 25 de abril, General de Sanidad (LGS), simplemente hacía una breve mención disponiendo que debía quedar constancia por escrito de todo proceso asistencial[323]. Actualmente, son el objeto principal sobre el que versa la inquietud del legislador relativa a protección de datos sanitarios. Los historiales clínicos incluyen datos identificativos del paciente, datos de identificación del centro sanitario, datos clínicos, diagnósticos y consentimiento escrito del paciente, que determinan desde la sintomatología del paciente en un momento, hasta los episodios asistenciales a los que ha sido sometido, pasando por el tratamiento y su diagnóstico.

---

[317] Ley 41/2002, de 14 de noviembre, op. cit.

[318] DE LORENZO SÁNCHEZ, A. "¿De quién son propiedad las historias clínicas?" *Deontología, Derecho y Medicina*. Colegio Oficial de Médicos, Madrid, 1977.

[319] Ibídem.

[320] Cfr. CODÓN HERRERA, A. "La historia clínica: concepto, normativa, titularidad y jurisprudencia", en GONZÁLEZ SALINAS, P.; LIZARRAGA BONELLI, E. (coordinadores). *Autonomía del paciente, información e historia clínica (estudios sobre la Ley 41/2002, de 14 de noviembre).* Thomson Civitas, Madrid, 2004, pp. 137-160.

[321] FOMBELLA POSADA, Mª. J.; CEREIJO QUINTEIRO, Mª. J., op. cit., pp. 21-26.

[322] SUÁREZ RUBIO, S. Mª. *Constitución y privacidad sanitaria.* Tirant lo Blanch, Valencia, 2015, p. 214.

[323] El derogado Artículo 10.11, de la LGS, contenía ésta disposición.

CRIADO DEL RÍO[324], define la HC como el documento médico-legal en donde queda registrada toda la relación del personal sanitario con el paciente, todos los actos y actividades médico-sanitarios realizados con él y todos los datos relativos a su salud, que se elabora con la finalidad de facilitar su asistencia.

Coincidimos con MARTINEZ AGUADO[325] en la definición que realiza acerca de la HC diciendo que: "*es el soporte documental biográfico de la asistencia sanitaria de un paciente. Siendo el documento mas privado que existe de una persona no en vano se contienen todos los detalles mas íntimos acerca de su personalidad física, psíquica y social".* Consideramos que el término "biográfico" es sumamente descriptivo que la realidad de la HC. Engloba la historia personal de cada individuo, pero ligada a su aspecto médico, por tanto, nos resulta satisfactoriamente descrita la conceptualización de HC que hace el autor.

La HC es una documentación única[326], que, en manos de médicos y profesionales de la salud, hará la función de "fotografía de nuestra salud", que servirá para que, al consultarse simplemente, el médico esté dotado de la información necesaria para tratarnos ante cualquier situación. Sin embargo, hay autores que sostienen lo contrario. Sostiene CORBELLA DUCH[327], que se tiende a dar un valor absoluto a la HC creyéndose que es portadora de la verdad absoluta, lo que no se corresponde con la realidad -dice- puesto que incorpora la expresión resumida de las actuaciones consideradas trascendentales realizados según la opinión subjetiva del médico, sin que puedan descartarse -añade- errores de transcripción. Nosotros nos vemos contrarios a ésta opinión, puesto que consideramos que no puede darse un valor, ya sea absoluto o no, pero de ninguna manera cuantitativo, sino que ha de interpretarse cualitativamente la HC, es decir, desde el punto de vista de su función, objetivo y razón de ser, y de las facilidades que genera a cualquier facultativo médico que deba intervenir en nuestra

[324] Vid. CRIADO DEL RÍO, Mª. T. *Aspectos Médico-Legales de la Historia Clínica.* Colex, 1999, Madrid, p. 23.

[325] Vid. MARTÍNEZ AGUADO, L. "Aspectos éticos de la historia clínica", en FERNÁNDEZ HIERRO, J. M. (Coordinador). *La historia clínica.* Comares, Granada, 2002, p. 78.

[326] La LGS, mencionaba en el Artículo 61 el principio de la HC única en cada institución asistencial, mencionando que: *"En cada Área de Salud debe procurarse la máxima integración de la información relativa a cada paciente, por lo que el principio de historia clínico-sanitaria única por cada uno deberá mantenerse, al menos, dentro de los límites de cada institución asistencial".* Abriendo así un peligroso vacío legislativo, según CORBELLA DUCH, que de forma diferente fueron llenando las Comunidades Autónomas hasta la promulgación de la LAP. Vid. CORBELLA DUCH, J., op. cit., 2006, p. 141.

[327] CORBELLA DUCH, J., op. cit., p. 143.

asistencia, el poder conocer con rapidez y de forma certera ciertas patologías, grupo sanguíneo, enfermedades, alergias, etc. Es evidente que la HC sirve para agilizar nuestro tratamiento. De la misma manera, discrepamos con la posibilidad que esboza CORBELLA DUCH[328] relativa a errores de transcripción, porque ello significa aceptar desde un primer momento que los facultativos médicos o el personal sanitario puede incurrir en errores, una teoría quizás demasiado amplia y pesimista, máxime teniendo en cuenta que la HC recoge datos que pueden ser considerados objetivos como son valores de pruebas médicas, análisis clínicos, etc.

Algunos autores son partidarios de una definición más completa de la HC[329], tanto desde el aspecto de su conceptualización, como desde el aspecto de los elementos que la componen. Entiende éste sector doctrinal[330], que la HC es un conjunto de información, único para cada paciente, al menos en cada institución asistencial, que se redacta obligatoriamente por los médicos en beneficio del paciente, y que reúne la máxima integración de la información a él relativa, a la que únicamente tienen acceso el paciente, los facultativos que intervengan en el tratamiento y las personas señaladas por la ley para fines de inspección sanitaria, científicos o docentes, o a requerimiento de la autoridad judicial, como expresión de los derechos a la intimidad personal y familiar y de las obligaciones de confidencialidad y de secreto profesional por parte de todos los que tengan acceso a la misma, y en la que deben constar los datos fundamentales de la relación clínica, esto es, consentimiento, información y curso de la relación.

Por su parte, COUDERT[331] sostiene que:

> El historial clínico contendrá la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente afirmando el derecho correlativo del paciente a que quede constancia, por escrito o en el soporte técnico más adecuado, la información obtenida en todos sus procesos asistenciales realizados por el servicio de salud, tanto en el ámbito de la atención primaria como de la atención especializada.

---

[328] Ibídem.

[329] Vid. MÉJICA, J.; DIEZ, J. M. *El Estatuto del Paciente. A través de la nueva legislación sanitaria estatal.* Thomson-Civitas, Navarra, 2006, pp. 163-164.; AULLÓ CHAVES, M.; PELAYO PARDOS, S. "La historia clínica", en DE LORENZO Y MONTERO, R. (Coordinador General) "Plan de formación en responsabilidad legal profesional". *Unidad didáctica núm. 1*. Madrid. Edicomplet. Asociación Española de Derecho Sanitario. 1997, p. 10.

[330] Ibídem.

[331] COUDERT, F., op. cit., p. 351.

Finalmente, coincidimos con la definición que da al respecto de la HC, GÓMEZ PIQUERAS[332], por entender que es la más completa y la que mejor resume y conceptualiza lo que engloba la HC. La autora sostiene que:

> La historia clínica es la narración escrita, en soporte papel o informático, clara, precisa, detallada y ordenada de todos los datos y conocimientos, tanto personales como familiares, que se refieren a un paciente y que sirven de base para el juicio definitivo de su enfermedad actual o de su estado de salud. Resume la herencia y hábitos de un ser humano, su constitución, fisiología y psicología, su ambiente y, siempre que sea posible, la etiología y evolución de la enfermedad.

LAÍN ENTRALGO[333] concluye en que la HC está integrada por tres partes. La primera parte es una estructura, la segunda un contenido constante y diverso, y la tercera parte está integrada por los denominados problemas que se van planteando.

MARTINEZ AGUADO[334] manifiesta que la HC contiene información acerca del paciente en las tres esferas personales: datos sociales, respecto a su vida pública y laboral; datos privados, acerca de su realidad familiar o amistosa; datos íntimos, sobre sus conductas sexuales u otras más ocultas. Las tres esferas, - social; privada; íntima - constituyen los tres ámbitos personales que habitualmente se plasman en una HC y que no son desvelables fuera del marco asistencial sin la autorización y consentimiento del paciente o usuario.

Una vez analizada la doctrina, podemos matizar, que, desde nuestro punto de vista, la HC consiste en la documentación de cada persona que se elabora individualmente para cada paciente, donde constan sus datos médicos, las consultas médicas realizadas y los tratamientos que le hayan sido practicados, con la indicación de los médicos que hayan intervenido en todo el proceso. Involucra directamente los principios de la

---

[332] GÓMEZ PIQUERAS, C. (25 de febrero de 2008). *Contenido, usos y finalidad de la Historia Clínica.* Ponencia presentada en Antigua. Disponible en Internet: <https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjen5mwze7RAhWCWxQKHSvvAfYQFggjMAE&url=http%3A%2F%2Fwww.redipd.es%2Factividades%2Fseminarios_2008%2Fcommon%2Fponencia3_250208.pdf&usg=AFQjCNFUyIAv25hsp2c2PYdy3k6VNkG6HA> [Consulta: 29 octubre 2016].

[333] Para profundizar más al respecto, véase: LAÍN ENTRALGO, P. *La historia clínica.* 3ª Edición, Triacasela, Madrid, 1998, pp. 738-754.

[334] MARTÍNEZ AGUADO, L., op. cit., p. 79, nota al pie 1.

dignidad de la persona humana, el derecho de la intimidad y el respecto por la autonomía de la voluntad del paciente.

A través de la utilización de la HC, se registra, por parte del médico o del personal sanitario, toda la información obtenida, ya sea en la entrevista médico-paciente, a través del interrogatorio, del examen físico, y de los resultados, tanto de los estudios de laboratorio clínico, como de los de diagnóstico por imágenes, y de las técnicas especiales. En ella, se recoge la información necesaria para la atención, en forma completa, de los pacientes. El registro de la HC, construye un documento principal en un sistema de información sanitario, imprescindible en su vertiente asistencial, administrativa, y además constituye el registro completo de la atención prestada al paciente durante su enfermedad, de lo que se deriva su trascendencia como documento legal. Por tanto, la HC conforma un documento válido médico legal, que contiene información que abarca los aspectos asistencial, preventivo y social del paciente.

1.2. Relevancia de la Historia Clínica.

Los datos de salud y la HC tienen una enorme importancia porque son instrumentos necesarios para garantizar la asistencia sanitaria de las personas, y, por tanto, están íntimamente vinculados al derecho a la vida[335] y a la protección de la salud[336]. La acumulación de datos sanitarios de los pacientes en las HC y su correcta conservación, según expresa TRONCOSO REIGADA[337], son elementos necesarios para poder llevar

[335] El Artículo 15, de la CE, establece que: *"Todos tienen derecho a la vida…"*. El derecho a la vida es un derecho básico y primario de todos los reconocidos en el texto constitucional, en la medida en que la afirmación de los demás sólo tiene sentido a partir del reconocimiento de éste. Este reconocimiento constitucional, que se legisla en el primer Artículo, de la Sección Primera, del Capítulo II, del Título I, de la CE (Artículos 15 a 29), sección que constituye el núcleo central de la declaración constitucional de derechos, es decir, en la que se ubican los derechos más relevantes, aquellos que gozan del máximo nivel de protección jurídica. Por tanto, el derecho a la vida es el primero, tanto desde la perspectiva de su enunciado, como desde su tratamiento constitucional.

[336] El Artículo 43, de la CE, consagra que: *"Se reconoce el derecho a la protección de la salud. Compete a los poderes públicos organizar y tutelar la salud pública a través de medidas preventivas y de las prestaciones y servicios necesarios…".*

[337] Vid. TRONCOSO REIGADA, A. "La confidencialidad de la historia clínica". *Cuadernos de Derecho Público*. Núm. 27, enero-abril 2006, pp. 45-143. Disponible en Internet:

un seguimiento del estado de salud de las personas. De hecho, la supresión de datos relevantes de la HC puede llegar a afectar gravemente a los tratamientos sanitarios, y, en última instancia, a la vida de las personas.

Con la finalidad asistencial que caracteriza a la medicina, se requiere necesariamente un acopio de información personal del paciente, que pueda poner de forma rápida en antecedentes al médico que nos va a atender tanto en los servicios sanitarios en atención primaria, como en atención especializada o en situación de una urgencia médica. En este sentido, TRONCOSO REIGADA[338], refiere a la necesidad de una acumulación masiva de información personal de los ciudadanos, porque en definitiva es a ellos a los que se intenta garantizar su salud.

TRONCOSO REIGADA[339] resume la importancia de la HC en sanidad explicando que:

> La actividad sanitaria tiene como soporte recursos humanos y materiales limitados. Se hace imprescindible una actuación de planificación sanitaria que garantice la equidad en el acceso a las prestaciones. Los servicios sanitarios tratan de manera masiva información del personal destinado en el Sistema Nacional de Salud. También, más en general, la búsqueda de la calidad a través del control en el desempeño de la actividad sanitaria mediante protocolos, guías y pautas clínicas conlleva el manejo de datos personales. La mejora de la efectividad del trabajo exige en muchas ocasiones el tratamiento masivo de información de los pacientes y de los empleados. Así, la necesidad de buscar la eficiencia en el recurso a las prestaciones sanitarias exige adaptar y equilibrarlos recursos para evitar dar a unos pacientes unos cuidados más costosos en detrimento de otros cuidados más básicos y necesarios.

Es evidente que de no contar con un soporte -ya sea físico o digital-, como trataremos en el Capítulo siguiente- es inviable que podamos gozar de una atención sanitaria

---

<http://revistasonline.inap.es/index.php?journal=CDP&page=article&op=viewFile&path%5B%5D=775&path%5B%5D=830> [Consulta: 26 noviembre 2016].

[338] Ibídem, p. 46. Explica el autor que: *"Además de la asistencia sanitaria como derecho subjetivo, la salud pública es un bien jurídico colectivo. Existe un interés social que comprende los beneficios colectivos de la investigación médica y las políticas de prevención y de salud pública, actividades éstas que se materializan sobre información sanitaria de personas".*

[339] Ibídem. Y otros autores citados por TRONCOSO REIGADA, A.: Vid. AA. VV., *Calidad en la asistencia sanitaria*. Instituto Europeo de Salud y Bienestar Social, Madrid, 1999, pp. 25-29 y 57-75.; AA.VV., *La gestión del proceso asistencial: impacto de los sistemas de información médica*. MSC, Madrid, 2000, pp. 15-37.; AA.VV. *Libro blanco para la mejora de los servicios públicos. Una nueva Administración al servicio de los ciudadanos*, MAP, Madrid, 2000, pp. 68-78.

acorde, personalizada, de calidad y sobre todo respondiendo a la máxima de la asistencia médica en situaciones de emergencia: rápida y ágil.

El motivo por el que el médico inicia la elaboración de la HC y la continua a lo largo del tiempo es el requerimiento de una prestación de servicios sanitarios por parte del paciente, según explica GÓMEZ PIQUERAS[340]. La HC puede considerarse el instrumento básico del buen ejercicio sanitario porque sin ella es imposible que el médico pueda tener una visión completa y global del paciente para prestarle asistencia.

Por ello, consideramos de absoluta relevancia el registro de información que contiene la HC, que se construye como un documento primordial en el sistema de información médico y hospitalario, imprescindible en su vertiente asistencial, administrativa, y, además, como hemos señalado *ut supra*, constituye el registro completo de la atención prestada al paciente durante su enfermedad, de lo que se deriva su trascendencia como documento legal.

1.3. Aspectos éticos de la historia clínica.

A partir de la era de Sigmund Freud la HC se convirtió en una biografía de la persona[341]. Pero nos podemos remontar al año 500 A.C., concretamente al Juramento Hipocrático[342] que ya contenía en aquél tiempo, una obligación solemne para el médico:

---

[340] GÓMEZ PIQUERAS, C., op. cit.

[341] Vid. MARTÍNEZ AGUADO, L., op. cit., pp. 79-80.

[342] Durante casi dos mil años la medicina estuvo dominada teóricamente por una tradición que, remontándose al médico griego Hipócrates (siglo V, a.c.), adoptó su forma definitiva de la mano de Galeno, quién ejerció la medicina en la Roma imperial en el siglo II. Según la tradición, el Juramento, fue redactado por Hipócrates o un discípulo suyo. Lo cierto es que forma parte del *Corpus Hipocraticum*, y se piensa que pudo ser obra de los pitagóricos. Según Galeno, Hipócrates creó el Juramento cuando empezó a instruir, apartándose de la tradición de los médicos de oficio, a aprendices que no eran de su propia familia. Los escritos de Galeno han sido el fundamento de la instrucción médica y de la práctica del oficio hasta casi el siglo XX. El contenido del juramento se ha adaptado a menudo a las circunstancias y conceptos éticos dominantes de cada sociedad. El Juramento Hipocrático ha sido actualizado por la Declaración de Ginebra de 1948, siendo la redacción actual respecto al secreto médico: *"Guardaré silencio sobre todo aquello que en mi profesión, o fuera de ella, oiga o vea en la vida de los hombres que no deba ser público, manteniendo estas cosas de manera que no se pueda hablar de ellas".* Declaración de Ginebra, adoptada por la 2ª Asamblea General de la AMM, Ginebra, Suiza, septiembre 1948 y enmendada por la 22ª Asamblea Médica

"Todo lo que vea y oiga en el ejercicio de mi profesión, y todo lo que supiere acerca de la vida de alguien, si es cosa que no debe ser divulgada, lo callaré y lo guardaré con secreto inviolable", donde se puede encontrar la evidencia de mantener en secreto las informaciones de los pacientes por parte del médico.

Sostiene MARÍNEZ AGUADO[343] que la HC es en nuestros días el documento privado que contiene más datos confidenciales de todo tipo acerca de una persona. Comenta el autor, que, cuanto mejor y mayor es la calidad en su elaboración más conflictiva es, sobre todo, porque contiene más información sensible. De ahí su carácter ético manifiesta MARTÍNEZ AGUADO[344].

El CDOMCE, tal como explicamos en el Capítulo II, impone a todos los médicos el deber de redactar y conservar la HC en interés del paciente[345], así como al propio centro sanitario donde el médico desempeña su profesión[346] y establece la garantía del secreto médico[347] promulgando que el secreto médico es inherente al ejercicio de la profesión de médico, definiéndolo como un pilar fundamental en la relación de confianza que une al médico con el paciente. Este deber de secreto se configura desde el punto de vista del paciente, es decir, que se establece como un derecho del paciente a salvaguardar su intimidad ante terceros y no desde el punto de vista del médico.

Y ésta obligación ética va más allá de lo estrictamente médico, porque el facultativo debe guardar secreto de todo lo que el paciente le haya confiado y de lo que de él haya conocido en el ejercicio de su profesión, aún incluso si se produce la defunción del paciente, el deber de secreto permanece. Asimismo, el secreto profesional, incluso debe ser mantenido en el ámbito privado y personal del médico, con relación a su propia vida social y familiar, es decir, que la obligación ética por salvaguardar la intimidad del paciente, invade incluso el círculo social, laboral y familiar del médico[348].

Mundial, Sydney, Australia, agosto 1968 y la 35ª Asamblea Médica Mundial, Venecia, Italia, octubre 1983 y la 46ª Asamblea General de la AMM, Estocolmo, Suecia, septiembre 1994.

[343] MARTÍNEZ AGUADO, L., op. cit., p. 80.

[344] Ibídem.

[345] Artículos 19.1 y 19.2, del CDOMCE.

[346] Artículo 19.3, del CDOMCE.

[347] Artículo 27, del CDOMCE.

[348] Artículo 27.7, del CDOMCE

Debemos ser conscientes que el ejercicio de la medicina y de las profesiones sanitarias, tanto en la asistencia pública como en la atención médica privada, está basada en la relación entre el médico y el paciente. Ésta relación es fuente de derechos y deberes recíprocos. Al respecto, DOLORS GIMÉNEZ[349] comenta que dentro del contexto médico-legal y deontológico del ejercicio de las profesiones sanitarias, la HC adquiere su máxima dimensión en el mundo jurídico, porque es el documento donde se refleja no sólo la práctica médica o acto médico, sino también el cumplimiento de algunos de los principales deberes del personal sanitario respecto al paciente: deber de asistencia, deber de informar, etc., convirtiéndose en la prueba documental que evalúa el nivel de la calidad asistencial en circunstancias de reclamaciones de responsabilidad a los profesionales sanitarios y/o a las instituciones públicas. Todo lo anteriormente expuesto nos indica la gran importancia de la HC desde varios puntos de vista: asistencial, ético y médico-legal.

2. Tratamiento normativo de la Historia Clínica en el derecho español.

La Ley de Autonomía del Paciente 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), es la protagonista en el escenario jurídico español en torno a la HC. Además, ha de observarse al respecto, los preceptos contenidos en la Ley 14/1986, de 25 de abril, General de Sanidad (LGS) y el Código de Deontología Médica de la Organización Colegial Médica de España (CDOMCE), cuya última modificación data del año 2011. Por su parte, las Comunidades Autónomas cuentan con legislación propia, que analizaremos brevemente en el siguiente epígrafe, aunque cabe resaltar que no existe una unificación normativa a pesar de la LAP, que solucione todos los inconvenientes que genera la HC desde el punto de vista de la protección de datos sanitarios y la defensa de los derechos del paciente y los deberes del médico que interviene.

[349] GIMÉNEZ, D. La historia clínica: Aspectos Éticos y Legales. [Blog post]. Blog Geosalud. Disponible en Internet: <http://geosalud.com/malpraxis/historiaclinica.htm> [Consulta: 22 octubre 2016].

2.1. Marco normativo nacional

El Artículo 8 de la LOPD, establece respecto a los datos relativos a la salud que, los centros sanitarios -se refiere tanto a públicos como a privados- y los profesionales correspondientes, podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de los pacientes, según lo dispuesto en la legislación estatal o autonómica sobre sanidad[350]. Advertimos que se deja la potestad legislativa en la materia a las Comunidades Autónomas. Esta circunstancia originó contrastes normativos entre las distintas Comunidades Autónomas. Este hecho condujo a la aprobación de la LAP, que viene a resolver las cuestiones suscitadas respecto al tratamiento de los datos de salud a través de la HC del paciente. La LAP tuvo por objetivo adaptar la LGS, 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 CE[351].

La LAP se refiere a la HC definiéndola 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"*[352]*.* Es sin duda una definición global que refiere a documentos en general, sin que se especifique si en la misma se incluyen además de las anotaciones que hacen los facultativos médicos, las diversas pruebas realizadas que no tienen un soporte de papel, como pueden ser, por ejemplo, pruebas de diagnóstico por imagen.

[350] En este sentido, el Artículo 8, de la LOPD, establece en referencia con los datos de salud 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".*

[351] Preámbulo de la LAP.

[352] Artículo 3, de la LAP.

SÁNCHEZ-CARO y ABELLÁN[353] manifiestan que, el concepto legal está envuelto en uno mucho más amplio, el de la documentación clínica, que a la vez remite a otros dos más concretos, los de información clínica y alta médica.

Sin embargo, la LAP sí que desarrolla en artículos posteriores que *"la historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente"*[354]*,* por lo tanto, si bien deja un amplio margen, sí que podemos apreciar la intención del legislador de incluir en ésta "fotografía" nuestra, todos aquellos documentos que hayan servido al médico para evaluar el estado de salud de cada persona, y almacenar dichos documentos -análisis clínicos, electrocardiogramas, etc.- en nuestro historial clínico.

Asimismo, la normativa menciona que debe dejarse constancia en la HC de cada paciente de los médicos que han intervenido en ella[355]. Este concepto parece un poco difuso, porque si bien es cierto que no hay dudas de que el médico que solicita unas determinadas pruebas para un paciente, deja constancia de las mismas en su historia, pero también puede ocurrir que el médico no realice ninguna intervención médica, pero sí accede a nuestra HC a fin de ver los antecedentes del paciente. Pues consideramos que la LAP ha querido que queden registrados todos los accesos por parte de los médicos u otros profesionales intervinientes en nuestro proceso asistencial, aunque sólo se hayan valido del acceso a nuestra HC para mera consulta sin añadir nada a nuestra "biografía sanitaria".

Coincidimos con DOMÍNGUEZ LUELMO[356] al decir que resulta un tanto contradictorio y pone de relieve una falta de sistemática del legislador, que el Artículo 14 incorpore una definición de carácter más descriptivo de la HC que el Artículo 3 que simplemente se limita a una definición demasiado abarcadora al referirse a "informaciones de cualquier índole".

---

[353] SÁNCHEZ-CARO, J.; ABELLÁN, F. *Derechos y deberes de los pacientes. Ley 41/2002 de 14 de noviembre: consentimiento informado, historia clínica, intimidad e instrucciones previas.* Comares, Granada, 2003, pp. 64.

[354] Artículo 14.1, de la LAP.

[355] El Artículo 14.1, de la LAP, sostiene al respecto que: *"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".*

[356] DOMÍNGUEZ LUELMO, A., op. cit., p. 494-495.

En éste sentido, sostiene CORBELLA DUCH[357] reflexionando sobre la definición que hace la LAP sobre la HC, que el legislador se enmienda a sí mismo, puesto que da una definición diferente en el Artículo 14 que en el Artículo 3 – señala el jurista - que el legislador se olvida del contenido del Artículo 3 al individualizar a la HC de forma diferente y añadirle la identificación de los médicos y de los profesionales que interceden. También, vemos que el legislador utiliza en ambas definiciones la expresión "conjunto de documentos", lo cual nos crea la ambigüedad de considerar si sólo se refiere a la HC de forma documental, o si, por el contrario, se adapta a cualquier forma o soporte, esgrime el reputado jurista.

No obstante, desde nuestro punto de vista, consideramos que la LAP sí que ha tenido perspectiva y abarca cualquier tipo de soporte al referirse a "conjunto de documentos", y ello porque en su cuerpo normativo se encarga de definir a la documentación clínica manifestando que es *el soporte de "cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial"*[358]*.* Asimismo, la LAP establece en su 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",* y en su Artículo 15.1 dice que: *"La historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente".* Y, continúa el precepto, especificando que: *"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"*[359]*.* En armonía con ello, también la reciente Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común, mantiene que los documentos electrónicos deberán conservarse en un formato que permita garantizar la autenticidad, integridad y conservación del documento y, a la vez, con los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados[360].

[357] Vid. CORBELLA DUCH, J., op. cit., p. 142.

[358] Artículo 3, de la LAP.

[359] Artículo 15.1, de la LAP.

[360] Artículo 17, de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común (BOE núm. 236, 2.10.2015).

Según lo expuesto, y basándonos en la normativa analizada *ut supra*, consideramos, contrariamente a lo señalado por CORBELLA DUCH[361], que la HC de los pacientes puede presentarse en cualquier forma o soporte. Por ello, y según las disposiciones citadas, y dados los avances tecnológicos que experimentamos y las facilidades que la utilización de los medios tecnológicos permiten, vemos una intención clara del legislador en aplicar las nuevas tecnologías a las demandas que se generan, facilitando así en este caso, el acceso a la información sanitaria del paciente a través de la HC digital -tema que analizaremos en el siguientes Capítulo-, claramente en observancia de las limitaciones que leyes determinen y de manera que quede garantizada la seguridad de los documentos.

Para acabar de perfilar el marco normativo de la HC, la LAP añade que la HC tiene por finalidad facilitar la asistencia sanitaria. En este punto sí que vemos la laxitud en la conceptualización, porque, incluso establece que los datos que en ella estén consignados, serán aquellos datos que, bajo el criterio de los médicos, permitan conocer de forma veraz y actualizada el estado de salud de un paciente[362].

Sin embargo, el tiempo apremia en la consulta ambulatoria y es a veces un enemigo natural de la minuciosidad en la recolección de datos. Diferente es el caso si el paciente se encuentra internado, porque, evidentemente en éste supuesto el tiempo disponible es mayor para hacer constar todos los datos vinculados a su ingreso hospitalario. En algunos establecimientos asistenciales se utiliza un formulario pre-impreso que debe ser llenado por el paciente antes de la consulta médica. Esto le resta contacto humano necesario a la relación médico-paciente, según consideramos, y, por tanto, los datos que se acaban recolectando en la HC no siempre resultan ser el reflejo de todo lo ocurrido con el paciente y relatado por él durante la consulta, sino aspectos que en el momento de la visita médica resulten relevantes. Por ejemplo, si el paciente acude a un centro asistencial por gripe, seguramente se tomará nota de aquel cuadro médico y de la medicación que se le prescriba para paliar los síntomas, en cambio, si el paciente también refiere que ha tenido en días previos dolor de cabeza, probablemente, esta situación ni se apunte en la HC por ser el motivo de la consulta la gripe, sin embargo, quizás ese síntoma al que no se le da importancia, si el médico no le otorga tal

[361] CORBELLA DUCH, J., op. cit., p. 142.

[362] El Artículo 15.2, de la LAP, establece que: *"La historia clínica tiene como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud".*

relevancia, pueda ser desencadenante de algún tipo de complicación en el estado de salud posterior del paciente, o incluso de la aparición de un ictus.

La idea de conocer el estado de salud, no sólo se construye sobre la noción del médico de poder tener acceso a la HC del paciente, sino también sobre la idea de que el mismo paciente pueda acceder a su HC. Y esta concepción normativa que utiliza la LAP ha seguido el criterio de la LGS que en su ya derogado Artículo 10.11, se refería al derecho del paciente a que quedase constancia por escrito de todo su proceso, como indicamos al inicio de éste Capítulo. Aunque, la LGS no concretó ni estableció concepto alguno de HC, como así tampoco veló por legislar sobre el contenido de la misma o la información que la integra[363], sí que sentó las bases que imperan en nuestra actual normativa. Analizando la nueva redacción que la LAP le ha dado a la HC, podemos sostener que se trata de una definición más completa desde el punto de vista de lo que la misma implica[364], dado que antes de la promulgación de la LAP los derechos fundamentales de los pacientes no estaban contemplados como tales, ni de forma tan extensa a como lo recoge la LAP; y en caso de vulneración, el paciente tenía que acudir a los Tribunales de Justicia, y en aquella instancia judicial se debía acreditar tanto el derecho como su vulneración, extremo que de por sí era difícil de acreditar, costoso y largo, lo cual desanimaba a las personas que habían visto transgredidos sus derechos como usuarios del sistema de salud.

[363] El Artículo 61, de la LGS, contenía esta previsión antes de que fuese derogado por la LAP, y establecía que: *"En cada área de salud debe procurarse la máxima integración de la información relativa a cada paciente, por lo que el principio de historia clínico-sanitaria única por cada uno deberá mantenerse, al menos, dentro de los límites de cada institución asistencial. Estará a disposición de los enfermos y de los facultativos que directamente estén implicados en el diagnóstico y el tratamiento del enfermo, así como a efectos de inspección médica o para fines científicos, debiendo quedar plenamente garantizados el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica. Los poderes públicos adoptaran las medidas precisas para garantizar dichos derechos y deberes".*

[364] Con anterioridad a la LAP, los derechos de los pacientes venían recogidos en la LGS, pero de manera muy somera y faltaban muchos derechos. Ante esa situación eran los Tribunales los que debían pronunciarse al respecto. Para profundizar más el tema, véase: GÓMEZ PIQUERAS, C. "La historia clínica. Aspectos conflictivos resueltos por la Agencia Española de Protección de Datos", en LESMES SERRANO, C., et al. *El derecho a la protección de datos en la historia clínica y en la receta electrónica.* Aranzadi-AEPD-Thomson Reuters, Navarra, 2009, pp. 127 y ss.

Al respecto, manifiestan SÁNCHEZ-CARO y ABELLÁN[365], que la HC está regulada por la LAP con un criterio de unidad y de integración en cada centro asistencial, lo cual importa una reforma importante a la LGS que hablaba del área de salud. Sin embargo, como venimos sosteniendo en ésta Tesis, la normativa no resulta completa desde el punto de vista de la protección de los datos contenidos en la HC de los pacientes.

2.2. Breve referencia al marco normativo autonómico.

Tal y como hicimos mención anteriormente, el Artículo 8 de la LOPD, deja la puerta abierta a la Comunidades Autónomas para legislar en materia de sanidad. Este escenario originó diferencias normativas entre las Comunidades Autónomas, según refiere GONZÁLEZ SALINAS[366], circunstancia que motivó la aprobación de dos normas a nivel nacional. Por un lado, la LAP a través de la cual el Estado intenta ofrecer en el ámbito de la información y la documentación clínica los mismos derechos y las mismas garantías a todos los ciudadanos españoles, regulando de forma general la definición de HC y el contenido mínimo que engloba, intentando con su promulgación, fortalecer el derecho a la protección de la salud que reconoce la CE. Por otro lado, el Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud[367].

En este contexto, analizaremos brevemente la normativa autonómica en la materia, para señalar las diferencias y similitudes que presentan, haciendo hincapié en la Comunidad de Cataluña, que cuenta con abundante en la materia, y a continuación haremos referencia al resto.

[365] SÁNCHEZ-CARO, J.; ABELLÁN, F., op. cit., p. 68.

[366] Vid. GONZÁLEZ SALINAS, P. "El alcance del carácter básico de la ley reguladora de la autonomía del paciente y su influencia en las leyes autonómicas sobre la misma materia", en GONZÁLEZ SALINAS, P.; LIZARRAGA BONELLI, E. (coordinadores). *Autonomía del paciente, información e historia clínica (estudios sobre la Ley 41/2002, de 14 de noviembre).* Thomson Civitas, Madrid, 2004, pp. 15-42.

[367] Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud (BOE núm. 225, 16.11.2010).

a) Comunidad Autónoma de Cataluña.

En la Comunidad Autónoma de Cataluña, a través de la Ley 12/1983, de 14 de julio, de administración institucional de la sanidad, la asistencia y los servicios sociales de Cataluña[368], -actualmente derogada-, se creó el Instituto Catalán de la Salud, que desempeña la función de entidad gestora de los servicios y las prestaciones sanitaras propias de la Generalidad de Cataluña y de los transferidos de la seguridad social, con el fin de desarrollar las competencias que la CE y que el propio Estatuto de Autonomía atribuyen a la Generalidad de Cataluña, con el fin de ejecutar los servicios y funciones que le habían sido traspasados.

Con posterioridad, se promulgó la Ley 15/1990, de 9 de julio, de ordenación sanitaria, cuyo objetivo es la ordenación del sistema sanitario público de Cataluña[369], de acuerdo con los principios de universalización, integración de servicios, simplificación, racionalización, eficacia y eficiencia de la organización sanitaria, concepción integral de la salud, descentralización y desconcentración de la gestión, sectorización de la atención sanitaria y participación comunitaria. A los efectos de dicha ordenación, se crea un ente público, el Servicio Catalán de la Salud, integrado por todos los centros, servicios y establecimientos sanitarios públicos y de cobertura pública de Cataluña.

Se pretende con el dictado de la Ley 15/1990, superar determinadas deficiencias de la organización sanitaria, como es la desvinculación entre las actuaciones en materia de ordenación y planificación y las de gestión de los servicios sanitarios, atribuidas en todas partes a órganos diferenciados, asignándolas a un organismo único que las desarrolle bajo una dirección única, con el objetivo de alcanzar una adecuada coordinación en las materias antedichas, del todo aconsejable, por otro lado, teniendo en cuenta su estrecha interrelación.

Cabe resaltar como uno de los aspectos más novedosos de ésta Ley, y que la diferencia notablemente de las leyes de creación de los servicios de salud de otras Comunidades Autónomas, la diversidad de fórmulas de gestión directa, indirecta o

[368] Ley 12/1983, de 14 de julio, de administración institucional de la sanidad, y de la asistencia y los servicios sociales de Cataluña (DOGC núm. 345, 15.07.1983).

[369] Ley 15/1990, de 9 de julio, de Ordenación Sanitaria de Cataluña (DOGC núm. 1324, 30.07.1990).

compartida que el Servicio Catalán de la Salud puede emplear a los efectos de la gestión y administración de los servicios y prestaciones del sistema sanitario público.

La Comunidad catalana también cuenta con la Ley 21/2000, sobre los derechos de información relativos a la salud, la autonomía del paciente y la documentación clínica[370], que tiene por objeto la regulación de la HC[371]. Ésta Ley se promulga con la intención de concreción práctica de los derechos a la información, al consentimiento informado y al acceso de la documentación clínica de los ciudadanos de Cataluña en el ámbito sanitario. La inclusión de la regulación sobre la posibilidad de elaborar documentos de voluntades anticipadas[372] en la parte relativa a la autonomía del paciente, constituye seguramente la novedad más destacada de la Ley. Debemos mencionar que ésta Ley es la primera en España en reconocer estos documentos.

Esta normativa abarca tanto la protección de los datos de salud, así como la forma de almacenarlos por parte de los centros asistenciales[373]. Pone el énfasis en los centros sanitarios y no en el personal que interviene en la HC, para referirse a la diligencia y custodia que de los datos de salud se debe guardar. El punto de custodia lo legisla a través de luna doble obligación de los centros sanitarios. Por un lado, los centros sanitarios deben almacenar las HC en instalaciones que garanticen la seguridad, la correcta conservación y la recuperación de la información[374]. Y, por otro lado, los centros sanitarios, deben adoptar las medidas técnicas y organizativas adecuadas con el fin de proteger los datos personales recogidos de los pacientes que en ellos se tratan, y evitar la destrucción o la pérdida accidental y también el acceso, la alteración, la comunicación o cualquier otro procedimiento que no esté autorizado con respecto a esos datos íntimos[375].

---

[370] Ley 21/2000, de Cataluña, sobre los derechos de información relativos a la salud, la autonomía del paciente y la documentación clínica (BOE núm. 29, 2.02.2001).

[371] Ibídem. El Artículo 1, promulga que: *"Esta Ley tiene por objeto a) Determinar el derecho del paciente a la información concerniente a la propia salud y a su autonomía de decisión. b) Regular la historia clínica de los pacientes de los servicios sanitarios".*

[372] Ibídem, Artículo 8. Para profundizar más el tema, véase al respecto: GÓMEZ JARA, M.; GÓMEZ MARICHALAR, N. *Consultas en Psiquiatría Legal.* Atelier. Barcelona, 2009, pp. 171 y ss.

[373] Ibídem. El Artículo 9.4, de la Ley 21/2000, de Cataluña, establece que: *"Los centros sanitarios han de adoptar las medidas técnicas y organizativas adecuadas para proteger los datos personales recogidos y evitar la destrucción o la pérdida accidental y también el acceso, la alteración, la comunicación o cualquier otro procedimiento que no esté autorizado".*

[374] Ibídem, Artículo 9.2.

[375] Ibídem, Artículo 9.4.

La normativa catalana propugna por la integración en un documento único -la HC- de todos aquellos datos de salud que refieren a un paciente, y consagra también la necesidad de que tanto médicos como personal sanitario que intervengan en el proceso asistencial, queden reflejados en la HC del paciente[376]. Vemos, que, a diferencia de la Ley estatal, la LAP, la Ley catalana agrega a la definición la singularidad de la HC, es decir, que no puede haber más de una. Consideramos que esta previsión legal es acertada y viene a responder al criterio de la HC digital, que ha de ser una única por cada paciente, evitándose así la duplicidad y dispersión de nuestra información sanitaria. En este sentido, CORBELLA DUCH[377] explica que la LGS, mencionaba ya por el año 1986 el principio de la HC única en cada institución asistencial, dejando así un vacío legislativo que de forma diferente fueron llenando las Comunidades Autónomas hasta la promulgación de la LAP.

También, la Ley 21/2000, es una Ley novedosa desde el punto de vista de las previsiones futuras relacionadas con las nuevas tecnologías que se verán involucradas en la HC, obligando, en este sentido, al centro sanitario a almacenarlas en instalaciones que garanticen la seguridad, la conservación correcta y la recuperación de la información, como hemos mencionado *ut supra*, y además, promulga que la HC se podrá elaborar en soporte papel, audiovisual e informático, siempre que se garantice la autenticidad del contenido y la plena capacidad de reproducción futura. Evidentemente esta previsión guarda mucha correlación con el Big Data sanitario y el avance exponencial de las nuevas tecnologías en el ámbito de la salud, tema al que nos referiremos en la Segunda parte de ésta Tesis. En el momento de promulgación de la Ley catalana, se concedió el plazo de un año para que los centros sanitarios pudieran adoptar dichas medidas técnicas y organizativas necesarias para adaptar el tratamiento de las HC a las previsiones que la Ley esboza[378].

---

[376] Ibídem. El Artículo 9.1, manifiesta que: *"1. La historia clínica recoge el conjunto de documentos relativos al proceso asistencial de cada enfermo, identificando a los médicos y al resto de los profesionales asistenciales que han intervenido en él. Se ha de procurar la máxima integración posible de la documentación clínica de cada paciente. Esta integración se ha de hacer, como mínimo, en el ámbito de cada centro, donde debe haber una historia clínica única por cada paciente".*

[377] Ver al respecto: CORBELLA DUCH, J., op. cit., p. 141.

[378] Ibídem. La Disposición transitoria, establece que: *"Los centros sanitarios disponen de un plazo de un año, contado a partir de la entrada en vigor de esta Ley, para adoptar las medidas técnicas y organizativas necesarias para adaptar el tratamiento de las historias clínicas a las previsiones que aquí se contienen y elaborar los modelos normalizados de historia clínica a que hace referencia el*

Otra notable característica que la Ley 21/2000 introduce, es la exigencia de dejar constancia escrita de los médicos que han intervenido en el proceso asistencial y de las acciones realizadas por ellos. Establece al respecto en su Artículo 10.2 que: *"En las historias clínicas hospitalarias, en las que suelen participar más de un médico o de un equipo asistencial, han de constar individualizadas las acciones, las intervenciones y las prescripciones realizadas por cada profesional".* Esta disposición nos parece sumamente importante, y a diferencia de la LAP, la Ley Catalana sí que establece la obligatoriedad de que conste la identidad de todos los médicos que intervienen en el proceso asistencial de un paciente, con la identificación expresa del profesional, junto a las acciones médicas que él mismo verifica en el historial del paciente. Sin duda creemos que es una estipulación normativa muy significativa, porque a la hora de dirimir posibles responsabilidades médicas -ente otras cosas-, la HC de por sí se basta como documentación acreditativa de todos los procedimientos asistenciales, los medicamentos suministrados, los tratamientos indicados, etc., junto al médico que lo ha diagnosticado, que ha prescrito el medicamento, etc.

Coincidimos con RODRÍGUEZ IZQUIERDO[379] al decir que con la Ley 21/2000, se establecen una serie de criterios fundamentalmente prácticos, puesto que hasta ese momento la normativa existente en la materia era dispersa, tanto para los usuarios de los servicios sanitarios, como para los profesionales sanitarios que son los que configuran las HC y trabajan con ellas a diario como instrumento básico de la asistencia sanitaria.

Asimismo, con la entrada en vigor en su momento, de la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos[380] -actualmente derogada-, se requería la inscripción de todos los ficheros automatizados de datos personales que integren la Administración local[381], otorgándose un plazo de dos años para realizar dicha

---

Artículo 10.2. Los procesos asistenciales que se lleven a cabo una vez transcurrido este plazo se han de reflejar documentalmente de acuerdo con los modelos normalizados aprobados".

[379] Vid. RODRÍGUEZ IZQUIERDO, R. "Los derechos y obligaciones de los pacientes", en RIVAS VALLEJO, P.; GARCÍA VALVERDE, M. (Directoras). *Derecho y Medicina. Cuestiones jurídicas para profesionales de la salud.* Aranzadi, Navarra, 2009, p. 397.

[380] Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos (BOE núm. 115, 14.05.2002).

[381] La disposición adicional primera de la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, establece que: *"En el plazo de tres meses a partir de la constitución del Consejo Asesor de Protección de Datos de Cataluña, ha de formalizarse la inscripción en el Registro de*

inscripción[382], hecho que en Cataluña se verificó, siendo una de las Comunidades que a día de hoy posee las HC informatizadas en su totalidad en los centros de salud públicos.

b) Otras Comunidades Autónomas.

En la Comunidad Autónoma de Aragón, se dispone de una reglamentación específica sobre la HC. Concretamente, la Ley 6/2002, de 15 de abril, de Salud de Aragón[383] viene a desarrollarla, en su Título III, Capítulo IV. Asimismo, contempla la normativa, que los centros asistenciales del Sistema de Salud de Aragón dispondrán de un único modelo normalizado de HC que recoja los contenidos mínimos que la misma Ley fija, adaptados al nivel asistencial que tengan y a la clase de prestación que realicen[384].

Al igual que la disposición catalana, la Ley aragonesa regula una HC de carácter unitario[385], define brevemente su contenido[386] y establece la necesidad de que los centros sanitarios adopten las medidas tendientes a facilitar el tratamiento de las historias clínicas y también pone el acento en la institución como responsable y custodio de los datos de salud contenidos en las historias clínicas de los pacientes.

Por su parte, en la Comunidad Autónoma de Galicia[387] también se legisla en la materia con la adopción de la Ley 3/2001, de 28 de mayo, reguladora del consentimiento

---

Protección de Datos de Cataluña de los ficheros automatizados de datos personales de titularidad de la Generalidad de Cataluña y de titularidad de los entes que integran la Administración local dentro del ámbito territorial de Cataluña que existían antes de la promulgación de la presente Ley".

[382] La disposición adicional segunda de la Ley 5/2002, de 19 de abril, op. cit., refiere a los ficheros y tratamientos de datos personales no automatizados, regulando que: *"Los ficheros y los tratamientos de datos personales no automatizados de titularidad de la Generalidad de Cataluña y de los entes que integran la Administración local dentro del ámbito territorial de Cataluña han de formalizar su inscripción en el Registro de Protección de Datos de Cataluña en el plazo de dos años a contar desde la entrada en vigor de la presente Ley, sin perjuicio de que las personas interesadas puedan ejercer los derechos de acceso, rectificación y cancelación".*

[383] Ley 6/2002, de 15 de abril, de Salud de Aragón (BOE núm. 121, 21.05.2002).

[384] Ibídem, Artículo 17.2.

[385] Ibídem, Artículos 16.2 y Articulo 19.

[386] Ibídem, Artículos 16 y 17.

[387] Ley 3/2001, de 28 de mayo, reguladora del consentimiento informado y de la historia clínica de los pacientes, de Galicia (BOE núm. 158, 3.07.2001).

informado y de la HC de los pacientes[388], que tiene por objeto *"regular el consentimiento informado de los pacientes así como su historia clínica, garantizando el acceso de aquéllos a la información contenida en la misma"*[389].

Al igual que la normativa autonómica catalana y la aragonesa, la legislación gallega también ha centrado las obligaciones en el centro sanitario y ha sido bastante vanguardista al legislar en el sentido de indicar que el Servicio Gallego de Salud es el encargado de adoptar medidas que tiendan a la informatización progresiva de las historias clínicas. Ya destaca ésta normativa que la documentación del paciente ha de ser única, y ello de manera independiente de si la HC se encuentra en papel o en cualquier otro medio tecnológico que lo reemplace. También consideramos que, junto a la normativa catalana, han sido las regulaciones más acordes con el futuro tecnológico y han sabido compaginar la legislación con los cambios que se vislumbraban en el sector de datos sanitarios.

La citada Ley, contiene una definición muy interesante sobre el concepto de la HC exponiendo que: *"… es el conjunto de documentos en los que se contienen los datos, las valoraciones y las informaciones de cualquier tipo sobre la situación y la evolución clínica de los pacientes a lo largo de su proceso asistencial, así como la identificación de los médicos y demás profesionales que intervinieron en éste"*[390]. Si bien es una definición corta, consideramos que abarca el concepto genérico de lo que ha de entenderse por HC. Aunque, advertimos, una ambigüedad al decir *"y las informaciones de cualquier tipo"*, dando lugar a un amplio abanico de posibles informaciones que entonces se podrían incorporar. Cabría preguntarse si éstas informaciones pueden llegar a ser incompatibles con la misma LOPD.

La Comunidad Riojana[391], por su parte, cuenta con la Ley 2/2002, de 17 de abril de Salud. Sin embargo, no contiene una definición expresa sobre la HC y simplemente se hace una breve referencia a que la información clínica individualizada se unifique, pero

---

[388] Ibídem. La disposición adicional tercera, señala que: *"El Servicio Gallego de Salud adoptará las medidas adecuadas tendentes a la informatización progresiva de las historias clínicas, garantizando la integración de la información relativa a cada paciente con independencia del soporte en que se encuentre".*

[389] Ibídem, Artículo 1.

[390] Ibídem, Artículo 13.

[391] Ley 2/2002, de 17 de abril, de Salud, de la Comunidad Autónoma de La Rioja (BOR núm. 49, 23.04.2002).

sólo haciendo mención que será dentro del Sistema Público de Salud de La Rioja, evidentemente es muy escueta esta normativa, y da poca cobertura legal a los procesos sanitarios donde se vinculan los datos de salud de los pacientes[392]. Sin embargo, consideramos que el sistema riojano de salud preveía la eliminación de la multiplicidad de HC de los pacientes -en pro de su unificación- y previó la implantación de la HC digital.

Sin embargo, la Comunidad Autónoma de La Rioja legisla el acceso a la HC por parte del paciente de una manera muy amplia. En su Artículo 11, establece que:

> El paciente tiene el derecho a conocer toda la información obtenida respecto a su salud y a disponer, en términos comprensibles para él, información veraz y adecuada referente a su salud y al proceso asistencial, incluyendo el diagnóstico, la relación riesgo/beneficio, las consecuencias del tratamiento y las del no tratamiento, las alternativas al tratamiento planteado y siempre que sea posible, el pronóstico. También, se ha de respetar la voluntad del paciente en el caso de que éste no quiera ser informado[393].

En el mismo sentido, opina LOMAS HERNÁNDEZ[394], considerando que la Comunidad de La Rioja ha obviado el límite de las anotaciones subjetivas previsto en la LAP, regulando que el paciente pueda acceder a la totalidad de su HC.

Por su parte, el País Vasco[395] cuenta con abundante normativa en la materia, destacando el Decreto 272/1986 de 25 de noviembre por el que se regula el uso de la HC de los Centros Hospitalarios de la Comunidad Autónoma del País Vasco, la Ley 8/1997, de 26 de junio, de Ordenación sanitaria de Euskadi, y el Decreto 45/1998, de 17

---

[392] Ibídem. En su disposición adicional primera, establece que: *"Conforme las disponibilidades y medios técnicos lo permitan, se unificará la información clínica individualizada para el conjunto del Sistema Público de Salud de La Rioja".*

[393] Ibídem, Artículo 11.1.

[394] LOMAS HERNÁNDEZ, V. "La protección del paciente en la reciente legislación sanitaria", en TOMILLO URBINA, J.; CAYÓN DE LAS CUEVAS, J. (directores). *La Protección Jurídica del Paciente como Consumidor.* Aranzadi, Navarra, 2010, p. 136.

[395] Ley 8/1997, de 26 de junio, de Ordenación sanitaria de Euskadi (BOE núm. 9, 11.01.2012); Decreto 272/1986 de 25 de noviembre por el que se regula el uso de la Historia Clínica de los Centros Hospitalarios de la Comunidad Autónoma del País Vasco (BOPV núm. 242, 6.12.1986); Decreto 45/1998, de 17 de marzo, por el que se establece el contenido y se regula la valoración, conservación y expurgo de los documentos del Registro de Actividades Clínicas de los Servicios de Urgencias de los Hospitales y de las Historias Clínicas Hospitalarias, de la Comunidad Autónoma del País Vasco (BOPV núm. 67, 8.04.1998).

de marzo, por el que se establece el contenido y se regula la valoración, conservación y expurgo de los documentos del Registro de Actividades Clínicas de los Servicios de Urgencias de los Hospitales y de las Historias Clínicas Hospitalarias.

El Decreto 272/1986, del País Vasco, hace referencia al contenido, a la valoración y a la conservación de los documentos del registro de actividades clínicas de los servicios de urgencias de los hospitales y de las historias clínicas hospitalarias. El Decreto 272/1986, centra su objeto en la regulación de un registro de información, que toma su base en la HC, formando un núcleo estandarizado de datos, de carácter impersonal, que todo hospital deberá obligatoriamente proveer, al objeto inmediato de configurar un sistema de información sanitaria comunitario denominado Registro de Altas Hospitalarias de Euskadi, todo ello en orden a garantizar la confidencialidad del individuo[396].

En la Comunidad Valenciana[397] se ha regulado sobre el particular, a través del Decreto 56/1988, de 25 de abril, del Consell de la Generalitat Valenciana, por el que se regula la obligatoriedad de la HC; la Ley 3/2003, de 6 de febrero, de la Generalitat, de Ordenación Sanitaria de la Comunidad Valenciana; Orden de 17 de febrero de 1994, de la Conselleria de Sanitat i Consum, por la que se regula la confidencialidad y custodia de los datos médicos de los servicios médicos de empresa y la Orden de 14 de septiembre de 2001, de la Conselleria de Sanidad, por la que se normalizan los documentos básicos de la HC hospitalaria de la Comunidad Valenciana y se regula su conservación.

El Decreto 56/1988, de Valencia, establece que la HC debe contener suficiente información para identificar al paciente, documentar las circunstancias por las que se acudió a la institución, informar acerca del régimen de financiación, apoyar el diagnóstico, justificar el tratamiento y documentar los resultados obtenidos y las

[396] Preámbulo del Decreto 272/1986, del País Vasco, op. cit.

[397] Decreto 56/1988, de 25 de abril, del Consell de la Generalitat Valenciana (DOCV núm. 817, 4.05.1988); Ley 3/2003, de 6 de febrero, de Ordenación Sanitaria de la Comunidad Valenciana (BOE núm. 55, 5.03.2003); Orden de 17 de febrero de 1994, de la Conselleria de Sanitat i Consum, por la que se regula la confidencialidad y custodia de los datos médicos de los servicios médicos de empresa (DOCV núm. 2227, 13.03.1994); Orden de 14 de septiembre de 2001, de la Conselleria de Sanidad, por la que se normalizan los documentos básicos de la historia clínica hospitalaria de la Comunidad Valenciana y se regula su conservación (DOGV núm. 4111, 22.10.2001).

circunstancias del alta[398]. Vemos que la normativa Valenciana incorpora como elemento novedoso a tener en cuenta, que en la misma HC se debe hacer constar de la posible financiación del tratamiento recibido, es decir, que en lo relativo al objeto de nuestro estudio, los datos contenidos en la HC en Valencia no sólo se limitan a los datos exclusivamente de salud, sino que se incorporan datos de carácter económico y financiero, que desde nuestro punto de vista, no guarda relación alguna con la finalidad que tiene nuestra HC.

Por su parte, la Ley 3/2003, de Valencia, consagra la necesidad de unicidad de la HC, esto en el mismo sentido que otras normativas autonómicas analizadas *ut supra*.

En Castilla y León[399] cuentan con el Decreto 101/2005 de 22 de diciembre, que refiere a la HC como elemento básico en la relación médico-paciente, que ha de estar a disposición de los profesionales que le asisten. En aras de su mejor utilización es preciso que la HC esté unificada dentro del mayor ámbito posible, que se determine qué documentos ha de contener, cómo ha de cumplimentarse y que se establezcan modelos normalizados de los documentos que incorpora[400]. Avanza aún más el presente Decreto y en su preámbulo reconoce que la utilización cada vez mayor de las nuevas tecnologías pone a disposición de los centros sanitarios medios electrónicos, informáticos y telemáticos que, aplicados también a la HC, suponen cambios en su configuración[401]. Ello puede contribuir a la implantación de la HC única, no ya en el marco de cada centro o Área de Salud, sino para el conjunto de la Comunidad Autónoma e incluso para el ámbito nacional.

Vemos como en la Comunidad Leonesa dan un paso más en la regulación normativa, en un intento de prever el futuro de la sanidad que se verá altamente influenciado por los avances tecnológicos, tal y como sostenemos en ésta Tesis, introduciendo la posibilidad de que la HC digital pueda ser utilizada por los médicos en todo el territorio español a efectos de la mejor asistencia a los pacientes, se realice ésta en la Comunidad de Castilla o León o fuera de la misma.

---

[398] Artículo 2, Decreto 56/1988, de Valencia, op. cit.

[399] Decreto 101/2005 de 22 de diciembre, por el que se regula la historia clínica, de Castilla y León (BOCyL núm. 249, 28.12.2005).

[400] Preámbulo del Decreto 101/2005, de Castilla y León, op. cit.

[401] Ibídem.

La Comunidad Extremeña[402] cuenta con la Ley 10/2001, de 28 de junio, de Salud de Extremadura, aunque la misma no aborda el tema puntual de las historias clínicas, y con la Ley 7/2011, de 23 de marzo, de salud pública de Extremadura, que abarca la seguridad del paciente y la promoción de la salud a través de la educación social.

La Comunidad Navarra[403] se rige por los preceptos contenidos en la Ley Foral 11/2002, de 6 de mayo, sobre los derechos del paciente a las voluntades anticipadas, a la información y a la documentación clínica, regulando de manera muy similar a la normativa catalana.

Finalmente, y a modo de conclusión destacábamos al principio de este breve análisis de la normativa autonómica, que seguramente el legislador pretendió con la LAP, homogenizar la regulación que existía en materia de documentación clínica del paciente. A pesar de ello, advertimos en la normativa autonómica brinda respuestas desiguales frente al régimen de los datos comprendidos en la HC, a su tratamiento y a su disposición y custodia. Por lo tanto, y tal como se ha expuesto, sólo algunas Comunidades Autónomas[404] disponen de regulación autonómica específica sobre HC, que son: Aragón, Canarias, Cantabria, Castilla La Mancha, Castilla y león, Cataluña, Extremadura, Galicia, Murcia, Navarra, País Vasco y Valencia.

---

[402] Ley 10/2001, de 28 de junio, de Salud de Extremadura (DOE núm. 76, 3.07.2001); Ley 7/2011, de 23 de marzo, de salud pública de Extremadura (DOE núm. 59, 25.03.2011).

[403] Ley Foral 11/2002, de 6 de mayo, sobre los derechos del paciente a las voluntades anticipadas, a la información y a la documentación clínica de Navarra (BON núm. 58, 13.05.2002).

[404] Las restantes Comunidades Autónomas sólo mencionan la HC o se atienen a la normativa estatal. En este sentido, en Andalucía se aprobó la Ley 2/1998, de 15 de junio de Salud de Andalucía (BOE núm. 185, 4.08.1998), aunque en ella no se desarrolla específicamente la HC. Sin embargo, en muchos de sus Decretos sí hacen referencia explícita al uso de la HC. Como por ejemplo la Resolución 184/2003 de 3 de marzo, Instrucciones sobre el procedimiento de ordenación y gestión de la documentación clínica en centros asistenciales del SAS. Como dato curioso, en esta comunidad a la HC se la denomina Historia de Salud. En Asturias, tienen una Ley sobre sanidad, la Ley 1/1992, de 2 de julio, del Servicio de Salud del Principado de Asturias (BOE núm. 211, 2.09.1992), sin referencias explícitas a la HC. En Baleares, tienen la Ley 5/2003, de 4 de abril, de salud de las Illes Balears (BOE núm.110, 8.05.2003). En su Artículo 14 se refiere a la HC, pero solamente desde un punto de vista genérico estableciendo que la HC ha de contener, en todo caso, los datos personales, los de la asistencia y los clínico-asistenciales, como así también han de constar las acciones, las intervenciones y las prescripciones hechas por cada profesional sanitario.

3. Características de la Historia Clínica.

La HC responde a una serie de características a las que la LAP[405] hace referencia. Estas características se basan en dos pilares fundamentales. Por un lado, la HC debe incorporar la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. Por otro lado, 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 en el de atención especializada[406].

Por su parte autores como SANCHEZ-CARO y ABELLAN[407] y MÉJICA[408] resumen las características que debe tener la HC sosteniendo que ha de ser:

(i) Completa, ello importa que recopile todos los actos médicos realizados con el paciente. Por su parte CORBELLA DUCH[409] discrepa porque considera que la HC no es completa, sino un mero resumen de las transcripciones –no siempre fidedignas- de los que intervienen en su redacción.

(ii) Ordenada y actualizada, esto significa que ha de reflejar de forma cronológica los acontecimientos y actos médicos realizados, debidamente fechados y con la indicación de las personas y del lugar donde se han realizado.

(iii) Inteligible, aquí los autores manifiestan que ha de emplearse letra legible, frases concisas y sin abreviaturas, aunque destacamos que este inconveniente es claramente una ventaja que la HC digital introduce, y, además, el ordenador permite al personal sanitario volcar el diagnóstico médico en formato digital, facilitando lo que anteriormente suponían las anotaciones en papel, tema que trataremos más adelante.

[405] Capítulo V, de la LAP.

[406] Artículo 15, de la LAP.

[407] SÁNCHEZ-CARO, J.; ABELLÁN, F., op. cit., pp. 69-70.

[408] MÉJICA, J.; DÍEZ, J. R., op. cit., pp. 184-185.

[409] CORBELLA DUCH, J., op. cit., pp. 143 y ss.

(iv) Respetuosa, esto es sin afirmaciones hirientes para el propio paciente, para otros colegas, o para la institución. Estas "afirmaciones" se conocen como "anotaciones subjetivas" y ello ha generado bastante debate en el sector doctrinal, pero no es objeto de estudio del presente trabajo[410].

(v) Con las rectificaciones y aclaraciones necesarias para complementarla.

(vi) Veraz, vemos que el acento legal y doctrinal siempre se pone en que los datos contenidos en la HC sean veraces, además consideramos que, de lo contrario, no tendría razón de ser su existencia.

(vii) Extendida en el soporte más adecuado sometido a la Ley. Este es el punto esencial en el que en esta Tesis nos centramos.

(viii) Única para cada paciente. Evidentemente esto tiene que ser así para evitar las duplicidades, y la repetición de pruebas médicas que supondrían una doble dolencia en los casos de pruebas invasivas para los pacientes y un incremento en el coste por parte del Sistema Nacional de Salud.

Tal como se comentó anteriormente, la HC se llevará con criterios de unidad y de integración en cada institución asistencial, lo que, según manifiestan SANCHEZ-CARO y ABELLAN[411], supone una importante modificación de la LGS que hablaba del área de salud.

MÉJICA y DÍEZ[412]destacan que en la HC concurren tres presupuestos: a) Que está formada por el conjunto de documentación e información sobre el proceso asistencial de cada paciente; b) Que la HC, en cuanto sometida al principio de unidad, debe existir una por cada paciente, al menos en el ámbito de cada centro sanitario; y, finalmente, c)

[410] Cabe destacar en éste punto que las anotaciones subjetivas han traído bastantes conflictos que de a poco se van solventando a través de las distintas opiniones doctrinales que intentan buscar solución al tema, hasta tanto la Jurisprudencia se pronuncie. Si por ejemplo el paciente solicita la copia de su historial clínico, qué pasaría con las anotaciones que el personal sanitario ha volcado en ella de manera subjetiva. Evidentemente es un tema muy complicado y que requiere de un estudio jurídico más exhaustivo.

[411] SÁNCHEZ-CARO, J.; ABELLÁN, F. *Enfermería y Paciente. Cuestiones prácticas de Bioética y Derecho Sanitario.* Comares, Granada, 2007, pp. 208 y ss.

[412] MÉJICA, J.; DÍEZ, J. R., op. cit., pp. 165-166.

Que la HC se redacta necesariamente y en primer lugar en beneficio e interés de la propia salud del paciente, por lo cual -concluyen los autores- que cualquier utilización con finalidad ajena a la asistencial, bien sea administrativa o de cualquier otra índole, por ejemplo de auditoría, deberá de respetar escrupulosamente la intimidad del paciente y el principio de confidencialidad en la actuación sanitaria.

4. Contenido de la Historia Clínica.

La HC ha de contener una serie de datos mínimos[413] de carácter obligatorio que se acuerdan por normativa estatal. Las normativas autonómicas amplían este espectro, tal como hemos hecho referencia anteriormente. Por tanto, la HC a nivel de la LAP incorpora los datos considerados básicos e importantes, que a criterio del médico deben estar incluidos y, estos datos considerados valiosos desde el puno de vista asistencial, deben estar registrados en la HC del paciente.

Evidentemente la HC no se hace en un día, sino que comprende una relación médico-paciente, que paulatinamente se va escribiendo y dejando constancia en nuestra "biografía sanitaria", de cada visita médica, ingreso hospitalario, pruebas practicadas, diagnóstico, tratamiento, etc., constituyendo la HC de cada paciente.

La LAP indica que la HC 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[414]. Por su parte, la Ley de Ordenación de las Profesiones Sanitarias[415], avanza más sobre la cuestión, afirmando que HC debe ser común para

[413] Nos referimos a "datos mínimos" para expresar que la HC ha de contener todos aquellos datos que el profesional médico necesite conocer para tener una idea clara sobre el estado de salud del paciente, de tal manera que estos datos han de ser veraces y actuales para el fin asistencial que se brinda al paciente.

[414] Artículo 14.1, de la LAP.

[415] Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias (BOE núm. 280, 22.11.2003).

cada centro y única para cada paciente atendido en él[416]. La HC tenderá a ser soportada en medios electrónicos y a ser compartida entre profesionales, centros y niveles asistenciales, aspecto que abordaremos más adelante.

La HC debe contener toda la información que se considere trascendental – desde el punto de vista médico[417] - 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[418].

Sostiene CORBELLA DUCH[419], que el legislador tiene un interés especial en que el contenido de la HC sea veraz, que sea un fiel reflejo de la realidad y por eso lo contempla en la Ley de Autonomía del paciente, obligando a los profesionales sanitarios a actuar con la máxima diligencia y, a las Administraciones públicas a establecer los mecanismos que lo garanticen. Al respecto, la LAP establece en su Artículo 14.3 que: *"Las Administraciones sanitarias establecerán los mecanismos que garanticen la autenticidad del contenido de la historia clínica y de los cambios operados en ella, así como la posibilidad de su reproducción futura".*

En el ámbito sanitario, según SANCHEZ-CARO y ABELLÁN[420], la HC, tanto manual como electrónica, tiene por objeto facilitar la asistencia médica al ciudadano, y, por tanto, la naturaleza de la información que se incluye en la misma ha de ser acorde con éste objetivo, debiéndose recoger exclusivamente toda la información clínica necesaria para asegurar, bajo un criterio médico, el conocimiento veraz, exacto y actualizado del estado de salud del paciente, por parte de los sanitarios que le atienden.

---

[416] Artículo 4.7 a) de la Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias (BOE núm. 280, 22.11.2003).

[417] Artículo 15.2, de la LAP.

[418] Artículo 15.1, de la LAP.

[419] CORBELLA DUCH, J., op. cit., p. 143.

[420] SÁNCHEZ-CARO, J.; ABELLÁN, F. *Telemedicina y protección de datos sanitarios. Aspectos legales y éticos.* Comares, Granada, 2002, p. 68. Ver también al respecto: SÁNCHEZ-CARO, J.; ABELLÁN, F. *La Historia Clínica.* Fundación Salud 2000, Granada, pp. 11 y 12.

4.1. Datos de inclusión obligatoria.

La LAP ha reseñado una lista de contenidos mínimos[421] que la HC ha de contener para que sirva para facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud, tal como se ha indicado *ut supra*. A su vez, ésta lista enunciada por la LAP, se desarrolla por el Real Decreto 1093/2010, del conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud[422], que en sus Anexos incluye el listado de datos que han de contener las HC según la atención sanitaria que se esté brindando. Aportamos al final de ésta Tesis los ocho Anexos de. Decreto 1093/2010, según se trate de:

(i) Informe clínico de alta, detallado en el Anexo I.

(ii) Informe clínico de consulta externa, detallado en el Anexo II.

(iii) Informe clínico de urgencias, detallado en el Anexo III.

(iv) Informe clínico de atención primaria, detallado en el Anexo IV.

(v) Informe de resultados de pruebas de laboratorio, detallado en el Anexo V.

(vi) Informe de resultados de pruebas de imagen, detallado en el Anexo VI.

(vii) Informe de cuidados de enfermería, detallado en el Anexo VII.

(viii) Historia clínica resumida, detallada en el Anexo VIII.

No obstante, para que la HC se considere completa y permita el conocimiento adecuado, actualizado y fidedigno del paciente, debería contener los datos que a continuación se indican:

(i) La documentación relativa a la hoja clínico estadística. Se estructura de varias partes que están orientadas a recoger datos personales del paciente:

[421] Artículo 15.2, de la LAP.

[422] Artículo 3, del Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud (BOE núm. 225, 16.11.2010).

a. Datos personales. Los datos personales deben anotarse en el encabezamiento de la historia clínica. El nombre, dirección, número de teléfono, género, edad, ocupación, raza, nacionalidad, religión, estado civil, numero de documento y el nombre del médico que lo refiere. Cada uno de estos datos, que encuadran al paciente, y sus costumbres culturales, aportan por si mismos información de utilidad médica.

b. Motivo de la consulta. Es el motivo o razón (Síntoma, Signo, Síndrome, Diagnóstico o Problema) que lleva al paciente a solicitar la opinión del médico. Es lo que lo lleva a recabar una entrevista con el profesional de la salud.

c. Enfermedad actual. La enfermedad actual es la narración del motivo de la consulta. En forma ordenada, lógica, gramaticalmente correcta, se describirá uno a uno los datos que movilizaron a buscar la opinión del facultativo. Esto debe desarrollarse con los datos aportados como con los que, por su ausencia, tienen importancia y contribuyen a la comprensión de los diferentes problemas.

d. Antecedentes personales. En esta sección del interrogatorio se toma nota de todos los episodios que afectaron la salud del paciente desde su nacimiento. Se toman en cuenta datos referidos a alergias, enfermedades, intervenciones quirúrgicas, traumatismos, etc.

e. Hábitos personales. Se apuntan datos referidos al hábito de sueño, de ingesta de alcohol, de drogas, si se es o no fumador y con qué frecuencia, si se practica deporte, etc.

f. Antecedentes familiares. Aquí se suele dejar constancia de enfermedades que hubiesen podido afectar al entorno familiar, o del fallecimiento de parientes muy próximos y la cause de defunción.

(ii) La autorización de ingreso. Es el documento por el cual el paciente o su responsable legal autorizan la hospitalización y la puesta en práctica de aquellas medidas diagnósticas o terapéuticas que los facultativos consideren oportunas.

(iii) El informe de urgencia. Es el tipo documental que registra la atención prestada en el área de urgencias, y deberá contener como mínimo, los datos de identificación del paciente y las circunstancias por las que se acude al servicio de urgencias.

(iv) La anamnesis y la exploración física. La anamnesis consiste en la información que el médico recopila del paciente en las visitas sanitarias, que se compone de los hábitos del paciente, sus antecedentes familiares, y demás impresiones que el médico pueda extraer de las informaciones que el propio paciente le comenta. La exploración física radica en la verificación de los síntomas que el paciente transmite al médico y éste objetivamente diagnostica en base a ello, sumado a las impresiones subjetivas que el médico extrae de la anamnesis.

(v) La evolución. La evolución del paciente consiste en los datos que su salud proporciona durante el curso de un tratamiento y el médico recoge en la historia clínica. Estos datos pueden ser síntomas, aversiones al tratamiento, complicaciones, mejoras, etc.

(vi) Las órdenes médicas. Se componen de las instrucciones que el médico le proporciona al paciente para mejorar su padecimiento. Son aquellas indicaciones tanto relativas a los medicamentos, forma de suministrarlos, consejos alimentarios, advertencias, etc.

(vii) La hoja de interconsulta. Una interconsulta es la comunicación entre dos profesionales médicos, con diferentes áreas de experiencia en donde el solicitante, requiere la opinión sobre alguna patología del paciente a un consultor, quien emite su opinión sobre el caso. Generalmente la interconsulta se realiza sin la presencia del paciente, mediante cualquier sistema de comunicación. El médico responsable busca el consejo respecto a un problema concreto de un paciente, bien por complejidad, severidad, especialización.

(viii) Los informes de exploraciones complementarias. Son aquellos informes que complementan un diagnóstico médico y también en caso de solicitarse una segunda opinión médica para dar certeza y seguridad al solicitarlo el paciente[423].

(ix) El consentimiento informado. Sobre el consentimiento informado hemos hecho referencia en el Capítulo II de ésta Tesis.

[423] Ver al respecto los Artículos 4.a) y 28.1 de la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud (BOE núm. 128, de 29 de mayo).

(x) El informe de anestesia. Es donde se recogen los datos sobre el procedimiento anestésico durante el acto asistencial. Contendrá el diagnóstico preoperatorio, la intervención, la medicación administrada, las dosis, las vías, los tiempos, los procedimientos aplicados, la monitorización, las gráficas de constantes y las incidencias, pero sólo si el paciente ha sido intervenido y se le ha suministrado anestesia, en caso contrario, no constará oda ésta información en la HC.

(xi) El informe de quirófano o de registro del parto. El informe de quirófano es el documento que recoge la información sobre el acto quirúrgico realizado al paciente. Contendrá el diagnóstico preoperatorio y postoperatorio, las incidencias, los hallazgos intraoperatorios y el tipo de intervención realizada. Este informe deberá cumplimentarse por el primer cirujano inmediatamente después de la intervención quirúrgica. El informe de registro de parto es el documento que recoge la información sobre el acto obstétrico realizado a la mujer. Contendrá las incidencias y el tipo de actuaciones realizadas. Este informe deberá cumplimentarlo el médico, la matrona que asista a la mujer o ambos.

(xii) El informe de anatomía patológica. Un informe de patología es un documento que contiene el diagnóstico que se determinó mediante el análisis de células y tejidos en un microscopio. El patólogo es el médico que hace este análisis y redacta el informe de patología.

(xiii) La evolución y planificación de cuidados de enfermería. Es el documento en el que se registran todas las incidencias que se observen durante la asistencia al paciente, así como los resultados del plan de cuidados y las modificaciones de dicho plan. También constarán todos los cuidados de enfermería, tanto derivados de las órdenes del médico como los administrados por la propia atención del servicio de enfermería.

(xiv) La aplicación terapéutica de enfermería. Consiste en el conjunto de cuidados y atenciones realizadas por el personal de enfermería bajo las indicaciones y órdenes dadas por los médicos.

(xv) El gráfico de constantes. Es el documento que registra gráficamente las constantes vitales del paciente, tales como pulso, temperatura, presión arterial, peso, etc.

(xvi) El informe clínico de alta. Implica el informe emitido por el médico responsable en un centro sanitario al finalizar cada proceso asistencial de un paciente, debiendo especificar los datos de éste, un resumen de su historial clínico, la actividad asistencial prestada, el diagnóstico y las recomendaciones terapéuticas.

4.2. Mecanismos para garantizar la autenticidad y uniformidad de los datos contenidos en la historia clínica.

La LAP ha querido dejar la potestad a las Comunidades Autónomas[424], para el dictado de las normas relativas a la adopción de las medidas organizativas, técnicas, y protectoras de las HC. Al respecto, la normativa indica que las Administraciones sanitarias tendrán que establecer los mecanismos que garanticen la autenticidad del contenido de la HC y de los cambios operados en ella, así como la posibilidad de su reproducción futura[425], siendo necesario que queden registrados todos los accesos a la HC y todos aquellos cambios que se produzcan[426].

Al trabajarse actualmente en la implantación de la historia clínica digital (en adelante, HCD), se busca evitar la duplicidad del contenido y su integración en todo el Sistema Nacional de Salud. En este sentido, el Ministerio de Sanidad y Consumo, en coordinación y con la colaboración de las Comunidades Autónomas competentes en la materia, promueve la implantación de un sistema de compatibilidad que, atendida la

[424] Al respecto, la Ley 7/2002, de Cantabria, sostiene que: *"El paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Esta custodia ha de permitir la recogida, la recuperación, la integración y la comunicación de la información sometida al principio de confidencialidad en los términos establecidos en la presente Ley".* Artículo 41.4, de la Ley 7/2002, de 10 de diciembre, de Ordenación Sanitaria de Cantabria (BOCT núm. 242, 18.12.2002). También, en Canarias, el Artículo 8.3 del Decreto 178/2005, establece que: *"El uso de soportes informáticos, ópticos o de cualquier otra naturaleza tecnológica en lugar de los soportes documentales en papel, deberá contar con las garantías que aseguren su confidencialidad, autenticidad, integridad y conservación. En cualquier caso, se debe garantizar que queden registradas todas las actuaciones e identificados todos aquellos profesionales que las han realizado. Se garantizará siempre el cumplimiento de lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal".* Decreto 178/2005, de 26 de julio, por el que se aprueba el Reglamento que regula la historia clínica en los centros y establecimientos hospitalarios y establece el contenido, conservación y expurgo de sus documentos, de Canarias (BOC núm. 154, 8.08.2005).

[425] Artículo 14.3, de la LAP.

[426] Artículo 16.7, de la LAP.

evolución y disponibilidad de los recursos técnicos, y la diversidad de sistemas y tipos de HC, posibilite su uso por los centros asistenciales de todo el territorio español que atiendan a un mismo paciente, en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición[427].

4.3. Derecho de acceso a la historia clínica. Anotaciones subjetivas.

En éste epígrafe nos centraremos en analizar el derecho que el paciente tiene a acceder a su HC, como así también el derecho de acceso a la HC por parte de las personas autorizadas. En el Capítulo II de ésta Tesis, hicimos referencia al derecho de acceso a los datos de salud, en el marco de la LOPD y de los derechos ARCO que fueron estudiados.

El derecho de acceso a la HC del paciente se encuentra regulado por la LAP. La Ley posibilita el derecho de acceso, con las reservas señaladas por la misma LAP -que a continuación trataremos-, a la documentación contenida en la HC y a obtener copia por parte del paciente, de los datos que figuran en ella. Los centros sanitarios son los encargados de regular el procedimiento que garantice la observancia de estos derechos[428].

Los límites que señala la LAP[429], son reservas en el ejercicio del derecho de acceso del mismo paciente a los datos contenidos en su HC. El Artículo 18.3 establece dos límites: a) el derecho de terceras personas a la confidencialidad de los datos que constan en la HC recogidos en interés terapéutico del paciente, y, b) el derecho de los profesionales participantes en la elaboración de la HC a oponer al derecho de acceso la reserva de sus anotaciones subjetivas.

[427] Disposición adicional tercera, de la LAP.

[428] Artículo 18.1, de la LAP.

[429] El Artículo 18.3, de la LAP establece unas limitaciones al derecho de acceso a la HC, manifestando 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".* Sobre las anotaciones subjetivas de los médicos en las historias clínicas de los pacientes, véase: SÁNCHEZ-CARO, J.; ABELLÁN, F. *Derechos y deberes de los pacientes,* op. cit., pp. 61 y ss.

Respecto al primer límite, cabe mencionar que es frecuente que en una HC se incluyan anotaciones o datos relativos a terceras personas, diferentes del paciente, por ser una información trascendente que guarda relación con su estado de salud. Pensemos, por ejemplo, en enfermedades de personas afines al paciente que puedan derivar en consecuencias para su propia salud. Otro ejemplo muy ilustrativo que dan los Dres. BROGGI TRÍAS y MEJÓN BERGÉS[430] es el caso del amigo de escuela de un enfermo que ingresa con un cuadro de confusión puede aportar el testimonio de haber asistido a sus alucinaciones, y tener interés en que el enfermo no conozca quién ha aportado la información. Es un dato valioso, quizá fundamental para pensar en una esquizofrenia e iniciar un tratamiento temprano; es lógico, por tanto, que quede registrado en la HC. Al mismo tiempo, es comprensible que se preserve su confidencialidad, incluso ante la mirada del paciente. En estos casos, esta información quedará fuera del alcance del derecho de acceso del paciente a su documentación clínica[431].

Respecto al segundo límite que enuncia la normativa, el relativo a las anotaciones subjetivas, suscita más discrepancias, como a continuación expondremos. Técnicamente se vislumbran dos problemas frente a éste límite: en primer lugar, qué se entiende por anotaciones subjetivas y, en segundo lugar, quién puede ejercer el derecho de reserva en relación con dichas anotaciones subjetivas. Al respecto, GALLEGO RIESTRA[432] señala que:

> No se debe perder la perspectiva de que esta figura responde, en su origen, a un supuesto derecho a la intimidad de los profesionales sanitarios respecto a las notas que obligatoriamente tienen que escribir en la historia. Se trata de anotaciones incorporadas en muchas ocasiones de forma precipitada y con escasa información pero que tienen que ser registradas dada la singularidad del trabajo en equipo que caracteriza al ejercicio de la medicina y que impide el uso de registros privados a los que no tengan acceso otros profesionales.

En relación al concepto de anotación subjetiva, la situación no es en absoluto consensuada, y ello se debe, en gran parte, porque la LAP, no define lo que ha de

---

[430] Vid. BROGGI TRÍAS, M. A.; MEJÓN BERGÉS, R. "Las «anotaciones subjetivas» en la historia clínica". *Revista de Medicina Clínica*. Vol. 122, núm. 7, febrero 2004, p. 279. Disponible en Internet: <http://www.elsevier.es/es-revista-medicina-clinica-2-articulo-las-anotaciones-subjetivas-historia-clinica-13058386> [Consulta: 22 octubre 2016].

[431] Para profundizar más al respecto, véase: GALLEGO RIESTRA, S. "Historia Clínica Electrónica y derecho a la autonomía del paciente: un conflicto de intereses". *Papeles Médicos*. Vol. 23, núm. 1, Año 2014, p. 12.

[432] Ibídem.

entenderse por anotaciones subjetivas, simplemente hace mención a ellas, aunque excluyendo el acceso del paciente a las mismas. Por lo tanto, se queda una brecha abierta, no sólo desde el punto de vista conceptual para saber exactamente qué abarcan dichas anotaciones, sino, desde el punto de vista de su tratamiento jurídico: si son anotaciones que le pertenecen al médico que las ha realizado e incorporado a la HC del paciente, o, por el contrario, si éstas, una vez volcadas en la HC del paciente pasan a ser de su propiedad y por tanto puede tener acceso a su contenido.

Es importante, como se ha hecho referencia *ut supra*, una definición de lo que es una anotación subjetiva o de lo que no lo es, porque el no hacerlo se presta a que la pretensión de que entren en éste concepto casi todas las anotaciones del profesional, o las que él defina a posteriori con su solo criterio, y esta situación nos lleve a una lectura a todas luces abusiva[433].

Consideran BROGGI TRÍAS y MEJÓN BERGÉS[434], que no deberían ser «anotaciones subjetivas» las observaciones de hechos, las descripciones de la evolución del paciente o las alternativas diagnósticas razonables, ni, en consecuencia, las decisiones que sobre ello se tomen.

Por tanto, desde el sector doctrinal que entiende que el paciente no puede tener acceso a todas las anotaciones subjetivas que consten en su HC, destacamos la definición que hacen BROGGI TRÍAS y MEJÓN BERGÉS[435] que incluyen en la definición de

[433] BROGUI TRÍAS, M. A.; MEJÓN BERGÉS, R., op. cit., p. 279. Explican los autores que la LAP intenta preservar el derecho del enfermo a conocer todo lo que «se sabe» sobre él. Por tanto, no deberían ser «anotaciones subjetivas» las observaciones de hechos, las descripciones de su evolución, las alternativas diagnósticas razonables ni las decisiones que sobre ello se tomen.

[434] Ibídem. Los autores sostienen que: *"lo que distingue a estos informes en el curso clínico o a la descripción de una evolución, es que se basan en hechos comprobables, que «se saben», y que, aunque sean valorados y priorizados por una elaboración personal, subjetiva, se refieren a datos objetivos en última instancia. «Encuentro al enfermo mejor, por lo que disminuyo la medicación», u «oriento el problema como a) sigmoiditis por diverticulitis; b) enfermedad de Crohn; c) carcinoma de sigma...» son ejemplos de anotaciones a las que, pensamos, no se refiere el supuesto de la ley y a las que el enfermo debería poder acceder sin más, como al informe de radiología".*

[435] Ibídem. Ver en el mismo sentido: ROMEO CASABONA, C. M.; CASTELLANO ARROYO, M. "La intimidad del paciente desde la perspectiva del secreto médico y del acceso a la historia clínica". *Derecho y Salud*. Vol. 1, núm. 1, julio-diciembre 1993, p. 15.; GALLEGO RIESTRA, S.; HINOJAL FONSECA, R.; RODRIGUEZ GETINO, J. A. "Los derechos de los pacientes: problemática práctica". *Medicina Clínica.* Núm. 100, 1993, pp. 538-541.; GALLEGO RIESTRA, S. "Derecho a la confidencialidad y acceso a la Historia Clínica". *Revista Clínica del Hospital Central de Asturias.* Núm. 2, julio-septiembre, 1996, pp. 4-7.

«anotaciones subjetivas» solamente las opiniones del facultativo cuyo origen no es deducible objetivamente y que no surgen de la observación de un hecho biológico o de su evolución, ni plantean alternativas diagnósticas o decisiones clínicas, y que son sólo consideraciones personales anotadas como ayuda propia o como orientación para algún colega. Citan los autores, como ejemplo de anotación subjetiva, el aviso de que se pospone la información sobre el diagnóstico a un enfermo porque, en aquel momento, se teme aumentar su negativismo o su angustia[436].

Siguiendo ésta línea doctrinal, las nuevas leyes autonómicas y la LAP, haciéndose eco de aquéllas reivindicaciones, sí que efectivamente limitaron el derecho de acceso del interesado. En ello tuvo, sin duda, un peso decisivo el criterio del Grupo de Expertos en Información y Documentación Clínica[437], que sostenía que el paciente tiene derecho a acceder a la HC pero que de este acceso deben quedar excluidos los datos que afecten a la intimidad de terceras personas y las observaciones, apreciaciones o anotaciones subjetivas elaboradas por los profesionales.

El Grupo de Expertos[438] llegó a la siguiente conclusión en referencia al acceso por parte del paciente a su HC:

> El acceso a la información de la historia clínica se realizará de acuerdo con las condiciones que establezca la norma, según los supuestos de asistencia sanitaria u otros excepcionales. El paciente tendrá acceso a los resultados de las exploraciones e informes médicos que le permitan conocer de manera adecuada lo que se le ha realizado durante el episodio

[436] BROGUI TRÍAS, M. A.; MEJÓN BERGÉS, R., op. cit., p. 279.

[437] En septiembre de 1997, en desarrollo de un convenio de colaboración entre el Consejo General del Poder Judicial y el Ministerio de Sanidad y Consumo, tuvo lugar un seminario conjunto sobre información y documentación clínica, en el que se debatieron los principales aspectos normativos y judiciales en la materia y, al mismo tiempo, se constituyó un grupo de dieciséis Expertos a quienes se encargó la elaboración de unas directrices para el desarrollo futuro del tema de la autonomía del paciente en consonancia con la LGS con respecto a los avances producidos en su definición y a la propuesta de desarrollo futura. Los temas abarcados por los Expertos fueron: Información clínica (incluyendo información para el consentimiento informado). Información para proyectos docentes y de investigación. Historia clínica. Información al usuario. Certificados acreditativos del estado de salud. Constatación del proceso (informe de alta). Información y documentación clínica informatizada. Este Grupo suscribió un dictamen el 26 de noviembre de 1997, que ha sido tenido en cuenta en la elaboración de los principios fundamentales de la LAP. Grupo de Expertos en Información y Documentación Clínica. "Informe final". *Revista Calidad Asistencial 1999*. Núm. 14, Madrid, 1997, pp. 76-87.

[438] Grupo de Expertos en Información y Documentación Clínica, op. cit.

asistencial, así como a los datos que sobre su estado de salud se disponen en la historia clínica.

Observamos como el Grupo descarta que el paciente pueda tenar acceso a las anotaciones subjetivas que realicen los facultativos.

Como referente del sector doctrinal que contrariamente entiende que las anotaciones subjetivas han de ser conocidas por el paciente, destacamos la aportación al respecto de SANCHEZ CARO y ABELLÁN[439], que definen las anotaciones subjetivas como: *"los comentarios o impresiones personales que puede hacer el médico en un momento determinado, siempre que tengan trascendencia clínica, pues en otro caso no deberían incluirse en el historial".* Por nuestra parte, también compartimos éste último criterio, y ello en base a que las divergencias doctrinales se manifiestan en la consideración o no como factor clínico importante la anotación subjetiva. Por tanto, si dicha anotación se encuentra en nuestra HC, aunque sea simplemente como un mero juicio de valor o desde un ámbito absolutamente subjetivo, o basándose simplemente en comentarios de otras personas, sólo tiene razón de ser si su inclusión tiene por objetivo facilitar la asistencia sanitaria.

En éste segundo criterio doctrinal se embarca la LAP, cuando en su Artículo 15, señala que la HC deberá incorporar toda aquella *"información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente".* Y por su parte, el Artículo 3, define a la HC como *"el conjunto de documentos que contienen los*

[439] SÁNCHEZ-CARO, J.; ABELLÁN, F. *Derechos y deberes de los pacientes*, op. cit., pp. 61 y ss. También en ésta línea: GALLEGO RIESTRA, S., op. cit., p. 12. A nivel autonómico, -según esquematiza GALLEGO RIESTRA-, se ha legislado sobre las anotaciones subjetivas, pero sin lograr unanimidad de criterios. En Extremadura han conceptualizado a las anotaciones subjetivas como las impresiones de los profesionales sanitarios que, en todo caso, carecen de trascendencia para el conocimiento veraz y actualizado del estado de salud del paciente, sin que puedan tener la consideración de un diagnóstico. De manera antagónica, en las Comunidades Autónomas, de Galicia (Decreto 29/2009, de 5 de febrero, por el que se regula el uso y acceso a la historia clínica electrónica en Galicia (DOG núm. 34, 18.02.2009)), Castilla-La Mancha (Decreto 24/2011, de 12 de abril, de la documentación sanitaria en Castilla- La Mancha (BOCM núm. 74, 15.04.2011)), y País Vasco (Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica (BOPV núm. 65, 29.03.2012)), consideran que se trata de valoraciones personales que tienen interés para la atención sanitaria del paciente y que pueden influir en el diagnóstico y futuro tratamiento médico una vez constatadas, coincidiendo además en que los profesionales sanitarios deberán abstenerse de incluir expresiones, comentarios o datos que no tengan relación con la asistencia o que carezcan de valor sanitario.

datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial". Por tanto, todo aquello que carezca de trascendencia para el conocimiento del estado de salud del enfermo, no debería estar incluido en la HC.

La cuestión relativa a quiénes pueden oponer el derecho de reserva de las anotaciones subjetivas frente al derecho de acceso a la HC por parte del paciente, tampoco es sosegada. Existe una corriente doctrinaria[440], que entiende que la revisión de las anotaciones subjetivas para su posible exclusión del derecho de acceso del paciente no debe dejarse al criterio de los propios facultativos que las crean. Por ello, consideran que el encargado de tal valoración debe ser el propio centro sanitario.

Frente a esta corriente de opinión[441], se encuentran quienes consideran que el propio tenor literal de la LAP obliga a entender que el derecho de reserva se configura como un "derecho de los profesionales que han participado en su elaboración" y no de los centros. Este también es el criterio de la Agencia Española de Protección de Datos. En su Resolución R/00633/2004 de 22 de noviembre de 2004[442], literalmente afirma: *"A este respecto, cabe señalar que la posible denegación del acceso a las anotaciones subjetivas la tiene que realizar el facultativo, no la entidad que la custodia"*.

Finalmente, existen además algunos problemas de procedimiento. El hecho de que se contemple la posibilidad de que los médicos puedan «oponer la reserva» de unas anotaciones obliga a que deba notificárseles cada vez que un enfermo pida su HC y a que se establezca un período de «alegaciones» antes de entregarla. Y, pudiendo ser muchos los que han intervenido en su proceso, la tarea no es fácil de organizar. También puede ocurrir que el médico en cuestión ya no se encuentre en el mismo centro hospitalario.

---

[440] CANTERO RIVAS, R. *El acceso de los pacientes y sus allegados a los datos personales contenidos en la historia clínica*, en *Historia clínica electrónica, confidencialidad y protección de la información. Experiencias en gestión sanitaria.* Escola Galega de Administración Sanitaria, FEGAS, 2008, p. 137 y ss.

[441] Vid. SAIZ RAMOS M.; LARIOS RISCO D. "El derecho de acceso a la historia clínica por el paciente: propuesta para la reserva de anotaciones subjetivas". *Derecho y Salud*. Vol. 18, núm. 1. Enero-junio 2009, pp. 21-41.

[442] Resolución de la AEPD Nº R/00633/2004, Procedimiento Nº TD/00218/2004. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/resultados-ides-idphp.php> [Consulta: 24 octubre 2016].

Por otro lado, una vez hecho esto, en los casos en que se pida el acceso a la documentación, o copia, y un médico opusiera dicha reserva, creemos que alguna instancia del centro debería poder valorar hasta qué punto es justa y se acomoda al espíritu de la LAP. Además de ello, se deben regular los plazos para dicho pronunciamiento, y ello es importante, porque habitualmente si alguien pide su HC es para llevarlo a otro médico privado o incluso a una segunda opinión fuera de España.

5. Propiedad de la Historia Clínica.

Antes de analizar el tema en concreto de la propiedad de la HC, debemos hacer una puntualización, coincidiendo con PORTERO LAZCANO[443], que al definir el concepto de "propiedad" nos conduce a revisar otros conceptos incluidos en el primero, como son la posesión y disposición. El propietario posee la cosa y además dispone de ella; es decir, tiene plena capacidad de decisión sobre la misma, siempre y cuando no contravenga alguna disposición legal.

Con respecto a la propiedad de la HC, no hay ninguna norma a nivel estatal que lo regule de manera expresa. Algunas Comunidades Autónomas, sí que han legislado sobre el particular[444]. Si bien la LAP no se ha pronunciado al respecto, esta cuestión ha sido doctrinalmente controvertida[445], como expenderemos en los siguientes epígrafes.

---

[443] PORTERO LAZCANO, G., op. cit., pp. 81-88.

[444] En la Comunidad Valenciana, se legisló sobre el particular, estableciendo que: *"1. Las historias clínicas son documentos confidenciales propiedad de la administración sanitaria o entidad titular del centro sanitario cuando el médico trabaje por cuenta ajena y bajo la dependencia de una institución sanitaria. En caso contrario, la propiedad corresponde al médico que realiza la atención sanitaria".* Artículo 23, de la Ley 1/2003, de 28 de enero, de la Generalitat, de Derechos e Información al Paciente de la Comunidad Valenciana (DOCV núm. 4430, 31.01.2003). También, la normativa de la Comunidad Autónoma de Galicia se refiere expresamente a la Propiedad y custodia de la HC, estableciendo que: *"1. Las historias clínicas son documentos confidenciales propiedad de las Administración sanitaria o entidad titular del centro sanitario cuando el médico trabaje por cuenta y bajo la dependencia de una institución sanitaria. En caso contrario, la propiedad corresponde al médico que realiza la atención sanitaria. 2. La entidad o facultativo propietario es responsable de la custodia de las historias clínicas y habrá de adoptar todas las medidas precisas para garantizar la confidencialidad de los datos o de la información contenida en las mismas. Asimismo, toda persona que en el ejercicio de sus funciones o competencias tenga conocimiento de los datos e informaciones contenidas en la historia clínica tendrá la obligación de reserva y sigilo respecto de los mismos".*

LOMAS HERNÁNDEZ[446] pone de manifiesto una de las contradicciones que el debate acerca de quién ostenta la propiedad de la HC supone. La LAP no se pronuncia de manera expresa sobre el inconveniente de la propiedad de la HC. Quizás la intención del legislador sobre el particular, ha sido no entrar en la cuestión y en el debate que supondría afirmar la existencia de una titularidad determinada. Vemos, que, en el especial caso de la HC, son muchos los agentes que intervienen y, por tanto, consideramos en el mismo sentido que DOMÍNGUEZ LUELMO[447], que una regulación al respecto sería sumamente conflictiva y no sería adecuada a la necesidad de regular sobre los derechos y los deberes de los pacientes y de los médicos.

Asimismo, la LAP hace referencia en su Disposición adicional tercera, a la coordinación de las HC, mandando al Ministerio de Sanidad y Consumo a coordinarse y a colaborar con las Comunidades Autónomas, a fin de implantar un sistema de compatibilidad que, atendida la evolución y disponibilidad de los recursos técnicos, y la diversidad de sistemas y tipos de HC, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de necesaria repetición[448].

Si bien la LAP deja de lado la cuestión relativa a la propiedad de las HC -sostiene CANTERO RIVAS[449]-, el problema de la determinación del dueño de éstas subsiste, no

---

Artículo 18, de la Ley 3/2001, de 28 de mayo, reguladora del consentimiento informado y de la historia clínica de los pacientes de la Comunidad de Galicia. (BOE núm. 158, 3.07.2001).

[445] Vid. DE LORENZO SÁNCHEZ, A., op. cit., pp. 497 y ss.; CASTELLANO ARROYO, M. "Problemática de la historia clínica". *Actas del seminario Conjunto sobre Información y Documentación clínica.* Consejo General del Poder Judicial y Ministerio de Sanidad y Consumo, Madrid 22 y 23 de septiembre de 1997, vol. I, Madrid, 1998, pp. 45-90.; CORBELLA DUCH, J., op. cit., p. 148-149.; GÓMEZ PIQUERAS, C., op. cit., pp. 129.

[446] LOMAS HERNÁNDEZ, V., op. cit., pp. 129-150.

[447] Cfr. DOMÍNGUEZ LUELMO, A., op. cit., pp. 498 y ss.; DÍAZ MÉNDEZ, N. "Historia clínica. Titularidad, acceso, uso y conservación", en ABEL LLUCH, X. (Director). *El juez Civil ante la investigación biomédica*. *Cuadernos de Derecho Judicial*. Año 2004-X, Consejo General del Poder Judicial, Madrid, 2005, pp. 309 y ss.; SAMPRÓN LÓPEZ, D. *Los derechos del paciente a través de la información y la historia clínica.* Edisofer, Madrid, 2002, pp. 57 y ss.; MARTÍN BERNAL, J. M. "Tratamiento jurídico de la historia clínica. Tema para un debate". *Actualidad Administrativa*. Núm. 27, 6 al 12 de julio de 1998, pp. 581-599.

[448] Disposición adicional tercera, de la LAP.

[449] CANTERO RIVAS, R. "La historia clínica: naturaleza y régimen jurídico", en CÁLIZ CÁLIZ, R., et al. *El derecho a la protección de datos en la historia clínica y en la receta electrónica.* Aranzadi-AEPD-Thomson Reuters, Navarra, 2009, pp. 204 y ss.

sólo doctrinalmente y como cuestión fútil, sino también porque las normas autonómicas insisten en la clarificación de la cuestión, hecho que tendrá incidencias respecto a la previsión de la disposición adicional tercera de la LAP, recién citada.

5.1. Consideración de la historia clínica como propiedad del centro sanitario.

La vertiente doctrinal que sostiene que la propiedad de la HC pertenece al centro sanitario[450], no presenta grandes inconvenientes a la hora del acceso del paciente a su HC. Esta teoría mantiene que es el centro asistencial el encargado de la custodia, gestión, información contenida en la HC y de la conservación de la misma.

DE ÁNGEL YAGÜEZ[451], sostiene que la propiedad de la HC debe atribuirse al centro sanitario en el que el médico presta sus servicios por entender que el fruto de la actividad intelectual del facultativo es propiedad del empresario. Para dicho autor cuando el médico presta sus servicios por cuenta ajena debe considerarse que toda su actividad habitual en ese desempeño redunda en beneficio del empleador, y ello sin perjuicio que aquél pueda invocar alguna de las facultades del llamado "derecho moral" del autor, a que se refiere la Ley de Propiedad Intelectual. Por esta misma razón, la propiedad de la HC debe atribuirse al médico cuando éste actúa en régimen de profesional libre.

En la misma línea, GÓMEZ PIQUERAS[452] pone de relieve que ésta teoría se basa en la obligación legal impuesta referente a la ubicación de la HC en el Área de salud, y en el hecho de que el soporte de la HC (papel, software…) es propiedad del centro, además, recalca GÓMEZ PIQUERAS[453], el hecho de que el médico trabaje en un centro sanitario de titularidad pública (como personal estatutario) o en un centro privado (como personal laboral por cuenta ajena), comporta la cesión de los frutos de la actividad profesional a

[450] Se muestran favorables a ésta teoría, entre otros: ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M. *La historia clínica: custodia y propiedad.* I Jornadas de Protección de Datos Sanitarios en la Comunidad de Madrid*,* Fundación Mapfre Medicina y APDCM, Madrid, 2000, p. 145.; DE ÁNGEL YAGÜEZ, R. "Información y Documentación Clínica"*. Actas del Seminario Conjunto sobre información y documentación clínica celebrado en Madrid los días 22 y 23 de septiembre de 1997.* Vol. I. Consejo General del Poder Judicial, Ministerio de Sanidad y Consumo, Madrid, 1997, pp. 116 y ss.; CASTELLANO ARROYO, M., op. cit., pp. 45-90.

[451] DE ÁNGEL YAGÜEZ, R., op. cit., pp. 111-121.

[452] GÓMEZ PIQUERAS, C., op. cit., pp. 129.

[453] Ibídem.

dicho empleador y, por tanto, el que la titularidad de la HC corresponde a la institución pública o privada, según el caso.

En este punto disentimos con la autora, puesto que consideramos que la HC no puede ser considerada como "fruto de la actividad profesional", puesto que no es un beneficio que el médico obtiene, simplemente es la constancia de un proceso asistencial que se le realiza a un paciente. Aunque sí creemos que el médico es un trabajador en un centro sanitario, tanto público como privado; un trabajador más que ha de cumplir con las normas del centro y atender a la legislación en la materia, como así también a las normas deontológicas y éticas a las que está vinculado, y por ello ha de completar la HC del paciente que le consulta. En nuestra misma línea de argumentación, MARTÍNEZ-CALCERRADA[454] sostiene que el profesional de la medicina asume el papel de trabajado con algunas peculiaridades. Manifiesta el citado autor que la llamada "ajenidad de los frutos" no se produce en el sentido material y estricto que se da en el supuesto específico del trabajo manual. La labor del médico no produce ni genera cosas materiales; los resultados de esta labor son los beneficios relativos a la salud y la curación que reciben los enfermos y las personas que el médico atiende.

Destaca LOMAS HERNÁNDEZ[455], que la Comunidad Valenciana atribuye de forma expresa la propiedad de la HC al centro sanitario, siempre y cuando el profesional médico preste sus servicios en un centro sanitario público[456], cuando, contrariamente, la LAP no hace una mención expresa al tema.

Por su parte CORBELLA DUCH[457], está a favor de ésta corriente doctrinal manifestando que las HC son de la institución o centro que las elabora (o del médico en el ejercicio privado de la profesión), pero al servicio de la atención sanitaria del enfermo. Manifiesta el citado autor, que por dicho motivo se reconoce al paciente el derecho a obtener copia del contenido de la HC, y se trabaja en el establecimiento de un sistema

---

[454] MARTÍNEZ-CALCERRADA, L. *Derecho Médico. Volumen I. Derecho Médico General y Especial.* Tecnos, Madrid, 1986, pp. 729 y ss.

[455] LOMAS HERNÁNDEZ, V., op. cit., pp. 129-150.

[456] El Artículo 23, de la Ley 1/2003, de 28 de enero, de la Generalitat, de Derechos e Información al Paciente de la Comunidad Valenciana, en referencia a la propiedad y custodia de la historia clínica, op. cit., establece que: *"1. Las historias clínicas son documentos confidenciales propiedad de la administración sanitaria o entidad titular del centro sanitario cuando el médico trabaje por cuenta ajena y bajo la dependencia de una institución sanitaria. En caso contrario, la propiedad corresponde al médico que realiza la atención sanitaria".*

[457] CORBELLA DUCH, J., op. cit., p. 148-149.

de coordinación de HC en el Sistema Nacional de Salud, a fin de poder atender al paciente en cualquier centro del Estado evitando la repetición de las exploraciones.

Finalmente, coincidimos con DOMÍNGUEZ LUELMO[458], que sostiene que ésta teoría puede sustentarse sin necesidad de recurrir a la propiedad de la HC, simplemente con la explicación del deber de conservación y custodia de la HC por parte del centro de salud.

5.2. Consideración de la historia clínica como propiedad del médico.

Esta teoría gira en torno al derecho intelectual del médico, puesto que no sólo se dedica a recoger y anotar datos concretos de análisis, sino que a través del tratamiento de esos datos realiza un diagnóstico, un pronóstico y encamina un tratamiento en base a ello.

Lo que se pretende poner de relieve, según refiere DOMÍNGUEZ LUELMO[459], es que la labor del médico no se reduce a una mera recopilación de datos, sino que lo esencial es su labor intelectual: en función de unos conocimientos previos, y de los datos que se obtienen del paciente, el médico realiza una labor de análisis y síntesis, transformando la información que ha obtenido en una creación científica, expresada en juicios de valor terapéutico: diagnóstico, pronóstico y tratamiento.

Por su parte, DE LORENZO SÁNCHEZ[460] es partidario de ésta tesis, puesto que manifiesta que la propiedad intelectual del médico sobre la HC se fundamenta en un derecho de autor y para ello -sostiene el doctrinario- no basta la mera recopilación, sino que el médico con los datos suministrados por el paciente realiza, mediante una labor de análisis y síntesis, una transformación de la información, que tiene por resultado una creación científica, expresada en juicios de valor terapéutico: diagnóstico, pronóstico y tratamiento.

[458] DOMÍNGUEZ LUELMO, A., op. cit., p. 505.

[459] Ibídem, p. 503.

[460] DE LORENZO SÁNCHEZ, A., op. cit., pp. 497 y ss.

Idéntica posición toman LUNA y OSUNA[461] al entender que, en el ejercicio privado de la profesión, el médico es el encargado y el propietario de la HC. Porque -sostienen los autores- la realización de la HC trasciende de la mera recopilación de datos, conllevando una labor intelectual en la que el médico, en función de unos conocimientos previos, orienta el interrogatorio que ha realizado al paciente e interpreta los datos clínicos y analíticos, de modo que, y según la Ley de Propiedad Intelectual, el médico sería el autor y propietario intelectual de la HC; por el contrario si el profesional es un médico estatutario o contratado laboralmente, la propiedad de la HC y, a la vez, su propiedad intelectual corresponderían al centro.

En contra de ésta postura se manifiestan ROMEO CASABONA y CASTELLANO ARROYO[462] al decir que la HC no puede considerarse como una creación literaria, artística o científica y por tanto no estaría al amparo de la Ley de Propiedad intelectual.

En conclusión, quienes defienden ésta postura se basan en el respeto a los derechos intelectuales del médico, así como a la posibilidad de que existan notas, anotaciones subjetivas del médico, comentarios o pronósticos que tal vez no sean convenientes para el enfermo, o datos científicos, que tal vez pudiesen no ser bien interpretados por el paciente[463].

5.3. Consideración de la historia clínica como propiedad del paciente.

Ésta teoría gira en torno a la defensa de la propiedad del paciente de su HC. Se basa en el Artículo 15.2 de la LAP, y su fundamento radica en que la redacción y elaboración de la HC se realiza en beneficio del paciente.

DOMÍNGUEZ LUELMO[464] sostiene que teniendo en cuenta la regulación del Artículo 14 y siguientes de la LAP, los argumentos a favor de la propiedad de la HC por el paciente no pueden compartirse. El autor se refiere a la necesidad de que la HC sea una y de por vida para cada paciente en todo el territorio nacional, o al menos en el ámbito de su Comunidad Autónoma, abriéndose desde la primera prestación asistencial, y

[461] LUNA, A.; OSUNA, E. "Problemas médico-legales en el almacenamiento y custodia de la historia clínica". *Medicina Clínica*. Vol. 88, núm. 2, 1987, pp. 631-632.

[462] Vid. ROMEO CASABONA, C. M.; CASTELLANO ARROYO, M., op. cit., pp. 8 y ss.

[463] MÉJICA, J.; DÍEZ, J. R., op. cit., pp. 175.

[464] DOMÍNGUEZ LUELMO, A., op. cit., pp. 501-502.

recogiendo en ella todos los datos que se irían completando en las sucesivas intervenciones, añadiendo nuevos datos clínicos, diagnósticos, tratamientos, etc.

GARCÍA HERNÁNDEZ y MARZO MARTÍNEZ[465] defienden esta teoría diferenciando entre los supuestos de que el médico trabaje por cuenta ajena o por cuenta propia. Sostienen los autores, que, si el médico trabaja por cuenta ajena a cambio de un salario, éste está vinculado a una relación laboral contractual, y por tanto la confección de la HC es parte de su cometido. Como al médico le paga el paciente, ya sea de forma directa (centros privados) o indirecta (centros públicos) por recibir una actividad sanitaria en la que está incluida la HC, ésta será siempre propiedad del paciente y nunca del médico o del centro hospitalario. Si, en cambio, el médico ejerce por cuenta propia, éste lo hace en virtud de unos honorarios puesto que el paciente arrienda sus servicios y le paga a tal fin. Por tanto, en este caso, el médico ha de entregarle al paciente la HC al finalizar dicho contrato.

5.4. Teoría mixta sobre la propiedad de la historia clínica.

Esta posición al respecto de la propiedad de la HC mantiene que no existe una única o un único propietario de la misma. Sostiene que convergen los tres agentes, es decir, que la HC pertenece tanto al paciente, por estar volcados en ella sus datos más íntimos; al médico porque es el que refleja en la HC el estudio, análisis y diagnóstico del paciente, por tanto, vuelca en ella su propiedad intelectual; y, finalmente, el centro sanitario al que pertenece el médico y donde el paciente se atiende.

En virtud de ésta posición mixta, ROMEO CASABONA y CASTELLANO ARROYO[466], ponen de manifiesto algunos problemas que la misma suscita. Dicen que por un lado están los problemas relativos a la gestión y organización del centro sanitario. Por otro lado, las cuestiones relativas a los datos del paciente relacionados con su proceso asistencial, y hay que añadir a ello, la emisión del médico de un juicio sobre el diagnóstico, pronóstico, tratamiento y otros juicios de valor.

[465] GARCÍA HERNÁNDEZ, T.; MARZO MARTÍNEZ, B. "La propiedad de la historia clínica". *La Ley: revista jurídica española de doctrina, jurisprudencia y bibliografía*. Núm. 5, 1996, pp.1629-1631.

[466] ROMEO CASABONA, C. M.; CASTELLANO ARROYO, M., op. cit., pp. 14 y ss.

Por su parte, MORENO VERNIS[467] sostiene que se va imponiendo una actitud más prudente y fundamentada, al mantener que la información pertenece al paciente y al médico. Este último posee una relativa propiedad intelectual sobre la HC. En esta postura, señala el autor, existe un tercer sujeto que es la institución, quién mantiene un derecho/deber de custodia y archivo de la HC. Comenta, concluyendo MORENO VERNIS, que se podría hablar de una copropiedad o condominio entre el paciente y la institución/profesional, ejerciendo ambas partes los deberes y derechos relativos a ese documento.

Asimismo, están los que consideran que el debate en torno a la propiedad de la HC es superfluo e intrascendente, porque sostienen que lo importante no es el derecho a la propiedad sobre la HC, sino el derecho de acceso a la misma[468]. Nosotros, sin embargo, consideramos que éste tema ha de tener una solución y dada desde la normativa, porque en caso que el paciente sólo tenga acceso a la HC, pero no la plena disposición de la misma, por ejemplo, destruyéndola, entonces no podemos estar hablando de un respeto constitucional a su derecho fundamental a su intimidad y a su autonomía como paciente[469]. Citamos este ejemplo de la destrucción de su HC, para ilustrar un caso extremo de un paciente que no quiera que su HC se mantenga en un centro de salud y que sus familiares conozcan alguna grave enfermedad o cualquier otra razón válida.

5.5. Nuestra postura en torno a la historia clínica.

---

[467] MORENO VERNIS, M. "Documentación clínica: organización, custodia y acceso", en FERNÁNDEZ HIERRO, J. M. (Coordinador). *La historia clínica.* Comares, Granada, 2002, p. 89.

[468] Esta corriente doctrinal es sostenida por: MÉJICA GARCÍA, J. M. *La historia Clínica: estatuto básico y propuesta de regulación.* Edisofer S.L, Madrid, 2002, pp. 81-85.; GALÁN CORTÉS, J. C. *"Aspectos legales de la relación clínica",* Jarpyo Editores, Madrid, 2000, pp. 16 y ss.

[469] El Artículo 17, de la LAP, se refiere a la conservación de la documentación clínica, y dice al respecto que: *"Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad,* […] *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. 2. 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".*

Tras haber analizado las distintas teorías en torno a la propiedad de la HC y su argumentación doctrinal, nuestra postura al respecto respalda la teoría de que los datos contenidos en la HC pertenecen al paciente, mientras que, solamente las anotaciones subjetivas, pertenecen al médico. No queremos hablar de propiedad en *strictu sensu* y tampoco de propiedad intelectual, puesto que el médico realiza un trabajo, presta un servicio que está dentro de sus funciones y por el cual recibe una contraprestación económica. Por tanto, lo vinculamos al derecho de confidencialidad, intimidad y secreto que atañe a la relación médico-paciente. Para llegar a esta conclusión nos basamos en la HC en sí, en su finalidad y en la necesidad de la misma para que el historial médico esté debidamente recopilado, adecuado y sea veraz respecto al estado de salud del paciente.

Por tanto, como punto de partida hemos considerado la finalidad de la HC. Tal como lo define el Artículo 16.1 de la LAP, que establece que:

> 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.

Por tanto, el legislador ha sido cauto y ha querido poner de relieve en primer término que la HC ha de servir como objetivo primordial para brindar asistencia adecuada al paciente, tal como lo manifiesta el Artículo 15.2 de la LAP, diciendo que: *"La historia clínica tendrá como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud".*

Añadimos a ello que, el médico está obligado a dejar constancia de las consultas que le realiza al paciente, así como el tratamiento y demás requisitos de incorporación obligatoria[470]. La LAP establece en su Artículo 15.3 que: *"La cumplimentación de la historia clínica, en los aspectos relacionados con la asistencia directa al paciente, será*

[470] El Artículo 15.2, de la LAP, regula el contenido mínimo que la HC debe tener: *"a. La documentación relativa a la hoja clínico estadística. 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".*

responsabilidad de los profesionales que intervengan en ella". Asimismo, el Artículo 15.1 sostiene que: *"La historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente".* Además, la LAP obliga al profesional sanitario a guardar reserva respecto al contenido, manifestando en el Artículo 2.7 que: *"La persona que elabore o tenga acceso a la información y la documentación clínica está obligada a guardar la reserva debida".* Vemos que el personal ha de mantener el secreto tal como lo establece el Artículo 16.6 de la LAP: *"El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto".*

También hay que destacar, el derecho que tiene el paciente a que se guarde constancia de sus procesos asistenciales tal como lo manifiesta el Artículo 15.1, que consagra que:

> 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.

Correlativo a ello, es el derecho del paciente al respecto de su intimidad. La LAP lo recoge en su Artículo 2.1: *"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".*

Finalmente, cabe reflexionar brevemente sobre el derecho de acceso a la HC, si bien ha sido analizado en el epígrafe 4.3. Observamos que el legislador deja el camino abierto en todo momento para que el paciente pueda acceder a los datos contenidos en su HC mientras que el médico o el personal sanitario sólo puede hacerlo cuando son consultados por el paciente para ello. La LAP lo regula en el Artículo 18.1 diciendo que: *"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".* Y el apartado 3 señala 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.

Por tanto, vemos que la única limitación podríamos decir, al acceso de la HC lo marca las anotaciones subjetivas realizadas por los médicos, las cuales han de ser consideradas en observancia a su propio derecho de intimidad y confidencialidad.

Por todo lo expuesto, sostenemos que no se debería hablar de "propiedad" de la HC, sino que la misma representa una serie de derechos, cuya titularidad pertenecen al paciente y otros que pertenecen al médico, pero no desde el punto de vista de su propiedad intelectual, sino de su apreciación subjetiva, que configura su derecho a la intimidad y confidencialidad[471]. En virtud de ello, consideramos conveniente una única HC, pero con un anexo reservado al médico para la realización de sus anotaciones subjetivas. Asimismo, se evitaría el acceso a éstas anotaciones del médico por parte del personal no sanitario.

Conclusión.

Tras haber analizado en éste Capítulo la HC, desde su origen, desde su definición y su tratamiento normativo, tanto estatal como autonómico, apreciamos que para que se cumplan los preceptos legales, la HC debe ser completa en los términos que analizamos, a fin de ser el fiel reflejo del estado de salud del paciente, que consideramos es el objeto primordial de la HC, y a través de su análisis el médico pueda actuar en consecuencia.

A raíz de ello, mostramos cómo los diferentes datos contenidos en la HC del paciente, pueden suscitar dudas acerca del ejercicio del derecho de acceso del paciente y sus limitaciones en observancia del derecho de los médicos a que se respete la confidencialidad de sus anotaciones subjetivas, problema que algunos doctrinarios han intentado dar repuesta a través de la delimitación del derecho de propiedad sobre la HC, sin que hasta el momento exista un consenso al respecto, y proponiéndose por nosotros una alternativa para zanjar la discusión doctrinaria en torno a ello, proponiendo la teoría por la cual los datos contenidos en la HC pertenecen al paciente, mientras que, solamente las anotaciones subjetivas, pertenecen al médico.

[471] DOMÍNGUEZ LUELMO, A., op. cit., pp. 507 y ss.

CAPÍTULO IV

La Historia Clínica Digital

SUMARIO: 1. Definición de historia clínica digital. 2. Incidencia de las nuevas tecnologías en el ámbito sanitario. 2.1. Retos tecnológicos en torno a la historia clínica digital. 2.2. Situación de la implementación de la historia clínica digital en España. 3. Riesgos que se plantean frente a los datos contenidos en la historia clínica digital 4. Finalidad de la historia clínica digital. 4.1. Otras finalidades de la historia clínica. 5. Eficiencia de la historia clínica digital. 6. Garantías para los pacientes. 6.1. Nuestra postura en torno a las garantías de implantación de la historia clínica digital. 7. Seguridad y confidencialidad en torno a la historia clínica digital. 7.1. Sistemas de seguridad. 8. Ventajas de la implementación de la historia clínica digital. 9. Inconvenientes que pueden plantearse en torno a la historia clínica digital. 10. Receta electrónica. 10.1. Ventajas de su implementación. 11. La necesidad de una Ley para regular sobre los datos de salud contenidos en la historia clínica digital y en la receta electrónica. 12. La tarjeta sanitaria individual electrónica.

Introducción.

En éste Capítulo nos centraremos en profundizar y analizar desde el punto de vista jurídico, social y con la incorporación de las nuevas tecnologías, la evolución que se ha vislumbrado en las últimas décadas en lo referente a la documentación médica donde se guarda nuestra "biografía sanitaria", denominada HC, que hemos analizado en el Capítulo anterior. Vamos explicar a continuación las especificidades que la digitalización incorporan en la HC, su funcionalidad, los datos que debe contener, las medidas de seguridad que debe respetar y las responsabilidades de los intervinientes en su consulta y redacción. Así mismo, haremos referencia a otros documentos digitales como son la receta digital y la tarjeta sanitaria digital.

Podemos intuir que en el futuro las HC abandonarán definitivamente el papel para ser volcadas en soporte electrónico. Esto se infiere de las mismas necesidades de las

personas que cada vez se mueven con más frecuencia, lo cual genera la necesidad de atención médica en otros puntos de España e incluso del exterior del país.

1. Definición de historia clínica digital.

La historia clínica digital, electrónica o informatizada (en adelante, HCD), consiste en un historial médico completo o una documentación similar del estado de salud físico y mental, pasado y presente de un individuo, en formato electrónico, que permite acceder fácilmente a estos datos a efectos de tratamientos médicos y otros fines estrechamente relacionados[472].

La HCD es una recopilación informatizada de los detalles de salud de un paciente, que podemos definir como el conjunto de documentos que contiene los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial. Se compone del conjunto de documentos, tanto escritos como gráficos o por imágenes, que hacen referencia a los sucesos de salud y enfermedad de un paciente, y la actividad sanitaria que se genera con motivo de esos sucesos. Pero es aún más que eso, es una nueva manera de almacenar y organizar la información del paciente.

SANCHEZ-CARO y ABELLÁN[473] apuntan que en el ámbito sanitario, se debe tener en cuenta, que la HC, sea manual o electrónica, tiene su razón de ser en facilitar la asistencia sanitaria al ciudadano y que, por tanto, la naturaleza de la información que se incluye en la misma ha de ser acorde con el citado objetivo, debiéndose recoger exclusivamente toda la información clínica necesaria para asegurar, bajo un criterio médico, el conocimiento veraz, exacto y actualizado del estado de salud del paciente, por parte de los sanitarios que le atienden.

[472] Documento de Trabajo del Artículo 29 de la Directiva 95/46/CE, (HME) 00323/07/ES, sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos, de 15 de febrero de 2007 (WP 131). Disponible en Internet: <https://www.apda.ad/system/files/wp131_es.pdf> [Consulta: 21 agosto 2015].

[473] SÁNCHEZ-CARO, J.; ABELLÁN, F. *La historia clínica.* Fundación salud 2000, Granada, 2000, pp. 11 y ss.

YUGUERO DEL MORAL[474] sostiene que la HC es un documento vivo y en evolución que incluye juicios, documentos, procedimientos e informaciones generados en la relación médico-paciente y manifiesta que, desde un punto de vista deontológico, la HC constituye el documento fundamental de la relación médico-enfermo. Manifiesta el autor que:

> La historia clínica es uno de los documentos más complejos que existen, debido a la multiplicidad de personas (médicos, diplomados en enfermería, personal sanitario, el propio paciente, sus familiares, etc.) y organismos (centros sanitarios públicos y privados, inspecciones de la Administración Sanitaria, Administración de Justicia, compañías de seguros, etc.) que en un determinado momento podrían estar interesados en tener acceso a los datos en ella contenidos, lo que comprometería la intimidad del paciente[475].

En España, se está llevando a cabo paulatinamente ésta introducción de la HCD en el ámbito de la sanidad pública, tal como explicaremos en el siguiente epígrafe, consistente en cambiar el soporte papel por el soporte electrónico, mucho más flexible, mucho menos voluminoso y previsiblemente más fácil de utilizar[476].

2. Incidencia de las nuevas tecnologías en el ámbito sanitario.

La realidad demuestra que la propia dinámica social, en donde la movilidad[477] de los ciudadanos es cada vez más habitual, se hace necesaria la posibilidad de disponer de

---

[474] Vid. YUGUERO DEL MORAL, L. *La implantación de los derechos del paciente.* Eunsa, Navarra, 2004, pp. 259 y ss.

[475] Ibídem.

[476] La HC tradicional en la práctica planteaba algunos problemas que podemos referir tales como: el desorden y la falta de uniformidad en los documentos, la probable ilegibilidad, la información resultaba fácilmente alterable, con una disponibilidad lenta y rígida, sólo disponible en el centro sanitario donde se almacenaba, errores en el archivo, una confidencialidad no garantizada, facilidad en el deterioro del soporte justamente por tratarse de papel, dificultades para tratar la información, entre otros.

[477] El Artículo 24, de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, op. cit., se refiere a las garantías de movilidad diciendo en su apartado 1 que: *"El acceso a las prestaciones sanitarias reconocidas en esta Ley se garantizará con independencia del lugar del territorio nacional en el que se encuentren en cada momento los usuarios del Sistema Nacional de Salud, atendiendo especialmente a las singularidades de los territorios insulares".*

la información precisa del paciente cuando las necesidades de atención sanitaria se producen fuera de la Comunidad Autónoma en la que se ha generado esta información.

Tal como adelantábamos *ut supra*, la sociedad actual requiere una modernización en el manejo de las HC, que facilite el acceso, las consultas y los desplazamientos de los pacientes. Debido a ello, es menester desarrollar un sistema para la administración electrónica de las HC. Desde el punto de vista técnico, la automatización de los registros, implica diseñar una base de datos y un sistema que responda, tanto a las necesidades de información de la institución, como a la necesidad objetiva de un sistema nacional de información médica, de un medio de enlace a ese sistema, hoy en fase de desarrollo y prueba, pero necesariamente real en un plazo breve. Ello obliga a que cada centro asistencial no tenga un modelo propio, sino que ha de existir un único sistema en todo el territorio español, que de forma normalizada pueda ser aplicado en todas las Comunidades Autónomas, con las garantías de seguridad necesarias. Consideramos que posteriormente, y una vez alcanzado éste objetivo, habrá de hacerse extensivos a la sanidad privada y a los consultorios médicos.

El sector sanitario no es ajeno al desarrollo tecnológico y la evolución que éste produce en todos los ámbitos de la sociedad. La necesidad de registrar cada vez más información clínica de los pacientes, además de datos administrativos, hace inviable la utilización del papel y el formato tradicional que hasta hace escasos años era el de referencia en el sistema sanitario. Pensemos simplemente en que dicho volumen de datos había que almacenarlo físicamente en archivadores, pero el espacio es un problema real, además de no ser seguro desde varios puntos de vista: posible riesgo de deterioro, pérdida o robo, inundaciones, incendio, etc.

Según TRONCOSO REIGADA[478], las tecnologías de la información se constituyen en un auténtico motor del cambio y del progreso en la calidad asistencial y en la equidad en el acceso a las prestaciones.

[478] TRONCOSO REIGADA, A. *La confidencialidad de la historia clínica*. Cuadernos de Derecho Público, (2006), p. 48. Disponible en Internet: <http://revistasonline.inap.es/index.php?journal=CDP&page=article&op=viewFile&path%5B%5D=775&path%5B%5D=830> [Consulta: 29 enero 2016]. También reflexiona el autor, manifestando que: "*Lo mismo se puede decir del impulso que las nuevas tecnologías han dado a la investigación genética que tiene que ser aprovechada para la mejora del derecho a la salud"*. Compartimos ésta reflexión, porque justamente en el ámbito de la investigación genética es donde mayores beneficios y logros

La aplicación de estas nuevas tecnologías en el sector médico, se evidencia en nuevos modelos de gestión y administración sanitaria, científica y asistencial, como la telemedicina, las HC informatizadas, la tarjeta sanitaria, la transmisión de datos médicos por Internet y el uso de nuevas herramientas telemáticas en orden a la prestación de servicios asistenciales.

En el ámbito de la asistencia sanitaria, esos cambios se aprecian de manera especial con la utilización de estas tecnologías de información y comunicación (en adelante, TIC), tanto para la gestión de la atención sanitaria universal prestada por los sistemas nacionales de salud, como por la propia atención a los pacientes, dando lugar a lo que comienza a denominarse "telemedicina" entendida, según refiere PÉREZ GÓMEZ[479], 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 actuación sanitaria, de gestión, de investigación, de formación, entre otras.

TRONCOSO REIGADA[480] alaba los avances tecnológicos en la sanidad, y entiende que las TIC son un instrumento muy positivo para la actividad sanitaria, que redunda en la mejora de la calidad asistencial de los pacientes. Las ventajas, tanto en el ámbito asistencial, como en el científico, de estas técnicas de tratamiento de datos son innumerables, según el doctrinario, ya que favorecen el desarrollo de investigaciones que tienen una importante repercusión para el conjunto de la sociedad. Mediante estas herramientas son abundantes los tratamientos de datos personales en el ámbito sanitario. Sostiene, al respecto, PIÑAR MAÑAS[481], que el uso de estas técnicas sobre los datos médicos y sanitarios tiene múltiples implicaciones para los profesionales de la sanidad y ha de gozar de las medidas que garanticen la intimidad de los pacientes y el control de sus datos personales.

Asimismo, LESMES SERRANO[482] comenta que debemos ser conscientes del despliegue de las tecnologías de la información y de la comunicación en el ámbito

---

científicos se están vislumbrando en estos años, a raíz de la utilización de instrumentos tecnológicos cada vez más vanguardistas.

[479] Vid. PÉREZ GÓMEZ, J. M., op. cit., p. 625.

[480] TRONCOSO REIGADA, A., op. cit., pp. 46 y ss.

[481] PIÑAR MAÑAS, J. L. "La Protección de Datos en el ámbito Sanitario", op. cit., pp. 42-44.

[482] LESMES SERRANO, C. "Prologo", en CÁLIZ CÁLIZ, R., et al., *El derecho a la protección de datos en la historia clínica y en la receta electrónica.* Aranzadi-AEPD-Thomson Reuters, Navarra, 2009, pp. 11-13.

sanitario, que constituye una innovación normalmente positiva para el desarrollo de esa actividad que redunda en la mejora de la calidad asistencial de los pacientes, pero, por otra parte, señala el autor, tienen una enorme potencialidad agresora a la privacidad del enfermo, en un ámbito tan íntimo como el de su salud. El almacenamiento informático de los datos de salud facilita el trabajo del personal sanitario y puede ayudar a una mejoría de la calidad asistencial, pero también puede conducir a un conocimiento indeseado por parte de terceros. Por tanto, comenta LESMES SERRANO[483], nos movemos en un terreno resbaladizo en el que confluyen intereses privados y colectivos, la eficacia del sistema sanitario y los derechos básicos del paciente.

En éste sentido, coincidimos con las opiniones de los doctrinarios LESMES SERRANO[484] y PIÑAR MAÑAS[485], porque tal como manifestamos en ésta Tesis, uno de los grandes inconvenientes del tratamiento de los datos de salud contenidos en la HC es justamente su "correcto almacenamiento y acceso", en observancia de las garantías constitucionales que protegen la intimidad de las personas, y es por ello que la HCD, si bien facilita el trabajo de los facultativos sanitarios, hace también más vulnerable la protección de los datos del paciente, que puede verse vulnerada por los accesos remotos e ilegítimos, por alteración de los datos, por la venta de los mismos con fines comerciales, etc. Por tanto, con la implementación de las TIC en el entorno sanitario, las garantías deben extremarse y a la vez se debe llevar un control constante, no bastará con implementar garantías si luego no existe un sistema que verifique su efectivo cumplimiento. A estos extremos haremos referencia en los siguientes epígrafes.

2.1. Retos tecnológicos en torno a la historia clínica digital.

Tiempo atrás era habitual que acudiéramos al médico de familia de toda la vida, al igual que nuestros hijos y nuestros padres. Era éste el conocedor de nuestra historia sanitaria y el único que tomaba las decisiones sobre nuestra salud. Probablemente el soporte de esos datos médicos estaría volcado en simples folios a modo de notas y en una gran carpeta junto con otras informaciones sanitarias de otros pacientes. Con el avance del tiempo, nuestros datos médicos se fueron ordenando en carpetas

[483] LESMES SERRANO, C., op. cit., pp. 11-13.

[484] Ibídem.

[485] PIÑAR MAÑAS, J. L., op. cit., pp. 42-44.

denominadas “HC del paciente”. GÓMEZ PIQUERAS[486] explica que antes los médicos atendían individualmente todas las necesidades de los pacientes, y la HC simplemente la constituía un cuaderno de notas donde registraba los datos más importantes, al criterio del médico; sin embargo, sostiene la autora que, al ir apareciendo las especializaciones y la medicina hospitalaria, la HC pasó a ser responsabilidad compartida entre los profesionales y obligó a estructurar los documentos que la componen. Actualmente es el personal de enfermería y administración que atienden en hospitales, clínicas y consultas privadas, las encargadas de gestionar nuestra HC y facilitárselo al doctor cada vez que éste lo solicite.

Tal y como pone de manifiesto, PÉREZ GÓMEZ[487], la necesidad de revisar y profundizar en la regulación de esta materia aparece como imprescindible para que la protección no pierda eficacia frente a los avances tecnológicos producidos en este campo y los cambios de comportamiento social y económico que han llevado aparejados.

ETREROS HUERTA[488] comenta que la informática empezó a introducirse en los centros sanitarios hace alrededor de doce años. Destaca que en los primeros años se orientó a dar soporte a los procesos menos complejos, pero también menos específicamente sanitarios de los hospitales refiriéndose a la gestión de pacientes (admisión, gestión de expedientes clínicos, gestión de personal, gestión de almacén) después se introdujo a los servicios centrales (laboratorios, informes de radiodiagnóstico) pasando a redactarse los informes clínicos, y finalmente en los últimos años comenzó su implantación en las Historias Clínicas. Comenta ETREROS HUERTA[489] que la HC electrónica se expandió más rápidamente en los Centros de Atención Primaria que en los Hospitales Públicos, pero que al día de hoy son escasos

[486] GÓMEZ PIQUERAS, C. “La historia clínica. Aspectos conflictivos resueltos por la Agencia Española de Protección de Datos”, en LESMES SERRANO, C., et al., *El derecho a la protección de datos en la historia clínica y en la receta electrónica.* Aranzadi-AEPD-Thomson Reuters, Navarra, 2009, pp. 128.

[487] PÉREZ GÓMEZ, J. M. “La protección de los datos de salud”, en RALLO LOMBARTE, A.; GARCÍA MAHAMUT, R. *Hacia un Nuevo Derecho Europeo de Protección de Datos*. Tirant Lo Blanch, Valencia, 2015, pp. 621 y ss.

[488] ETREROS HUERTA, J. J. “Historia clínica electrónica”, en AA.VV. *El derecho a la protección de datos en la historia clínica y la receta electrónica.* Aranzadi-AEPD, Pamplona, 2009, p. 182.

[489] Ibídem.

los hospitales que no cuentan con las HCD, y vaticina que en pocos años la implementación de la HCD será una realidad[490].

LESMES SERANO[491] recalca que tanto la HCD, como la receta electrónica, son instrumentos innovadores y normalmente positivos en el desarrollo de la actividad sanitaria que procurarán en el futuro una mejora indudable en la calidad asistencial de los pacientes. Añade LESMES SERRANO[492], que la HCD evita la repetición de pruebas diagnósticas al facilitar su almacenamiento y facilita a la vez, al personal sanitario el acceso a la información relevante para el paciente. Permite, según refiere el autor, mejorar la atención sanitaria a pacientes desplazados al facilitar todos los datos sanitarios relevantes.

El Ministerio de Sanidad define la HCD diciendo que es un registro electrónico específicamente diseñado para facilitar la anotación de las mencionadas observaciones, acciones e instrucciones de manera automática y ofrece la posibilidad de acceso remoto a la misma[493].

2.2. Situación de la implementación de la historia clínica digital en España.

El Ministerio de Sanidad, Servicios Sociales e Igualdad ha diseñado el nombrado Sistema de HCD del Sistema Nacional de Salud (HCDSNS)[494]. La legitimación

[490] Asimismo, según el Informe de Situación de enero de 2017 del Proyecto Historia Clínica Digital del Sistema Nacional de Salud (HCDSNS), publicado por el Ministerio de Sanidad, Servicios Sociales e Igualdad, se presentan datos reales de cobertura de la población en relación con la HCD y de los 46.438.422 habitantes censados, a 31/12/2016 ya cuentan con HCD en el Sistema Nacional de Salud, 35.745.083 ciudadanos, lo que equivale a una cobertura nacional del 77,53% de la población. Disponible en Internet: <http://www.msssi.gob.es/profesionales/hcdsns/contenidoDoc/Inf_Sit_HCDSNS_Enero2017.pdf> [Consulta: 12 enero 2017].

[491] LESMES SERRANO, C., op. cit., pp. 11-13.

[492] Ibídem.

[493] Vid. Ministerio de Sanidad y Política Social, documento sobre la "Utilización de las tecnologías de la información para mejorar la atención a los ciudadanos". Disponible en Internet: <http://www.msps.es/organizacion/sns/planCalidadSNS/pdf/tic/sanidad_en_linea_WEB_final.pdf> [Consulta: 2 diciembre 2016].

[494] Puede consultarse el contenido, la documentación y las distintas fases del proyecto de HCDSNS en el Ministerio de Sanidad, Servicios Sociales e Igualdad: <https://www.msssi.gob.es/profesionales/hcdsns/home.htm> [Consulta: 2 diciembre 2016].

normativa para su creación se encuentra en la LAP[495], que, en su disposición adicional tercera, establece que el Ministerio de Sanidad y Consumo, en coordinación y con la colaboración de las Comunidades Autónomas, promoverá la implantación de un sistema de compatibilidad de las HC. Ulteriormente, la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud[496], encomienda al Ministerio de Sanidad y Consumo el mandato de coordinar los mecanismos de intercambio electrónico de información clínica y salud individual, para permitir el acceso tanto al usuario como a los profesionales en los términos estrictamente necesarios para garantizar la calidad de la asistencia y la confidencialidad e integridad de la información. Al respecto, recalca el Ministerio de Sanidad[497], que la aplicación de criterios de normalización de la información, junto con el desarrollo de una Intranet sanitaria del Sistema Nacional de Salud, permitirá alcanzar uno de los objetivos principales del sistema sanitario: facilitar al máximo la protección de la salud de los ciudadanos en todo momento y con independencia del lugar donde precisen atención sanitaria.

La HC a nivel nacional se encuentra prácticamente informatizada en cada Comunidad Autónoma[498], para la totalidad de los pacientes. En España, se estima que unos cuatro millones de personas reciben cada año atención sanitaria en una Comunidad Autónoma distinta de aquella en la que está activa su Tarjeta Sanitaria Individual (en adelante, TSI). Esto implica la necesidad de trabajar en la comunicación de información clínica interoperable por encima del ámbito autonómico, extendiendo los beneficios que proporciona la tecnología respecto a la información clínica a nivel nacional.

---

[495] La disposición adicional tercera de la LAP, establece que: *"El Ministerio de Sanidad y Consumo, en coordinación y con la colaboración de las Comunidades Autónomas competentes en la materia, promoverá, con la participación de todos los interesados, la implantación de un sistema de compatibilidad que, atendida la evolución y disponibilidad de los recursos técnicos, y la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición".*

[496] Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, op. cit.

[497] Ver al respecto: Historia Clínica Digital en el Sistema Nacional de Salud. Disponible en Internet: <www.msps.es> [Consulta: 2 diciembre 2016].

[498] A finales de octubre de 2015 el número de tarjetas sanitarias individuales con nuevo formato ascienden a 4.660.000. Las Comunidades Autónomas que emiten ya tarjetas de acuerdo al mismo son Andalucía, Aragón, Asturias, Baleares, Cantabria, Castilla y León, Extremadura, Galicia, Murcia, Navarra y País Vasco. Fuente: Informe Anual del Sistema Nacional de Salud 2015, publicado por el Ministerio de Sanidad, Servicios Sociales e Igualdad. Disponible en Internet: <https://www.msssi.gob.es/estadEstudios/estadisticas/sisInfSanSNS/tablasEstadisticas/Inf_Anual_SNS_2015.1.pdf> [Consulta: 2 diciembre 2016].

El Ministerio de Sanidad implementó el Proyecto de HCD en el Sistema Nacional de Salud[499] en los primeros meses del año 2006, para responder a las necesidades de los ciudadanos cuando se desplazan y requieren atención sanitaria en situación de movilidad, habitualmente fuera de la Comunidad Autónoma en la que son atendidos. Asimismo, el Proyecto de HCD, refleja que la propia dinámica social, donde la movilidad de los ciudadanos es cada vez más frecuente, hace necesaria la implantación de un sistema que facilite la extensión territorial de dichas funcionalidades al conjunto del Sistema Nacional de Salud y que permita a los profesionales sanitarios, la posibilidad de disponer de la información precisa cuando las necesidades de atención médica se producen fuera de la Comunidad Autónoma en la que se ha generado esta información.

3. Riesgos que se plantean frente a los datos contenidos en la historia clínica digital.

Al mismo tiempo que es evidente que los servicios sanitarios trabajan con información personal de los pacientes, y que dicha información sólo puede ser gestionada eficazmente con la utilización e implementación de las TIC, dado el momento social en el que nos encontramos y la tendencia actual de todos los centros asistenciales de trabajar sin papeles, tenemos que reflexionar y hacer especial hincapié en que los datos de salud de un paciente forman parte de la esfera más personal e íntima. También es menester recalcar que la HCD no sólo contempla datos exclusivos de salud, sino que también se recopilan en ella, datos relativos a la raza, a la orientación sexual o a las creencias de la persona[500].

[499] El Proyecto de HCD en el Sistema Nacional de Salud, tiene como finalidad garantizar a los ciudadanos y a los profesionales sanitarios el acceso a aquella información clínica relevante para la atención sanitaria de un paciente desde cualquier lugar del Sistema Nacional de Salud, asegurando a los ciudadanos que la consulta de sus datos queda restringida a quién está autorizado para ello. Consiste en las adaptaciones funcionales y organizativas de los procesos asistenciales y del tratamiento de la información, que supone abordar todas las actuaciones de análisis, consenso, diseño y prestación de servicios técnicos para alcanzar el objetivo de aplicar la HCD en todo el territorio español. Véase al respecto: <http://www.msssi.gob.es/organizacion/sns/e_salud.htm> [Consulta: 2 diciembre 2016].

[500] Como ejemplo de ésta situación, cabe citar el caso de Testigos de Jehová, quienes justamente por pertenecer a esa religión no admiten transfusiones médicas, por tanto, es un dato que a simple vista ni

Luego de ésta reflexión, cabe resaltar que, en determinadas ocasiones, puede ocurrir que un paciente quiera reservarse para sí, según qué datos o determinadas patologías. Citemos, por ejemplo, un paciente que padece trastorno bipolar, o un ex alcohólico, o un portador de sida, etc., en estos casos puede ocurrir, por ejemplo, que su ingreso al mundo laboral se vea obstaculizado por su HCD, y, por tanto, el paciente puede preferir mantenerlo en secreto. Por ello, su conocimiento por terceras personas puede atentar gravemente a la intimidad personal de ese paciente, vulnerando sus derechos fundamentales[501].

Al respecto, señala TRONCOSO REIGADA[502] que:

> La confidencialidad de la HC -el acceso a la información sanitaria sólo las personas autorizadas y no terceras personas- es también un instrumento de garantía de la asistencia sanitaria ya que la atención sanitaria está basada en la confidencialidad de la relación médico-paciente, que es, sobre todo, una relación de confianza. Si el paciente piensa que la información que revela al facultativo va a ser conocida por terceras personas, se daña la confianza en la relación médico-enfermo, se limita la información que el paciente da al facultativo y, en definitiva, se perjudica la asistencia. Por tanto, junto al interés personal en el respeto al derecho a la intimidad, la confidencialidad de las historias clínicas es un bien constitucional colectivo.

Coincidimos con el autor en esta preocupación, porque desde sus orígenes la medicina se ha basado en la relación que se entabla entre el médico y su paciente, que presupone una confianza, un secreto y ello, porque la salud y la vida es el bien más preciado del que disponemos todos, por ello, "ponerte en manos" de un médico, conlleva intrínsecamente esa necesidad de confianza absoluta en dicho profesional.

4. Finalidad de la historia clínica digital

Tal como se ha comentado anteriormente, la finalidad primordial que se persigue con la implementación de la HCD, es que la misma sirva de fiel reflejo de los datos de salud de un paciente, siendo éstos actualizados, veraces para que, con la misma, el

---

debería incluirse en una HCD, pero dada la trascendencia sanitaria que implica dicha creencia, es menester recogerlo en la HCD de ese paciente.

[501] Vid. TRONCOSO REIGADA, A., op. cit., p. 48.

[502] Ibídem, pp. 48 y 49.

facultativo médico pueda brindar la asistencia sanitaria necesaria en el momento que el paciente lo requiera.

El Documento Final del Grupo de Expertos elaborado el 26 de noviembre de 1997[503], determinó que el fin principal de la HC es facilitar la asistencia sanitaria del ciudadano, recogiendo toda la información clínica necesaria para asegurar, bajo un criterio médico, el conocimiento veraz, exacto y actualizado de su estado de salud por los sanitarios que le atienden. Y como hemos comentado anteriormente, éste Documento sirvió de inspiración para la elaboración de la LAP, que legisló ulteriormente sobre la finalidad de la HC en su Artículo 15.2, promulgando que: *"La historia clínica tendrá como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud".*

Exactamente la misma finalidad es perseguida por la HCD, con la gran diferencia de su utilidad en toda España y su constante actualización al estado real de salud del paciente y al mismo tiempo que dicha información se produce. En este sentido, siempre que un médico realice un acceso a la HCD guardará los datos de la consulta realizada, del tratamiento indicado o de las pruebas, en su caso, indistintamente la Comunidad Autónoma donde se encuentre el paciente y se ha realizado dicha atención, y ésta información estará disponible para el facultativo que deba atender al mismo paciente, por ejemplo, a la vuelta de su viaje.

GALLEGO RIESTRA[504] manifestó que la finalidad del establecimiento de la HCD, es crear una HCD compartida, que posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, a fin de evitar la repetición innecesaria de exploraciones y procedimientos.

Por lo tanto, la HCD del Sistema Nacional de Salud, cuyo propósito es lograr la cohesión del sistema sanitario público español, está orientada a satisfacer, por un lado, las necesidades de los ciudadanos cuando requieren atención sanitaria en sus desplazamientos por el territorio nacional, y, por otro lado, las necesidades de los profesionales sanitarios de todas las Comunidades y Ciudades Autónomas a los que el paciente demande asistencia y autorice para conocer su información clínica relevante.

---

[503] Grupo de Expertos en Información y Documentación Clínica. "Informe final". Madrid, 1997. *Revista Calidad Asistencial 1999.* Núm. 14, Madrid, pp. 76-87.

[504] GALLEGO RIESTRA, S., op. cit., p. 17.

En base a ello, podemos decir que la HCD tiene como finalidad primordial recoger datos del estado de salud del paciente con el objeto de facilitar la asistencia sanitaria. Subrayamos que es el objetivo principal de la HCD, aunque no el único como veremos más adelante. Puede considerarse a la HCD como el instrumento básico del buen ejercicio sanitario, porque sin ella es imposible que el médico pueda tener una visión completa y global del paciente para prestarle la asistencia sanitaria necesaria y de calidad. Ante ésta razón podemos sostener que la HCD en sí, constituye una exigencia para la prestación de servicios sanitarios por parte del médico al paciente.

Sostiene MARTÍNEZ AGUADO[505] que la HC además de tener una finalidad asistencial, constituye el elemento básico y mínimo para ofrecer atención de calidad. El autor añade que puede decirse que es el primer elemento asistencial, y por tanto la HC debe elaborarse y utilizarse también con planteamientos éticos. Por tanto - concluye - su fin principal es la toma de decisiones para la orientación de estrategias y la resolución de problemas en el ámbito de la asistencia a los pacientes. Conceptos que sirven de presupuesto a la HCD, que según comentamos ut supra, facilitará al profesional sanitario brindar una asistencia sanitaria con una visión global del paciente y de calidad.

Asimismo, SANCHEZ-CARO y ABELLÁN[506] manifiestan que los datos personales pueden recabarse por muchas personas y para muchas finalidades. Destacan los autores en primer término al paciente o a las personas vinculadas a él; a las fuerzas y cuerpos de seguridad del Estado que pueden solicitar datos relacionados con la filiación, estancia, localización y datos clínicos; por la inspección sanitaria; por la Seguridad Social, para la tramitación de pensiones; por diferentes órganos de las Administraciones públicas, para intereses públicos, epistemológicos; y finalmente agrupan los autores a todo el personal médico que tiene por finalidad la asistencia sanitaria, siendo los médicos, enfermeras y demás personal sanitario los responsables de la creación de la HC y de su actualización.

Aunque hay que destacar que la LOPD consagra 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[507]. Vemos que ésta premisa legislativa

[505] MARTÍNEZ AGUADO, L., op. cit., pp. 78 y 79.

[506] SÁNCHEZ-CARO, J.; ABELLÁN, F. *Enfermería y Paciente.*, op. cit., pp. 203 y ss.

[507] Artículo 4.2, de la LOPD.

es de aplicación a los datos de salud en general y a los que quedan recogidos y plasmados en la HCD del paciente.

Al respecto, el TC se pronunció sobre la finalidad de los datos, en su Sentencia 94/1998[508], señalando que:

> La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, desarrollando lo previsto en el art. 18.4 C.E., plasma como principio cardinal de la protección de datos la congruencia y la racionalidad de su utilización, en cuya virtud ha de mediar una nítida conexión entre la información personal que se recaba y trata informáticamente y el legítimo objetivo para el que se solicita y, en consecuencia, prohíbe tajantemente el uso de los datos para finalidades distintas de las que motivaron su recogida (apartados 1 y 2 del art. 4). Asimismo, otorga una tutela reforzada a los datos sensibles.

En la Sentencia 202/1999[509], el TC mantuvo el precedente creado, sosteniendo que:

> La creación y el mantenimiento por la entidad crediticia del fichero automatizado denominado, donde se conservan los datos referidos a las bajas laborales causadas por el ahora solicitante de amparo no puede ampararse en la existencia de un interés general (art. 7.3 L.O.R.T.A.D. y, por remisión, arts. 10.11 y 61 L.G.S.), que justificaría la autorización por ley, sin necesidad del consentimiento del trabajador, para el tratamiento automatizado de los datos atinentes a su salud, ni tampoco en lo dispuesto en los arts. 22 y 23 de la Ley de Prevención de Riesgos Laborales. El tratamiento y conservación en el preciso soporte informático de los datos atinentes a la salud del trabajador, prescindiendo del consentimiento expreso del afectado, ha de calificarse como una medida inadecuada y desproporcionada que conculca por ello el derecho a la intimidad y a la libertad informática del titular de la información.

Sin embargo, el TC fue más allá de la previsión legal contenida en el Artículo 4.2 de la LOPD, y a pesar de que los datos fuesen recogidos con los fines legítimos e informándose a la persona afectada; si los mismos datos no tienen garantías de que su tratamiento se limitará a aquellos fines, se entiende vulnerado el derecho fundamental a la intimidad. Así lo recoge en la Sentencia 143/1994[510], en la que el TC apuntó que:

> Un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso

[508] STC 94/1998, de 4 de mayo de 1998, Fundamento Jurídico número 4 (BOE núm. 137, 9.06.1998. Suplemento, pp. 8-13).

[509] STC 202/1999, de 8 de noviembre de 1999, Fundamentos Jurídicos números 3, 4 y 5 (BOE núm. 300, 16.12.1999. Suplemento, pp. 19-26).

[510] STC 143/1994, de 9 mayo de 1994, Fundamento Jurídico número 7 (BOE núm. 140, 13.05.1994).

> potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta.

Cabe hacer una reflexión en éste apartado y manifestar que para que exista una vulneración a la protección de los datos de carácter personal relativos a la salud, no basta con su mera recopilación, sino que lo que importará es el tratamiento que a los mismos se les realice y a la finalidad a los que serán sometidos. En este sentido coincidimos con la opinión de TRONCOSO REIGADA[511] al decir que: *"…para que entre en juego el derecho fundamental a la protección de datos personales es necesario que los datos de carácter personal se hallen registrados en un soporte físico que los haga susceptibles de tratamiento (art. 2.1 LOPD)".* Refiere el autor, que la protección que otorga la LOPD *"no protege los datos personales a toda costa, sino sólo frente a los tratamientos. Si no hay tratamiento, no hay derecho fundamental a la protección de datos, aunque puede haber un derecho a la intimidad"*[512]*.*

4.1. Otras finalidades de la historia clínica digital.

Además de la finalidad primordial que hemos comentado *ut supra*, cabe mencionar otras finalidades legales que la HCD puede tener[513].

(i) En primer lugar, podemos mencionar la finalidad de Docencia e investigación. A partir de las HCD pueden realizarse estudios e investigaciones sobre determinadas patologías, publicaciones científicas, avances científicos en enfermedades, etc. Por tanto, podemos considerar que otra finalidad importante a destacar, es la docente. Asimismo, no hay que olvidar, que al igual que en otros ámbitos, la HCD es útil para realizar estudios de investigación como, por ejemplo, en epidemias, pandemias, etc., y ello dado la rapidez con la que se puede acceder a los datos, sobre todo en éste tipo de situaciones donde el tiempo apremia para frenar los posibles contagios.

---

[511] TRONCOSO REIGADA, A. (Director). *Transparencia Administrativa y Protección de Datos Personales. V Encuentro entre Agencias Autonómicas de Protección de Datos.* Thomson Civitas, Madrid, 2008, pp. 43 y ss.

[512] Ibídem.

[513] Para profundizar más al respecto, véase: MARTÍNEZ AGUADO, L., op. cit., pp. 78 y 79.; SÁNCHEZ-CARO, J.; ABELLÁN, F., op. cit., pp. 203 y ss.; GIMÉNEZ, D., op. cit.

Pero, éste derecho a la docencia e investigación que asiste a todo profesional sanitario, en virtud de lo preceptuado por la Ley de ordenación de las profesiones sanitarias[514], puede contraponerse el derecho a la autonomía del paciente, a su intimidad y a la confidencialidad de sus datos[515]. Sin embargo, este derecho a la docencia e investigación, viene reforzado con la previsión, que determina que toda la estructura asistencial del sistema sanitario estará en disposición de ser utilizada para la investigación sanitaria y para la docencia de los profesionales, aunque ya se ocupe de aclarar la LGS, que lo anterior estará sometido a la autorización previa y por escrito del paciente.

Al respecto, apuntan ABELLÁN y GARCÍA DÍAZ[516], que la potencial colisión de estos derechos de paciente e investigador, respectivamente, exige establecer unas reglas de juego que ponderen los intereses de una y otra parte, que busquen un equilibrio que concilie el respeto a la autonomía e intimidad del primero con el legítimo interés del profesional sanitario a la investigación, que es también el interés de la sociedad en su conjunto a fin de que se incremente el conocimiento científico y se beneficien todos los ciudadanos. Según refieren ABELLÁN y GARCÍA DÍAZ[517], en este punto es donde ha de intervenir la Administración sanitaria, por ejemplo, exigiendo que los proyectos de investigación obtengan el visto bueno previo de un Comité ético de investigación y sometiendo a autorización los casos en los que proceda.

(ii) Otra finalidad que podemos destacar, es la Evaluación de la calidad asistencial. La HC es considerada por las normas deontológicas y por las normas legales como un derecho del paciente derivado del derecho a una asistencia médica de calidad.

Según GÓMEZ PIQUERAS[518], el estudio y valoración de la HC permite establecer el nivel de calidad asistencial prestada. Y ello, porque se trata de un

[514] Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias, op. cit.

[515] Nos referimos a la LAP y a la LOPD.

[516] ABELLÁN, F; GARCÍA DÍAZ, A. *Acceso a la historia clínica con fines de investigación. Estado de la cuestión y Controversias.* Informe del Experto Nº 12, Fundación Salud 2000, 2015, pp. 6 y ss.

[517] Ibídem.

[518] Vid. GÓMEZ PIQUERAS, C. *Contenido, usos y finalidad de la Historia Clínica.*, op. cit., p. 23.

fiel reflejo de la relación médico-paciente, así como un registro de la actuación médico-sanitaria prestada al paciente.

Consideramos que la HCD se constituye como la forma idónea de responder a ésta finalidad, porque, además de poseer los datos del paciente actualizados de forma simultánea a la asistencia prestada por el médico, permite que el facultativo disponga de su historial completo, y ello, le facilitará tener una visión integrada, como hemos referido anteriormente, que le permitirá tomar una decisión médica, seguramente mucho más acertada y acorde con el diagnóstico, según los síntomas referidos del paciente, y sus antecedentes médicos. Este factor hará posible una asistencia médica de calidad.

(iii) En tercer lugar, también cabe hablar de una finalidad Administrativa. La HC es elemento fundamental para el control y gestión de los servicios médicos de las instituciones sanitarias.

A través de la vigilancia y observancia de la HCD, la Administración Pública puede verificar que los objetivos legales se están respetando y llevando a cabo según lo preceptuado por la normativa. Asimismo, permitirá a la Administración conocer de forma estadística las necesidades de la población, respecto a medicamentos, tratamientos, etc., lo cual facilitará una mejor estimación de costes y gastos en el sector sanitario, además de las inversiones que pueden preverse.

(iv) En cuarto lugar, la HC también tiene una función de Inspección. Asimismo, la HC facilita el ejercicio de las funciones propias de la Inspección Médica.

El permiso de acceso de los inspectores a la HCD tiene más relación con una función de peritaje (en general, con la evaluación de la idoneidad de una prestación por incapacidad temporal) que una función clínica. Desde esta consideración, precisa un permiso explícito que debería restringirse a los documentos y anotaciones relacionados exclusivamente con el motivo de la incapacidad temporal, según refiere DE CASTRO VILA[519]. Sin embargo, el

[519] DE CASTRO VILA, C.; RUBIO MONTAÑÉS, M. L.; ALADID VILLAR, C. (mayo, 2015) Ética y acceso a datos clínicos desde los servicios de inspección y evaluación médicas. [Blog post]. Blog Formación Médica Continuada en Atención Primaria (FMC). Disponible en Internet: <http://www.fmc.es/es/tica-acceso-datos-clinicos-desde/articulo/90429633/#.WNzrXY4IFuU> [Consulta: 11 noviembre 2016].

acceso a la HCD es general y no ha sido precedido del permiso del paciente. El inspector tiene acceso a todos los problemas de salud y todas las anotaciones clínicas realizadas en la HCD.

(v) Así también, podemos destacar una finalidad Médico-legal. La HC colabora estrechamente con la Administración de Justicia. En éste sentido, hay un imperativo legal que obliga a realizarla, según la normativa vigente, es decir, en observancia de lo establecido por la Ley General de Sanidad, Ordenación de prestaciones sanitarias, Derechos de los Usuarios, Código Deontológico Médico, Normas Internacionales, como hemos hecho referencia en el Capítulo anterior.

En el ámbito judicial, la HC constituye un elemento de prueba en los casos de responsabilidad médica profesional. Podemos sostener que tiene un extraordinario valor jurídico en los casos de responsabilidad médica profesional, al convertirse por orden judicial en la prueba material principal de todos los procesos de responsabilidad profesional médica, constituyendo un documento médico-legal fundamental y de primer orden. En tales circunstancias la HC, es el elemento que permite la evaluación de la calidad asistencial tanto para la valoración de la conducta del médico como para verificar si cumplió con el deber de informar, de realizar la HC de forma adecuada y eficaz para su finalidad asistencial, puesto que el incumplimiento de tales deberes también constituye causa de responsabilidad profesional.

Asimismo, sirve como testimonio documental de ratificación o sobre la comprobación de la veracidad de declaraciones sobre actos clínicos y conducta profesional realizados. Observamos que la HCD, facilitará ésta labor Médico-legal, por cuanto constará de un único documento, donde estarán registradas todas las actuaciones del facultativo sanitario, evitando que ciertos datos contenidos en soporte de papel puedan ser destruidos o no tenidos en cuenta a la hora de juzgar, por simplemente no contar en los documentos objetos de peritaje.

De igual forma, cabe destacar su importante valor como instrumento de dictamen pericial, puesto que la HC se convierte en el elemento clave en la elaboración de informes médico-legales sobre responsabilidad médica profesional. El objeto de estudio de todo informe pericial sobre responsabilidad médica profesional es la HC, a través de la cual se pueden valorar algunos aspectos como la enumeración de todos los documentos que la integran, la reconstrucción de la HC, análisis

individualizado de los actos médicos realizados en el paciente, personas que intervinieron durante el proceso asistencial, etc.

El valor médico–legal de la HC también sirve para proteger a los pacientes. El TS condenó a un agresor por violencia machista, que a pesar de que la víctima no quiso declarar contra él, en el parte de lesiones de la víctima contenido en su HC, en el que se objetivaban lesiones en la mujer, sirvió como instrumento probatorio de entidad suficiente para que el TS imputara dichas lesiones al autor, condenándolo como agresor de su pareja[520].

5. Eficiencia de la historia clínica digital.

El ordenador es una herramienta habitual del médico en la consulta. A través de su utilización se podrá acceder a la HCD del paciente. En ella, quedan registradas todas las visitas, las pruebas realizadas, los resultados de las mismas y la información médica relevante del paciente. Esta información podrá ser consultada por médicos o personal autorizado de la misma Comunidad Autónoma, o de otras Comunidades con la simple facilidad de acceder a través de un ordenador.

El proyecto de implementar en España la HCD, supondrá evitar tiempo y molestias a los pacientes y mejorará el servicio sanitario. A través de su utilización, se facilitará a los médicos de cualquier lugar de España acceder a la HC de un paciente.

Por tanto, con la implementación y utilización a nivel nacional de la HCD se permitirá registrar toda la información clínica que vincule al paciente, gestionar los resultados de las pruebas médicas prescritas, su tratamiento, incluso facilitará las comunicaciones entre el personal sanitario[521]. De ésta manera, el médico también podrá acceder a las pruebas que impliquen un radiodiagnóstico. Se podrán consultar las radiografías y los resultados de cualquier diagnóstico específico realizado por imagen, desde el

[520] STS 533/2008, 19 de septiembre de 2008. Recurso 10066/2008 (Roj: STS 4779/2008 – ECLI: ES:TS:2008:4779).

[521] Vid. SABARTÉS FORTUNY, R. (2013) *Historia Clínica Electrónica en un Departamento de Obstetricia, Ginecología y Reproducción: desarrollo e implementación. Factores Clave* (Tesis Doctoral). Universidad Autónoma de Barcelona, Facultad de Medicina, Barcelona, España, 2013, pp. 22 y ss. Disponible en internet: <http://www.tdx.cat/bitstream/handle/10803/117304/rsf1de1.pdf?sequence=1> [Consulta: 28 noviembre 2016].

ordenador de un médico de cualquier punto de España. La informatización de las pruebas de radiodiagnóstico abrirá una puerta a la telemedicina.

Desde éste punto de vista, es evidente la eficiencia de la HCD en comparación con la HC tradicional en formato papel.

6. Garantías para los pacientes.

A través de la utilizaron de la HCD en todo el territorio español, se pretende garantizar la confidencialidad y protección de la información de carácter personal y sanitaria[522]. Realizar un cambio y plantearse la HCD ha de suponer una mejora en la calidad de la asistencia sanitaria. La atención médica podrá llevarse a cabo de manera más ágil y evitándose pruebas innecesarias que conduzcan conocer información del paciente de forma más inmediata, como, por ejemplo, su grupo sanguíneo, alergias, entre otras. Esto sorteará tiempo y costes de las mencionadas pruebas, e incluso, dolor innecesario por parte del paciente que no deberá someterse a su reconocimiento previo.

Por lo tanto, la HCD garantizará a los profesionales de salud el acceso a la información del paciente, a la vez que se garantiza el derecho del mismo a una atención sanitaria precoz y de excelencia. Toda ésta documentación clínica volcada en la HCD, debe contar con medidas de seguridad adecuadas, y máximas, desde nuestro punto de vista, para evitar cualquier posible vulneración a la intimidad del paciente[523].

---

[522] El Artículo 56, de la Ley 16/2003 de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, op. cit., se refiere al Intercambio de información en salud entre organismos, centros y servicios del Sistema Nacional de Salud, estableciendo que: *"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".*

[523] Para profundizar más el tema, véase: ÁLVAREZ GUISASOLA, F. J. "Visión desde Castilla y León. Jornadas del I y II Encuentro Interautonómico sobre protección jurídica del paciente como consumidor", en TOMILLO URBINA, J.; CAYÓN DE LAS CUEVAS, J. (directores). *La Protección Jurídica del Paciente como Consumidor.* Aranzadi, Navarra, 2010, p. 45. Sostiene el autor que: *"Los derechos relativos a la documentación clínica recogen un conglomerado de medidas que garantizan tanto la*

Sin duda, la implementación y utilización de éste avanzado método de consulta de nuestro historial médico, ha de venir respaldado por una serie de garantías a fin de prever el uso que se dará a nuestros datos personales y garantizar así la protección de los contenidos en él, datos sensibles especialmente protegidos.

6.1. Nuestra postura en torno a las garantías de implantación de la historia clínica digital.

Las principales garantías que, desde nuestro punto de vista, ofrece la implementación de la HCD, puede estructurarse en torno a cuatro ejes fundamentales.

(i) El primer eje, lo constituye la seguridad. La HCD de cada paciente será segura, ello, al menos desde el punto de vista de su custodia en servidores, y porque se almacenará y se conservará, permaneciendo siempre disponible a favor del personal sanitario o del paciente en caso de solicitarlo éste, desde cualquier punto de España. Además, se contará con copias de seguridad a fin de evitar cualquier pérdida o deterioro de la información digitalizada, que pudiera sufrir.

(ii) El segundo eje, es la confidencialidad. El acceso y la utilización de la HCD sólo se podrá realizar legítimamente, es decir, la Ley limita taxativamente los accesos que a la misma se pueden hacer, y de la misma manera, éstos accesos se quedan debidamente registrados para que, en caso de necesitarse, se pueda conocer fehacientemente qué facultativo o miembro del personal sanitario ha accedido a los datos del paciente y cuándo ha tenido acceso. En relación a ello, la Audiencia Provincial de Palma de Mallorca en Sentencia de 11 de febrero de 2009, condenó a un médico de atención primaria a 3 años y tres meses de prisión, multa e inhabilitación de 9 años por acceder a la HCD de otro facultativo, sin finalidad asistencial, utilizando para ello su clave de acceso al programa de HCD. El médico implicado alegó que accedió a la HCD con la finalidad de

---

calidad de la información clínica que se recoge en la historia clínica, como la prestación de una asistencia sanitaria adecuada al paciente, junto con las medidas necesarias para asegurar la protección de datos personales recogidos en la documentación clínica". En el mismo sentido, LAFARGA I TAVER, J. L. "Problemas legales asociados al tratamiento informático de la historia clínica: la responsabilidad médica en el tratamiento de datos". *Derecho y Salud*. Vol. 7, núm. 2, julio-diciembre 1999, pp. 43-48.

conocer quién era el médico de cabecera de su compañero para cambiar impresiones con él de cara a solucionar una serie de problemas laborales. El sistema de HCD guarda los registros de acceso y ello sirvió para demostrar que el médico en cuestión accedió a la HCD sin el consentimiento del compañero y sin que mediara un motivo asistencial, sin embargo, el TS absolvió al médico por entender que no se había cometido un delito en los términos del Artículo 197.2 del Código Penal por entender que el acceso a la HC sólo para conocerse el nombre del médico de cabecera, no supuso un perjuicio para los datos contenidos en ella del paciente[524].

(iii) El tercer eje, consiste en la facilidad de acceso y el control por parte del titular de la HCD. El acceso electrónico a la HCD requiere de un ordenador y una clave que el médico posee. Por ello, el acceso es totalmente sencillo y rápido, a la vez de que queda siempre sujeto a la posibilidad del paciente a conocer quién ha accedido a su HCD. Recordemos que sólo tiene acceso a los datos del paciente, él mismo y la persona a quien él autorice; su representante en caso de que el paciente fuese incapaz y los profesionales del centro implicados en su asistencia. Además de saberse quién ha accedido, otra de las principales garantías ha de consistir en que los pacientes puedan saber desde qué centro o centros se ha accedido a su HCD.

(iv) Finalmente, el cuarto eje lo constituye la calidad de los datos. El contenido de la HCD permite mantener un contenido integrado que se actualiza constantemente en cada acceso que el profesional hace, que se corresponde con los requerimientos de la finalidad asistencial que implica la HC. Además de ello, la HCD será completa, porque contendrá todos los datos necesarios para que el paciente reciba una adecuada asistencia médica. Sobre todos estos temas, profundizaremos más adelante.

[524] STS 1328/2009, de 30 de diciembre de 2009. Recurso 1142/2009 (Roj: STS 8457/2009 – ECLI: ES:TS:2009:9457).

7. Seguridad y confidencialidad en torno a la historia clínica digital.

Tal como sostienen SÁNCHEZ-CARO y ABELLÁN[525], las cuestiones relativas a las HCD están dotadas de gran complejidad, ya que afectan a multiplicidad de personas. En particular a médicos y otros profesionales sanitarios, además de pacientes y usuarios en general. Coincidimos en este sentido y cabe puntualizar que, el acceso por parte de varios facultativos médicos, enfermeros, y personal administrativo, hace que la información sensible contenida en la HCD pueda ser más vulnerable desde el punto de vista de la seguridad y la confidencialidad de la misma.

Los hospitales y centros médicos deberían contar con un sistema que permita dotar de seguridad a los pacientes a la hora de saber quiénes acceden a sus datos. Si bien esto existe, como hemos hecho referencia anteriormente, no descarta que se haya accedido a nuestro HCD sin nuestro previo consentimiento. Es decir, los médicos, el personal sanitario y las personas habilitadas, pueden tener acceso a nuestra HCD sin la presencia física del paciente. Pero ésta circunstancia, tal y como ocurrió en el caso de Mallorca[526], puede dar lugar a que se acceda a nuestros datos, y si el paciente no solicita un listado de accesos, jamás tendría conocimiento que determinada persona consultó sus datos de la HCD.

Consideramos que ésta circunstancia podría evitarse y dotar de más seguridad aún el acceso a nuestros datos sensibles, a través de la utilización de la huella digital del paciente. De ésta forma, el médico sólo requerirá el ordenador y un pequeño dispositivo en el cual el paciente coloca su huella a fin de tener acceso a la HCD y brindarle asistencia sanitaria. De ésta manera, el paciente sabrá exactamente quién es la persona que conoce sus datos de salud, el resultado de sus pruebas médicas y toda la información contenida en su HCD, con la simple identificación de su huella digital.

ABELLÁN y GARCÍA DÍAZ[527] prefieren un acceso más sencillo a las HCD, pero, hacen especial referencia a los fines de la investigación. Los autores son contrarios a las trabas burocráticas que implica la rigidez de las Leyes y a las dificultades de acceso

[525] Vid. SÁNCHEZ-CARO, J.; ABELLÁN, F. *Derechos y deberes de los pacientes*., op. cit., pp. 61 y ss.

[526] STS 1328/2009, de 30 de diciembre de 2009, op. cit.

[527] ABELLÁN, F; GARCÍA DÍAZ, A., op. cit., p. 7.

que supondría solicitar el consentimiento a un número elevados de pacientes para realizar diferentes labores de investigación científica, por tanto, y basándonos en su criterio, encontramos que la utilización de la huella digital del paciente, en este sentido, es cierto que condicionaría un campo tan necesario como es el desarrollo de la investigación científica en el campo médico, pero sin embargo, consideramos que existiendo una norma capital en el ámbito de datos de salud, podría excluirse dicho consentimiento cuando la información contenida en la HCD del paciente es necesaria para esos fines netamente investigativos y de progreso científico, con las debidas garantías.

Por tanto, la información del paciente al estar digitalizada no permanecerá inmóvil en un centro asistencial, entonces, si el paciente se desplaza, el médico perteneciente a otra Comunidad Autónoma puede acceder a la información sanitaria del paciente, a través de la consulta de su HCD, pero, para que este flujo de información sea una realidad y no suponga un peligro para la información que contiene, el Ministerio de Sanidad ha creado una Intranet Sanitaria. La Intranet Sanitaria es una red privada contratada por el Ministerio de Sanidad y Política Social, con cifrado a nivel físico, con lo cual en Ministerio pretende garantizar los niveles de servicio y la seguridad que precisa el sistema por su sensibilidad y criticidad. Todos los intercambios de información se realizan utilizando mensajes XML, no existiendo aplicaciones ni ningún otro medio de acceso a la información[528].

En relación con la seguridad con la que se debe contar para archivar las HCD, la LAP, encomienda a los centros hospitalarios encargados de recoger la información clínica del paciente de velar por la seguridad y por el mantenimiento de dicha información. Al

[528] MUÑOZ MONTALVO, J. F. (22.10.2009) "La interoperabilidad: el nodo central del Sistema Nacional de Salud". Ponencia presentada en el 3er Foro sobre el Sistema de Información del Sistema Nacional de Salud, celebrado el 22 de octubre de 2009, Ministerio de Sanidad y Política Social, Madrid, 2009. Disponible en Internet: <http://www.msps.es/estadEstudios/estadisticas/sisInfSanSNS/3ForoSISNS/docs/JuanFernando_ponencia3Foro.pdf> [Consulta: 29 noviembre 2016]. La implementación de la Intranet Sanitaria para la comunicación de los datos sanitarios entre los distintos facultativos y centros médicos, está mostrando resultados positivos, según el Ministerio de Sanidad. Sin embargo, también se prevé, un mecanismo de auditorías, que, desde nuestro punto de vista puede ser un instrumento muy idóneo, a través de las cuales pueda controlarse periódicamente, si se ha realizado el uso adecuado de las HC y si el personal que ha accedido a la información contenida en el fichero de la HC es el autorizado y si ha accedido en virtud de su profesión y según la necesidad del paciente. Ver al respecto: Informe Anual del Sistema Nacional de Salud 2015, op. cit.

respecto, dispone 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"*[529]*.* Ésta seguridad y confidencialidad es objeto de estudio del Ministerio de Sanidad en la actual implementación del Sistema Nacional de Salud, con el objetivo de encriptar los datos y ello consistirá en garantizar la confidencialidad de la información, mediante técnicas de cifrado.

Asimismo, la Ley 55/2003, de 16 de diciembre, del Estatuto Marco del personal estatutario de los servicios de salud, en su Artículo 19.j, referente a los deberes del personal sanitario, establece que los profesionales han de mantener la debida reserva y confidencialidad de la información y documentación relativa a los centros sanitarios y a los usuarios obtenida, o a la que tengan acceso, en el ejercicio de sus funciones. En este sentido, y para acceder a las HCD consideramos necesario que primero estén identificados como "médico" o "personal sanitario" a fin de realizar un primer control de acceso. Posteriormente, con palabras claves, es decir una clave o *"password"* seguras o con sistemas de control de acceso biométrico que esté relacionados con un sistema autentificador del personal de salud, el cual clasificaría a los usuarios acorde a su autorización a acceder a determinada información y a desarrollar ciertas funciones.

Cabe resaltar, que la aplicación de técnicas informáticas en el tratamiento de los datos sanitarios, y por el especial carácter que los mismos revisten, obliga a establecer una serie de controles y de cautelas a fin de respetar el derecho a la intimidad personal, en la faceta que se denomina intimidad informática[530].

7.1. Sistemas de seguridad.

Tal como lo hemos adelantado en el primer Capítulo de ésta Tesis, la LOPD y el RD 1720/2007 establecen que los datos personales de carácter personal, han de ser tratados con el nivel de seguridad más alto que la normativa regula.

---

[529] Artículo 14.2, de la LAP.

[530] Vid. CORBELLA DUCH, J., op. cit., p. 127.; ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M. *La defensa de la intimidad de los ciudadanos y la tecnología informática.* Aranzadi, Pamplona, 1999, pp. 14 y ss.; MORALES PRATS, F. "Derecho a la intimidad versus tratamiento de datos sanitarios". *Derecho y Salud.* Vol. 9, núm. 2, julio-diciembre 2001, pp. 114-124.

La seguridad para el registro, tratamiento, almacenamiento, utilización y confidencialidad de los datos médicos ha de ser máxima. Entra en juego el derecho fundamental de la persona a su intimidad y a la dignidad humana[531]. Por tanto, hay que recalcar que las medidas de seguridad en los casos de las HC tienen que ser aún más extremas y preventivas que las indicadas por el RD 1720/2007[532].

Asimismo, la LOPD encarga de la seguridad de los datos al responsable del fichero y, en su caso, el encargado del tratamiento es quien deberá adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evite 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, del medio físico o natural[533].

SÁNCHEZ PATRÓN[534] considera que la automatización de los datos de salud, conlleva mayor riesgo en que se vulnere con facilidad su confidencialidad. Ante estas

[531] La Carta Europea de Derechos Fundamentales de la Unión Europea, *"Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan",* Diario Oficial de las Comunidades Europeas del 18 de diciembre de 2000, Capítulo II d, Artículo 8; la Declaración Universal de Derechos Humanos, establece en el Artículo 12 que: *"Nadie será objeto de injerencias arbitrarias en su vida privada....Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques"*; asimismo el Convenio 108, de 28 de enero de 1981, para la Protección de las Personas se pronuncia respecto de los derechos humanos y de las libertades fundamentales, concretamente el derecho al respeto de la vida privada; finalmente, citaremos a 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, que establece: *"3.1. 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. 3.2. Los datos médicos sólo pueden recogerse y procesarse si existen medidas de protección adecuadas establecidas por la ley nacional".*

[532] Título VIII, sobre las medidas de seguridad en el tratamiento de datos de carácter personal del RD 1720/2007. En éste sentido, la LAP en su Artículo 14.4, exige a las Comunidades Autónomas que implementen medidas de seguridad, estableciendo que: *"Las Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental".* Sobre el particular, véase el Artículo 23.3 del Estatuto de Autonomía de Cataluña (BOE núm. 172 de 20 de julio de 2006).

[533] Artículo 9.1, de la LOPD.

[534] Vid. SÁNCHEZ PATRÓN, J. M. "El régimen jurídico europeo aplicable a la confidencialidad de los datos relativos a la salud de las personas", en GACÍA RUIZ, Y., et al. *La salud: intimidad y libertades informadas.* Tirant lo Blanch, Valencia, 2006, pp. 211 y ss.

preocupaciones por parte de la doctrina, el Ministerio de Sanidad[535] está estudiando la posibilidad de la implementación de un sistema que permita añadir firmas electrónicas para las entradas a las HC y que sirva para detectar si alguna entrada ha sido alterada. Sin embargo, ÁLVAREZ-CIENFUEGOS SUÁREZ[536] considera que precisamente la implantación de la firma electrónica en el mundo sanitario, constituye todo un reto para los servicios de salud, dada la especial sensibilidad de los datos relativos a la salud de los ciudadanos y debido a que, para permitir su circulación electrónica, se requiere, además de unas estrictas medidas de seguridad para evitar accesos no autorizados, y una perfecta identificación de los usuarios.

Por tanto, apreciamos que la seguridad en relación con los datos de salud, siempre ha sido motivo de preocupación tanto del legislador nacional como europeo[537]. Evidentemente la manipulación impropia de nuestros datos sanitarios, hace que se pretenda evitar el riesgo que su utilización y difusión pudiera causar. En virtud de ello, desde ésta Tesis se pretende dar respuesta a algunas lagunas que las legislaciones presentan al respecto.

Los elementos de seguridad del Sistema Nacional de Salud tienen valor estratégico recalca el Ministerio de Sanidad, dada la criticidad del sistema y la naturaleza de los

---

[535] ETREROS HUERTA, como Consejero Técnico del Ministerio de Sanidad y Política Social, sostiene que: "Nuestro criterio ha consistido en buscar elementos suficientemente exigentes que garanticen la autorización para acceder de los profesionales, pero no tanto que condicionen la imposibilidad para acceder por los profesionales que han de atender, reforzando los elementos que garantizan la autenticidad del agente que accede y reforzando mucho los elementos de control posterior basados en la autenticidad". ETREROS HUERTA, J. J. "Historia clínica electrónica", en AA.VV. *El derecho a la protección de datos en la historia clínica y la receta electrónica.* Aranzadi-AEPD, Pamplona, 2009, p. 196.

[536] ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M. "La aplicación de la firma electrónica y la protección de datos relativos a la salud". *Revista Actualidad Informática Aranzadi.* Núm. 39, abril, 2001, pp. 4-5.

[537] En el ámbito europeo, y tal como se ha hecho referencia en el Capítulo I de ésta Tesis, el Convenio 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado por España el 27 de enero de 1984, establece en el Artículo 6, que los datos referidos a la salud gozan de una protección adicional que permite a los Estados Partes a tratarlos automáticamente siempre y cuando se adopten las garantías pertinentes en cada una de las legislaciones nacionales. En el mismo sentido, véase: Decisión del Consejo, de 13 de septiembre de 2004 por la que se adoptan las normas de desarrollo del Reglamento (CE) Nº 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DOUE L 296, 21.09. 2004, pp. 16-22).

datos de carácter personal que requieren el más alto nivel de protección de los que establece la LOPD y el RD 1720/2007. En virtud de ello, se refuerzan las medidas de control previo para el acceso mediante el uso de certificación electrónica que ofrece mayores garantías de autenticidad, la asignación de los profesionales a grupos distintos según la función que desempeñen con acceso a contenidos de información diferenciados según el grupo. Se refuerzan sobre todo los sistemas de control posterior mediante acceso de los propios ciudadanos a los Registros de auditoría interna del sistema, medida en la que juega un papel relevante el propio ciudadano, como auditor externo, al poder llevar a cabo el seguimiento de los accesos realizados a sus datos de salud, o a los de su representado[538].

En el mismo sentido, ÁLVAREZ-CIENFUEGOS SUÁREZ[539] sostiene que:

> La Ley de Protección de Datos de 1999, concebida como una garantía general y básica de la intimidad de los ciudadanos, en los términos que ha reconocido recientemente el Tribunal Constitucional en sus Sentencias de 30 de noviembre de 2000, al proclamar el derecho de los ciudadanos a la 'libertad informática', resulta insuficiente para una adecuada protección de los datos relativos a la salud de las personas, siendo necesario la publicación de una ley que, de forma específica, contemple esta protección.

Después de haber analizado la normativa, la doctrina y las manifestaciones del Ministerio de Sanidad, y adelantando las conclusiones de ésta Tesis, sostenemos la importancia y subrayamos la necesidad de una Ley específica en materia de protección de datos sanitarios que regule de manera exclusiva su régimen, el tratamiento que estos datos especiales han de recibir, su manipulación y que haga especial énfasis en las medidas de seguridad que han de observarse, en consonancia con la necesidad de informatizar los datos de salud.

8. Ventajas de la implementación de la historia clínica digital.

La incorporación de la HCD implica innumerables ventajas, que podemos agrupar en tres niveles: tanto para el paciente, como para el médico y así también para el centro de

[538] Ver al respecto Ministerio de Sanidad y Política Social <www.msps.es> [Consulta: 28 noviembre 2016].

[539] ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M., op. cit., pp. 4-5.

salud. ABERASTURI GORRIÑO[540] sostiene que en el sector sanitario se conjugan tres intereses. Por un lado, las del ciudadano que está interesado en recibir una asistencia sanitaria de calidad y que en dicha prestación se respeten sus derechos fundamentales; por otro lado, los intereses del centro sanitario para que los recursos se gestionen con la mayor eficiencia posible; y, finalmente, explica el autor, que existe el interés de la sociedad a que se realicen investigaciones para la evolución científica, a fin de salvaguardar la salud pública, a que se controle el gasto y en general al buen funcionamiento de la sanidad.

Sin lugar a dudas, la HCD representa una gran ventaja respecto a la HC tradicional o en papel, respecto a la posibilidad que ofrece su accesibilidad e inmediatez a la información clínica, porque, según consideramos, estos factores constituyen piezas claves para mejorar la continuidad asistencial, la seguridad clínica y la calidad de la atención que reciben los ciudadanos en sus desplazamientos[541]. Existirá una disponibilidad de los datos de 365 días las 24 horas.

La HCD en el Sistema Nacional Sanitario (en adelante, HCDSNS) es una aplicación que permite el acceso, tanto a profesionales del ámbito sanitario, como a los ciudadanos a la información sobre su salud más relevante, desde el punto de vista clínico, que se encuentra en las HCD de las Comunidades Autónomas. En ella se encuentran la HC Resumida, los informes asistenciales y los resultados de pruebas de laboratorio e imagen[542].

Explica GALLEGO RIESTRA[543] que la HCDSNS permite al paciente ejercer electrónicamente el derecho de acceso a sus propios datos de salud y a la vez incorpora otras dos funciones. Por un lado, el acceso al registro de accesos y, por otro lado, la posibilidad de ocultar datos clínicos que no quiere que sean conocidos por profesionales distintos de quienes habitualmente le atienden.

Respecto a la posibilidad de que el paciente pueda ocultar aquellos datos que no quiere que sean conocidos por profesionales distintos a los que habitualmente le atienden, el Ministerio de Sanidad señala que es una consecuencia del ejercicio de la autonomía del

---

[540] ABERASTURI GORRIÑO, U. *La Protección de Datos en la Sanidad.* Thomson Reuters Aranzadi, Navarra, 2013, p. 93.

[541] Ver al respecto: Informe Anual del Sistema Nacional de Salud 2015, op. cit.

[542] Vid. GALLEGO RIESTRA, S., op. cit., p. 17.

[543] Ibídem, pp. 17 y ss.

paciente y que la incorpora siguiendo los criterios del Documento del Grupo de Trabajo del Artículo 29 (WP 131)[544].

Desde el punto de vista doctrina[545], en el VII Congreso de Derecho y Salud, desde el sector médico y jurídico, entienden que el sistema a través del que se implementa la HCD ha de ser ágil y sencillo en el acceso, al servicio de ciudadanos y de los profesionales sanitarios. Esto supondrá un sistema más seguro de acceso que a la vez garantiza al ciudadano la confidencialidad de los datos de carácter personal relativos a su salud. En el referido Congreso, se han señalado algunas conclusiones[546] sobre las ventajas que la implementación de la HCD supondrá, que a continuación citaremos algunas de las más destacables.

(i) Hubo consense doctrinario con respecto a la implementación de la HCD, y que la misma supondrá la garantía de homogeneidad de las HC y por tanto su recopilación resultará estructurada y facilitará su consulta y su utilización. Esta circunstancia, también permitirá el acceso concurrente de profesionales, es decir, médicos que se encuentren físicamente en diversas Comunidades Autónomas y que se ven en la necesidad de atender al paciente desplazado y, por tanto, requerirán el acceso a su información clínica. Por ende, la HCD resultará totalmente accesible en tiempo y espacio. Asimismo, los contenidos de la HCD al ser informatizados serán plenamente legibles y sin posibilidad de comprensión errónea o falta de la misma por parte de otros profesionales sanitarios.

Por un lado, la HCD garantizará al ciudadano el acceso por vía telemática a los datos de salud, propios o de sus representados, que se encuentren disponibles en formato digital en alguno de los Servicios de Salud que se integran en el Sistema Nacional de Salud, siempre que cumplan los mínimos requisitos de seguridad establecidos para proteger sus propios datos contra la intrusión

[544] Documento de Trabajo del Artículo 29 de la Directiva 95/46/CE, (HME) 00323/07/ES, sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos, de 15 de febrero de 2007 (WP 131). Disponible en Internet: <https://www.apda.ad/system/files/wp131_es.pdf> [Consulta: 26 noviembre 2016].

[545] Ver al respecto las conclusiones de las mesas de trabajo del VII Congreso de Derecho y Salud, celebrado en Pamplona en noviembre de 2009, en: IRABURU ELIZONDO, M. "La Historia Clínica informatizada". *Derecho y Salud.* Vol. 17, Extraordinario XVII Congreso, Madrid, 2009, pp. 118-120.

[546] Ibídem.

ilegítima de quienes no hayan sido facultados para acceder. Esto también implica que el paciente puede conocer en todo momento quién ha accedido a su HCD.

Y, por otro lado, garantizará a los profesionales sanitarios, facultados por cada Servicio de Salud para esta función y autorizados en cada caso por el paciente, el acceso a determinados conjuntos de datos de salud, generados en una Comunidad Autónoma distinta de aquélla desde la que se requiere la información, siempre que el usuario o paciente demande sus servicios profesionales desde un centro sanitario público del Sistema Nacional de Salud. Esto minimizará y reducirá también los tiempos de consulta que se perdían en la búsqueda de diversos papeles.

(ii) Asimismo, y desde el punto de vista de las prescripciones médicas y los tratamientos a seguir, se intuye que la HCD facilitará la prescripción farmacéutica. La transferencia de la información del paciente automáticamente entre diferentes territorios acelerará su entrega y reducirá las posibilidades de realizar complementarios y prescripciones duplicadas.

(iii) También, la HCD evitará la repetición de pruebas diagnósticas al facilitar su almacenamiento y facilita a la vez, al personal sanitario el acceso a la información relevante para el paciente. También cabrá la posibilidad por parte de los médicos, de seguir el caso de un paciente a lo largo de todo el sistema de salud, independientemente del nivel de atención en que se trate o donde se encuentre físicamente. Por tanto, también permitirá mejorar la atención sanitaria a pacientes desplazados al contarse con todos los datos sanitarios relevantes.

(iv) Además, la HCD evitará los problemas que implican la documentación en papel: almacenamiento, custodia, seguridad. Facilita la ordenación y disminuye progresivamente el espacio necesario para su almacenamiento. Además de ello, supone un ahorro en el papel que ya no necesitarán los centros sanitarios.

(v) Al mismo tiempo, la automatización disminuirá los errores y mejorará la eficiencia y los cuidados que brindan los diferentes servicios de salud. Facilita el acercamiento entre la tarea asistencial y la de gestión.

(vi) Asimismo, y desde el punto de vista de la gestión sanitaria, el análisis de la información clínica, recogida a través de los diferentes centros de salud, servirá

de guía ante la necesidad de priorizar las inversiones en el campo de la salud pública.

(vii) Finalmente, destacan los expertos[547] que la HCD servirá de instrumento de ayuda para la investigación y la docencia mediante el fácil acceso a datos estadísticos y fuentes bibliográficas.

9. Inconvenientes que pueden plantearse en torno a la historia clínica digital.

Desde el punto de vista de la implementación y funcionamiento de la HCD pueden intuirse algunos inconvenientes que expondremos brevemente a continuación.

(i) En primer lugar, dada la cantidad de información que deberán almacenar los servidores, puede ocurrir que el sistema se vea sobrecargado y por tanto que se colapse. El volumen de datos que deberán soportar los ordenadores, es muy considerable en el sector sanitario, y, por ello, en algún momento dado, es probable que se genere una sobrecarga que impida el acceso del profesional médico a los datos del paciente. Aun así, en estos casos, y si el médico se encuentra ante una urgencia, con hacer las pruebas tradicionales al paciente, se le podrá brindar la atención sanitaria necesaria, hasta tanto el sistema informático esté en condiciones de proporcionar los datos de la HCD del paciente.

(ii) Otro inconveniente que se relaciona con el anterior, puede ser la pérdida brusca, total o parcial de los datos. En este caso, también consideramos que se deben tomar medidas de copias de seguridad, *backup*[548], etc., que hagan constantemente un resguardo de la información almacenada, y sobre todo que estos servidores que contengan estas copias se encuentren físicamente en España, para que nuestra legislación en materia de protección de datos sea la aplicable y no exista riesgo alguno al respecto.

[547] Ibídem.

[548] El *backup* es una palabra inglesa que en ámbito de la tecnología y de la información, es una copia de seguridad o el proceso de copia de seguridad. *Backup* se refiere a la copia y archivo de datos del ordenador de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.

(iii) También puede ocurrir que el sistema informático se “caiga”, que se sufra la pérdida temporal de la luz o cualquier fallo técnico que pueda amenazar seriamente el uso habitual de la HCD. Por tanto, para solventar los posibles problemas planteados se requerirá una respuesta técnica adecuada, capaz de dar solución a los problemas emergentes y la instalación de generadores de luz ante la falta de la misma.

(iv) Del mismo modo, podría considerarse un leve inconveniente que muchas Comunidades Autónomas tienen sus propios modelos de HCD. Sin embargo, la información relevante del paciente y lo que en definitiva permita un rápido conocimiento de su estado de salud por parte del médico, siempre está contenido en la información volcada en la HCD, independientemente del modelo según la Comunidad Autónoma que se trate. Además, este inconveniente podría solventarse utilizándose un modelo en concreto de HCD que todos los centros deban completar a fin de guardar coherencia a nivel nacional con los datos volcados sobre el paciente. Si no existe una metodología adecuada al cargar los datos, las búsquedas seguramente serán inexactas.

(v) También cabe resaltar que hay que ingresar muchos datos para cada paciente. En una primera fase de implantación, será lento y engorroso cargar los datos, pero esto evidentemente ocurriría en una primera fase porque luego el médico o el personal sanitario que acceda a la HCD irá actualizando la información contenida a medida que va atendiendo al paciente y dejando constancia de ello. Ante esto, quizás surja la poco probable, pero posible resistencia a utilizar una metodología distinta que obliga a estudiar cosas nuevas tecnológicas, por parte de los facultativos médicos y del personal sanitario a fin de su día a día laboral. Y ello, porque su implementación supone ciertas habilidades y actitudes necesarias por parte del profesional sanitario, puesto que ha de introducir los datos nuevos que recoja en la consulta del paciente, y ha de saber cómo utilizar las herramientas informáticas para introducir correctamente los datos.

(vi) Finalmente, debemos puntualizar que la incorporación del sistema digital en todos los centros sanitarios, requieren una inversión económica para el equipamiento informático. Asimismo, se requiere una inversión constante en el mantenimiento y en la renovación del equipo informático para que no devenga obsoleto.

Sin embargo, además de los inconvenientes que hemos descrito *ut supra*, también podemos hacer referencia a algunos posibles problemas en torno a la HCD relacionados con las personas que intervienen en el proceso de la misma. Al respecto, queremos señalar que la HC tradicional, en soporte de papel no conllevaba la implicación de un nuevo agente que resulta necesario en imprescindible en la gestión de la HCD, como, por ejemplo, puede ser el informático que será el encargado de traspasar los datos contenidos en la HC a la HCD.

Hemos de destacar que la informatización de nuestras HC, conlleva la necesaria adecuación a un sistema informático. Si bien el personal sanitario ha de estar capacitado para la incorporación de los ficheros al archivo informático, hemos de tener en cuenta que cualquier problema informático relacionado con el programa de las HCD, ha de ser solventado por un informático. Contemplación que la Ley no ha tenido en cuenta y que a nuestro criterio se debe de legislar sobre el particular.

No obstante, aquí cabe hacer dos puntualizaciones. Por un lado, debemos preguntarnos si será el mismo personal sanitario el que haga el trabajo de "*data entry*" para incorporar los datos de todas las HC de los pacientes de un centro de salud que se encuentren en papel, al ordenador para que formen parte de un fichero informático. Ante éste planteo tenemos dos respuestas posibles. En caso afirmativo, no conlleva mayor problema puesto que el personal sanitario está bajo el secreto profesional que la LOPD establece en su Artículo 7.6. Sin embargo, si la respuesta es negativa, entonces aquí se plantea el problema. Si será personal externo contratado para la realización de tales funciones, es evidente que tendrán acceso a nuestros datos de salud y estarán sujetos al deber de secreto que enunciamos en la primera parte de ésta Tesis, y según contempla el Artículo 10 de la LOPD. Pero nuevamente hemos de preguntarnos si podríamos incluirlos bajo ésta previsión legal. El Artículo 10 establece el deber de secreto para el responsable del fichero y los que intervengan en el tratamiento de los datos que en él se contenga. Asimismo, el Artículo 16.6 de la LAP, manifiesta que: *"El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto".* Pero, ¿un grupo de informáticos podría decirse que hacen un tratamiento de nuestros datos conforme a esta previsión legal, o simplemente mecanizan una documentación?

Asimismo, el Artículo 15.3 de la LAP, destaca la responsabilidad de los profesionales que intervengan en la cumplimentación de la HC. Entonces significa esto que, si los informáticos o el personal sanitario que se ocupe de trasladar la información del papel

al soporte informático se equivocan en algún aspecto referido a un dato de salud de un paciente, incurrirá en responsabilidad. Y en este caso, ¿hasta dónde llega esa responsabilidad? Y si el paciente sufre cualquier afección por culpa de ése error, ¿significa que el médico no tendrá responsabilidad alguna? Pero, ¿quién responde ante el paciente? Por su parte, el Artículo 14.2 de la LAP, hace responsable a cada centro de garantizar la seguridad de las HC. Y el Artículo 14.3 de la LAP, estable que las Administraciones sanitarias deben establecer los mecanismos que garanticen la autenticidad del contenido de la HC y de los cambios operados en ella, así como la posibilidad de su reproducción futura. Ante estas cuestiones planteadas, consideramos que se debe dar solución a través de una regulación específica que contemple tales supuestos.

Por otro lado, y en relación con éste particular, el Artículo 17 del anterior Código de Ética y Deontología Médica de 1999, establece *que "Los sistemas de informatización médica no comprometerán el derecho del paciente a la intimidad"*[549]*.* Pero en virtud de lo expuesto, vemos que no está claramente definida la función que ejerce el personal informático sobre las HCD de los pacientes, y por tanto al tratarse de los datos de salud, su derecho a la intimidad puede verse comprometido. Asimismo, dispone que: *"Los sistemas de informatización utilizados en las instituciones sanitarias mantendrán una estricta separación entre la documentación clínica y la documentación administrativa"*[550]*.* Frente a estas disposiciones éticas, nos cuesta ver la brecha separadora entre la documentación clínica y la documentación administrativa a la que se refiere el Código Ético, puesto que en la Historia Clínica constan la totalidad de los datos a que se refiere esta disposición, es decir, en un único documento que es la HCD.

10. Receta electrónica.

Además de resaltar la trascendencia sobre la funcionalidad de la HCD, a la que nos hemos referido en éste Capítulo, debemos mencionar la relevancia que ha de tener la creación de la receta electrónica en el sistema sanitario.

[549] Artículo 17.1, del Código de Ética y Deontología Médica de 1999. Éste Código se encuentra vigente con respecto a aquellas disposiciones que no contradigan al CDOMCE del 2011, op. cit. Disponible en Internet: <http://www.cgcom.es/sites/default/files/codigo_deontologia_medica.pdf> [Consulta: 22 noviembre 2016].

[550] Ibídem, Artículo 17.2.

La Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud[551], contempla, junto con la Ley 29/2006, de 29 de julio, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios[552], por primera vez en nuestro ordenamiento, la posibilidad de que las recetas médicas puedan extenderse o en su caso editarse en soporte informático, facilitando con ello la implantación de la denominada receta electrónica.

La receta médica electrónica es un procedimiento tecnológico que permite desarrollar las funciones profesionales sobre las que se produce la prescripción de medicamentos de manera automatizada, de manera que las órdenes de tratamiento se almacenan en un centro de datos al cual se accede desde el punto de dispensación para su entrega al paciente[553].

Esto facilitará a los ciudadanos la posibilidad de retirar con su receta electrónica y tarjeta electrónica (TSI) sus medicamentos en una farmacia situada en una Comunidad Autónoma distinta a aquella en la que se haya prescrito el fármaco. Su implementación consiste en dispensar recetas *on-line*, es decir, persigue la creación de un sistema de prescripción y entrega de recetas electrónicas en el ámbito del Sistema Nacional de Salud. Lo que implica la posibilidad de acceder electrónicamente a las órdenes de prescripción de medicamentos desde cualquier punto de dispensación del país.

CARNICERO GIMÉNEZ DE AZCÁRATE[554] explica que la receta electrónica consiste en un sistema de información que relaciona al médico con la oficina de farmacia y a ésta con la entidad responsable del pago de la prestación, que suele ser el servicio de salud.

---

[551] Artículo 33, de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, op. cit.

[552] Artículo 77, de la Ley 29/2006, de 29 de julio, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios (BOE núm. 178, 27.07.2006).

[553] ESTEBAN GONZALO, S. "Sistema de información del Sistema Nacional de Salud". *Revista Índice.* Instituto de Información Sanitaria. Enero 2007, pp. 6-8. Disponible en internet: <http://www.revistaindice.com/numero20/p6.pdf> [Consulta: 26 noviembre 2016].; SÁNCHEZ-CARO, J. "La Ley de Protección de Datos e innovaciones tecnológicas farmacéuticas". *Revista de Administración Sanitaria*. Vol. V, núm. 19, julio-septiembre 2001.

[554] CARNICERO GIMÉNEZ DE AZCÁRATE, J. "Protección de datos y receta electrónica", en PÉREZ GÓMEZ, J. M. *El Derecho a la Protección de Datos en la historia clínica y la receta electrónica.* Thomson Reuters, Madrid, 2009, p. 22.

A pesar de que en el derecho español no se contiene una definición sobre la receta electrónica, algunas Comunidades Autónomas[555] ya han legislado sobre ella, y de las diferentes iniciativas llevadas a cabo hasta el momento, según puntualizan SUBIRÀ y PRADELL DE MONTAGUT[556], cabe conceptuar como "sistema de receta electrónica", a aquella aplicación que permita a los facultativos médicos legalmente capacitados, prescribir por medios electrónicos la medicación a los pacientes para la posterior dispensación por las farmacias.

10.1. Ventajas de su implementación.

Con la introducción de la receta electrónica podemos apreciar a grandes rasgos, dos ventajas genéricas. Por un lado, desde el punto de vista de los pacientes, supone una mejora instrumental, como así también, supone una mejora en los procedimientos que debe permitir la integración, la seguridad y la fiabilidad de la información. De ésta manera, se evitarán errores y se aportará seguridad a la prescripción médica, con la

[555] En Andalucía se ha legislado sobre la receta electrónica en particular, a través del Decreto 181/2007, de 19 de junio, por el que se regula la receta médica electrónica, de Andalucía (BOJA núm. 123, 22.06.2007). En su Artículo 2, se define la Receta electrónica, estableciendo que: *"Se entiende por receta médica electrónica, conforme a lo previsto en la normativa vigente, la extendida en soporte informático por el profesional sanitario facultado para ello. En esta receta dicho profesional podrá prescribir los medicamentos y productos sanitarios, incluidos en la prestación farmacéutica del Sistema Sanitario Público de Andalucía, a los pacientes con derecho a esta prestación, para su dispensación por las farmacias".* En Cataluña también se ha legislado sobre el tema, a través del Decreto 159/2007, de 24 de julio, por el que se regula la receta electrónica y la tramitación telemática de la prestación farmacéutica a cargo del Servicio Catalán de Salud (DOGC núm. 4934, 26.07.2007). En su Artículo 2.c), define de forma muy escueta la receta electrónica, estableciendo que es *"la receta en soporte electrónico".* En Extremadura disponen del Decreto 93/2009, de 24 de abril, por el que se regula la implantación de la receta electrónica en el ámbito del Sistema Sanitario Público de Extremadura (DOE núm. 82, 30.04.2009). En su Artículo 2.a) define a la receta electrónica, consagrando que es: la *"receta extendida en soporte informático en el acto de prescripción, que permite la dispensación por las Oficinas de Farmacia de los medicamentos y productos sanitarios prescritos e incluidos en la prestación farmacéutica del Sistema Sanitario Público de Extremadura a los ciudadanos con derecho a esta prestación"*. También, en Galicia disponen del Decreto 206/2008, de 28 de agosto, de receta electrónica, de Galicia (DOG núm. 181, 18.11.2008). Define su Artículo 2.a) a la receta electrónica, estableciendo que: *"es el documento electrónico por el que el profesional sanitario facultado para eso prescribe a los/las pacientes con derecho a prestación farmacéutica medicamentos y productos sanitarios para su dispensación en las oficinas de farmacia".*

[556] SUBIRÀ, C.; PRADELL DE MONTAGUT, A. "La receta electrónica en España". *Revista Garrigues Abogados y asesores Tributarios.* Barcelona, 2003, pp. 1-5.

resultante mejora de la protección de la salud de los pacientes. Por otro lado, y desde el punto de vista de las entidades responsables de la prestación farmacéutica, la receta electrónica permitirá mejorar el control y la gestión del gasto farmacéutico y disponer de información necesaria para la planificación y gestión sanitaria.

La introducción de la receta electrónica supone que los datos de la prescripción se incorporen automáticamente a una base de datos integrada en un sistema informático que permitirá generar a favor del paciente lo que se podría denominar una "cuenta farmacéutica"[557], de la que se podrá disponer cuando se dirija a una oficina de farmacia para solicitar la dispensación de los productos incluidos en la prestación farmacéutica.

La extensión de la receta electrónica, pretende evitar a los enfermos crónicos el tener que acudir de forma regular a la consulta para que el médico le extienda la receta que requieren periódicamente. Consideramos que este hecho evitará la saturación en las consultas de atención primaria, evitándose así consultas que tienen por objetivo la simple extensión de una receta médica habitual. Asimismo, redundará en el beneficio de poder incrementar el tiempo de las consultas de los pacientes que lo precisen. Por lo tanto, la atención sanitaria podrá ser de mayor calidad puesto que el facultativo médico tendrá la ventaja de ofrecer mayor tiempo de atención a los pacientes que lo requieran.

También, la receta médica electrónica también permitirá agilizar el trámite del control sanitario mediante el visado o cualquier otro medio de control que pueda establecerse para conseguir una utilización más racional de determinados medicamentos o productos sanitarios, en la medida que se pueda constatar automáticamente que se cumplen los requisitos establecidos para dichos controles.

Aunque, debemos señalar que el sistema de receta electrónica debe garantizar el derecho de toda persona a su intimidad y a la confidencialidad de sus datos clínicos, poniéndose especial énfasis normativo en el deber del secreto profesional de los médicos y farmacéuticos y el acceso a los datos por parte de la administración sanitaria y las oficinas de farmacia con el fin de gestionar la prestación farmacéutica.

Por ello, consideramos que, será ineludible establecer los requisitos bajo los cuales podrán extenderse en soporte informático las recetas de los medicamentos y de los productos sanitarios incluidos en la prestación farmacéutica, así como los

[557] Exposición de motivos, del Decreto 159/2007, de 24 de julio, del Servicio Catalán de Salud, op. cit.

procedimientos y requisitos necesarios para la dispensación de las mismas por parte de las oficinas de farmacia, siempre en aras de proteger los datos de los pacientes, preservando su intimidad y confidencialidad.

11. La necesidad de una Ley para regular sobre los datos de salud contenidos en la historia clínica digital y en la receta electrónica.

Por un lado, el derecho a la vida que implica la atención sanitaria, y ésta para poder llevarse a cabo, de manera necesaria requiere datos de salud de las personas, y, por otro lado, el derecho a la intimidad personal que exige la confidencialidad, intimidad y secreto de esta información personal, constituyen son dos derechos constitucionales que asiduamente pueden resultar confrontados, pero deben ser adecuadamente armonizados. Es posible que el derecho a la vida y a la salud pueda primar en ocasiones sobre el derecho a la intimidad de las personas, pero también la intimidad personal obliga a modificar muchos modelos de gestión sanitaria que actualmente tenemos en España. Reconoce TRONCOSO REIGADA[558] al respecto que: "*no se trata de optar entre el derecho a la intimidad y una eficaz atención sanitaria sino buscar el respeto a todos ellos teniendo en cuenta el principio de proporcionalidad"*.

El tratamiento de los datos de carácter personal para la finalidad de la prestación del servicio sanitario, sostiene APARICIO SALOM[559], plantea numerosas peculiaridades que, incluso, sería oportuno que se regulara en una Ley específica, adecuadamente y de forma integral, tanto la forma de confección de la HCD por el profesional médico y la información que debe y no debe integrarse en dicho documento, como el derecho del paciente y disponer de la HC, en cuanto a poder rectificar y exigir la cancelación de los datos y, finalmente, el régimen de uso de la HC por profesionales de la medicina y, en su caso, por terceros.

El hecho de que la HCD incorpore datos personales, el que una pluralidad de sujetos pueda tener acceso a ella, el desarrollo de nuevas tecnologías, la cantidad de

[558] TRONCOSO REIGADA, A. *La confidencialidad de la historia clínica.*, op. cit., p. 49.

[559] APARICIO SALOM, J. *Estudio sobre la Ley Orgánica de Protección de Datos de carácter personal.* 3ª Edición, Aranzadi-Thomson Reuters. Navarra, 2009, p. 317.

documentos que incorpora y la necesidad de un manejo eficiente, hacen precisa la regulación específica, desde nuestro punto de vista, de esta materia[560].

Asimismo, la receta electrónica también contiene datos personales que deben ser protegidos por una normativa a fin de que no se vulnere el derecho del paciente a su intimidad y a su confidencialidad, estableciéndose para ello, desde nuestro punto de vista, límites en el acceso a los datos por parte de la administración sanitaria y de las oficinas de farmacia, como así también sobre deber del secreto profesional de los médicos, farmacéuticos y cualquier persona que acceda a ellos en base a una disposición legal.

En el XVII Congreso sobre Derecho y Salud[561], celebrado en Pamplona en noviembre de 2008, se puso de manifiesto que a día de hoy existe una multiplicidad normativa dispersa que contiene regulaciones en esta materia, por lo que cabe plantear si este modelo es el más adecuado para los futuros desarrollos, o si encajan mejor otros, como podrían ser la adaptación expresa del grupo normativo de la LOPD al ámbito sanitario o su remisión en bloque a la normativa sanitaria. Asimismo, las Conclusiones del Congreso respaldan nuestra teoría al sostener que:

> El desarrollo normativo en esta materia debe asegurar el equilibrio entre los derechos implicados -a la protección de la salud, a la intimidad y a la protección de los datos-, sin que la garantía de los dos últimos derechos fundamentales suponga un impedimento para la consecución de una historia clínica única para el mayor ámbito geográfico posible.

12. La tarjeta sanitaria individual electrónica.

La tarjeta sanitaria electrónica es el documento que identifica individualmente a los usuarios ante el Sistema Sanitario. Además, sirve para facilitar el acceso a la HCD, para prescribir mediante receta electrónica, y para retirar los medicamentos en la

[560] En el mismo sentido se manifiesta el Preámbulo del Decreto 101/2005 de 22 de diciembre, por el que se regula la historia clínica, de Castilla y León (BOCyL núm. 249, 28.12.2005).

[561] ORTIZ DE ELGUEA, P. "Historia Clínica: su regulación en la legislación sanitaria y en la protección de datos de carácter personal". *Derecho y Salud.* Vol. 17, Extraordinario XVII Congreso sobre Derecho y Salud, Pamplona, noviembre 200, p. 124.

farmacia. Asimismo, según refiere BARRANCO ORTEGA[562], aporta criterios para la asignación de recursos económicos, humanos, físicos, tecnológicos, etc.

Por tanto, a la vez que es un documento que refleja la identidad de una persona que tiene acreditado el derecho a recibir la atención sanitaria pública, en la medida que pueda almacenar información o incluso contener un microprocesador que integre un sistema de firma electrónica, puede constituir un elemento valioso para la atención de pacientes en situaciones de urgencia[563].

A través de la implementación de la HCD, se pretende evitar situaciones tales como que, al trasladarse fuera de nuestra Comunidad Autónoma, o al salir de España, los pacientes no puedan acceder a medicamentos esenciales que hayan agotado, olvidado o perdido, no puedan comunicar detalles sobre su estado de salud a profesionales sanitarios que desconocen su lengua y la prescripción de tratamientos sin el previo conocimiento por parte de los médicos de los datos relevantes en su HC.

La Tarjeta Sanitaria Individual del Sistema Nacional de Salud (TSI-SNS) representa el sistema normalizado de identificación de todo usuario al derecho a la protección de la salud en el conjunto del Sistema Nacional de Salud. Dicha tarjeta identificativa es la que permite el acceso a los datos clínicos y administrativos de cada persona cada vez que acude a un centro del sistema sanitario público[564]. La TSI es emitida por cada

[562] BARRANCO ORTEGA, V. (22.10.2009) "La Tarjeta Sanitaria. Base de Datos población protegida SNS". Ponencia presentada en el 3er Foro sobre el Sistema de Información del SNS, Ministerio de Sanidad y Política Social, Madrid, 2009. <http://www.msps.es/estadEstudios/estadisticas/sisInfSanSNS/3ForoSISNS/docs/VictorBarranco_ponencia3Foro.pdf> [Consulta: 29 noviembre 2016].

[563] PÉREZ GÓMEZ, J. M., op. cit., p. 625.

[564] Con el objetivo de poder reconocer a cada persona de manera segura y unívoca, el Ministerio de Sanidad, Servicios Sociales e Igualdad coordina una Base de Datos de Población Protegida del Sistema Nacional de Salud (BDPP-SNS) y genera para cada usuario un código de identificación personal, único y vitalicio. El código actúa como clave de vinculación de cuantos otros códigos de identificación personal autonómicos pueda tener asignados el usuario a lo largo de la vida. Esto va a permitir la posterior recuperación de la información clínica que se encuentre asociada a dichos códigos. La BDPP-SNS incluye, además de a las personas aseguradas y beneficiarias según el 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 (BOE núm. 98, 24.04.2012), a aquellas otras que por diferentes circunstancias tienen acceso a la atención sanitaria del Sistema Nacional de Salud, asignándoles, igualmente, el código de identificación personal. Fuente: Informe Anual del Sistema Nacional de Salud 2015, op. cit.

Comunidad Autónoma para la población residente en su territorio, pero con dicha tarjeta el paciente puede acudir a cualquier otro centro del Sistema Nacional de Salud y ser atendido por otros facultativos, que tendrán acceso a su HCD. Por lo tanto, el formato de la TSI es válido para todo el Sistema Nacional de Salud. Su incorporación se hizo en el año 2013 con una serie de datos básicos comunes y una banda magnética homologada que facilitan su uso en todas las comunidades autónomas.

Conclusión.

La situación social demuestra que la movilidad de los ciudadanos es cada vez más usual, y ello hace necesaria la posibilidad de disponer de la información médica del paciente cuando las necesidades de atención sanitaria se producen fuera de la Comunidad Autónoma en la que se ha generado esta información. Sin embargo, y después de haber analizado la normativa, la doctrina y las manifestaciones del Ministerio de Sanidad, y adelantando las conclusiones de ésta Tesis, destacamos que si bien existe una necesidad real de informatizar los datos de salud, con las consiguientes ventajas que hemos analizados en relación con la HCD, la receta electrónica y la tarjeta sanitaria electrónica, consideramos que debe otorgarse una protección mayor, más definida y específica que ampare al paciente en lo que a su intimidad y confidencialidad respecta.

Probablemente, el futuro en el entorno de las HCD, obligará a los legisladores a idear garantías legales frente a las tecnologías de la información, destacando la necesidad de una Ley específica en materia de protección de datos sanitarios que regule de manera exclusiva su régimen, su tratamiento y las medidas de seguridad que se deben aplicar, para evitar intromisiones en el aspecto íntimo y personal de la persona, pero permitiéndosele a la vez, el goce de una atención médica personalizada, de calidad, rápida y eficiente, evitando el acceso a nuestra HCD a terceros que no se ajuste adecuadamente a los fines asistenciales que la HCD de por sí involucra, siendo más sosegados a la hora de permitir accesos para fines científicos, de estadísticas, para investigaciones de efectos de según qué fármaco, etc., evitando que según qué información contenida en la HCD caiga en manos no deseadas.

SEGUNDA PARTE

LOS DATOS DE SALUD EN EL MARCO EUROPEO - REGLAMENTO (UE) 2016/679 Y EL NUEVO MODELO DE PRIVACIDAD. BIG DATA EN SALUD.

CAPÍTULO I

Antecedentes en la Unión Europea en el marco de la regulación de los datos personales, objetivos y nuevos retos. Futuro de la protección de datos: análisis del Reglamento (UE) 2016/679 y el nuevo modelo de privacidad.

SUMARIO: 1. Principales problemas que se presentan en materia de protección de datos en la UE en torno a la Directiva 95/46/CE. 1.1. El impacto de las nuevas tecnologías. 1.2. El reforzamiento del mercado interior de la protección de datos. 1.3. La seguridad de las personas en el tratamiento de sus datos. 1.4. La globalización y la mejora de las transferencias internacionales de datos. 2. Objetivos estratégicos de la Comisión Europea para la adopción del Reglamento de Protección de Datos. 3. El Reglamento General de Protección de Datos. Nuevas perspectivas legales en la UE en el marco de la regulación de los datos personales. a) Fundamento legal sobre el que se asienta el Reglamento General de Protección de Datos. b) Objetivo de la reforma. 3.1. Diferencias de enfoque del RGPD con respecto a la Directiva 95/46/CE. 3.2. Convivencia con la LOPD. 4. Los Principios sobre los que se asienta el RGPD. 4.1. La licitud de tratamiento. 4.2. La transparencia. 4.3. La información. 4.4. Especial mención al consentimiento del interesado. 4.5. Principio de Responsabilidad "proactiva". 5. Derechos de los ciudadanos en torno al RGPD. 5.1. Derecho de acceso. 5.2. Derecho a la rectificación y al olvido. 5.3. Nuevo derecho a la portabilidad de datos. a) Excepciones al derecho a la portabilidad de los datos. 6. Alcance territorial del RGPD. 6.1. Transferencias a terceros países. 7. Margen de maniobra en algunos ámbitos permitidos por el RGPD. 8. Los datos de salud en el RGPD. 8.1. Obligaciones específicas sobre el tratamiento de los datos de salud en el RGPD. 8.2. Nuevas categorías de datos sensibles: datos biométricos y datos genéticos. 8.3. Tratamiento de los datos en el ámbito sanitario. 9. Nivel de protección y seguridad. 9.1. Notificación de violaciones de seguridad. 10. La nueva figura del Delegado de Protección de Datos.

Introducción.

La vertiginosa evolución tecnológica y la globalización, constituyen dos elementos que han planteado nuevos retos para la protección de los datos personales. Tanto a nivel nacional como, en la UE, e incluso, extendiéndose al ámbito internacional, es notorio el

incremento del intercambio transfronterizo de datos personales entre los operadores públicos y privados, incluidas las personas físicas, las asociaciones y las empresas, como resultado de la integración económica y social.

Estos avances requieren un marco más sólido y coherente para la protección de datos en la UE, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.

Estas circunstancias llevan a plantearse la necesidad en la uniformización normativa, al menos, en la UE donde formamos parte, a fin de que dichos avances no resulten vulneradores de un derecho fundamental, como lo es, la protección de datos. En base a ello, y con el fin de avalar un nivel análogo y elevado de protección de las personas físicas por lo que se refiere al tratamiento de los datos personales, debe ser equivalente en todos los Estados miembros, a la vez que se deben superar los obstáculos relacionados con la circulación de datos personales dentro de la UE, el nivel de protección de los derechos y la libertad de las personas físicas.

Estas circunstancias han dado lugar a la aprobación del Reglamento General de Protección de Datos[565] (en adelante, RGPD). El RGPD introduce varias novedades englobadas en un nuevo modelo de protección de datos para Europa. Esta nueva ordenación legal, pasa de la gestión de los datos, al uso responsable de la información. Esto conllevará dar un mayor protagonismo a una figura de nueva creación que es el Delegado de Protección de Datos en adelante, DPO), en el que recaerá la responsabilidad de determinar y adoptar las medidas que sean necesarias para garantizar la adecuada protección de los datos. Además de esta gran novedad, el RGPD introduce en el marco de los datos de salud, dos nuevas categorías como los datos biométricos y genéticos, asimismo reformula algunos de los principios que inspiran la protección de datos e introduce otros nuevos, y reformula los derechos de los interesados con la introducción de algunas aportaciones novedosas que estudiaremos en el presente Capítulo.

[565] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, (Reglamento General de Protección de Datos) (DOUE L 119, 4.05.2016, pp. 1-88).

1. Principales problemas que se presentan en materia de protección de datos en la UE en torno a la Directiva 95/46/CE.

El texto de la vigente Directiva 95/46/CE[566], que será sustituida por el RGPD[567], fue transpuesto en su momento por cada uno de los Estados miembros con cierto margen de maniobra, situación que ha dado lugar a una serie de diferencias entre las normas nacionales y, en ocasiones, a diferentes interpretaciones del mismo texto, lo cual evidenciaba unas importantes diferencias entre los Estados miembros a la hora de aplicar el derecho comunitario vigente en la materia.

Aunque es menester destacar que desde nuestro punto de vista, el marco jurídico actual sigue siendo adecuado por lo que respecta a los objetivos y principios que sirvieron de base a la Directiva 95/46/CE[568], sin embargo, sostenemos que la

[566] Directiva 95/46/CE, op. cit.

[567] El RGPD entrará en vigor el próximo 25 de mayo de 2018.

[568] La posibilidad de un nuevo Reglamento que venga a unificar la legislación europea en materia de protección de datos, es una iniciativa que ha sido resultado de una amplia consulta a todas las partes interesadas sobre la revisión del actual marco jurídico para la protección de datos de carácter personal, que se prolongó durante más de cuatro años e incluyó una conferencia celebrada en mayo de 2009, además de dos fases de consulta pública: a) del 9 de julio al 31 de diciembre de 2009, la Consulta sobre el marco jurídico para el derecho fundamental a la protección de datos de carácter personal. La Comisión Europea recibió 168 respuestas, 127 de personas físicas, organizaciones y asociaciones empresariales, y 12 de autoridades públicas; y b) del 4 de noviembre de 2010 al 15 de enero de 2011, la Consulta sobre el enfoque global de la Comisión Europea sobre la protección de datos de carácter personal en la UE. La Comisión Europea recibió 305 respuestas, de las cuales 54 procedían de ciudadanos, 31 de autoridades públicas y 220 de organizaciones privadas, especialmente de asociaciones empresariales y organizaciones no gubernamentales. Mediante su Resolución de 6 de julio de 2011 el Parlamento Europeo aprobó un informe que respaldaba el enfoque adoptado por la Comisión Europea de cara a reformar el marco de la protección de datos. En sus conclusiones adoptadas el 24 de febrero de 2011, el Consejo de la UE manifestó su apoyo en general a la intención de la Comisión Europea de reformar el marco de protección de datos y mostró su acuerdo con muchos elementos de la posición de la Comisión Europea. También el Comité Económico y Social Europeo se mostró a favor del objetivo de la Comisión Europea de garantizar una aplicación más coherente de las normas de la UE en materia de protección de datos en todos los Estados miembros y una revisión adecuada de la Directiva 95/46/CE. Durante la Consulta sobre el enfoque global de la Comisión Europea sobre la protección de datos de carácter personal en la UE, que tuvo lugar en el año 2010 y 2011, una gran mayoría de los participantes se mostró de acuerdo en que los principios generales siguen siendo válidos, si bien es necesario adaptar el marco vigente para responder mejor a los retos que plantea el rápido desarrollo de las tecnologías (especialmente en

fragmentación en cómo se aplica en la UE la protección de datos de carácter personal, existiendo diferencias en los niveles de protección de los datos personales que se deben a la disparidad existente entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros, genera inseguridad jurídica y la percepción generalizada de la opinión pública[569] de que existen riesgos significativos, especialmente por lo que se refiere a la actividad en línea "*online*" y a los datos sobre salud.

---

línea "online") y la globalización creciente, al tiempo que se mantiene la neutralidad tecnológica del marco jurídico. Véase al respecto: Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Un enfoque global de la protección de los datos personales en la Unión Europea. Bruselas, 4.11.2010 COM (2010) 609 final. Disponible en Internet: <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_es.pdf> [Consulta: 17 septiembre 2015]. También España contestó la Consulta de la Comisión Europea, a través de la AEPD, en la Contribución de la Agencia Española de Protección de Datos a la consulta de la Comisión Europea sobre un enfoque global de la protección de datos personales en la Unión Europea. Disponible en Internet: <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/aepd_dpa_es.pdf pdf> [Consulta: 17 septiembre 2015].

[569] El propósito de este estudio fue obtener información sobre la divulgación de información personal por parte de los europeos, con un enfoque más especial en Internet. Asimismo, se pretendió valorar en nivel de información, de conocimiento y la percepción que los ciudadanos europeos tenían sobre sus datos personales, sobre la forma de protegerlos, y la regulación jurídica que les gustaría al respecto. Las conclusiones del Eurobarómetro, demostraron que en general los ciudadanos europeos estaban bastante preocupados por su privacidad. Muchos de ellos habían sufrido usurpación de identidad *online*, robos de datos, tarjetas bancarias duplicadas, ofertas comerciales vinculadas a sus búsquedas en Internet, etc. Sin embargo, la mayoría reconoció que el uso de Internet, redes sociales y aplicaciones de móviles en todas las variantes, es parte de la vida diaria. Por lo tanto, si conocen quién es el responsable de la información que proporcionan, estarían más seguros y también casi todos encuestados coincidieron en que estaban a favor de una legislación armonizada en la UE, y que se sentirían más seguros si el control lo ejerciera la Comisión Europea y otros órganos en relación con la protección de datos. Véase al respecto, las encuestas: Eurobarómetro especial (EB) 359, *Data Protection and Electronic Identity in the EU* (Protección de datos e identidad electrónica en la UE). Fecha de publicación: junio 2011. Disponible en internet (versión en inglés): <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> [Consulta: 17 de septiembre 2015].; Eurobarómetro especial (EB) 404, *European citizens' digital health literacy* (La alfabetización digital de la salud de los ciudadanos europeos). Fecha de publicación: noviembre 2014. Disponible en internet (versión en inglés): <https://open-data.europa.eu/es/data/dataset/S1073_79_4_404> [Consulta: 17 septiembre 2015].

Esta circunstancia ha dado lugar a que el tratamiento de los datos personales, y las medidas de seguridad relativas a la protección de los derechos y libertades de las personas físicas, que se aplican en los distintos Estados miembros, puedan impedir la libre circulación de los datos de carácter personal en la UE. Por tanto, éste contraste en los niveles de protección, se debe a la existencia de divergencias en la ejecución y aplicación de la Directiva 95/46/CE, que analizaremos en los siguientes epígrafes.

En esencia, se evidenció, que en la UE se debe garantizar que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal, ha de ser coherente y homogénea en todos los Estados miembros, según puso de relieve el Supervisor Europeo de Protección de Datos[570] (en adelante, SEPD).

Por todo ello, consideramos, que era el momento adecuado para establecer un marco legal más sólido y análogo en materia de protección de datos en la UE, con una aplicación estricta que permita el desarrollo de la economía digital en el mercado interior, que otorgue a los ciudadanos el control sobre sus propios datos y venga a reforzar la seguridad jurídica y la práctica de los operadores económicos y las autoridades públicas.

Frente a estas evidencias, la UE realizó una serie de consultas[571] para individualizar los problemas a fin de darles solución legal. A raíz de los diversos resultados que se

[570] El éste sentido, BUTARELLI, G. (SEPD) manifestó que: *"En una época en la que la protección de los datos y la legislación sobre la privacidad proliferan en todo el mundo, esto debería ser una plataforma para ampliar la construcción de puentes hacia otras zonas del mundo, lo que permitiría aumentar el diálogo y la cooperación con todos los países que se enfrentan al mismo desafío digital".* Conclusiones del Dictamen del Supervisor Europeo de Protección de Datos, sobre el cumplimiento efectivo de la legislación en la economía de la sociedad digital (DOUE C 463/8, 13.12.2016) Disponible en Internet: <https://edps.europa.eu/sites/edp/files/publication/17-01-13_big_data_ex_summ_es.pdf> [Consulta: 2 abril 2017].

[571] Además de la Consulta sobre el marco jurídico para el derecho fundamental a la protección de datos de carácter personal y la Consulta sobre el enfoque global de la Comisión Europea sobre la protección de datos de carácter personal en la UE (véase nota al pie 562), se realizaron múltiples reuniones, debates, estudios e investigaciones: en junio y julio de 2010 se organizaron actos específicos con las autoridades de los Estados miembros y operadores del sector privado, así como con organizaciones de consumidores y entidades dedicadas a la protección de datos y la intimidad. Disponible en internet: <http://ec.europa.eu/justice/newsroom/data-protection/events/100701_en.htm> [Consulta: 17 de septiembre de 2015]. En noviembre de 2010, la Vicepresidenta de la Comisión Europea Viviane Reding organizó una mesa redonda sobre la reforma de la protección de datos. El 28

obtuvieron en las múltiples y diversas consultas realizadas por la UE sobre la situación actual de la protección de datos, se pudieron extraer varias conclusiones; entre ellas, que los principios fundamentales de la Directiva 95/46/CE siguen siendo válidos y que conviene preservar su neutralidad desde el punto de vista tecnológico. No obstante, se identificaron varios problemas y retos específicos, a los que a continuación nos referiremos.

---

de enero de 2011 la Comisión Europea y el Consejo de Europa organizaron una conferencia de alto nivel con el fin de debatir cuestiones relacionadas con la reforma del marco jurídico de la UE y con la necesidad de establecer unas normas de protección de datos comunes a escala mundial. Disponible en internet: <http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day2011_en.asp> [Consulta: 17 de septiembre de 2015]. Las presidencias húngara y polaca del Consejo acogieron sendas conferencias sobre protección de datos los días 16 y 17 de junio de 2011 y el 21 de septiembre de 2011, respectivamente. A lo largo de 2011 se celebraron talleres y seminarios consagrados específicamente a temas concretos. En enero, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), que se ocupa de temas de seguridad relacionados con las redes de comunicación y los sistemas de información, organizó un taller sobre las notificaciones de la violación de datos en Europa. Disponible en internet: <http://www.enisa.europa.eu/act/it/data-breach-notification> [Consulta: 17 de septiembre de 2015]. En febrero, la Comisión Europea organizó un taller con las autoridades de los Estados miembros para debatir sobre cuestiones de protección de datos en el ámbito de la cooperación policial y judicial en materia penal, incluida la ejecución de la Decisión Marco, y la Agencia de los Derechos Fundamentales celebró una reunión consultiva con los distintos actores sobre la «Protección de Datos y la Intimidad». El 13 de julio de 2011 tuvo lugar un debate sobre cuestiones clave de la reforma con las autoridades nacionales de protección de datos. Se consultó a los ciudadanos de la UE mediante un Eurobarómetro realizado en noviembre-diciembre de 2010. Disponible en internet: <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> [Consulta: 17 de septiembre de 2015]. Asimismo, se pusieron en marcha algunos estudios, destacando el *"Study on the economic benefits of privacy enhancing technologies"* (Estudio sobre los beneficios económicos de las tecnologías que mejoran la privacidad); *"Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments"* (Estudio comparativo de diferentes enfoques de los nuevos desafíos de la privacidad, en particular a la luz de los avances tecnológicos), enero de 2010. El Grupo de Trabajo del Artículo 29 emitió diversos dictámenes y realizó aportaciones útiles a la Comisión Europea, que pueden consultarse en Internet: <http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm> [Consulta: 17 de septiembre de 2015]. El Supervisor Europeo de Protección de Datos también emitió un dictamen general sobre los temas planteados en la Comunicación de la Comisión de noviembre de 2010. Disponible en internet: <http://www.edps.europa.eu/EDPSWEB> [Consulta: 17 de septiembre de 2015].

1.1. El impacto de las nuevas tecnologías.

Existe una improrrogable necesidad de clarificar y precisar la aplicación de los principios de la protección de datos a las nuevas tecnologías, con el fin de garantizar una protección real y efectiva de los datos personales, cualquiera que sea la tecnología utilizada para tratar estos datos, y que los responsables del tratamiento de los datos tengan plena conciencia de las implicaciones de las nuevas tecnologías en la protección de datos.

Vivimos en una era donde impera en un marco legal superado por los diferentes progresos tecnológicos producidos en los últimos 20 años, fundamentalmente, por los avances científicos, las comunicaciones y sobre todo Internet, circunstancias que hemos puesto de manifiesto a lo largo de ésta investigación. La rápida evolución tecnológica ha supuesto nuevos retos para la protección de los datos personales. Se ha incrementado enormemente la magnitud del intercambio y la recogida de datos. Cada vez que se abre una cuenta bancaria online, se une a una red social en Internet, se reserva un vuelo en línea, se solicita cita al médico de cabecera, se nos remite una baja médica, una receta electrónica, etc. se está facilitando información personal esencial, como el nombre, dirección, número de tarjeta de crédito, número de la tarjeta de la seguridad social, según el caso. Los datos propiciados son muchos y absolutamente personales. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de desarrollar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. Hoy en día somos testigos de que la tecnología ha transformado tanto la economía como la vida social[572].

En el contexto social actual, es posible invadir la privacidad de las personas hasta unos límites que hace pocas décadas era insospechado. Hoy en día es posible conocer el contenido de un correo electrónico, de las llamadas de los teléfonos móviles que están al alcance de todos -incluso menores de edad-, de mensajes de texto sms o de mensajes de *whatssapp*, el contenido que recogen las apps de salud, etc.

[572] Exposición de Motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Comunicación COM (2012) 11 final 25.01.2012).

Ya en el año 2008, el doctrinario PIÑAR MAÑAS[573] se cuestionaba acerca de la realidad o no de la existencia de la privacidad. Los dispositivos de radiofrecuencia conocidos como RFID (identificadores por radiofrecuencia) son capaces de determinar la localización de una persona, se encuentre en cualquier lugar del mundo[574]. Sostiene PIÑAR MAÑAS[575] que la nanotecnología[576] permite actualmente crear dispositivos capaces de captar grandes cantidades de información de una forma totalmente desapercibida, como es el caso de los nanorobots[577]. Además de estos riesgos mencionados, existe otro gran inconveniente que estos avances tecnológicos suponen: el coste. Cada vez que avanza la tecnología, su coste se reduce. Al respecto, señala PIÑAR MAÑAS[578], que el coste económico de los avances tecnológicos y de los nuevos dispositivos es cada vez menor, lo que facilita aún más su uso e implantación. Evidentemente esto hace más accesible y extensible su uso a múltiples personas, lo cual dificulta un control sobre la utilización de esa información obtenida.

A pesar de que es evidente que la tecnología va por delante de la normativa, sí que es preocupante desde nuestro punto de vista, lo fácil que puede resultar acceder o conocer información personal con éstas nuevas herramientas digitales, algunas de ellas prácticamente imperceptibles, o incluso indetectables, como pueden ser aplicaciones en los móviles. Evidentemente son múltiples los ejemplos que pueden citarse, pero requerirían otro trabajo de investigación específico. Pero entonces, la cuestión es poner

---

[573] Vid. PIÑAR MAÑAS, J. L. *¿Existe la privacidad? Inauguración Curso Académico 2008-2009.* CEU Ediciones, Universidad CEU San Pablo, Madrid, 2008.

[574] Ibídem, p. 14.

[575] Ibídem, pp. 17 y ss.

[576] La nanotecnología trabaja con materiales y estructuras cuyas magnitudes se miden en nanómetros, lo cual equivale a la milmillonésima parte de un metro. La nanotecnología comprende el estudio, diseño, creación, síntesis, manipulación y aplicación de materiales, aparatos y sistemas funcionales a través del control de la materia a nanoescala. En biología y medicina, los nanomateriales se emplean en la mejora del diseño de fármacos y su administración dirigida. En el campo de la ingeniería electrónica, las nanotecnologías se emplean, por ejemplo, en el diseño de dispositivos de almacenamiento de datos de menor tamaño, más rápidos y con un menor consumo de energía.

[577] Los nanobots son máquinas o robots, de tamaño microscópico o nanométrico. Se trata de una tecnología de excepcional valor para manipular de una forma precisa con objetos de pequeñísima escala. Las primeras aplicaciones útiles de las nanomáquinas podrían darse en la tecnología médica, estos dispositivos podrían ser usados para identificar y destruir células cancerígenas.

[578] PIÑAR MAÑAS, J. L. *Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio.* Fundación Alternativas, Madrid, 2009, p. 18. Disponible en Internet: http://www.cepc.gob.es/docs/ley-de-transparencia/ponencia-j-luis-pi%C3%B1ar.pdf?sfvrsn=0 [Consulta: 8 enero 2017].

en jaque a la normativa, adoptar medidas de seguridad más exigentes y establecer controles a nivel de auditoría, más periódicos, más rigurosos y cuyas consecuencias en la inobservancia legal desencadene en sanciones importantes.

La Comisión Europea sostuvo ya en el año 2010[579], que los métodos de recogida de los datos personales son cada vez más abundantes, complicados y se detectan con mayor dificultad. Por ejemplo, la utilización de herramientas sofisticadas permite a los agentes económicos localizar mejor a las personas, mediante el registro de su comportamiento. El mayor recurso a procedimientos que permiten la recogida automática de datos, como el pago electrónico de billetes, el cobro de peajes en carreteras, o instrumentos de geolocalización facilitan la determinación de la ubicación de un individuo por el mero uso por su parte de un dispositivo móvil. Las autoridades públicas también utilizan cada vez más datos personales con distintos fines: para buscar personas cuando se declara una enfermedad transmisible, para prevenir y luchar más eficazmente contra el terrorismo y la delincuencia, para gestionar su régimen de seguridad social o a efectos fiscales, en el marco de sus aplicaciones de administración *on line*, etc.

El inconveniente radica en que se pueden conocer y por tanto utilizar, sin la debida autorización, datos personales, de salud, datos genéticos, datos biométricos, afectando gravemente nuestros derechos fundamentales. Toda ésta información personal y sensible que circula a través del flujo diario de información tecnológica y digital puede ser tratada sin nuestro consentimiento a falta de regulación específica. A éste inconveniente, hay que brindarle una respuesta legal, que ampare la protección de los datos personales y respete la intimidad y la confidencialidad de las personas, máxime en el ámbito de los datos sensibles. Lo cierto es que, estas consideraciones ponen de manifiesto que la actual legislación de la UE en materia de protección de datos no es capaz de hacer frente plena y eficazmente a estos retos, tal como hemos hecho mención *ut supra*.

La AEPD dentro del marco de consultas realizadas en torno a la protección de datos, propuso a la Comisión Europea[580], configurar una definición lo suficientemente amplia para anticiparse a las posibles evoluciones de la tecnología que incluya los

[579] Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Bruselas, 4.11.2010 COM (2010) 609 final.

[580] Vid. Contribución de la AEPD a la consulta de la Comisión sobre un enfoque global de la protección de datos personales en la Unión Europea, op. cit.

procedimientos y técnicas para el tratamiento de la información que permitan singularizar a una persona o usuario.

1.2. El reforzamiento del mercado interior de la protección de datos.

Otro inconveniente que se plantea actualmente en la UE, radica en que resulta insuficiente la unificación y armonización de las legislaciones de los Estados miembros en materia de protección de datos, a pesar de la existencia de un marco jurídico común.

Las empresas plantean la necesidad de aumentar la seguridad jurídica, de reducir las cargas administrativas y de garantizar la igualdad de condiciones a los agentes económicos y a otros responsables del tratamiento. Esto es un punto muy importante a la hora de fomentar la actividad de empresas pequeñas y medianas (PYMES), que teniendo menores trabas burocráticas pueden operar de manera más competitiva junto a grandes empresas, garantizándose a las personas el buen empleo de sus datos personales en virtud de la seguridad jurídica que se les otorgaría.

Teniendo en cuenta que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros, siendo este objetivo esencial para el mercado interior, no pudiendo lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el Artículo 7 del Tratado de Funcionamiento de la UE (en adelante TFUE)[581] siendo necesario que la Comunidad Europea intervenga para aproximar las legislaciones.

[581] El Artículo 7, del TFUE establece que: *"La Unión velará por la coherencia entre sus diferentes políticas y acciones, teniendo en cuenta el conjunto de sus objetivos y observando el principio de atribución de competencias".* Tratado de Funcionamiento de la Unión Europea (DOUE C 83, 30.03.2010, p. 47).

Para reforzar el marco institucional, la AEPD[582] sostuvo que se debe hacer especial hincapié en las mejoras en los procedimientos de cooperación e intercambio de información entre las autoridades de control nacionales, así como en el diseño de un marco que permita el desarrollo de actividades conjuntas con plena seguridad jurídica, incluyendo los aspectos de cumplimiento normativo, con autoridades de control fuera del ámbito de la UE. Asimismo, manifestó la AEPD que sería conveniente permitir la posibilidad de que una autoridad de control pudiera participar con pleno amparo legal en actividades de investigación y auditoría realizadas en otro Estado miembro cuando los hechos objeto de análisis afecten a individuos bajo su tutela, y que el resultado de dichas investigaciones pueda ser utilizado con plena eficacia, en su caso, en el marco del régimen sancionador aplicable en su jurisdicción.

1.3. La seguridad de las personas en el tratamiento de sus datos.

Otro reto que se ha de abordar es la analogía entre la protección de datos y su relación con la seguridad ciudadana. Desde los terribles atentados que hemos sufrido en la última década, los gobiernos, de forma independiente, han tomado medidas de seguridad que afectan notablemente a la protección de los datos personales. La *Patriot Act*[583] que ha sido aprobada por el Gobierno americano tras el atentado del 11 de septiembre, permite a ese gobierno acceder a los datos de los pasajeros que viajan en avión, que cruzan aduanas, o aquellas personas que hacen una transferencia de divisas usando el sistema *Swift*.

---

[582] Contribución de la AEPD a la consulta de la Comisión sobre un enfoque global de la protección de datos personales en la Unión Europea, op. cit.

[583] La Ley Patriota, denominada en inglés USA *Patriot Act*, es un texto legal estadounidense que fue aprobado por una abrumadora mayoría tanto por la Cámara de Representantes como por el Senado estadounidense para después ser promulgada por el presidente de los Estados Unidos George Bush el 26 de octubre de 2001, con posterioridad a los atentados del 11 de septiembre de 2001. El objetivo de esta Ley es ampliar la capacidad de control del Estado en aras de combatir el terrorismo, mejorando la capacidad de las distintas agencias de seguridad estadounidenses al coordinarlas y dotarlas de mayores poderes de vigilancia contra los delitos de terrorismo. Asimismo, la Ley también estableció nuevos delitos y endureció las penas por delitos de terrorismo. La Ley Patriota ha sido duramente criticada por diversos organismos y organizaciones de derechos humanos, debido a la restricción de libertades y garantías constitucionales que ha supuesto para los ciudadanos, tanto estadounidenses como extranjeros.

Evidentemente se ha de buscar un equilibrio entre la seguridad ciudadana que se pretende y la vulneración de la privacidad de las personas[584]. Puede ser peligroso que tanta información personal esté al alcance de empresas, por ejemplo, subcontratadas para la seguridad, por el uso indebido que puedan hacer de la misma, que a día de hoy desconocemos la trascendencia o el impacto que puede tener en nuestras vidas privadas.

Según advierte SÁNCHEZ GARCÍA[585], el escenario de la seguridad de los datos de salud es susceptible todavía de complicarse y lo está haciendo. El nuevo reto viene de la mano de las apps en el entorno sanitario. Desde hace poco, están apareciendo en el mercado numerosas aplicaciones orientadas a lo que en inglés se denomina *self tracking o* autoseguimiento*,* con las que los individuos pueden registrar sus datos de salud y las constantes vitales que constituyen su evolución.

En el mismo sentido, LUNA[586] indica que el número de pasos que damos al día, las calorías que quemamos, horas de sueño o ejercicio diario. Actualmente existen infinidad de aplicaciones que recopilan información sobre nuestra salud. Dispositivos como los *smartphones* y sobre todo *wearables* también cuentan con tecnologías destinadas a lo mismo. Ahora piensen en los millones de usuarios que están compartiendo estos datos, que tienen que ver con algunas de nuestras funciones vitales, en redes sociales, *apps* y aparatos electrónicos. Y en el increíble potencial de toda esta información.

Estas aplicaciones, a veces aisladas y otras veces vendidas con dispositivos que capturan las constantes vitales del usuario (tensión, peso, saturación de oxígeno en sangre, actividad física …) dejan la información en manos de las empresas fabricantes

[584] Para profundizar más al respecto, véase: PIÑAR MAÑAS, J. L., op. cit., pp. 22 y ss.

[585] SÁNCHEZ GARCÍA, J. J. (3.03.2015) La privacidad de los datos de salud en la era digital. [Blog post]. Blog A un click de las TIC, blogthinkbig.com. Disponible en Internet: <aunclicdelastic.blogthinkbig.com/la-privacidad-de-los-datos-de-salud-en-la-era-digital/> [Consulta: 13 febrero 2017].

[586] LUNA, A. G. (22.11.2014) Los datos de tu salud que recopilan los dispositivos, un negocio para las empresas. El número de pasos que damos al día, las calorías que quemamos o las horas de sueño. Infinidad de 'apps' y 'gadgets' recopilan datos de salud pero, ¿son seguros? [Blog post]. Blog El Confidencial, 22-11-2014. Disponible en Internet: <http://www.elconfidencial.com/tecnologia/2014-11-22/tus-datos-de-salud-que-recopilanlosdispositivosunnegocio-para-las-empresas_500297/> [Consulta: 13 febrero 2017].

y ésta acaba normalmente en almacenes de datos en la nube en EE.UU, fuera del control de las legislaciones nacionales.

La Comisión Federal de Comercio de Estados Unidos[587] se ha reunido con varios representantes de Apple[588] para conocer todos los datos sanitarios que recoge *HealthKit* y la forma en que conserva esa información. La preocupación del organismo estadounidense es clara: que ni Apple ni otros terceros puedan comercializar estos datos. Y tiene su fundamento. Según la Comisión, los desarrolladores de varias aplicaciones móviles de salud y *fitness* compartieron la información de sus usuarios con hasta 76 empresas, entre las que se incluyen varios anunciantes.

1.4. La globalización y la mejora de las transferencias internacionales de datos.

El movimiento internacional de datos constituye uno de los mayores riesgos que el tratamiento de datos personales puede generar en la protección de la privacidad de las personas. Sin embargo, según señala AEPD[589], resulta impensable el desarrollo y mantenimiento de un sistema como el actual, caracterizado por un importante componente de globalización, sin que dichos movimientos se lleven a cabo en la práctica.

El incremento en la subcontratación del tratamiento, muy a menudo fuera de la UE, plantea varios problemas vinculados a la legislación aplicable al tratamiento y a la atribución de la responsabilidad correspondiente. Por lo que respecta a las transferencias internacionales de datos, los regímenes actuales no son plenamente satisfactorios y deben revisarse y racionalizarse[590].

Los canales de tráfico de datos a escala global han de estar sujeta a una legislación uniforme y armonizada. En este punto es muy importante que países asiáticos, Canadá y los Estados Unidos suscriban acuerdos con la UE cuando entre en vigor el RGPD.

---

[587] Comisión Federal de Comercio de Estados Unidos <https://www.ftc.gov/es> [Consulta: 13 febrero 2017].

[588] Noticia de la Agencia Reuters. Disponible en Internet: <http://www.reuters.com/article/us-apple-ftc-exclusive-idUSKCN0IX2I520141113> [Consulta: 13 febrero 2017].

[589] Vid. Contribución de la AEPD a la consulta de la Comisión sobre un enfoque global de la protección de datos personales en la Unión Europea, op. cit.

[590] Vid. Comunicación 4.11.2010 COM (2010) 609 final, op. cit.

Son países que manejan un volumen diario de información personal de ciudadanos de todo el mundo y ello se debe en gran parte a que muchas de las empresas de las que somos usuarios en Europa tienen su sede en estos países, circunstancia que hace muy complicado para un europeo acceder a los datos que propició en su momento y que pretende simplemente borrarlos, como puede ser el caso de una foto subida a una plataforma americana como es Facebook, o simplemente referencias a nuestra persona que puedan aparecen en los buscadores más habituales como Google[591].

El Programa de Estocolmo[592], a través del Plan de acción del Programa de Estocolmo[593] de la UE, reitera la interconexión entre la dimensión interna y externa de

[591] La sentencia del Tribunal de Justicia de Luxemburgo en el caso Google y la Agencia Española de Protección de Datos es pionera y con ella el Alto Tribunal ha resuelto una cuestión prejudicial presentada por la Audiencia Nacional en el año 2012 sobre la manera de interpretar las normas de protección de datos en Internet. Y ha avalado el llamado derecho al olvido al fallar que "en determinadas condiciones" los buscadores están obligados a eliminar enlaces con información personal. El Alto Tribunal precisa que el interesado debe presentar su solicitud "directamente" al buscador (Google, Yahoo, Bing o cualquier otro), que deberá examinar si es fundada. En caso de que el buscador no acceda a retirar la información, el afectado podrá acudir a la autoridad de control o a los Tribunales para que estos lleven a cabo las comprobaciones necesarias y, en su caso, ordenen al buscador la retirada de la información. Es decir, el TJUE abre la puerta a un examen caso por caso de cada una de las reclamaciones presentadas a cualquier buscador. STJUE de 13 de mayo de 2014 (Asunto Google, C-131/12). ECLI:EU:C:2014:317.

[592] El Programa de Estocolmo (DO C 115, 4.05.2010) establece las prioridades de la UE durante el periodo 2010 y pretende hacer frente a los desafíos del futuro y reforzar el espacio de libertad, seguridad y justicia, con medidas centradas en los intereses y las necesidades de los ciudadanos. Para conseguir una Europa segura donde se respeten los derechos y las libertades fundamentales de los ciudadanos, el Programa de Estocolmo se centra en las siguientes prioridades: 1) Promover los derechos de los ciudadanos: Una Europa de derechos, en el sentido de construir el Espacio de Libertad, Seguridad y Justicia, y crear una única área de libertad de movimientos donde los derechos de los ciudadanos sean respetados y protegidos, en el marco que ofrece la carta de Derechos Fundamentales. Se da especial importancia a la protección de los grupos vulnerables (lucha contra el racismo, protección de los niños, de la etnia gitana, de las víctimas de crímenes, personas implicadas en un proceso criminal) y a la protección de los datos personales y la privacidad. 2) Una Europa que protege: Proteger a los ciudadanos europeos de amenazas de carácter internacional, como el crimen organizado, el tráfico de drogas, el terrorismo o el tráfico de seres humanos. Para ello, el Programa de Estocolmo prevé la creación de una Estrategia de Seguridad Interior, que mejore las herramientas existentes para la lucha contra el crimen. También pretende una mayor solidaridad y eficacia de la respuesta europea a las catástrofes naturales. 3) Una Europa de responsabilidad, solidaridad y asociación en asuntos de migración y asilo: Con base en el Pacto Europeo sobre Migraciones y Asilo, la Unión buscará una mayor solidaridad de los países europeos en materia migratoria, combatiendo la inmigración ilegal, promoviendo la migración legal y promoviendo el desarrollo de los países de origen.

las políticas de justicia, libertad y seguridad, estableciendo acciones que refuerzan la dimensión externa, en particular para una cooperación y un intercambio de información mejores entre los países de la UE. El Plan de acción[594] establece medidas para garantizar la protección de los derechos fundamentales. Éstas consisten en reforzar la legislación sobre la protección de datos mediante un nuevo marco jurídico global, así como incorporar la protección de datos en todas las políticas de la UE.

2. Objetivos estratégicos de la Comisión Europea para la adopción del Reglamento General de Protección de Datos.

Para su implementación y de acuerdo con su política de «legislar mejor», la Comisión Europea realizó una evaluación de impacto de distintas posibilidades de actuación. La evaluación de impacto se basó en tres objetivos estratégicos. En primer lugar, mejorar la dimensión de mercado interior de la protección de datos; en segundo lugar, hacer más efectivo el ejercicio de los derechos de protección de datos por los ciudadanos, y, en tercer lugar, crear un marco general y coherente que abarque todos los ámbitos de competencia de la UE, incluida la cooperación policial y judicial en materia penal.

En base a estos objetivos estratégicos trazados, se valoraron tres opciones de actuación con diferentes grados de intervención. Una primera opción que consistía en la

---

En materia de asilo, el objetivo es la creación de un Sistema Común Europeo de Asilo para el año 2012. 4) Hacer más fácil la vida de las personas: una Europa del Derecho y de la justicia: Para que los ciudadanos europeos puedan hacer valer sus derechos en todo el territorio de la Unión es necesario extender el principio de mutuo reconocimiento de las decisiones judiciales, mejorar la cooperación judicial creando una cultura judicial europea y aplicar las nuevas tecnologías en el ámbito de la justicia. 5) Europa en un mundo global: la dimensión externa del Espacio de libertad, seguridad y justicia: En un mundo interconectado, es imprescindible impulsar el diálogo y la cooperación con terceros países, afrontando juntos retos globales como la migración y el asilo, la seguridad, la justicia, los derechos humanos y un intercambio de información seguro y eficiente. Disponible en Internet: <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:jl0034> [Consulta: 11 febrero 2017].

[593] Este Plan de acción proporciona una hoja de ruta para aplicar las prioridades políticas establecidas en el Programa de Estocolmo, op. cit., para el espacio de justicia, libertad y seguridad entre 2010-2014. Plan de Acción de Estocolmo (Comunicación COM (2010) 171 final 20.04.2010). Disponible en Internet: <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:jl0036> [Consulta: 11 febrero 2017].

[594] Ibídem.

introducción de mínimas enmiendas legislativas y el uso de comunicaciones interpretativas y medidas de apoyo estratégico, como programas de financiación y herramientas técnicas; una segunda opción que abarcaba un paquete de disposiciones legislativas que abordaban cada una de las cuestiones identificadas en el análisis, y la tercera opción consistía en la centralización de la protección de datos a nivel de la UE mediante normas precisas y detalladas para todos los sectores y la creación de una agencia de la UE destinada a la supervisión y ejecución de las disposiciones.

Una vez analizado el posible impacto global[595], la Comisión Europea se declinó por el desarrollo de la segunda opción estratégica[596]. Según la evaluación de impacto, su ejecución comportará, entre otras cosas, mejoras considerables en materia de seguridad jurídica para los responsables del tratamiento de datos y los ciudadanos, la reducción de la carga administrativa, la coherencia en la aplicación de la protección de datos en la UE, la posibilidad efectiva para las personas físicas de ejercer sus derechos de protección de los datos de carácter personal y la eficiencia en la supervisión y en la aplicación de la protección de datos.

Por todos estos motivos analizados en los epígrafes precedentes, se han establecido normas comunes en la UE para garantizar que los datos personales gocen de un elevado nivel de protección en cualquier parte de la UE a través del RGPD.

[595] Con arreglo a la metodología consolidada de la Comisión Europea, cada opción fue evaluada, con ayuda de un grupo director interservicios, en función de su efectividad a la hora de alcanzar los objetivos estratégicos, su impacto económico en los interesados (también sobre el presupuesto de las instituciones de la UE), su impacto social y su incidencia en los derechos fundamentales.

[596] Con la adopción de la segunda opción, se prevé que se contribuya al objetivo de la Comisión Europea de simplificar y reducir la carga administrativa y a lograr los objetivos de la Agenda Digital para Europa (Comunicación, de 19 de mayo de 2010, de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, COM(2010) 245 final); del Plan de Acción de Estocolmo (Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 20 de abril de 2010 - Garantizar el espacio de libertad, seguridad y justicia para los ciudadanos europeos- COM (2010) 171 final); y la Estrategia Europa 2020 (Europa 2020: Una estrategia para un crecimiento inteligente, sostenible e integrador COM (2010) 2020 final, 3.03.2010).

3. El Reglamento General de Protección de Datos. Nuevas perspectivas legales en la UE en el marco de la regulación de los datos personales.

Como enunciamos en el apartado anterior, la protección efectiva de los datos personales en la UE ha hecho necesario que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes.

En base a ello, y haciendo caso a varios sectores que propugnaban por la modificación del marco legislativo en torno a la protección de datos, en enero de 2012 la Comisión Europea[597] propuso la realización de una anhelada reforma en nuestra materia de investigación: reformar la legislación sobre protección de datos en la UE. Después de cuatro años de negociaciones[598], los Estados miembros y las instituciones de la UE finalmente han alcanzado un consenso político sobre la necesidad de reformar la legislación vigente en materia de protección de datos a través del Reglamento General de Protección de Datos (UE) 2016/679, del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) destinado a sustituir la Directiva 95/46/CE.

Al respecto, señaló el Grupo de Trabajo del Artículo 29[599], que:

> La reforma de la protección de datos es un factor clave del mercado único digital, considerado prioritario por la Comisión. El objetivo de este nuevo conjunto de normas es volver a dar a los

[597] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos), (Comunicación COM (2012) 11 final 25.01.2012).

[598] Véase al respecto: notal al pie 568.

[599] Vid. Comunicado de Prensa de la Comisión Europea: El acuerdo sobre la reforma de la protección de datos promovida por la Comisión reforzará el mercado único digital (15.12.2015) Disponible en Internet: <http://europa.eu/rapid/press-release_IP-15-6321_es.htm> [Consulta: 3 enero 2016].

> ciudadanos el control de sus datos personales y simplificar el contexto reglamentario para las empresas. La reforma permitirá que los ciudadanos y las empresas europeas se beneficien plenamente de las ventajas de la economía digital.

El acuerdo se basó en un proyecto para actualizar la Directiva 95/46/CE[600], legislación de referencia actual como se explicó en la primera parte de éste trabajo, que sin duda constituirá un paso gigante legislativo que pretende dar la UE, y a través del cual se pretende poner fin a la actual obsolescencia y vendrá a unificar la aplicación de las normas en relación con la protección y tratamiento de los datos. Este nuevo marco jurídico refuerza los derechos de los individuos y responsabiliza considerablemente a los responsables y encargados del tratamiento. La norma contempla un nuevo régimen sancionador a este tipo de infracciones, con multas mucho más elevadas.

Aunque los aspectos formales de la norma no han generado discrepancias destacables, el contenido ha desencadenado diferentes desavenencias entre los defensores del texto y los defensores de sectores como el bancario, proveedores de Internet, telecomunicaciones, salud, etc. En este contexto, las negociaciones han afrontado la compleja tarea de encontrar un equilibrio entre los intereses económicos[601] y los de los ciudadanos de la UE.

El texto inicial de la normativa, propuesto por la Comisión Europea el 25 de enero de 2012, ha sido muy controvertido y objeto de presiones provenientes de muchos

[600] Con este fin, se pusieron en marcha algunos estudios, principalmente los realizados por el Grupo de Trabajo del Artículo 29, que emitió diversos dictámenes y realizó aportaciones útiles a la Comisión Europea. Véase, en particular, los siguientes dictámenes: sobre el «El futuro de la intimidad» (2009, WP 168); sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» (1/2010, WP 169); sobre la publicidad del comportamiento en línea (2/2010, WP 171); sobre el principio de la obligación de rendir cuentas (3/2010, WP 173); sobre la legislación aplicable (8/2010, WP 179), y sobre el consentimiento (15/2011, WP 187). A petición de la Comisión Europea, también adoptó los tres documentos de orientación siguientes: sobre notificaciones, datos sensibles y la aplicación práctica del artículo 28, apartado 6, de la Directiva de protección de datos. Todos pueden ser consultados en: <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm> [Consulta: 19 septiembre 2015].

[601] La actual fragmentación de la protección de datos personales en la Unión ha sido blanco de duras críticas, especialmente por parte de los operadores económicos, que solicitaron una mayor seguridad jurídica y la armonización de las normas relativas a la protección de los datos de carácter personal. Se considera que la complejidad de las normas en materia de transferencias internacionales de datos personales constituye un impedimento sustancial a su funcionamiento, ya que se necesita transferir con regularidad datos personales de la UE a otras partes del mundo.

sectores, corporaciones e incluso reguladores de otras geografías, que ven como una norma europea en materia de privacidad estricta, puede suponer un freno para el desarrollo de muchos de los negocios internacionales de sus firmas empresariales. La discusión se centraba en dos inconvenientes principales. Por una parte, satisfacer la necesidad de actualizar y dinamizar la economía digital a la altura de otros mercados como Estados Unidos y Asia, quienes consideran los datos personales como una mercancía como cualquier otra, susceptible de apropiación y de comercio[602]. Y, por otra parte, atender la defensa de los derechos y la privacidad de los ciudadanos, limitando el procesamiento de estos datos y asegurando el control de los individuos sobre los mismos[603]. Conjugar estas dos perspectivas, tan opuestas, es lo que ha venido a trabar un posible consenso con anterioridad.

Cabe resaltar que estamos frente a una norma que aún no está en vigencia. El RGPD entrará en vigor el próximo 25 de mayo de 2018, y será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro. También, en la misma fecha, quedará derogada la Directiva 95/46/CE que ha servido de base a nuestro ordenamiento nacional en materia de protección de datos. El resto de normas relacionadas con este tema (el Convenio 108 del Consejo de Europa[604] y las Directrices de la OCDE de 1980[605]) deberán adaptarse al Reglamento en la medida en que fueran

[602] El denominado "modelo estadounidense" se caracteriza por la consideración de mercancía tanto a los objetos fungibles como a los no fungibles, y en este sentido, los datos personales obtenidos tienen la consideración de mercancía intercambiable por un valor económico.

[603] Por el contrario, los modelos alemanes y franceses tienden a la protección más rigurosa y absoluta sobre la privacidad, individualidad e intimidad del individuo, y los datos personales no tienen la consideración de un bien que pueda enajenarse.

[604] Convenio Nº 108, op. cit.

[605] Las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales "directrices de privacidad", fueron adoptadas como una recomendación del Consejo de la OCDE apoyando los tres principios que aglutinan a los países de la OCDE: democracia pluralista, respeto delos derechos humanos y economías de mercado abiertas. Se hicieron efectivas el 23 de septiembre de 1980. Las directrices de privacidad suponen la unanimidad internacional sobre las guías generales para la recogida y gestión de información personal. Los principios establecidos en las directrices de privacidad se caracterizan por su claridad y flexibilidad de aplicación, y por su formulación, que es lo suficientemente general para permitir su adaptación a los cambios tecnológicos. Los principios abarcan todos los medios del procesamiento informático de datos sobre individuos (desde computadoras locales a redes con complejas ramificaciones nacionales e internacionales), todos los tipos de procesamiento de datos personales (desde la administración de personal hasta la compilación de perfiles de consumidores) y todas las categorías de datos (desde datos de tráfico hasta datos de contenidos, desde el más trivial al más delicado). Fuente: Directrices de la OCDE sobre protección de

interferir en su regulación ya que ambas pertenecen a sistemas jurídicos diferentes. En cuanto a la actual LOPD permanecerá vigente hasta que se derogue o bien, se modifiquen sus disposiciones para adecuarla al RGPD[606].

Dada la importancia de ésta novedad en el marco legislativo europeo y que a nuestro país vinculará necesariamente el año próximo, hemos considerado la necesidad de analizar el RGPD, que si bien, aún no es efectivo, es necesario adaptar tanto las Administraciones Públicas y Privadas, como las grandes empresas y también las pequeñas y medianas empresas, para adecuarlas al nuevo imperativo legal, que tendrán el deber de implementar y la obligación de respetar.

a) Fundamento legal sobre el que se asienta el Reglamento General de Protección de Datos.

El proyecto jurídico del RGPD, encuentra su génesis legal en el Artículo 16 del TFUE[607], que constituye la nueva base jurídica para la adopción de las normas de protección de datos. Esta disposición permite la adopción de normas relativas a la protección de las personas físicas con respecto al tratamiento de datos de carácter personal, por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la UE. También permite la adopción de normas relativas a la libre circulación de datos de carácter personal, incluidos los datos personales tratados por los Estados miembros o por operadores privados.

---

la privacidad y flujos transfronterizos de datos personales. 2002, OCDE. Disponible en Internet: <https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiRm3iJ_SAhXG1hoKHSe_AbEQFggcMAA&url=http%3A%2F%2Fwww.oecd.org%2Fsti%2Fieconomy%2F15590267.pdf&usg=AFQjCNG0flNpNVFvCDeLfFCo-j0nUESGdA> [Consulta: 13 febrero 2017].

[606] Actualmente se está trabajando en el Proyecto de Reforma de la LOPD, véase al respecto: nota al pie 629.

[607] El Artículo 16 del TFUE establece que*: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes".*

b) Objetivo de la reforma.

El objetivo de la reforma que se ha materializado en el ámbito de la protección de datos en el marco europeo, es doble: por un lado, regular el derecho fundamental a la protección de datos[608], y, por otro lado, garantizar la libre circulación de los datos[609]. Este objetivo se desprende del mismo título del RGPD *"relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos".* Según recuerda PIÑAR MAÑAS[610], la libre circulación de los datos en ningún caso puede justificar una reducción en el nivel de protección. Además de este doble objetivo, se ha tenido en cuenta la patente incidencia de las nuevas tecnologías en la protección de datos[611].

Y la forma de alcanzar estos objetivos que el RGPD marca, se basa en dos conceptos fundamentales: la coherencia y la homogeneidad normativa en relación con todos los Estados miembros y con su aplicación. Esto se desprende del Considerando 10 que establece que: *"Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea"*[612]. Asimismo, para alcanzar estas metas, el RGPD promulga que:

> Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado

[608] El derecho a la protección de datos ya venía siendo reconocido, como se comentó en la primera parte de ésta Tesis, por el Artículo 8 de la Carta Europea, en la que se establece que: *"Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.2. 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 la conciernan y a su rectificación.3. El respeto de estas normas quedar· sujeto al control de una autoridad independiente".* Carta de los Derechos Fundamentales de la Unión Europea (DOCE C 364, 18.12.2000, pp. 1-22).

[609] Según lo enuncia textualmente el Considerando (166) del RGPD: *"A fin de cumplir los objetivos del presente Reglamento, a saber, proteger los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, y garantizar la libre circulación de los datos personales en la Unión".*

[610] PIÑAR MAÑAS, J. L. "Objeto del Reglamento", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016, p. 61.

[611] El RGPD lo reconoce expresamente en el Considerando (6): *"La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales".*

[612] Considerando (10), del RGPD.

> interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros"[613].

Por tanto, la misma normativa brinda la justificación del instrumento legislativo comunitario elegido, es decir, el Reglamento.

Con el propósito de conseguir estos objetivos y verificar el cumplimiento del RGPD con respecto a su aplicación en los diferentes Estados miembros, el RGPD contiene una previsión, cuanto menos interesante, desde el punto de vista del control que del mismo se ha de hacer. La Comisión Europea debe presentar un informe, y señala para ello, el RGPD, como plazo máximo el 25 de mayo de 2020[614], es decir dos años después de la entrada en vigor del RGPD. Dicho informe deberá evaluar y revisar la aplicación del RGPD, en particular la aplicación y el funcionamiento de transferencia de datos personales a países terceros u organizaciones internacionales, particularmente respecto de las decisiones adoptadas en virtud del Artículo 45, apartado 3, del presente Reglamento, y de las adoptadas sobre la base del Artículo 25, apartado 6, de la Directiva 95/46/CE, para lo cual podrá solicitar información a los Estados miembros y a las autoridades de control.

En base a ello, el RGPD también contiene una previsión basada en los avances tecnológicos, y contempla en el Artículo 97.5. que: *"La Comisión presentará, en caso necesario, las propuestas oportunas para modificar el presente Reglamento, en particular teniendo en cuenta la evolución de las tecnologías de la información y a la vista de los progresos en la sociedad de la información".*

No obstante, consideramos que, si uno de los objetivos para adoptar el RGPD era la uniformización de los diferentes ordenamientos jurídicos, dado lo comentado *ut supra*, podría concluirse que este objetivo no se ha alcanzado. En este sentido se han

[613] Considerando (13), del RGPD.

[614] Artículo 97, del RGPD. A partir del año 2020, el RGPD prevé una revisión periódica que tendrá lugar cada cuatro años.

pronunciado algunos doctrinarios[615], quienes tampoco ven cumplido el ansiado objetivo del RGPD de uniformizar los ordenamientos jurídicos de los Estados miembros.

PIÑAR MAÑAS[616] opina al respecto que, las reglas de juego son más uniformes a nivel de la UE, pero al mismo tiempo se deja mayor margen de apreciación y valoración a los responsables y encargados.

ÁLVAREZ-RIGAUDIAS[617], considera desafortunado por parte del RGPD dejar libertad a los Estados miembros para incluir condiciones adicionales en relación con los datos genéticos, biométricos o de salud, porque cualquier fragmentación del mercado interior incidirá negativamente -como ya demuestra la normativa vigente, sostiene la autora- en el desarrollo de la investigación científica en la UE. Y en este sentido coincidimos plenamente con ÁLVAREZ-RIGAUDIAS, puesto que el RGPD contiene una contradicción en el Considerando 53 en el cual se propugna por la no obstaculización de la libre circulación de los datos personales en la UE.

Y con especial atención a los datos de salud, dado el contenido similar del RGPD y la Directiva 95/46/CE en el tratamiento de datos personales de salud, consideramos acertado la idoneidad de aplicar la interpretación que ya se efectuó por parte del Grupo de Trabajo del Artículo 29 sobre el Artículo 8 de la Directiva 95/46/UE, de tal forma que las excepciones recogidas por el RGPD y la Directiva 95/46/CE en el tratamiento de datos personales relativos a la salud deben ser limitadas, exhaustivas y tienen que ser interpretadas de forma restrictiva[618].

3.1. Diferencias de enfoque del RGPD con respecto a la Directiva 95/46/CE.

---

[615] PIÑAR MAÑAS, J. L. (Director)., op. cit., p. 17.; ÁLVAREZ-RIGAUDIAS, C. "Tratamiento de Datos de Salud", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016, p. 178.

[616] PIÑAR MAÑAS, J. L. (Director)., op. cit., p. 17.

[617] ÁLVAREZ-RIGAUDIAS, C., op. cit., p. 178.

[618] Vid. Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 15 de febrero de 2007, 00323/07/ES (WP 131). Disponible en Internet: <https://www.apda.ad/system/files/wp131_es.pdf> [Consulta: 26 noviembre 2016].

Como adelantamos, el RGPD viene a derogar la Directiva 95/46/CE, porque la misma devino obsoleta, no generaba confianza, y por el contrario nos encontrábamos en un punto de inseguridad jurídica dados los avances tecnológicos de la sociedad, que la Directiva 95/46/CE no contempló en su día.

Una de las principales diferencias entre la Directiva 95/46/CE y el RGPD radica justamente en la circunstancia de que se trata de un Reglamento, y por tanto vincula directamente a los 28 Estados miembros. En efecto, los Reglamentos de la UE tienen alcance general y son obligatorios en todos sus elementos y directamente aplicables en los Estados miembros[619]. Por tanto, no necesitan transposición, pero sí pueden ser objeto de desarrollo por parte de normativa interna de cada Estado miembro.

GARCÍA MEXÍA[620], razona diciendo que el RGPD no es un Reglamento como los demás, sino que es una norma que se asemeja más a una Directiva, y advierte el autor, que dejar a la interpretación posterior la infinidad de materias que ya puede intuirse que plantearán problemas de aplicación, debe solucionarse modificando las disposiciones nacionales contrarias al RGPD.

La adopción de un texto de estas características entraña un compromiso especialmente delicado dado que se trata de una regulación uniforme para los diferentes Estados miembros que no estará sujeta a "ajustes" nacionales[621].

---

[619] El Artículo 288 del TFUE, establece que: *"El reglamento tendrá un alcance general. Será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro. La directiva obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medio".*

[620] GARCÍA MEXÍA, P. "La singular naturaleza jurídica del Reglamento General de Protección de Datos de la UE. Sus efectos en el acervo nacional sobre protección de datos", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016, pp. 31-33.

[621] A través del Programa de Estocolmo "Una Europa abierta y segura que sirva y proteja al ciudadano", (DO C 115, 4.5.2010), la Comisión Europea subrayó la necesidad de garantizar que el derecho fundamental a la protección de datos de carácter personal se aplique de forma coherente en el contexto de todas las políticas de la UE. En el mes de junio del año 2015 se ha concluido después de varios años de debates políticos y económicos, lográndose llegar a un acuerdo para sustituir la Directiva por un Reglamento Europeo. El proyecto jurídico se basó en dos propuestas, por un lado una propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos Comunicación COM (2012) 9 final), y por otro lado, una propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las

Ésta novedad es sustancial, ya que el Reglamento es un acto legislativo de alcance general, obligatorio en todos sus elementos, sin ofrecer a sus destinatarios la forma y medios de aplicación, evitando así, discordancias normativas entre los Estados miembros. Creemos que es un avance intensamente significativo, porque como punto de partida, la simple forma jurídica que adoptará, evitará ya de manera inicial cualquier divergencia entre los ordenamientos jurídicos internos de los países miembros de la UE. En el día a día, las empresas, autoridades públicas y particulares transfieren enormes cantidades de datos personales a otros países de forma constante. Si los distintos Estados tuvieran normas contradictorias en materia de protección de datos, esto perturbaría el normal desarrollo de los intercambios internacionales. Otra consecuencia negativa es que los ciudadanos también podrían mostrarse contrarios a transferir datos personales al extranjero, si desconfiaran del nivel de protección existente en otros países o desconociesen sus legislaciones al respecto.

Además, de no ser un Reglamento, no podría obligar a todos los Estados miembros a respetar los mismos medios para sancionar en caso de que se infrinjan los derechos de las personas en relación con sus datos personales[622]. Siendo, que ahora, existirá un Comité europeo de protección de datos que responderá a los fines de coherencia y cooperación[623] para homogenizar su aplicación en todos los Estados miembros, a la vez que el RGPD enuncia expresamente las sanciones[624] que han de aplicarse en caso de vulneraciones.

Según GARCÍA MEXÍA[625] sólo una norma dotada de tales características está en condiciones de adaptarse a los objetivos que persigue, porque la coherencia y la coordinación que ella misma exige, no se habría podido conseguir con una norma comunitaria del tipo Directiva.

---

personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes a efectos de la prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y a la libre circulación de estos datos (Comunicación COM (2012) 10 final).

[622] Artículos 83 y 84, del RGPD.

[623] Capítulo VII, del RGPD.

[624] Capítulo VIII, del RGPD.

[625] GARCÍA MEXÍA, P., op. cit., p. 24.

La aplicabilidad directa de un reglamento[626], reducirá la fragmentación jurídica y ofrecerá una mayor seguridad jurídica merced a la introducción de un conjunto armonizado de normas básicas, la mejora de la protección de los derechos fundamentales de las personas y la contribución al funcionamiento del mercado interior.

La diferencia sustancial entre la Directiva 95/46/CE y el RGPD reside en el enfoque del derecho a la protección de datos que cada norma realiza. Por su parte, la Directiva 95/46/CE trataba de armonizar la protección de las normas estatales de protección de datos. Por el contrario, el RGPD tiene por misión establecer un nivel de protección equivalente en todos los Estados miembros, y garantizar una aplicación de estas normas coherente y homogénea[627].

Desde la entrada en vigor del RGPD en el año 2018, existirá un único derecho europeo en materia de protección de datos, a diferencia de los 28 actuales, uno por cada Estado miembro.

Una vez que entre en vigor, la nueva regulación será equiparable a una Ley nacional, dejando únicamente al Tribunal de Justicia de la UE la tarea de interpretar y hacer respetar de manera uniforme la norma en todo el territorio europeo. Sin duda un avance que repercutirá muy favorablemente en la unidad, uniformidad, analogía y equilibrio de la normativa sobre protección de datos de cada Estado miembro[628].

---

[626] GÓMEZ SÁNCHEZ, Y. *Derecho Constitucional Europeo: Derechos y Libertades*. Sanz y Torres. Madrid 2008, p. 21.

[627] Considerando (23), del RGPD.

[628] En éste sentido se pronunció la Comisión Europea que fue invitada en el año 2010 por el Consejo a evaluar el funcionamiento de los instrumentos de la UE en materia de protección de datos y a presentar, en caso necesario, nuevas iniciativas legislativas y no legislativas (Programa de Estocolmo - Una Europa abierta y segura que sirva y proteja al ciudadano», DO C 115 de 4.5.2010, p.1.). En su resolución sobre el Programa de Estocolmo, el Parlamento Europeo (Resolución del Parlamento Europeo sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada «Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos - Programa de Estocolmo», adoptada el 25 de noviembre de 2009 (P7_TA (2009) 0090)), acogió favorablemente un régimen general de protección de datos en la UE y, entre otras cosas, abogó por la revisión de la Decisión Marco. En su Comunicación titulada «Un enfoque global de la protección de los datos personales en la UE» (Comunicación COM (2010) 609 final), la Comisión Europea concluyó que la UE necesita una política más integradora y coherente en materia del derecho fundamental a la protección de los datos de carácter personal.

3.2. Convivencia con la LOPD.

La entrada en vigor del RGPD plantea la duda de cómo va a convivir en España con la LOPD. Al respecto, ya se ha creado en el seno del Ministerio de Justicia, una Ponencia dentro de la Comisión General de Codificación con la finalidad de que estudie la materia y eleve una propuesta a la Sección de Derecho Público para la regulación en el ordenamiento jurídico español de las premisas de la norma europea[629].

En éste sentido, tanto PIÑAR MAÑAS[630] como GARCÍA MEXÍA[631], apuntaron recientemente a que parece que la LOPD podrá seguir siendo aplicable en lo que esté fuera del Derecho de la UE, pues, además, el RGPD hace numerosas remisiones a la legislación nacional de los Estados miembros. Sin embargo, ambos autores, consideran necesaria una modificación de la LOPD. Al respecto, PIÑAR MAÑAS[632], considera que la LOPD no se verá derogada pero sí desplazada por el RGPD en su aplicación, y necesitará reformas para adaptarse al RGPD.

Entre los inconvenientes que se vislumbran, podemos señalar que suscita dudas en materias como el registro de ficheros ¿Habrá que seguir realizándolo en nuestro país por efecto de la LOPD o cabe entender una derogación tácita de sus disposiciones en este sentido? Igualmente, también cabe preguntarse en qué papel quedará al AEPD y qué valor tendrán sus circulares en el nuevo contexto.

---

[629] En nuestro país, ha sido encargado a la Sección de Derecho Público de la Comisión General de Codificación, del Ministerio de Justicia, en colaboración con la Agencia Española de Protección de Datos, a través de la Orden de 2 de noviembre de 2016, por la que se constituye una ponencia para la adaptación del Reglamento (UE) general de protección de datos, el estudio de las implicaciones que el RGPD tendrá en la LOPD y que deberá presentarse como plazo máximo el 1 de mayo de 2017. Para más información, véase: <http://www.mjusticia.gob.es/cs/Satellite/Portal/1292428235215?blobheader=application%2Fpdf&blobheadername1=ContentDisposition&blobheadername2=Grupo&blobheadervalue1=attachment%3B+filename%3DOrden_de_2_de_noviembre_de_2016_por_la_que_se_constituye_una_ponencia_para_la_adaptacion_del_Regla.PDF&blobheadervalue2=Docs_CGC_Propuestas> [Consulta: 13 febrero 2017].

[630] PIÑAR MAÑAS, J. L. "Introducción. Hacia un nuevo modelo europeo de Protección de Datos", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016, pp. 15-22.

[631] GARCÍA MEXÍA, P., op. cit., p. 23-34.

[632] PIÑAR MAÑAS, J., op. cit., p. 18.

4. Los Principios sobre los que se asienta el RGPD.

Los principios que inspiran al RGPD, tienen una relevancia fundamental puesto que no sólo sirven de fundamentos para la protección de datos de carácter personal, sino que actúan como base para la interpretación de las normas que, sobre protección de datos, viniendo a suplir lagunas que muchas veces la normativa adolece en relación con los avances tecnológicos[633]. Por tanto, su observancia resulta obligatoria, y podemos afirmar que son verdaderos principios normativos que vienen a complementar las regulaciones contenidas en el RGPD.

HERRÁN ORTIZ[634], entiende que los principios generales de protección de datos constituyen el contenido esencial del derecho a la protección de datos, y que, a través de ellos, se configura un sistema de tutela que garantiza una utilización más racional y razonable de los datos personales. APARICIO SALOM[635] considera que los principios deben ser obligatorios para los responsables del tratamiento de datos de carácter personal. Sin embargo, PUYOL MONTERO[636] va más allá, y opina que los principios tienen un alcance y una trascendencia de mayor envergadura, y ello, porque no sólo afectan al responsable del tratamiento, sino a todas las personas físicas o jurídicas que intervengan en el tratamiento de datos, sirviendo los mismos como pauta normativa e interpretativa, en todos los ámbitos donde exista un tratamiento de datos de carácter personal.

Según el RGPD, los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado[637]. El RGPD introduce estos nuevos principios que deberán observarse en relación con todos los intervinientes en el tratamiento de los datos personales. Se introduce el principio de minimización de los

[633] PUYOL MONTERO, J. "Los principios del Derecho a la Protección de Datos", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016, p. 135.

[634] HERRÁN ORTIZ, A. I. *El derecho a la protección de datos personales en la sociedad de información.* Universidad de Deusto, Instituto de Derechos Humanos, Bilbao, 2003, p. 53.

[635] APARICIO SALOM, J. "Título II. Principios de la Protección de Datos. Artículo 4", en TRONCOSO REIGADA, A. *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Civitas, Madrid, 2010, pp. 323-340.

[636] PUYOL MONTERO, J., op. cit., p. 136.

[637] Artículo 5.1.a), del RGPD.

datos, estableciéndose que los mismos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados[638].

Asimismo, los datos deben ser recogidos con fines determinados, explícitos y legítimos, y no pueden ser tratados posteriormente de manera incompatible con dichos fines[639]. El RGPD introduce una limitación de la finalidad del tratamiento de los datos, que únicamente exceptúa el caso del tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales.

También, los datos personales deben ser exactos y, si fuera necesario, actualizados. Y para lograr este propósito, el RGPD establece que se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan[640].

Así también, se introduce una limitación en el plazo de conservación de los datos. El RGPD establece que los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales recogidos. La excepción a este principio, la da el mismo RGPD estableciendo que los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el RGPD a fin de proteger los derechos y libertades del interesado[641].

Además, el RGPD introduce el principio de integridad que lo une con el de confidencialidad. Para ello, establece que los datos personales deben ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas[642].

---

[638] Artículo 5.1.c), del RGPD.

[639] Artículo 5.1.b), del RGPD.

[640] Artículo 5.1.d), del RGPD.

[641] Artículo 5.1.e), del RGPD.

[642] Artículo 5.1.f), del RGPD.

4.1. La licitud de tratamiento.

Para que el tratamiento de datos personales pueda ser considerado lícito y leal en los términos que legista el RGPD, debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen a las personas físicas, así como la medida en que dichos datos son o serán tratados.

Asimismo, para que el tratamiento resulte lícito, los datos personales deben ser tratados con el consentimiento del interesado[643]. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la UE o de los Estados miembros, y constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar objetivos como la seguridad del Estado, la defensa, la seguridad pública[644], etc., el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, las siguientes circunstancias[645]:

(i) Cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto.
(ii) El contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento.
(iii) La naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales.
(iv) Las posibles consecuencias para los interesados del tratamiento ulterior previsto.
(v) La existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización[646].

[643] Artículo 6.1.a), del RGPD.

[644] Artículo 23, del RGPD.

[645] Artículo 6.4, del RGPD.

[646] La seudomización existe cuando los campos identificativos de un registro de datos se sustituyen por uno o más identificativos artificiales. El Artículo 4.53 del RGPD define la seudomización estableciendo que es: "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

El RGPD, dentro de lo que denominamos margen de maniobra[647], establece que los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del RGPD con respecto al tratamiento, fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento[648].

4.2. La transparencia.

TOMÁS MALLÉN[649] sostiene que la transparencia debe ser entendida como un "subderecho", ya que no sólo opera como un terreno limitado o restringido con respecto a la protección de datos personales, sino que se ha configurado como un derecho prestacional desde el punto de vista de que requiere una actuación positiva por parte de las autoridades públicas precisamente en el ejercicio del derecho a la protección de datos.

El principio de transparencia exige que toda información y comunicación relativa al tratamiento de los datos personales sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro[650]. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento.

---

[647] Haremos referencia al tema, en el epígrafe 7 del presente Capítulo.

[648] Artículo 6.2, del RGPD.

[649] TOMÁS MALLÉN, B. "Transparencia y protección de datos", en RALLO LOMBARTE, A.; GARCÍA MAHAMUT, R. *Hacia un Nuevo Derecho Europeo de Protección de Datos.* Tirant Lo Blanch, Valencia, 2015, p. 832.

[650] Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender. Considerando (58), del RGPD.

Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica, tal como comentamos anteriormente en éste Capítulo.

4.3. La información.

Los principios de tratamiento leal y transparente, exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específico en que se traten los datos personales. Se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran. Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente[651].

Asimismo, el RGPD menciona que se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso. Si los datos personales pueden ser comunicados legítimamente a otro destinatario, se debe informar al interesado en el momento en que se comunican al destinatario por primera vez. El responsable del tratamiento que proyecte tratar los datos para un fin que no sea aquel para el que se recogieron debe proporcionar al interesado, antes de dicho tratamiento ulterior, información sobre ese

[651] Considerando (60), del RGPD.

otro fin y otra información necesaria. Cuando el origen de los datos personales no pueda facilitarse al interesado por haberse utilizado varias fuentes, debe facilitarse información general[652].

Sin embargo, no es necesario imponer la obligación de proporcionar información cuando el interesado ya posea la información, cuando el registro o la comunicación de los datos personales estén expresamente establecidos por ley, o cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado. Tal podría ser particularmente el caso cuando el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas[653].

4.4. Especial mención al consentimiento del interesado.

Una de las novedades del RGPD para todos los datos personales es la importancia del concepto de consentimiento que el nuevo Reglamento define como: *"toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen"*[654].

Coincidimos con ADSUARA VARELA[655], quién sostiene que ésta definición tiene importancia porque viene a dejar de lado el consentimiento tácito, y abre dos caminos para otorgar el consentimiento:

(i) A través de una declaración.
(ii) A través de una acción.

Se deja de lado el consentimiento tácito, porque para otorgar su consentimiento, el interesado ha de hacerlo de forma clara y para unos fines específicos[656]. Sin que pueda

[652] Considerando (61), del RGPD.

[653] Considerando (62), del RGPD.

[654] Artículo 4. 11), del RGPD.

[655] ADSUARA VARELA, B. "El consentimiento", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016, p. 152.

[656] Considerando (32), del RGPD.

considerarse que la inacción de la persona pueda dar lugar a que por silencio se considere dado el consentimiento.

En éste sentido, el RGPD establece que:

> El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta[657].

Por tanto, el RGPD introduce importantes novedades en cuanto a las condiciones que debe reunir el consentimiento del interesado para legitimar el tratamiento de sus datos:

(i) El propio concepto de consentimiento alude a una manifestación de voluntad libre, específica, informada e inequívoca, ya sea mediante una declaración o una clara acción afirmativa, aportando el RGPD ejemplos de lo que puede considerarse un acto afirmativo claro (el marcado de una casilla en Internet o escoger parámetros técnicos para la utilización de servicios de la sociedad de la información), y también de lo que no puede ser considerado como tal (el silencio, las casillas pre marcadas o la inacción)[658].

(ii) Se aclara que, si el tratamiento tiene varios fines, el consentimiento del interesado debe solicitarse para cada uno de ellos, utilizando un lenguaje claro y sencillo.

(iii) El responsable debe ser capaz de demostrar que trata los datos con el consentimiento del interesado.

[657] Ibídem.

[658] Ibídem.

Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En particular, en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace[659]. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno[660].

Respecto a los tratamientos de datos que están en vigor o se inicien con anterioridad a la fecha en la que el RGPD entra en vigencia, es decir, el 25 de mayo de 2018, se ha hecho una previsión en el RGPD que supone literalmente que la Directiva 95/46/CE debe ser derogada por el RGPD. Todo tratamiento ya iniciado en la fecha de aplicación del RGPD debe ajustarse al RGPD en el plazo de dos años a partir de la fecha de su entrada en vigor. Cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del RGPD, a fin de que el responsable pueda continuar dicho tratamiento tras la fecha de aplicación del RGPD. Las decisiones de la Comisión Europea y las autorizaciones de

---

[659] De acuerdo con la Directiva 93/13/CE, debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Directiva 93/13/CE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores (DO L 95, 21.4.1993, p. 29), Disponible en Internet: <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L:1993:095:TOC> [Consulta: 11 febrero 2017].

[660] Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento. Considerando (43), del RGPD.

las autoridades de control basadas en la Directiva 95/46/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas[661].

4.5. Principio de Responsabilidad “proactiva”.

En lo que se refiere al catálogo de principios aplicables al tratamiento de los datos, se incorpora el llamado "principio de responsabilidad proactiva", también conocida como *“accountability*”, según la cual el responsable del tratamiento no sólo debe cumplir con todos los principios establecidos en el RGPD, sino que, además, debe ser capaz de demostrarlo[662]. Para demostrar el cumplimiento por parte del responsable del tratamiento de los datos, la normativa alude a la adhesión a códigos de conducta o mecanismos de certificación.

PIÑAR MAÑAS[663] manifiesta que a partir de ahora será necesario adoptar decisiones propias en función de los tratamientos de datos que se lleven a cabo y la naturaleza de estos. Y coincidimos con PIÑAR MAÑAS[664] al señalar que ésta responsabilidad proactiva va a estar mucho más al alcance de las grandes compañías y Administraciones públicas, pero no resultará tan sencillo para las pymes y para los organismos públicos pequeños.

Para ello, el responsable del tratamiento, deberá realizar en todo caso una valoración del riesgo del tratamiento de datos personales para los derechos y libertades de las personas de conformidad con el servicio prestado por el encargado, y aplicar medidas técnicas y organizativas adecuadas a cada caso.

Por lo tanto, existirán las denominadas evaluaciones del impacto. Es decir, cuando el tratamiento de datos pueda ocasionar un mayor riesgo para los derechos y libertades de las personas, las empresas deben llevar a cabo evaluaciones del impacto que las mismas pueden ocasionar en los datos personales.

---

[661] Considerando (171), del RGPD.

[662] El Artículo 5.2, del RGPD, establece que: *“El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)”.*

[663] PIÑAR MAÑAS, J. L. “Introducción. Hacia un nuevo modelo europeo de Protección de Datos”, en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016, p. 17.

[664] Ibídem.

5. Derechos de los ciudadanos en torno al RGPD.

El RGPD busca proteger los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, tanto si son procesados por entidades privadas como por Administraciones Públicas.

No sólo se reconocen los ya clásicos derechos de acceso, rectificación, cancelación y oposición, sino que éstos devienen superados, introduciendo el RGPD nuevos derechos: el denominado “derecho al olvido” como efectivo derecho de supresión, y la portabilidad de los datos, quedando estructurados todos los derechos en la normativa, de la siguiente manera: Transparencia (Artículo 12), Información (Artículos 13 y 14), Acceso (Artículo 15); Rectificación (Artículo 16); Supresión o derecho al olvido (Artículo 17); Limitación del tratamiento (Artículo 18); Portabilidad de los datos (Artículo 20) y Oposición (Artículo 21).

También se detallan mejor como garantías adecuadas para los interesados, las especificaciones y excepciones del deber de información y de los diversos derechos, los deberes de transparencia o la limitación del tratamiento de datos personales con fines de archivo en interés público, de investigación científica e histórica o fines estadísticos, como hemos hecho referencia en los epígrafes precedentes.

5.1. Derecho de acceso.

El RGPD dota de un acceso más sencillo a los datos personales, proporcionando al interesado más información sobre cómo se tratan esos datos y garantizando que la información esté disponible de una forma clara y comprensible, y que se pueda acceder a la misma, si el interesado así lo considera.

En este sentido, el RGPD establece que deben arbitrarse por parte de los Estados miembros, fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del propio RGPD, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios

electrónicos. El responsable del tratamiento viene a estar obligado, según el RGPD, a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas[665].

Los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Ello incluye el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo, los datos de sus HC que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas.

Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento.

El RGPD va más allá, e incluso establece que, si es posible, el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales. Este derecho no debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos. No obstante, estas consideraciones no deben tener como resultado la negativa a prestar toda la información al interesado. Si trata una gran cantidad de información relativa al interesado, el responsable del tratamiento debe estar facultado para solicitar que, antes de facilitarse la información, el interesado especifique la información o actividades de tratamiento a que se refiere la solicitud[666].

5.2. Derecho a la rectificación y al olvido.

El RGPD ha estructurado un derecho más claro a la supresión de los datos, denominado “derecho al olvido”. Este derecho entra en juego cuando un interesado no

[665] Considerando (59), del RGPD.

[666] Considerando (63), del RGPD.

desea que se sigan tratando sus datos, o cuando no exista ninguna razón legítima para conservarlos. En estos casos, y a instancia del interesado, sus datos personales deberán ser suprimidos. El derecho al olvido está vinculado al derecho de oposición y al derecho de cancelación, relacionados con los buscadores de Internet. Sostiene la AEPD que es el "derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima"[667].

No podemos abordar en ésta Tesis el derecho al olvido, que por sí mismo es merecedor de una Tesis y por su extensión no lo trataremos en profundidad[668], pero sí que debemos, al menos de forma breve, hacer algunas puntualizaciones al respecto.

Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un derecho al olvido, si la retención de tales datos infringe el RGPD o el Derecho de la UE o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el RGPD.

Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho, aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal,

---

667 Vid. AEPD, Nota informativa. Disponible en Internet: <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php> [Consulta: 11 agosto 2016].

668 Para profundizar más respecto al Derecho al olvido, véase: ÁLVAREZ CARO, M. *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital.* Reus, Madrid, 2015, pp. 67 y ss.; SIMÓN CASTELLANO, P. *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*. Bosch, Barcelona, 2015, pp. 203-286.; SIMÓN CASTELLANO, P. *El régimen constitucional del derecho al olvido digital.* Tirant lo Blanch, Valencia 2012, pp. 179-212.; RALLO LOMBARTE, A. *El derecho al olvido en internet: Google versus España*. Centro de Estudios Políticos y Constitucionales, Madrid, 2014, pp. 55 y ss.; TOURIÑO, A. *El derecho al olvido y a la intimidad en Internet*. Catarata, Madrid, 2014, pp. 33-45.

para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones[669].

A fin de reforzar el derecho al olvido en el entorno *online*, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales, esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales[670].

Actualmente la Jurisprudencia ha dado cabida a los casos que fueron presentados ante la justicia española, a través de los cuales se solicitaba la supresión de los datos personales de determinada persona que constaba en Internet. Sin embargo, ha de contemplarse como un derecho establecido y la UE debe tratar en su conjunto debido al incremento de quejas y demandas de los ciudadanos a fin de que las informaciones sobre sus personas sean eliminadas de buscadores y páginas webs.

En España este aumento se evidencia en el número creciente de demandas de protección de datos personales solicitadas frente a la AEPD[671]. Como consecuencia de esta concienciación por parte de la sociedad de la protección de sus derechos

[669] Considerando (65), del RGPD.

[670] Considerando (66), del RGPD.

[671] Según la memoria de la AEPD, presentada el 24 de mayo de 2011, las solicitudes de ciudadanos que piden que se cancelen sus datos en la Red o que se oponen a que éstos sean recuperados por buscadores ha crecido un 56 por ciento hasta acercarse al centenar, frente a las 57 recibidas en 2009, las 18 en 2008 y en 2007 sólo tres. En concreto, se trata de peticiones para que la Agencia tutele los derechos de cancelación y oposición, por la publicación de datos personales, principalmente, en diarios oficiales, medios de comunicaciones digitales y sentencias, y su indexación por parte de buscadores. Asimismo, la AEPD resolvió en este ámbito en torno a 110 tutelas en 2010 -frente a las 24 de 2009-, de las cuales 98 se refirieron al derecho de cancelación y oposición de ciudadanos respecto a la indexación por buscadores de Internet de datos. El 75,5% de las resoluciones estimaron las reclamaciones de los ciudadanos. Fuente: <www.agpd.es>

fundamentales en la red, se empieza a ampliar el contenido de ese derecho fundamental de la protección de datos con el denominado "derecho al olvido".

Este derecho al olvido puede ejercitarse frente a páginas web concretas e identificadas, pero también frente a buscadores[672]. La reacción de páginas web y buscadores no ha sido la misma, y mientras las primeras suelen acatar las decisiones de la AEPD a raíz de demandas de cancelación y oposición al tratamiento de los datos, en virtud de lo establecido en LOPD y en el RD 1720/2007, los buscadores, concretamente Google, se ha opuesto a acatar estas decisiones y ha acudido a la jurisdicción contencioso-administrativa, alegando que deben ser las páginas que incluyeron la información las que deberían satisfacer las demandas de cancelación y oposición de los titulares, además de proteger derechos fundamentales como la libertad de expresión e información. Es tal el punto de indeterminación en este tema debido a la antigüedad de la Directiva 95/46/CE, que la Sala de lo Contencioso-Administrativo de la Audiencia Nacional ha planteado una cuestión prejudicial pionera en la materia, ante TJUE para que resuelva estas cuestiones.

Recientemente el TJUE se pronunció al respecto[673], y en contra de lo que recomendó Abogado General del Tribunal de Justicia del TJUE que propuso al TJUE que se

---

[672] Véase al respecto: SAN, de 29 de diciembre de 2014, Recurso 725/2010 (Roj: SAN 5129/2014 ECLI:ES:AN:2014:5129). Siguiendo el criterio jurisprudencial, la AEPD se ha pronunciado al respecto, a través de varias Resoluciones: AEPD Resolución Nº: R/01239/2015 Procedimiento Nº: TD/01997/2014; AEPD Resolución Nº: R/01119/2015 Procedimiento Nº: TD/01955/2014; AEPD Resolución Nº: R/00555/2015 Procedimiento Nº: TD/01533/2014; AEPD Resolución Nº: R/00741/2015 Procedimiento Nº: TD/01843/2014). Todas las Resoluciones pueden consultarse en <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php> [Consulta: 11 agosto 2016]. También en el mismo sentido: *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"* C-131/12 (Criterios comunes para aplicar la sentencia sobre el "derecho al olvido"), del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 26 de noviembre de 2014, 14/EN. Disponible en Internet (versión en inglés): <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf> [Consulta: 10 agosto 2016].

[673] STJCE de 19 de mayo de 2009, en los Asuntos acumulados C-171/07 y C-172/07. Disponible en Internet: <http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A62007CJ017>; STJCE de 13 de mayo de 2014, Asunto C-131/12, Google Spain, S.L. Contra AEPD y Mario Costeja González. Disponible en Internet: <http://www.abc.es/gestordocumental/uploads/Internacional/sentenciagoogle.pdf> [Consulta: 7 julio 2015].

manifieste sobre el llamado "derecho al olvido" en Internet en el sentido de entender que los proveedores de servicios de motor de búsqueda en Internet no son responsables, sobre la base de la Directiva sobre Protección de Datos, de los datos personales incluidos en las páginas web que tratan[674], el TJUE sentenció que Google, el mayor buscador del mundo, deberá obtenerse de exhibir en sus resultados de búsquedas los datos personales de una persona que se considera afectada por la difusión de tales informaciones, según estableció el TJUE. En base a la STJUE, dictada a petición de la AN española, Google o cualquier otro buscador está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona, los enlaces a páginas web publicadas por terceros que contengan información relativa a esta persona, si el afectado lo solicita. De esta manera, el TJUE clarifica que esa obligación puede existir también en el supuesto de que este nombre o

[674] El Abogado del Alto Tribunal, Sr. NIILO JÄÄSKINEN, concluyó lo siguiente respecto al derecho al olvido: "*A la luz de las observaciones precedentes, propongo al Tribunal de Justicia que responda del siguiente modo a las cuestiones prejudiciales planteadas por la Audiencia Nacional: 1) Se lleva a cabo tratamiento de datos personales en el marco de las actividades de un «establecimiento» del responsable del tratamiento, en el sentido del artículo 4, apartado 1, letra a), 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, cuando la empresa que provee el motor de búsqueda establece en un Estado miembro, con el fin de promover y vender espacios publicitarios en su motor de búsqueda, una oficina o una filial que orienta su actividad hacia los habitantes de dicho Estado. 2) Un proveedor de servicios de motor de búsqueda en Internet cuyo motor de búsqueda localiza información publicada o incluida en Internet por terceros, la indexa automáticamente, la almacena con carácter temporal y, por último, la pone a disposición de los usuarios de Internet, «trata» datos personales, en el sentido del artículo 2, letra b), de la Directiva 95/46 cuando esta información contiene datos personales. Sin embargo, no se puede considerar al proveedor de servicios «responsable del tratamiento» de tales datos personales, en el sentido del artículo 2, letra d), de la Directiva 95/46, a excepción de los contenidos del índice de su motor de búsqueda, siempre que el proveedor del servicio no indexe o archive datos personales en contra de las instrucciones o las peticiones del editor de la página web. 3) Los derechos de cancelación y bloqueo de datos, establecidos en el artículo 12, letra b), y el derecho de oposición, establecido en el artículo 14, letra a), de la Directiva 95/46, no confieren al interesado el derecho a dirigirse a un proveedor de servicios de motor de búsqueda para impedir que se indexe información que le afecta personalmente, publicada legalmente en páginas web de terceros, invocando su deseo de que los usuarios de Internet no conozcan tal información si considera que le es perjudicial o desea que se condene al olvido".* Conclusiones del Abogado General del Tribunal de Justicia, Sr. NIILO JÄÄSKINEN, en el Asunto C-131/12: Google Spain, S.L. y Google Inc. / Agencia Española de Protección de Datos, M. C. G (Conclusiones de fecha 25.05.2013. ECLI:EU:C:2013:424) <http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=19636> [Consulta: 19 noviembre 2015].

esta información no se borren previa o simultáneamente de esas páginas web donde han sido publicadas e incluso aunque la publicación en dichas páginas hubiera sido en sí misma lícita. La STJUE resuelve la demanda del Sr. Mario Costeja que aparecía en Internet en una noticia del periódico La Vanguardia, vinculado a un embargo de la seguridad social, que ya había sido resuelto y liquidado. La aparición de esa noticia, que, si bien era cierta, le causaba un daño grave a su reputación. A partir de ésta STJUE pionera en la materia, se abre una importante puerta que permitirá a los interesados ejercer el derecho al olvido, eliminándose sus datos personales de Internet. Así también el TJUE concluye que *"el gestor de un motor de búsqueda en Internet es responsable del tratamiento que aplique a los datos de carácter personal que aparecen en las páginas web publicadas por terceros"* y, por tanto, debe respetar la directiva comunitaria sobre protección de datos. En ese sentido, se recoge que las personas tendrán derecho a solicitar directamente del motor de búsqueda, que deberá entonces examinar debidamente si son fundadas, con las condiciones establecidas en la directiva de protección de datos, *"la eliminación de referencias que les afectan, aunque esta información no haya sido eliminada por el editor ni dicho editor haya solicitado su desindexación".* En caso de no atenderse su solicitud, las personas tienen derecho a recabar la tutela de la AEPD y de los Tribunales para llevar a cabo las comprobaciones necesarias y ordenen al responsable que adopte medidas precisas en consecuencia.

La AEPD también ha desestimado reclamaciones que le han sido planteadas por particulares contra Google, por entender en el mismo sentido que JÄÄSKINEN[675], que el buscador no tenía vinculación directa con la noticia a la que conducía, y, además, de ser ésta importante a los fines públicos, no podía obligar al buscador a eliminar dicho enlace[676]. La AEPD determina que es relevante a los fines públicos que se conozcan

[675] Ibídem.

[676] Véase al respecto: Resolución de la AEPD formulada por la reclamación de B.B.B. contra Google INC. y Google Spain, S.L. (Resolución Nº: R/00853/2015 Procedimiento Nº: TD/01671/2014) en la que se solicita por parte de un particular la eliminación de sus datos personales que aparecen en un enlace de Google. En el citado enlace aparecen los datos del interesado en una noticia publicada en un medio de comunicación del año 2012 en el que se informaba que el reclamante en su condición de farmacéutico había adulterado recetas por lo que fue condenado a prisión e indemnización por falsedad en documento oficial y estafa. Google contestó denegando la solicitud del afectado al considerar que la información posee interés público. La AEPD resolvió desestimando la denuncia del farmacéutico, entendiendo que: *"nos encontramos con una información que se considera de interés para los ciudadanos de la que no se ha demostrado con prueba documental que sea inveraz y obsoleta, por lo que, en lo que respecta a la normativa de protección de datos, nos encontraríamos ante un tratamiento legitimado y no supondría vulneración de la normativa en materia de protección de*

ciertas noticias sobre los particulares, cuando éstas noticias resultan importantes para toda la ciudadanía y no se estaría vulnerando la protección de datos que contempla la normativa vigente. Es interesante ver como la AEPD pondera el derecho a la información pública sobre el derecho a la protección de datos, cuando se pretende tergiversar su protección y esconder aspectos delictivos de una persona[677].

5.3. Nuevo derecho a la portabilidad de datos.

El RGPD incorpora un nuevo derecho, que la Directiva 95/46/CE no contemplaba en su articulado. El RGPD lo denomina "derecho a la portabilidad de los datos" y se trata de un derecho que se configura a favor de los interesados, facilitando la transmisión de datos personales entre proveedores de servicios, de modo tal, que los datos personales relativos a la persona en cuestión y que esta haya proporcionado a un responsable del tratamiento pueden ser "portados" de un operador a otro, siempre y cuando así lo autorice, otorgando el interesado su consentimiento[678].

---

datos, por lo que procede desestimar la solicitud de tutela de derechos formulada". Asimismo, la Resolución de la AEPD formulada por la reclamación de B.B.B. contra Google INC. y Google Spain, S.L. (Resolución Nº: R/00646/2015 Procedimiento Nº: TD/01846/2014) por la que el denunciante solicita se borren unos enlaces de Google en los que aparecen los datos del interesado en unas noticias publicadas en varios medios de comunicación en el año 2008, en relación a su detención como médico chileno sin titulación convalidada en España que utilizaba la identidad de otro facultativo, que convenció a una anciana de 94 años para un matrimonio de conveniencia que legalizara su estancia en España; y a la que estafó 20.000 euros para facilitar una intervención quirúrgica. Google contestó denegando la solicitud del afectado al considerar que la información es relevancia y de interés público en relación a su vida profesional. La AEPD desestimó la denuncia por entender que: *"nos encontramos con una información que se considera de interés para los ciudadanos, al referirse a la actuación de una persona acusada, entre otros, de delitos de intrusismo laboral y contra la salud pública, de la que no se ha demostrado con prueba documental que sea inveraz y obsoleta, por lo que, en lo que respecta a la normativa de protección de datos, nos encontramos ante un tratamiento legitimado y no supondría vulneración de la normativa en materia de protección de datos, por lo que procede desestimar la solicitud de tutela de derechos formulada".* Pueden consultarse todas las Resoluciones en: <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php> [Consulta: 19 septiembre 2015].

[677] Véase al respecto, las Resoluciones de la AEPD: Resolución Nº: R/00853/2015 Procedimiento Nº: TD/01671/2014 y AEPD Resolución Nº: R/00646/2015 Procedimiento Nº: TD/01846/2014. Pueden consultarse todas las Resoluciones en: <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php> [Consulta: 19 septiembre 2015].

[678] Artículo 20, del RGPD.

Éste derecho, tiene por objetivo reforzar el control del interesado sobre sus propios datos[679], permitiendo a los interesados copiar o transmitir sus datos personales fácilmente de un entorno informático a otro, y entre diferentes proveedores o responsables del tratamiento[680]. De hecho, el objetivo primordial de la portabilidad de los datos es facilitar el cambio de un proveedor de servicios a otro, reforzando así la competencia entre servicios, resultando de ésta manera, más fácil para las personas la opción de cambiar entre diferentes proveedores.

En nuestro país[681] se está utilizando éste derecho -aunque sin que reciba denominación específica-, cuando se hace uso de la HCD, porque diversos operadores sanitarios pueden tener acceso a nuestra HC, siempre y cuando medie nuestro consentimiento para tratar los datos de salud, y, además, se verifica otra premisa del RGPD, que exige que se trate de datos estructurados, es decir, datos personales contenidos en un soporte electrónico, susceptible de ser trasladados.

Por tanto, el interesado tendrá derecho a recibir los datos personales que le incumban y que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y el derecho a exigir al responsable que los transmita a otro responsable del tratamiento sin que pueda impedirlo el responsable al que se los hubiera facilitado, pero con dos limitaciones. Por un lado, éste tratamiento y portabilidad debe estar basado en el consentimiento de la persona; y, por otro lado, el tratamiento

---

[679] Al respecto, el Considerando (68) del RGPD establece que: *"Para reforzar aún más el control sobre sus propios datos, cuando el tratamiento de los datos personales se efectúe por medios automatizados, debe permitirse asimismo que los interesados que hubieran facilitado datos personales que les conciernan a un responsable del tratamiento los reciban en un formato estructurado, de uso común, de lectura mecánica e interoperable, y los transmitan a otro responsable del tratamiento. Debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de datos. Dicho derecho debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato".*

[680] Directrices sobre el derecho a la portabilidad de los datos del Grupo de Trabajo sobre protección de datos del Artículo 29 (GT 242), 13 de diciembre de 2016. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricesportabilidad.pdf> [Consulta: 15 febrero 2017].

[681] En España podemos encontrar un primer antecedente que se denominó "derecho a la portabilidad numérica", que permitía a las personas abonadas a una línea telefónica, mantener su número de teléfono al cambiar de domicilio, o al cambiar de operador telefónico. Ésta disposición fue recogida en el Real Decreto 2296/2004, de 10 de diciembre, por el que se aprueba el Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración (BOE núm. 314, 30.12.2004).

debe efectuarse por medios automatizados, lo cual presupone la necesidad de que la información que se trate sea de carácter estructurado.

No obstante, el derecho a la portabilidad de datos, no es un derecho absoluto, tal y como recuerdan FERNÁNDEZ-SAMANIEGO y FERNÁNDEZ-LONGORIA[682], porque el mismos RGPD se encarga de poner restricciones, limitaciones y excepciones[683]. Éstas restricciones se basan en las nociones de necesidad y proporcionalidad.

En base a ello, éstas restricciones se ven reflejadas, según establece el Artículo 23 del RGPD, en el Derecho de la UE o de los Estados miembros de tal forma que, el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance del derecho a la portabilidad de datos cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

(i) la seguridad del Estado,
(ii) la defensa,

---

[682] FERNÁNDEZ-SAMANIEGO, J.; FERNÁNDEZ-LONGORIA, P. "El Derecho a la Portabilidad de los Datos", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016, p. 267.

[683] El Considerando (73) del RGPD establece que: *"El Derecho de la Unión o de los Estados miembros puede imponer restricciones a determinados principios y a los derechos de información, acceso, rectificación o supresión de datos personales, al derecho a la portabilidad de los datos, al derecho de oposición, a las decisiones basadas en la elaboración de perfiles, así como a la comunicación de una violación de la seguridad de los datos personales a un interesado y a determinadas obligaciones conexas de los responsables del tratamiento, en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano, la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública o de violaciones de normas deontológicas en las profesiones reguladas, y su prevención, otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un importante interés económico o financiero de la Unión o de un Estado miembro, la llevanza de registros públicos por razones de interés público general, el tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios, o la protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios. Dichas restricciones deben ajustarse a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales".*

(iii) la seguridad pública,

(iv) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención,

(v) otros objetivos importantes de interés público general de la UE o de un Estado miembro, en particular un interés económico o financiero importante de la UE o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social,

(vi) la protección de la independencia judicial y de los procedimientos judiciales,

(vii) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas,

(viii) una función de supervisión, inspección o reglamentación vinculada,

(ix) la protección del interesado o de los derechos y libertades de otros, y,

(x) la ejecución de demandas civiles[684].

a) Excepciones al derecho a la portabilidad de los datos.

Las excepciones al derecho a la portabilidad de los datos, las recoge el RGPD en su Artículo 89, al establecer que el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas[685], con arreglo al RGPD, para los derechos y las libertades de los interesados. Estas garantías consistirán en la aplicación de medidas tanto técnicas como organizativas, que el RGPD, para las cuales se pone el acento en el encargado del tratamiento para que las evalúe y las aplique en función de los datos que se están tratando.

[684] Artículo 23, del RGPD.

[685] El RGPD se refiere a las posibles garantías en varios de sus Artículos. En éste sentido, el Artículo 89.1 menciona la seudomización como posible garantía para minimizar los datos y que el posterior tratamiento no pueda revelar la identidad de la persona. El Artículo 5.e) menciona la posibilidad de limitación del plazo de conservación de los datos. El Artículo 9.2.j) establece que, si el tratamiento es necesario para fines públicos, debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Asimismo, el RGPD establece que se debe autorizar a los Estados miembros a que establezcan limitaciones del tratamiento, a la portabilidad de los datos y de oposición, cuando se traten datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos[686].

Sin embargo, el RGPD no establece una forma o un procedimiento específico para que el interesado pueda ejercer el derecho a la portabilidad de datos. Al respecto, sostienen FERNÁNDEZ-SAMANIEGO y FERNÁNDEZ-LONGORIA[687], que, aunque el RGPD no indica el contenido que debe tener una solicitud de derecho de portabilidad, por la propia naturaleza de este derecho las solicitudes a presentar por parte de los interesados deberán indicar los datos concretos a los que se refiere, si lo que se pretende es que se transfieran los datos a otro interesado, y, también deberá el usuario proporcionar la información sobre el responsable al que deben ser enviados éstos datos, a fin de que el receptor de la solicitud pueda contactar con él y portarle los datos.

6. Alcance territorial del RGPD.

Respecto a la eficacia territorial del RGPD, hay una primicia destacable y es que los legisladores europeos han tenido en cuenta a la hora de elaborar el RGPD una realidad muy patente en nuestra actividad diaria que es la utilización cada vez más frecuente de Internet, para realizar actividades *on line*, y por tanto esto podía escaparse a la protección que brindaban los ordenamientos europeos, tan sólo con tratarse de empresas que estaban situadas fuera de la UE, por tanto, era fácil burlar la normativa de protección de datos[688].

---

[686] El Considerando (156), del RGPD, establece que: *"Debe autorizarse que los Estados miembros establezcan, bajo condiciones específicas y a reserva de garantías adecuadas para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición, cuando se traten datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos".*

[687] FERNÁNDEZ-SAMANIEGO, J.; FERNÁNDEZ-LONGORIA, P., op. cit., p. 268.

[688] Para profundizar más este tema, véase: RIPOL CARULLA, S. "Aplicación territorial del Reglamento", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016, pp. 77-95.

Ahora, el RGPD se aplicará al procesamiento de datos de ciudadanos europeos por entidades establecidas en Europa, pero también por aquellas empresas situadas fuera de la UE que realicen actividades dentro de la UE y que impliquen el tratamiento de datos personales, incluso aunque no tengan presencia física en el territorio de la UE.

La finalidad de esta amplitud en el alcance territorial es garantizar que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud del RGPD, por tanto, el tratamiento de datos personales de las personas que residen en la UE por parte de un responsable o un encargado no establecido en la UE, debe regirse por el RGPD si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados. El RGPD incluso añade, que ésta protección reglamentaria regirá independientemente de que medie pago o no por los bienes o servicios.

Ahora bien, ésta previsión podía dar lugar a incertidumbres respecto a la determinación de si dicho responsable o encargado, ofrece bienes o servicios a ciudadanos que residan en la UE, o planea ofrecer servicios a residentes en uno o varios de los Estados miembros de la UE. Frente a ésta duda, el RGPD ha previsto que hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la UE, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a ciudadanos en la UE[689].

Por tanto, el RGPD deja claro que sus disposiciones no sólo se aplican al tratamiento de datos realizado por un responsable o encargado del tratamiento en el marco de un establecimiento ubicado en la UE, sino también al tratamiento de datos de interesados que residan en la UE por parte de responsables o encargados no establecidos en la UE, en dos situaciones:

a) cuando el tratamiento de datos tenga por objeto la oferta de bienes o servicios a dichos interesados en la UE;

b) cuando el tratamiento consista en el control de su comportamiento (por ejemplo, mediante cookies u otros dispositivos similares).

[689] Considerando (23), del RGPD.

Según RIPOL CARULLA[690], con la aplicación el RGPD las sociedades establecidas fuera de la UE, pero que actúan en su territorio, tendrán que aplicar las mismas reglas cuando ofrezcan bienes y servicios en el mercado comunitario, creando así un campo de juego nivelado, garantizando tanto la libre circulación de datos en la UE, como la homogenización del derecho de los ciudadanos de la UE a la protección de sus datos personales.

Evidentemente, consideramos que es un avance muy significativo, y que viene a dar respuesta en gran parte a los problemas que comentábamos en el Capítulo anterior. No sólo asegura la protección de los datos personales cuando un ciudadano de la UE realiza una compra *on line*, o solicita determinado servicio, sino que va más allá y también prevé el control del comportamiento, lo cual nos parece una novedad sustancial desde el punto de vista de los datos sensibles. Hoy en día, puede conocerse el comportamiento –lo que denominamos perfil del cliente- tan sólo a través de algoritmos matemáticos que recogen a través de cookies nuestras búsquedas en Internet, la información que guardamos en nuestras apps, etc. Y ésta información es lo que hace que mientras navegamos por la web nos aparezcan publicidades relacionadas con nuestras búsquedas anteriores y nuestros gustos. Esto, relacionado exclusivamente con los datos sensibles, es muy notorio respecto a las apps que tenemos en nuestros dispositivos móviles, por ejemplo, que contienen información absolutamente íntima sobre nosotros, como, por ejemplo, una dieta determinada, el calendario de ovulación, etc.[691].

---

[690] RIPOL CARULLA, S. "Aplicación territorial del Reglamento", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016, p. 92.

[691] Sólo por citar algunas apps de salud que recogen datos médicos, podemos destacar algunas de las más populares, sin embargo, en el mercado ya existen centenares de estas aplicaciones para móviles. La más conocida quizás es Nike Plus. La aplicación de Nike es una de las apps de salud de referencia entre los aficionados al *running*. Las posibilidades que ofrece son diversas para monitorizar la actividad física, mediante el GPS y la geolocalización incorporados en la aplicación, detectan los kilómetros que has recorrido y el tiempo que has tardado. Endomondo, es la app de salud y entrenamiento que registra todo tipo de deportes: correr, bicicleta, caminar, kayak, etc., haciendo un seguimiento de la actividad física, mientras que la analiza y lleva un registro de la actividad cardíaca. Cardiograph de Macropinch, es un verdadero cardiógrafo que controla el ritmo cardíaco utilizando sensores e incluso la cámara del smartphone. La app Tension arterial va más allá, y con ella se puede llevar un control de la tensión arterial o presión sanguínea, posibilitando de envío de los datos por mail o SMS. Doctoralia permite emitir *feedback* de los pacientes hacia los profesionales sanitarios. IDoctus

Coincidimos con RIPOL CARULLA[692], al comentar que el RGPD establece unas disposiciones sobre la aplicación territorial claras, racionales y simples, que contribuyen al objetivo de la reforma del derecho comunitario de protección de datos, tanto desde el punto de vista de la defensa de los derechos de los particulares, como desde el punto de vista del establecimiento de las condiciones que dotarán de seguridad jurídica en las relaciones de libre circulación de datos.

6.1. Transferencias a terceros países.

Con la nueva reglamentación, la UE prevé normas específicas para la transferencia de datos personales fuera de la UE, con el fin de garantizar la mejor protección posible de los datos cuando estos se exporten al extranjero. Después de muchas negociaciones, finalmente el 8 de septiembre de 2015 se llegó a un "*Umbrella Agreement*" (Acuerdo Marco) entre la UE y Estados Unidos sobre el alto nivel de protección de datos en los intercambios de información entre la UE y los Estados Unidos[693], que fue firmado por las partes el 2 de junio de 2016[694], sobre fundamentalmente datos personales, registros

---

permite un diagnóstico clínico en el mismo teléfono. Dermomap, ayuda al diagnóstico y a detectar enfermedades de la piel, entre ellas alergias e hinchazones. Socialdiabetes, ayuda al control de la diabetes tipo 1 y 2 y hace posible que los pacientes calculen las dosis de hidratos y la administración de insulina.

[692] RIPOL CARULLA, S., op. cit., p. 95.

[693] Las negociaciones sobre el *"Umbrella Agreement"* (Acuerdo Marco), de fecha 8.09.2015, pueden consultarse en Internet: <http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm> [Consulta: 19 septiembre 2015].

[694] El 2 de junio de 2016, la UE y los Estados Unidos firmaron el denominado "Umbrella Agreement" (Acuerdo Marco), que establece un marco amplio de protección de datos de alto nivel para la cooperación en materia penal. El acuerdo mejora, en particular, los derechos de los ciudadanos de la UE mediante la igualdad de trato con los ciudadanos estadounidenses en lo que se refiere a los derechos de reparación judicial ante los tribunales estadounidenses. El Acuerdo abarca todos los datos personales intercambiados entre las autoridades policiales y de justicia penal de los Estados miembros de la UE y las autoridades federales estadounidenses con el fin de prevenir, investigar, detectar y perseguir delitos, incluido el terrorismo. El acuerdo facilitará la cooperación en materia de aplicación de la legislación penal, al mismo tiempo que se establecerán salvaguardias y garantías de la legalidad de las transferencias de datos. Entre ellas figuran, por ejemplo, disposiciones sobre limitaciones claras en el uso de los datos, la obligación de solicitar el consentimiento previo antes de cualquier transferencia de datos, la obligación de definir períodos de retención adecuados, el derecho de acceso y rectificación, etc. El Acuerdo complementará los acuerdos existentes y futuros entre la UE

de antecedentes penales, nombres y direcciones, pudiendo los ciudadanos de ambas partes acceder a sus datos, cancelarlos y/o modificarlos.

El Reglamento también abarca la transferencia de datos personales a terceros países u organizaciones internacionales. Con este fin, encomienda a la Comisión Europea la evaluación del nivel de protección que ofrece un territorio o un sector de tratamiento en un tercer país. Cuando la Comisión Europea no haya adoptado una decisión de adecuación sobre un territorio o sector, la transferencia de datos personales se puede seguir realizando en casos especiales o cuando existan garantías apropiadas (cláusulas tipo de protección de datos, normas corporativas vinculantes, cláusulas contractuales).

Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la UE y organizaciones internacionales, resultan necesarios para la expansión del comercio y la cooperación internacional. El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. No obstante, si los datos personales se transfieren de la UE a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la UE por el RGPD, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional. En todo caso, las transferencias a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el RGPD, es decir, cuando el responsable o encargado cumple las disposiciones del RGPD relativas a la transferencia de datos personales a terceros países u organizaciones internacionales[695].

---

y los Estados Unidos y entre los Estados miembros y los Estados Unidos entre las autoridades encargadas de hacer cumplir la ley. No constituye en sí mismo un instrumento jurídico para la transferencia de información personal a los Estados Unidos, sino que complementa, cuando sea necesario, salvaguardias de protección de datos en los acuerdos de transferencia de datos existentes o futuros o en las disposiciones nacionales que autorizan dichas transferencias. Disponible en Internet: <http://www.consilium.europa.eu/de/press/press-releases/2016/06/02-umbrella-agreement/> [Consulta: 2 abril 2017].

[695] Considerando (101), del RGPD.

7. Margen de maniobra en algunos ámbitos permitidos por el RGPD.

Si bien, el RGPD como figura de derecho comunitario, obliga de por sí a todos sus destinatarios, es decir a los Estados miembros, sí que detectamos que el RGPD deja margen a las legislaciones nacionales para que amplíen las garantías contenidas en él.

El RGPD dota de lo que viene a denominar "margen de maniobra" y junto con la normativa general y horizontal sobre protección de datos, los Estados miembros cuentan con distintas normas sectoriales específicas en ámbitos que precisan disposiciones más específicas. Dado esa presuposición previa y como punto de partida del RGPD, establece que: *"El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»)"*[696].

En el caso de los menores de edad, aunque es un tema que no podemos abordar por su extensión, sí queremos hacer referencia a que, el RGPD fija la edad mínima en 16 años para que un menor pueda dar el consentimiento en relación con el tratamiento de sus datos personales, no obstante, hace mención expresa a que: *"Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años"*[697].

También vemos esta posibilidad de ampliar garantías por parte de un Estado miembro en el caso de los datos de salud, datos genéticos y datos biométricos. Establece el RGPD en este sentido que: *"Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud"*[698]. Cierto es, que, por la relevancia misma de ésta categoría de datos, según explicamos en la primera parte de ésta Tesis, la UE utiliza como punto de partida una presuposición sobre la existencia de normas internas en los diferentes Estados miembros, que legislan y protegen a esta especial categoría de datos sensibles. Por ello, se adelanta a legislar sobre el particular, intentando que esa normativa que presupone existe, se complete con el RGPD.

---

[696] Considerando (10), del RGPD.

[697] Artículo 8.1, del RGPD.

[698] Artículo 9.4, del RGPD.

Al respecto, el RGPD también contiene una previsión, que según GARCÍA MEXÍA[699], resulta curiosa desde el punto de vista de la Jurisprudencia del TJUE, por cuanto autoriza a integrar en normas nacionales en la materia disposiciones del RGPD, en aras a una mayor claridad, manifestando el precepto que:

> En los casos en que el presente Reglamento establece que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, estos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del presente Reglamento[700].

8. Los datos de salud en el RGPD.

La nueva regulación europea de protección de datos proporciona una definición del concepto de datos sanitarios, algo que no incluía la anterior Directiva 95/46/CE. Esta definición es la siguiente: «datos relativos a la salud»: *datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud*[701]*.* También el RGPD, contempla una subcategoría de datos de salud, que son los datos biométricos, a los que haremos referencia en el siguiente epígrafe.

Ésta definición no sólo refiere a la salud de la persona, sino que es mucho más abarcadora, y comprende, desde nuestro punto de vista, el estado de salud general de la persona, entendiéndose por tal, todos los datos de carácter sanitario que envuelvan a la misma persona y forman parte de su HC, y que reflejen todas sus enfermedades, dolencias, padecimientos, etc. Y en este sentido, el RGPD considera que:

> Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia (…), de conformidad con la todo número, símbolo o dato asignado a una persona

[699] Para profundizar más al respecto, véase: GARCÍA MEXÍA, P., op. cit., p. 25.

[700] Considerando 8, del RGPD.

[701] Artículo 4.15, del RGPD.

> física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro"[702].

El RGPD realiza una definición más precisa y más extensa de lo que se debe entender por datos de salud, respecto a la prevista en nuestro ordenamiento interno[703].

Coincidimos con ÁLVAREZ-RIGAUDIAS[704], que expresa que ésta definición que ha asumido el RGPD es amplía porque se ha basado en la opinión del Grupo de Trabajo del Artículo 29[705], que hizo una reflexión sobre la información que captan o procesan distintos dispositivos, que antes no eran tenidos en cuenta a nivel de salud, pero que registran nuestros pasos, nuestro ritmo cardíaco, las calorías consumidas, etc. En base a ésta reflexión, el Grupo de Trabajo del Artículo 29, determinó que han de tener consideración de datos de salud aquellos que sean:

(i) Datos indubitadamente de carácter médico. En éste sentido, los datos personales que se relacionan con la salud deberían incluir en particular todos los datos que pertenecen al estado de salud de un sujeto de datos, información sobre el registro

---

[702] Considerando (35), del RGPD. En el mismo sentido, véase: Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88, 4.4.2011, p. 45). Disponible en Internet: <http://eur-lex.europa.eu/legalcontent/ES/TXT/?uri=uriserv:OJ.L_.2011.088.01.0045.01.SPA&toc=OJ:L:2011:088:TOC> [Consulta: 15 febrero 2017].

[703] Nuestro ordenamiento interno define a los Datos de carácter personal relacionados con la salud, estableciendo que se trata de *"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".* Artículo 5.1.g) del RD 1720/2007.

[704] ÁLVAREZ-RIGAUDIAS, C. "Tratamiento de Datos de Salud", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016, p. 174.

[705] Grupo de Trabajo del Artículo 29. *ANNEX. Health data in apps and* devices (datos de salud en apps y dispositivos). 5 de febrero de 2015. Disponible en Internet: <http://ec.europa.eu/justice/dataprotection/article29/documentation/otherdocument/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf> [Consulta: 15 febrero 2017].

del individuo para la provisión de Seguridad Social, información sobre pagos o elegibilidad para asistencia médica en lo que concierne al individuo, un número, símbolo o particular asignado a un individuo para únicamente identificar al individuo para objetivos de salud, cualquier información sobre el individuo se reunió en el curso de la provisión de Seguridad Social al individuo, la información sacada de las pruebas o el examen de un cuerpo se separa o la sustancia corporal, incluyendo muestras biológicas, identificación de una persona como proveedor de asistencia médica al individuo, o cualquier información sobre por ejemplo, una enfermedad, incapacidad, riesgo de enfermedad, HC, tratamiento clínico, o el estado real fisiológico o biomédico del sujeto de datos independiente de su fuente, como por ejemplo, de un médico u otro profesional de salud, un hospital, un dispositivo médico, o una prueba in vitro diagnóstica[706].

(ii) Datos en bruto provenientes de los sensores, que se pueden usar por sí mismos, o combinados con otros de la misma persona para inferir una conclusión respecto al estado de salud o el riesgo de salud de la persona. Al respecto el Grupo de Trabajo del Artículo 29, señala que los datos de salud, abarcan un concepto mucho más amplio que el término médico. Asimismo, han concluido que la información como el hecho que una mujer ha roto su pierna, que una persona lleva gafas o lentillas de contacto, datos sobre la capacidad intelectual y emocional de una persona, la información sobre fumar y bebida alcohólica, datos sobre alergias reveladas a entidades privadas (como líneas aéreas) o a cuerpos públicos, constituyen todos ellos datos sobre la salud[707].

(iii) Conclusiones sobre el estado de salud o riesgo de salud de una persona -con independencia de que esas conclusiones resulten o no certeras, legítimas u oportunas-. También, el Grupo de Trabajo del Artículo 29, asume que hay una categoría de datos personales generados por el modo de vivir de la sociedad a

[706] Vid. Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos), (Comunicación COM (2012) 11 final 25.01.2012). Disponible en Internet: <https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjlrPzE0IrTAhVMtBQKHR9uAmkQFggsMAE&url=http%3A%2F%2Fwww.europarl.europa.eu%2FRegData%2Fdocs_autres_institutions%2Fcommission_europeenne%2Fcom%2F2012%2F0011%2FCOM_COM(2012)0011_EN.pdf&usg=AFQjCNG0VBRS36IGUTt_C2F00diCYC9lyw> [Consulta: 6 abril 2015].

[707] Ibídem.

través de la utilización de las apps y dispositivos en general, que no será considerado como datos de salud. Esto concierne a los datos de los cuales no pueden obtenerse conclusiones razonables sobre el estado de salud de una persona. No todos los datos obtenidos en bruto por una app que brinda información sobre la persona, pueden ser considerados que constituyen datos salud[708].

8.1. Obligaciones específicas sobre el tratamiento de los datos de salud en el RGPD.

El RGPD incluye la consideración de tratamiento de datos a "gran escala". Resulta cuanto menos curioso el empleo terminológico que hace, puesto que no existe definición de lo que debe entenderse por gran escala o cómo cuantificar los datos para considerarlos a gran escala[709].

En este sentido, podemos citar el Artículo 30 del RGPD sobre el registro de las actividades de tratamiento, que establece en su apartado 5 que las obligaciones sobre el registro de las actividades de tratamiento no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1[710]. Por lo tanto, el precepto no acaba de aclarar si debe considerarse un tratamiento a gran escala a partir de 250 personas, o siempre que se trate de datos de salud deben tomarse las especiales precauciones que señala el RGPD.

Sin embargo, el RGPD contempla que, si se tratan datos de salud a gran escala, obligatoriamente se ha de atender a los siguientes requerimientos:

(i) El responsable o el encargado del tratamiento no establecido en la UE que esté tratando datos personales de interesados que residan en la UE y cuyas actividades de tratamiento están relacionadas con la oferta de bienes o servicios a dichos interesados en la UE, independientemente de si se requiere un pago por parte de estos, o con el control de su comportamiento en la medida

[708] Ibídem.

[709] ÁLVAREZ-RIGAUDIAS, C., op. cit., pp. 183-184.

[710] Artículo 30 y Considerando (91), del RGPD.

en que este tenga lugar en la UE, debe designar a un representante, a menos que el tratamiento sea ocasional, no incluya el tratamiento a gran escala de categorías especiales de datos personales o el tratamiento de datos personales relativos a condenas e infracciones penales, y sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, vista la naturaleza, el contexto, el ámbito y los fines del tratamiento, o si el responsable del tratamiento es una autoridad u organismo público[711].

(ii) La designación de un Delegado de Protección de Datos, cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 del RGPD[712].

(iii) La realización de una evaluación de impacto relativa a la protección de datos, cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, que por su naturaleza entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, cuando se lleve a cabo el tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9 del RGPD[713].

(iv) Finalmente, el RGPD establece la necesidad de que el responsable consulte a la autoridad de control antes de proceder al tratamiento, cuando la evaluación de impacto realizada relativa a la protección de los datos a gran escala muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo[714].

8.2. Nuevas categorías de datos sensibles: datos biométricos y datos genéticos.

A las categorías especiales de datos personales ya existentes hasta este momento - origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la

[711] Considerando (80) y Artículo 27.2.a), del RGPD.

[712] RGPD, op. cit. Artículo 37.1.c).

[713] Artículo 35.3.b), del RGPD.

[714] Artículo 36.1, del RGPD.

pertenencia a sindicatos, datos relativos a la salud o a la sexualidad, y las infracciones o condenas-, se añaden los datos genéticos y los datos biométricos, cuyo tratamiento, en consecuencia, pasa a estar prohibido, con carácter general, en este caso siempre que se lleve a cabo con el fin de identificar de forma única a una persona.

El RGPD se encarga de definir qué debe entenderse por "datos genéticos", consagrando que son:

> Datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona[715].

Los datos genéticos, pasan a ser incorporados como una subcategoría de los datos de salud, según el RGPD.

LÓPEZ CALVO[716] describe los datos biométricos esgrimiendo que: *"son los resultantes de la transformación técnica específica relativa a las características físicas, fisiológicas o de comportamiento de un individuo que permite o confirma la identificación única de ese individuo, tales como imágenes de la cara, o los datos dactiloscópicos".*

Sin embargo, los datos biométricos no se califican como datos de salud, aunque, según sostiene ÁLVAREZ-RIGAUDIAS[717], el RGPD asimila en ocasiones los datos biométricos a los datos de salud, aplicándoles las mismas reglas, y cita la autora, el caso de las causas de legitimación[718], que el RGPD define como datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos. Por su parte, LÓPEZ CALVO[719], entiende que es una nueva categoría que se incluye entre las categorías especiales de datos, pero únicamente cuando están siendo procesados con la finalidad de identificar de forma inequívoca a una persona.

---

[715] Artículo 4, del RGPD.

[716] LÓPEZ CALVO, J. *Comentarios al Reglamento Europeo de Protección de Datos*. Sepin, Madrid, 2017, p. 185.

[717] ÁLVAREZ-RIGAUDIAS, C., op. cit., p. 174.

[718] Artículo 4.14, del RGPD.

[719] LÓPEZ CALVO, J., op. cit., p. 185.

8.3. Tratamiento de los datos en el ámbito sanitario.

Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales[720].

El RGPD en su artículo 9 incluye a los datos relativos en la salud entre las categorías especiales de datos. Estos datos tienen una especial protección y su tratamiento queda limitado a casos concretos. Sostiene PUYOL MONTERO[721] que la regulación del Artículo 9 del RGPD es equiparable al Artículo 7 de la LOPD. Pero a pesar de ser un Artículo de tinte general prohibitivo, el mismo precepto sienta las bases para algunas excepciones.

En el caso de datos de salud, el RGPD establece que el tratamiento de datos relativos a la salud está permitido cuando *"el interes*ado dio su consentimiento explícito para el tratamiento de dichos datos personales"[722] y también cuando el tratamiento de éstos datos, resulte necesario:

(i) Por razones médicas. En éste sentido, el RGPD establece que se podrá realizar el tratamiento de datos sanitarios cuando los fines sean *de "medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social"*[723].

(ii) Por razones de salud pública. Otro fundamento legal para el tratamiento de datos sanitarios será el interés público en casos como la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud[724]. Aunque el reglamento destaca que ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas y

[720] Considerando (51), del RGPD.

[721] PUYOL MONTERO, J., op. cit., p. 146.

[722] Artículo 9.2.a), del RGPD.

[723] Artículo 9.2.h), del RGPD.

[724] Considerando (52), del RGPD.

que no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines[725].

(iii) Por razones de investigación científica o estadística. También se autoriza el tratamiento de datos personales de salud para actividades de investigación científica siempre que se adopten medidas efectivas de anonimización de datos que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo[726].

Al respecto, señala el RGPD, que el tratamiento de las categorías especiales de datos personales como los de salud, debe ser realizado por un *"profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad"*[727].

9. Nivel de protección y seguridad.

SÁIZ PEÑA[728] explica que la seguridad de la información puede definirse desde tres dimensiones diferentes. En primer lugar, desde la confidencialidad de los datos, estableciendo quién puede acceder a la información y conocerla. En segundo lugar, la integridad, refiriéndose el autor a que la información no puede ser manipulada. Y, en tercer lugar, la disponibilidad, refiriéndose a que la información ha de ser accesible en el momento en que se la precise. A partir de éstas tres diferentes dimensiones, es cuando, según SÁIZ PEÑA[729], puede determinarse si hay "brechas de seguridad", o como las denomina el RGPD, "violaciones de seguridad".

[725] Considerando (54), del RGPD.

[726] Artículo 89.1, del RGPD.

[727] Artículo 9.3, del RGPD.

[728] SÁIZ PEÑA, C. A. "La notificación de brechas de seguridad", en RALLO LOMBARTE, A.; GARCÍA MAHAMUT, R. *Hacia un Nuevo Derecho Europeo de Protección de Datos.* Tirant Lo Blanch, Valencia, 2015, pp. 771-772.

[729] Ibídem.

El RGPD establece un principio general por el que el responsable y el encargado del tratamiento deben aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, técnicas respetuosas con la privacidad, como la seudonimización (cuando los campos identificativos de un registro de datos se sustituyen por uno o más identificativos artificiales) y el cifrado (cuando se codifican los datos de tal manera que solamente puedan leerlos las partes autorizadas). El tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas. Y para lograr este fin, los Estados miembros deben establecer garantías adecuadas para el tratamiento de los datos personales[730].

Las condiciones y garantías en cuestión pueden conllevar procedimientos específicos para que los interesados ejerzan dichos derechos si resulta adecuado a la luz de los fines perseguidos por el tratamiento específico, junto con las medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los principios de proporcionalidad y necesidad. El tratamiento de datos personales con fines científicos también debe observar otras normas pertinentes, como las relativas a los ensayos clínicos[731].

Asimismo, el RGPD prevé que, si las operaciones de tratamiento suponen un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento deberá realizar una evaluación de impacto relativa a la protección de datos que permitirá evaluar el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. A su vez, el resultado de dicha evaluación deberá proponer medidas de seguridad y de anticipación adecuadas que deberán ser tomadas en consideración con el fin de demostrar que el tratamiento de los datos personales se realizará en conformidad con el RGPD. No obstante, no se detallan en el RGPD las medidas concretas a adoptar para alcanzar dicho objetivo.

[730] Considerando (156) y Artículo 89, del RGPD.

[731] Ibídem.

Además, deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento[732].

9.1. Notificación de violaciones de seguridad.

Otra novedad del RGPD es la introducción de una obligación por parte del responsable del tratamiento de datos, que es la notificación de cualquier violación de seguridad que suponga un riesgo para los derechos y las libertades de las personas físicas, a la autoridad de control.

El RGPD ha querido ser muy riguroso con estas situaciones, y de hecho marca un plazo de 72 horas[733] después de que el responsable del tratamiento haya tenido constancia de la violación de la seguridad de los datos personales, para notificar de ésta circunstancia a la autoridad de control competente[734]. Sin duda el RGPD pone el énfasis en los medios tecnológicos y en los *cyber* ataques. Pero a pesar de ello, el RGPD no deja claro que ha de entenderse exactamente por violación de seguridad, estableciendo supuestos claros o tipificando qué hechos deben notificarse a la Autoridad de Control.

El RGPD, establece, de manera muy amplia a nuestro juicio, la definición de violación de la seguridad de los datos personales, entendiéndose por tal: *"toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos"*[735].

[732] Considerando (39), del RGPD.

[733] En el Proyecto del Reglamento de Protección de Datos se barajó un plazo de 24 horas que finalmente fue elevado a 72 horas. La idea inicial del plazo breve de 24 horas surge del Reglamento (UE) Nº 611/2013 de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas (DOUE L 173, 26.06.2013, pp. 2-8).

[734] Artículo 3, del RGPD.

[735] Artículo 4.12, del RGPD. El RGPD se ha visto influido por la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013 relativa a los ataques contra los sistemas de

Ésta definición, deja lagunas que la legislación interna de cada Estado miembros, deberá completar. En éste sentido, SÁIZ PEÑA[736] explica que existen tipologías muy diferentes de actos que podrían encuadrarse en lo que se denomina "violaciones de seguridad", como, por ejemplo, dentro de la misma empresa o Administración, un trabajador que accede a información a la que no debería, utilización de ingeniería social para hacerse con claves de usuarios autorizados, etc.

Ésta circunstancia de no delimitar de forma taxativa los supuestos que constituyen o no una violación de seguridad, puede llevar a colapsar a la Autoridad de Control, si recibe cientos de consultas al día relacionadas con éstas notificaciones[737]. Los sistemas informáticos tienen incidencias diarias constantes, ya sea su paralización, su suspensión, el apagado del mismo, etc. Pero estas situaciones no constituyen una amenaza a los derechos de las personas, simplemente es que el sistema se ha "colgado", se ha "interrumpido" o se ha "apagado inesperadamente".

Asimismo, compete al responsable del tratamiento de los datos personales, la comunicación al propio interesado, sobre la violación de la seguridad de sus datos personales, si ésta entraña un alto riesgo para los derechos y libertades del mismo[738]. Esta comunicación debe realizarse en un lenguaje claro y sencillo, describiendo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información del nombre y los datos de contacto del Delegado de Protección de Datos o de otro punto de contacto en el que pueda obtenerse más información, la descripción de las posibles consecuencias de la violación de la seguridad de los datos personales, y la descripción de las medidas adoptadas o propuestas por el responsable del tratamiento, para poner remedio a la violación de la seguridad de los datos

información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo (DOUE L 218, 14.08.2013, pp. 8-14). La Directiva tiene por objeto establecer *normas mínimas relativas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información. También tiene por objeto facilitar la prevención de dichas infracciones y la mejora de la cooperación entre las autoridades judiciales y otras autoridades competentes* (Artículo 1), y define la expresión «sin autorización», estableciendo que es *un comportamiento al que se refiere la presente Directiva, incluido el acceso, la interferencia o la interceptación, que no haya sido autorizado por el propietario u otro titular del derecho sobre el sistema o parte del mismo o no permitido por el Derecho nacional* (Artículo 2).

[736] SÁIZ PEÑA, C. A., op. cit., pp. 772-773, 785 y 806.

[737] Ibídem, p. 772.

[738] Artículo 34, del RGPD.

personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos[739].

Coincidimos con ARIAS POU[740], que sostiene que, el fundamento primordial de esta nueva obligación deriva de que, si no se toman a tiempo medidas adecuadas, estas violaciones pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como la pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdida de la confidencialidad de los datos de carácter sanitario, etc. Máxime teniendo en cuenta los avances tecnológicos y lo rápido y sencillo que resulta enviar o transportar información de un lugar a otro.

Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la Autoridad de Control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. El RGPD establece que, si la notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida[741].

10. La nueva figura del Delegado de Protección de Datos.

Tal y como hemos expuesto hasta el momento, el RGPD introduce varias novedades englobadas en un nuevo modelo de protección de datos para la UE. Esta nueva ordenación legal, pasa de la gestión de los datos –aplicada a su recopilación y almacenamiento-, al uso responsable de la información –al tratamiento que de la misma

[739] Artículo 33. b), c) y d), del RGPD.

[740] ARIAS POU, M. "Definiciones a efectos del Reglamento General de Protección de Datos", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016, p. 129.

[741] Considerando (85), del RGPD.

se realice-. Ésta novedad implica que se otorgará un mayor protagonismo a una figura de nueva creación que es el Delegado de Protección de Datos (en adelante, DPO), en el que recaerá la responsabilidad de determinar y adoptar las medidas que sean necesarias para garantizar la adecuada protección de los datos.

A partir de la entrada en vigencia del RGPD, será obligatorio para las empresas y para las Administraciones públicas designar a un "delegado de protección de datos" (*Data Protection Officer*) para garantizar el cumplimiento de la normativa europea. La diferencia principal con el Responsable de Seguridad, radica principalmente en la exclusividad del DPO en sus funciones. El DPO deberá ser designado en atención a sus cualidades profesionales y conocimientos normativos y prácticos especializados debidamente acreditados.

El RGPD impone la obligatoriedad de su nombramiento, que recae en el responsable y el encargado del tratamiento[742], quienes designarán un DPO siempre que el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial; siempre que las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala; y siempre que las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales[743] -los datos de salud- y de datos relativos a condenas e infracciones penales[744].

El DPO deberá desempeñar sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento[745]

Entre las funciones del DPO[746], destacan la de informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de datos, supervisar que el RGPD se cumple en el ámbito de sus funciones, realizará las evaluaciones de impacto relativas a la protección de datos cuando sea probable que un

[742] Artículo 37.1, del RGPD.

[743] Artículo 9, del RGPD.

[744] Artículo 10, del RGPD.

[745] Artículo 39.2, del RGPD.

[746] Artículo 39.1, del RGPD.

tipo de tratamiento, en particular si se utilizaran nuevas tecnologías, o que por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas[747], cooperará con las autoridades de control y a la vez actuará como punto de contacto con éstas.

Conclusión.

El enorme intercambio y la consecuente recogida de datos propiciado por el desarrollo tecnológico, el uso de estos datos por parte de autoridades públicas y empresas privadas, desconociéndose el impacto real que supone el almacenamiento y uso que se les da a los datos, ha dado lugar al RGPD, dejando absolutamente obsoleta la Directiva 95/46/CE, que queda derogada.

Sin duda la aprobación del RGPD supone la uniformización de los diversos ordenamientos jurídicos de los Estados miembros en materia de protección de datos de carácter personal. Pero también hemos de reconocer el peligro que puede entrañar que se deposite mayor responsabilidad en los responsables y en el encargado del tratamiento de los datos, a quienes se les encarga la valoración y la apreciación en relación con los riesgos que puede conllevar los datos que deben tratar. Por lo tanto, el margen de decisión que recae en estas personas es altamente destacable.

En conclusión, si uno de los objetivos para adoptar un RGPD era la uniformización de los diferentes ordenamientos jurídicos, dado lo comentado anteriormente, podría decidirse que este objetivo no se ha alcanzado. PIÑAR MAÑAS[748] opina al respecto que las reglas de juego son más uniformes a nivel de la UE, pero al mismo tiempo se deja mayor margen de apreciación y valoración a los responsables y encargados.

También destacamos que el RGPD introduce un cambio de modelo jurídico. Con la Directiva 95/46/CE teníamos un modelo basado en la recopilación y el tratamiento de los datos. Ahora, toda la atención legal se focaliza en el uso que de estos datos se debe hacer.

Por lo expuesto, y, dado el contenido similar del RGPD y la Directiva 95/46/CE respecto al tratamiento de datos personales de salud, consideramos que resulta idóneo aplicar la

[747] Artículo 35.1, del RGPD.

[748] PIÑAR MAÑAS, J. L. (Director)., op. cit., p. 17.

interpretación que ya se efectuó por parte del Grupo de Trabajo del Artículo 29 sobre el Artículo 8 de la Directiva 95/46/CE[749], de tal forma que las excepciones recogidas por el RGPD y la Directiva 95/46/CE en el tratamiento de datos personales relativos a la salud deben ser limitadas, exhaustivas y tienen que ser interpretadas de forma restrictiva.

Finalmente, queremos señalar luego del análisis efectuado del RGPD un dato que desde nuestro punto de vista es trascendente y posiblemente preocupante de cara al futuro: el RGPD no contempla específicamente cuestiones como el Big Data, el *Cloud Computing*[750], la Internet de las cosas[751] o *BioTech*[752]. Por tanto, puede pensarse que se ha perdido una ocasión para adaptar completamente la norma al entorno digital que le permitiese envejecer bien.

---

[749] Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME) 00323/07/ES del Grupo de Trabajo sobre protección de datos del Artículo 29 (WP 131), 15 de febrero de 2007, p. 8. Disponible en Internet: <https://www.apda.ad/system/files/wp131_es.pdf> [Consulta: 11 febrero 2017].

[750] El *cloud computing* consiste en la posibilidad de ofrecer servicios a través de Internet. La computación en la nube es una tecnología nueva que busca tener todos nuestros archivos e información en Internet, sin preocuparse por poseer la capacidad suficiente para almacenar información en nuestro ordenador.

[751] Internet de las cosas (en inglés, *Internet of things*, abreviado IoT) es un concepto que se refiere a la interconexión digital de objetos cotidianos con internet. El Internet de las cosas potencia objetos que antiguamente se conectaban mediante circuito cerrado, como comunicadores, cámaras, sensores, etc., y les permite comunicarse globalmente mediante el uso de la red de redes.

[752] En 1919, el ingeniero agrónomo húngaro Karl Ereky tuvo la visión de una época en la que la biología podría utilizarse para convertir las materias primas en productos útiles. Fue él quien acuñó el término *biotecnología* para describir esa fusión de la biología con la tecnología. La visión de Ereky se ha vuelto realidad ahora en miles de empresas y centros de investigación. La creciente lista de productos biotecnológicos incluye medicamentos, dispositivos médicos y diagnósticos, así como cosechas más resistentes, biocombustibles, biomateriales y controles de la contaminación. Los medicamentos biotecnológicos son moléculas grandes similares o idénticas a las proteínas y otras sustancias complejas de las que depende el cuerpo para mantenerse sano. Son demasiado grandes y complejas para elaborarse por métodos exclusivamente químicos. En vez de esto, se preparan empleando "fábricas vivas", es decir, microbios o líneas celulares que se modifican genéticamente para producir la molécula deseada. Los medicamentos biotecnológicos deben inyectarse o infundirse en el organismo para evitar que su compleja estructura se degrade durante la digestión, lo que ocurriría si se administraran por vía oral. Fuente: <http://www.biotechnology.amgen.com/es/biotechnology-explained.html> [Consulta: 11 febrero 2017].

CAPÍTULO II

Big Data en la salud y sus implicancias jurídicas.

SUMARIO: 1. Acerca del denominado "Big Data" en el ámbito de la salud. 1.1. Las cinco "Vs" del Big Data en salud. 1.2. Cómo "trabaja" Big Data. 2. Aspectos positivos del Big Data en la salud, ¿un nuevo paradigma? 3. Aspectos negativos del Big Data en la salud. 3.1. La anonimización versus la re-identificación. La anonimización no garantiza la privacidad de los datos personales. 4. Nuevos retos frente al Big Data. 4.1. Recopilación y gestión de los datos. 4.2. Protección de la intimidad y privacidad frente al avance tecnológico. 4.3. Acceso al Big Data sanitario.

Introducción.

Evidentemente el panorama social actual hace necesario una toma de conciencia de las personas en relación con los datos sensibles que continuamente facilitamos, muchas veces sin darnos cuenta siquiera. No sólo cuando vamos al médico de cabecera, éste detalla en nuestra historia clínica el estado de nuestra salud, sino que es habitual que nos atendamos indistintamente en centros médicos privados, que nos hagamos diversos análisis, radiografías, que acudamos al dentista, que vayamos al gimnasio y practiquemos fitness, que nuestros móviles inteligentes tengan aplicaciones vinculadas a nuestra forma física, alimentación o salud, etc.

Sin embargo, en el ámbito estrictamente sanitario, esos datos dispersos por sí mismos no resultan útiles para una atención sanitaria ágil, personalizada y efectiva. Si además de nuestra HC, el médico pudiese contar con todas las pruebas que se nos han practicado, radiografías, resonancias, etc., con las prescripciones de medicamentos que nos han realizado a lo largo de nuestra vida, con los diferentes informes médicos y notas de otros facultativos, sin duda su diagnóstico será más infalible y más rápido, evitará que nos sometamos a otras pruebas duplicadas o innecesarias y posibilitará que nuestro tratamiento y curación resulten más efectivos.

En este campo se mueve el Big Data sanitario, que no es más que el esfuerzo de aunar la información sanitaria dispersa, y en diversos formatos, que se dispone de cada paciente a fin de agruparla, organizarla y sacarle un beneficio constatable para el

paciente, pero también para el sector médico, para la organización hospitalaria, y para las farmacéuticas, todo ello, en un entorno tecnológico que marcará en un futuro próximo, un cambio de paradigma en el modo de entender la atención sanitaria.

El objetivo de Big Data en salud, es convertir el dato en información que facilita la toma de decisiones, incluso en tiempo real, con los beneficios médicos evidentes que la rapidez y la precisión implican en la atención sanitaria.

1. Acerca del denominado "Big Data" en el ámbito de la salud.

La locución Big Data es un vocablo reciente en la sociedad, que viene a definir el tratamiento de grandes volúmenes de datos mediante algoritmos matemáticos con el fin de establecer analogías entre ellos, predecir tendencias y tomar decisiones[753]. Big data se refiere al conjunto de datos e información tan grandes y tan complejos que hace muy difícil su procesamiento utilizando herramientas de gestión de bases de datos convencionales[754].

Se trata sin duda de un concepto nuevo, aunque su origen radica en un concepto mercantil, el *"Business Inteligence"* (inteligencia en los negocios o estrategia en los negocios), que utilizan sobre todo los empresarios para convertir sus empresas en organizaciones eficaces y eficientes. El *Business Inteligence* tradicional captura información de las fuentes disponibles de la organización y tras la aplicación de algoritmia de análisis la muestra con el fin de ayudar a la toma de decisiones estratégicas en la empresa[755].

---

[753] LLÀCER MATACÁS, Mª R.; CASADO, M.; BUISAN ESPELETA, L. (coord.). *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública.* Observatori de Bioètica i Dret, Universidad de Barcelona Publicacions i Edicion. Barcelona, 2015. pp. 33 y ss. Disponible en Internet: <http://hdl.handle.net/2445/104585> [Consulta: 16 octubre 2016].

[754] JOYANES AGUILAR, L.; POYATOS DÍAZ, J. M. (2013) Big Data y el sector de la salud: el futuro de la sanidad. [Blog post]. Blog Juan Miguel Poyatos. The power of costumer connection. Disponible en Internet: <http://poyatosdiaz.com/index.php/big-data-y-el-sector-de-la-salud-el-futuro-de-la-sanidad> [Consulta: 14 noviembre 2016].

[755] LÓPEZ LÓPEZ, V. (4.05.2015) Big data sanitario: el acelerador del conocimiento y la decisión clínica. [Blog post]. Blog A un clic de las TIC. Disponible en Internet:

Esta explosión de datos es relativamente nueva. En el año 2000, sólo un cuarto de toda la información almacenada en el mundo era digital. El resto se conservó en papel, película, radiografías, y otros medios analógicos. Pero debido a que la cantidad de datos digitales se expande tan rápidamente -duplicándose cada tres años-, esa situación fue rápidamente invertida. Actualmente, menos del dos por ciento de toda la información almacenada es no digital[756].

En el ámbito sanitario, los centros de salud, públicos o privados, y los pacientes, acumulan grandes cantidades de datos en distintos formatos, tanto en papel como en soportes electrónicos, que por su dispersión resultan imposibles de utilizar. La gran novedad del Big Data es el procesamiento de información no estructurada unida a la estructurada[757]. Big Data consiste, por tanto, en la organización de toda esa información de forma efectiva, por lo que se podrían integrar a los datos estructurados ya existentes hoy en día, por ejemplo, las HC de los pacientes, a aquellos que permanecen ocultos al sistema actual de almacenamiento y sólo existen de forma analógica en poder de los pacientes, por ejemplo, recetas de papel, registros médicos, notas manuscritas de los doctores o resultados de pruebas médicas[758]. A todos estos datos hay que añadirles los

---

<http://aunclicdelastic.blogthinkbig.com/big-data-sanitario-el-acelerador-del-conocimiento-y-la-decision-clinica/> [Consulta: 12 enero 2017].

[756] KENNETH, N. C.; MAYER-SCHOENBERGER, V. (May/June) The Rise of Big Data. How It´s Changing the Way We Think About the World (El auge del Big Data. Cómo está cambiando la manera en la que pensamos el mundo). [Blog post]. Blog Foregin Affars. Disponible en Internet: (versión en inglés): <https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data> [Consulta: 8 enero 2017].

N.A.: Un ejemplo muy ilustrativo se refleja en las fotografías. Hace algunos años, cuando no existían las cámaras digitales o los móviles, sacábamos muy pocas fotos porque luego había que revelarlas y resultaba un proceso costoso. Actualmente con la aparición de las cámaras de alta definición incorporadas a los teléfonos móviles inteligentes que la mayoría poseemos, no paramos de hacer fotos, incluso sacamos dos o tres de la misma escena por si ha quedado mal. Es evidente que esas fotografías digitales se guardan en la memoria del teléfono, pero cuando este llega a su límite, se recurre a su almacenaje en la nube, pero si el ritmo sigue *in crescendo* como es la tendencia, es lógico que nos tengamos que plantear a nivel Big Data un sistema de almacenamiento capaz de guardar todos los bytes que implica cada recuerdo fotografiado.

[757] Los datos estructurados consisten en datos que tienen definida su longitud y su formato (números, fechas, DNI, dirección, edad, todos aquellos contenidos en una HC, etc.). Por el contrario, los datos no estructurados son aquellos que carecen de un formato específico (diagnóstico por imágenes, recetas, etc.).

[758] Se trata de la acumulación de todos los datos que se disponen, tanto estructurados, como no estructurados.

que provienen de las redes sociales y de otros dispositivos que permiten monitorizar al paciente y se irán incorporando a la recopilación de información a través de internet de las cosas: dispositivos, sensores, instrumentos médicos, aparatos de fitness, etc.[759].

BARÓ[760] sostiene que los métodos y herramientas de Big Data se caracterizan por el volumen, la complejidad y la velocidad de la información que manejan. Sin duda, la propia definición de Big Data en salud tiene sus matices, y la evolución que se vislumbra en los próximos años, perfilará lo que debe entenderse y delimitarse por "Big Data sanitario".

1.1. Las cinco "Vs" del Big Data en salud.

Tal y como hemos hecho referencia *ut supra*, las empresas ya vienen utilizando el Big Data a través de lo que explicamos como *Business Inteligence*. Y ello, en base a que, para el sector empresarial, analizar un volumen importante de datos resulta muy útil para entender el perfil, las necesidades y el sentir de sus clientes respecto a los productos y/o servicios vendidos, a la vez que se evalúan a los competidores. Esto adquiere especial relevancia, ya que permite adecuar la forma en la que interactúa la empresa con sus clientes y en cómo les prestan su servicio[761]. Para lograr el procesamiento de esta magnitud de información, las empresas se valen de las nuevas tecnologías y de herramientas de análisis para lograr procesar los datos.

Por lo tanto, podemos afirmar que los medios tecnológicos ya existen y son utilizados en el sector empresarial. En consecuencia, la diferencia entre las aplicaciones

[759] Véase al respecto: LOGICALIS. (25.08.2014) Atención médica personalizada: Big Data y el futuro de la medicina. [Blog post]. Blog sobre Business Intelligence. Disponible en Internet: <http://www.lantares.com/blog/atencion-medica-personalizada-big-data-y-el-futuro-de-la-medicina> [Consulta: 13 enero 2017].

[760] BARÓ E.; DEGOUL S.; BEUSCART R.; CHAZARD E. (2.06.2015) Toward a literature-driven definition of big data in healthcare. [Blog post]. Blog BioMed Research International, Universidad de Lille, Francia, 2015, p. 639021. Disponible en Internet (versión en inglés): <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4468280/> [Consulta: 10 enero 2017].

[761] Ver al respecto: CÁRCAR BENITO, J. E. (julio 2016) El Big Data en la organización sanitaria: nuevos tiempos y nuevos cambios. Un estudio previo. [Blog post]. Blog Federación Española de Sociología (FES). Disponible en Internet: <http://www.fessociologia.com/files/congress/12/papers/5342.pdf#page=3&zoom=auto,-185,685> [Consulta: 23 enero 2017].

analíticas y de gestión, y los nuevos conceptos de Big Data radica en lo que la doctrina[762] de referencia asocia a las tres "Vs" del Big Data: Volumen, Variedad y Velocidad, según nos referiremos a continuación.

No obstante, estas tres "Vs" de las bases de datos, según explica GIL GONZÁLEZ[763], eran incompatibles años atrás, creando una tensión que obligaba a elegir entre ellas. Se podía analizar un gran volumen de datos y a alta velocidad, pero era necesario que fueran datos sencillos, como datos estructurados en tablas; esto es, había que sacrificar la variedad de los datos. Del mismo modo, se podían analizar grandes volúmenes de datos muy variados, pero no a gran velocidad; era necesario dejar que los sistemas trabajaran durante horas, o incluso días.

Con la implementación del Big Data, estas tres "Vs" ya no son excluyentes, sino que devienen complementarias y, además, en base a la práctica adquirida por las empresas precursoras en Big Data, se han añadiendo nuevas características como son dos "Vs" más: la Veracidad y Valor. Siguiendo la definición de CÁRCAR BENITO[764], analizaremos brevemente lo que se entiende por cada una de las "Vs":

(i) El Big Data existe cuando los *volúmenes* superan la capacidad del software habitual para ser manejados y gestionados. Big se refiere a grandes cantidades. Este concepto se encuentra en continuo movimiento, ya que los avances tecnológicos permiten tratamientos de volúmenes superiores de datos. Si hablamos de grandes volúmenes de información nos referimos a tratamientos de Terabytes[765] o Petabytes[766].

(ii) Con el concepto de *variedad*, nos referimos a la inclusión de otros tipos de

[762] Vid. PUYOL MONTERO, J. "UNA aproximación a Big Data". *Revista de Derecho UNED*. Núm. 14, 2014, pp. 471-506.; SÁIZ PEÑA, C. A. "Uno de los mayores retos en el entorno digital: el Big Data". *Actualidad jurídica Aranzadi.* Núm. 874, 2013, p. 14.; DAVARA RODRÍGUEZ, M. A. "Big Data". *El consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal.* Núm. 15-16, 2013, pp. 1552-1558.

[763] GIL GONZÁLEZ, E. *Big data, privacidad y protección de datos.* Agencia Española de Protección de Datos, Madrid 2016, p. 20.

[764] CÁRCAR BENITO, J. E., op. cit.

[765] Terabyte es una unidad de almacenamiento de información cuyo símbolo es TB, equivalente a 10^{12} bytes = 1.000.000.000.000 de bytes.

[766] Un Petabyte es una unidad de almacenamiento de información cuyo símbolo es PB, y equivale a 10^{15} bytes = 1.000.000.000.000.000 de bytes.

fuentes de datos diferentes a las que se utilizan de forma habitual. Por ejemplo, la información obtenida a través de los diferentes dispositivos electrónicos que utilizamos a diario, redes sociales, sensores que permiten conocer los movimientos y hábitos de vida, de información externa de diversas fuentes, diversas pruebas médicas, etc.

(iii) Hablamos de *velocidad* para referirnos a la rapidez con que los datos se reciben, se procesan y se pueden tomar decisiones a partir de ellos. A la mayoría de los sistemas tradicionales les es imposible analizar de forma inmediata los grandes volúmenes de datos que les llegan, sin embargo, al incorporar el concepto de tiempo real estamos hablando de Big Data y algoritmos capaces de analizar y procesar tanto la información estructurada como la información desestructurada, y garantizar que dichos resultados sean precisos y exactos.

(iv) Nos referimos a la *veracidad* para explicar la calidad y la fiabilidad de esos datos y, por tanto, la confianza de los mismos. Big Data logra a través de la combinación de las otras "Vs", que los datos, especialmente los no estructurados, combinen diversas fuentes de datos para dar lugar a una información más fiable, y que apoyados en ésta información, se va a llegar a un resultado certero, que dará lugar a una correcta toma de decisiones.

(v) Finalmente, se añade al concepto de Big Data la característica del *valor*. La definición del valor del dato por sí misma es fundamental; saber qué datos son los que se deben analizar va a llevar a la consecuencia de un resultado fiable y apto para la toma de una decisión al respecto. GIL GONZÁLEZ[767] comenta al respecto que la finalidad última de los procesos de Big Data es crear valor, ya sea entendido como oportunidades económicas o como innovación. Sin él, los esfuerzos dejan de tener sentido. Y en lo concerniente al ámbito médico, el valor es esencial para que se tome la decisión más acorde con las necesidades del paciente y la aplicación del tratamiento más oportuno.

1.2. Cómo "trabaja" Big Data.

Dada esta escala masiva de los datos que se recopilan y se procesan, de acuerdo a las

[767] GIL GONZÁLEZ, E., op. cit., p. 24.

cinco “Vs” a las que antes hemos hecho referencia, el Big Data está permitiendo nuevos usos con la ayuda de la memoria de ordenadores, de procesadores de gran alcance, de algoritmos inteligentes, de software inteligente, de matemáticas y de estadísticas básicas.

Pero, ¿cómo se logra esto? En lugar de tratar de "enseñar" a un ordenador cómo hacer las cosas, cómo manejar un coche o traducir entre lenguas -lo que los expertos en inteligencia artificial han intentado hacer sin éxito durante décadas-, el nuevo enfoque es alimentar suficientes datos en un ordenador para que pueda deducirse la probabilidad de que, por ejemplo, un semáforo sea verde y no rojo[768].

El uso de grandes volúmenes de información de esta manera, requiere tres cambios profundos en cómo obtenemos los datos según explican NEIL CUKIER y MAYER-SCHOENBERGER[769].

(i) El primero, consiste es recolectar y utilizar una gran cantidad de datos en lugar de conformarse con pequeñas cantidades o muestras, como lo han hecho los estadísticos durante más de un siglo.

Tradicionalmente, nos basábamos en que cantidades de información pequeñas se pudieran manejar de forma fácil y explicaran realidades complejas. GIL GONZÁLEZ[770] sostiene al respecto, que:

> En cuestiones generales, las muestras y la estadística funcionan bien, pero cuando queremos obtener conclusiones de subgrupos concretos de la muestra, la estadística deja de ser fiable.

[768] Para profundizar más el tema, véase: KENNETH, N. C.; MAYER-SCHOENBERGER, V., op. cit. Los autores explican que, durante la mayor parte de la historia, la gente ha trabajado con cantidades relativamente pequeñas de datos porque las herramientas para recopilar, organizar, almacenar y analizar la información eran sencillas. La gente relacionó y seleccionó la información en la que confiaron en el mínimo de líneas de modo que pudieran examinarla más fácilmente. Este fue el origen de la estadística moderna, que apareció por primera vez a finales del siglo XIX y permitió a la sociedad comprender realidades complejas incluso cuando existían pocos datos. Exponen los autores los grandes avances que logran los algoritmos de los ordenadores, citando a modo de ejemplo: la ubicación, que se ha dado a conocer, primero con la invención de la longitud y la latitud, y más recientemente con los sistemas de satélite GPS.

[769] Ibídem.

[770] GIL GONZÁLEZ, E., op. cit., p. 26.

Ello es porque las muestras aleatorias son suficientes para describir las realidades globales, pero no para detectar comportamientos particulares de subgrupos.

(ii) El segundo cambio, consiste en descartar nuestra preferencia por los datos altamente estructurados y limpios (originales sin tratar) y en su lugar aceptar el desorden. Según refieren NEIL CUKIER y MAYER-SCHOENBERGER[771], en un número creciente de situaciones, un poco de inexactitud puede ser tolerado, porque los beneficios de utilizar muchos más datos de calidad variable, superan los inconvenientes de la utilización de pequeñas cantidades de datos muy exactos.

(iii) En tercer lugar, en muchos casos, tendremos que renunciar a nuestra búsqueda para descubrir la causa de las cosas, a cambio de aceptar las correlaciones. Con muchos datos, en vez de intentar entender exactamente por qué el efecto secundario de una droga desaparece, los investigadores pueden recopilar y analizar cantidades masivas de información sobre tales eventos y todo lo que está asociado con ellos, buscando patrones que puedan ayudar a predecir y prevenir los sucesos futuros. Los grandes volúmenes de datos ayudan a contestar qué, no el por qué, pero es allí cuando el médico asume su labor.

En el Big Data, se trabaja entonces a partir de puras estadísticas, es decir basándose en probabilidades, pero con tantas variables que el resultado deviene prácticamente infalible. Trabajar a base de probabilidades en medicina, estableciendo patrones, resulta ciertamente muy útil desde el punto de vista de la propagación de las enfermedades, el estudio de sus orígenes y, por tanto, su mejor tratamiento.

Así lo demostró un estudio que hizo Google en el año 2009[772], en el que los investigadores de la compañía demostraron que era posible un seguimiento de los brotes de la gripe estacional, haciendo uso únicamente de los expedientes archivados de búsquedas de Google. Google maneja más de 1 billón de búsquedas en Estados Unidos todos los días y los almacena todos. La empresa analizó y relacionó los 50 millones de términos más buscados entre 2003 y 2008 y comparó esos datos con los

[771] KENNETH, N. C.; MAYER-SCHOENBERGER, V., op. cit.

[772] GINSBERG, J.; et al. "*Detecting influenza epidemics using search engine query data*" (Detección de epidemias de influencia utilizando datos de consulta de los motores de búsqueda). *Revista Nature*. Vol. 457, 19.02.2009. Disponible en Internet: <http://www.nature.com/nature/journal/v457/n7232/full/nature07634.html> [Consulta: 9 enero 2017].

datos históricos de influencia de los centros de control y prevención de enfermedades. La idea era descubrir si la incidencia de ciertas búsquedas coincidió con brotes de la gripe, en otras palabras, ver si un aumento en la frecuencia de ciertas búsquedas en Google realizadas en un área geográfica particular, se correlacionaba con datos históricos reales de los centros asistenciales sobre brotes de gripe sucedidos. De los registros sanitarios se recabaron datos reales sobre visitas de pacientes a hospitales y clínicas en todo el país, pero esa información tenía un desfase de una o dos semanas, una eternidad en el caso de una pandemia. Google, por el contrario, trabajó en tiempo casi real, ideando un algoritmo que correlacionó con brotes de gripe. Google identificó 45 términos -palabras tales como "dolor de cabeza" y "congestión nasal"- que tenía una fuerte correlación con los datos de los registros de los centros asistenciales sobre brotes de gripe, logrando prácticamente idénticos resultados que los que constaban en los registros médicos.

2. Aspectos positivos del Big Data en la salud, ¿un nuevo paradigma?

En el sector sanitario, como se ha explicado *ut supra*, se maneja infinidad de información. Esta información convertida en datos de los pacientes, innegablemente constituye una información valiosa y bien acumulada y gestionada tendría una utilidad innegable en el ámbito de la salud. Desde el punto de vista del paciente, facilitaría su seguimiento, evolución, prescripción de tratamiento, etc. A modo ilustrativo, desde el punto de vista de la gestión sanitaria, optimizaría los recursos y evitaría duplicidades innecesarias eliminando dichos costes; podrían detectarse de forma precoz epidemias; permitiría a los médicos un diagnóstico más certero y ágil, etc. Desde el punto de vista de las farmacéuticas, también serviría para detectar de forma rápida efectos secundarios de los medicamentos, reduciría los costes de investigación, y probablemente los medicamentos serían más seguros, entre otros beneficios.

PLANAS[773] pone de relieve que cada 50 años históricamente se produce una revolución en el sector sanitario basada en las tendencias de la época. Ahora, a medida

[773] PLANAS, J. (2015) La próxima revolución en el sector sanitario. [Blog post]. Blog del Dr. Jorge Planas. Disponible en Internet: <http://www.clinicaplanas.com/jorge-planas/2012/10/29/la-proxima-revolucion-en-el-sector-sanitario/> [Consulta: 13 febrero 2017].

que nos acercamos al año 2020, existe una clara tendencia hacia un gran volumen de datos. Al respecto señala PLANAS[774], que las herramientas y la sistematización de la atención al paciente van a revolucionar la forma de trabajar de hospitales y médicos, sobre todo la forma de tratar a los pacientes.

RODRIGO LARRUCEA[775] sostiene que, si el Big Data asegura la privacidad de las personas, se abre un horizonte inabarcable para el estudio de estadísticas, datos biométricos, hábitos o actuaciones en salud pública que contiene un valor impagable en el diseño de estrategias sanitarias a medio y largo plazo. La autora, en el mismo sentido que entendemos nosotros, pone de manifiesto, ante todo, que la privacidad de las personas debe preservarse y prevalecer, ante cualquier otro beneficio del Big Data en salud.

Asimismo, PLANAS[776] comenta que el Big Data en el ámbito de la salud, representa una gran oportunidad en cuanto a la posibilidad de obtener mejores resultados y menores tasas de mortalidad de los pacientes. La salud "impulsada por datos" ha estado cada vez mejor definida y comprendida en los últimos años. Grandes grupos de registros pueden asegurar que se apliquen los mejores algoritmos de tratamientos personalizados para cada paciente.

Las aplicaciones relacionadas con la sanidad permitirán mejoras en el área médica, en la síntesis de datos de las HC de los pacientes y análisis clínicos, la gestión de centros de salud y hospitales, la administración hospitalaria, la distribución de material sanitario y medicamentos, la detección y prevención de posibles efectos secundarios de medicamentos y tratamientos, o la generación, almacenamiento y explotación de la documentación científica[777].

En éste sentido, la consultora McKinsey ha publicado un informe en el que vislumbran

---

[774] Ibídem.

[775] RODRIGO LARRUCEA, C. (14.04.2016) Mhealth y Bigdata en sanidad. [Blog post]. Blog Derecho y salud no van siempre de la mano. Disponible en Internet: <https://carmenrodrigodelarrucea.wordpress.com/2016/04/14/mhealth-y-bigdata-en-sanidad/#more-793> [Consulta: 11 febrero 2017].

[776] PLANAS, J., op. cit.

[777] Ver al respecto: LOGICALIS. (11.05.2014) Big Data: el futuro del sector de la salud. [Blog post]. Blog sobre Business Intelligence. Disponible en Internet: <http://www.lantares.com/blog/big-data-el-futuro-del-sector-de-la-salud> [Consulta: 13 enero 2017].

grandes ventajas en la implementación del Big Data en la salud[778]. Pero las ventajas a las que hace referencia el informe, son fundamentalmente de carácter económico: reducción de costes y optimización del gasto. Por su parte, la fundación Rock Health, emitió un informe sobre Big Data en el ámbito de la salud[779] en el que concluyó que podría conllevar un ahorro de entre 300 y 500 millones de dólares gracias a tres factores: 1) La mejora de la coordinación de la atención al ciudadano; 2) La lucha contra los fraudes y los abusos; y, 3) La reducción de ineficiencias administrativas y clínicas.

Seguramente también la investigación experimentará una mejora a la hora de poder determinar las causas de las enfermedades y establecer mejores terapias. A través de la implementación del Big Data en salud se podrán predecir, prevenir y personalizar enfermedades gracias a los avances en la atención y medicina personalizadas, investigación y secuenciación del genoma, monitorización remota de pacientes, etc.[780].

La monitorización del propio estado de salud y el vuelco de la información obtenida en grandes bases de datos para su posterior tratamiento y estructuración permitirán, en un futuro muy cercano, avanzar hacia un nuevo concepto de la atención médica

---

[778] El estudio calcula que las aplicaciones de Big Data en el sector sanitario podría representar unos beneficios de hasta 250.000 millones de euros los sistemas de salud públicos en Europa y de hasta 300.000 millones de dólares en Estados Unidos. Un ahorro considerable si se tiene en cuenta que la mayoría de sistemas sanitarios de la sociedad occidental presentan unas pérdidas mayores cada año. MCKINSEY GLOBAL INSTITUTE - MANYIKA J.; et al. (mayo 2011). Big Data: The next frontier for innovation, competition, and productivity (La siguiente frontera para innovación, competición, y productividad). [Blog post]. Blog Digital McKinsey. Disponible en Internet (versión en inglés): <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation> [Consulta: 10 enero 2017].

[779] Según las conclusiones de éste informe, Big Data cambiaría la eficiencia del modelo de atención sanitaria en base a los siguientes fundamentos: a) Transformación de datos en información; b) Apoyo al autocuidado de las personas; c) Respaldo a los proveedores de cuidados médicos; d) Aumento del conocimiento y la concienciación del estado de salud; e) Agrupamiento de los datos para expandir el ecosistema; y f) Rentabilidad para la Investigación y la prevención. FUNDACIÓN ROCK HEALTH. (1.10.2012) Big Data *in digital health* (Big Data en salud digital). [Blog post]. Blog Rock Healt. Disponible en Internet (versión en inglés): <http://es.slideshare.net/RockHealth/rock-report-big-data> [Consulta: 10 enero 2017].

[780] Ver al respecto: LOGICALIS. (25.08.2014) Atención médica personalizada: Big Data y el futuro de la medicina. [Blog post]. Blog sobre Business Intelligence. Disponible en Internet: <http://www.lantares.com/blog/atencion-medica-personalizada-big-data-y-el-futuro-de-la-medicina> [Consulta: 13 enero 2017].

personalizada[781]. En el mismo sentido, PLANAS[782] también comparte el criterio de que la atención personalizada con el Big data será una realidad.

Otras de las grandes ventajas que representa el Big Data en el ámbito de la salud es que tiene la capacidad, mediante el almacenamiento y análisis de diversas fuentes de información, de responder preguntas, no en base a una investigación puntual, sino con lo que llamamos la *Real World Evidence*[783]. Este término traducido significaría "Datos de la Vida Real", sin embargo, difiere del concepto *Real World Data* ya que éstos son los que debidamente analizados nos conducen a las evidencias (*Real World Evidence*). Entre ambos colocamos los procesos analíticos que nos permiten convertir datos en evidencias[784].

En la 3ª Jornada denominada *"Hacia un sistema sanitario basado en la creación de valor: La era de los datos, nuevo paradigma en la financiación de fármacos innovadores",* especialistas de diferentes ámbitos del sector sanitario y de distintas Comunidades Autónomas, han analizado las expectativas que se presentan ante el desarrollo del *Real World Data, Real World Evidence y Big Data,* y han puesto de relieve entre sus conclusiones que *"el Big Data supone un cambio de paradigma a la hora de extraer conclusiones y tomar decisiones"*[785]*.* Evidentemente jugará un rol

[781] Ibídem.

[782] Vid. PLANAS, J., op. cit. Ejemplifica el Dr. Planas argumentando que la medicina moderna trata a un paciente diabético de 83 años de edad con hipertensión manera similar a un atleta de 45 años de edad con hipertensión, basándose en que se agrupan en el mismo ensayo clínico; en el futuro, la atención será mucho más personalizada en base a lo que funcionó mejor para millones de pacientes similares con anterioridad. Este nivel de atención personalizada ofrece la promesa de una atención mejor y más adecuada.

[783] SOLER, I. (23.02.2016) Entre el imperativo moral y el Big Data sanitario. El Periódico. Disponible en Internet: <http://www.elperiodico.com/es/noticias/mas-valor/impertativo-moral-gran-hermano-sanitario-4917353> [Consulta: 18 enero 2017].

[784] VALENCIA, E. (28.09.2016) ¿Qué es el Real World Evidence y para qué sirve? [Blog post]. Blog Singular Data & Analytics. Disponible en Internet: <https://data.sngular.team/es/art/63/real-world-evidence-definicion-y-beneficios> [Consulta: 18 enero 2017].

[785] Otra de las conclusiones destacadas de la jornada fue que el manejo correcto de los datos que proporcionan las nuevas tecnologías permitirá desarrollar un modelo de financiación basado en la Medicina personalizada y en el riesgo compartido. Vid. HERNÁNDEZ MEDRANO, I. (29.11.2016) En la 3ª Jornada "Hacia un sistema sanitario basado en la creación de valor: La era de los datos, nuevo paradigma en la financiación de fármacos innovadores", celebrada el en Madrid. El Médico Interactivo. Disponible en Internet: <http://www.elmedicointeractivo.com/articulo/noticias/big-data-supone-cambio-

importante en la sociedad médica, y a pesar de ser un cambio que se vislumbra complicado, a la postre y gracias a las nuevas tecnologías, está mucho más cerca y es más viable de lo que imaginamos.

3. Aspectos negativos del Big Data en la salud.

Sin embargo, también hay preocupaciones provenientes del sector jurídico en la aplicación en España del Big Data sanitario, y ello se debe fundamentalmente a las dudas que genera el fin último que se le puede dar al Big Data. LLÀCER, CASADO y BUISAN[786] argumentan que no es lo mismo utilizar datos de pacientes con fines de investigación, que, por el contrario, proporcionar esos datos a empresas que puedan utilizarlos para comercializar con ellos o en su propio beneficio.

Según GIL GONZÁLEZ[787], algunos de los retos más importantes en la utilización del Big Data, pueden ser el riesgo de caer en conclusiones erróneas que nadie revisa, el riesgo que para las personas pueda tener tomar decisiones automatizadas sin un sesgo humano, y el riesgo para la privacidad de las personas. Los dos primeros riesgos que explica la autora, son muy parecidos, desde el punto de vista de la desconfianza que genera que no exista un factor humano que revise una cierta información, que lleva a una conclusión determinada. Sin embargo, consideramos que el factor más importante a tener en cuenta es el tercer riesgo, es decir, el vinculado con la privacidad de las personas.

Es unánime entre los expertos en protección de datos, la advertencia sobre la necesidad que existe de que mecanismos seguros, fiables y consistentes permitan la total anonimización de los datos de los pacientes, y que estos mecanismos impidan la identificación del sujeto mediante la vuelta atrás del proceso y su re-identificación[788].

---

paradigma-extraer-conclusiones-y-tomar-decisiones/20161129173258107417.html> [Consulta: 13 enero 2017].

[786] LLÀCER MATACÁS, Mª R.; CASADO, M.; BUISAN ESPELETA, L. (coord.)., op. cit., pp. 33-36.

[787] GIL GONZÁLEZ, E., op. cit., p. 32.

[788] Ver al respecto: LLÀCER MATACÁS, Mª R.; CASADO, M.; BUISAN ESPELETA, L. (coord.)., op. cit., pp. 33-36.; LÓPEZ LÓPEZ, V., op. cit.; RODRIGO LARRUCEA, C., op. cit.; MIRALLES LÓPEZ, R. (25.07.2014) Aspectos a considerar en relación al Big Data. [Blog post]. Blog Observatorio Iberoamericano de

Las incertidumbres sobre los potenciales impactos negativos que pueda generar el tratamiento masivo de información aconsejan adoptar posturas garantistas, especialmente en relación al derecho a la protección de los datos de carácter personal, la privacidad y la intimidad[789].

Sobre ésta preocupación latente, en torno a la privacidad y la intimidad, MIRALLES LÓPEZ[790] señala que:

> Las políticas públicas y las tecnologías, juegan un papel importante en la protección de los derechos y libertades que puedan verse afectados por el tratamiento masivo de información y, especialmente, respecto del uso que se pueda hacer del resultado del procesamiento de esa información.

Según PARRA CALDERÓN[791], a medida que aumenta la aplicación del Big Data se identifican nuevos retos a los que enfrentarse, así como nuevas oportunidades que acrecientan el interés por el desarrollo de la investigación en este dominio.

Una vez analizada la doctrina, podemos manifestar que las preocupaciones son muchas en torno a las nuevas implicaciones jurídicas del Big Data en salud. Éstas preocupaciones en relación a su aplicación, conllevan nuevos retos que la normativa deberá dar respuesta y cobertura legal, y que podemos resumir, desde nuestro punto de vista, de la siguiente manera:

(i) Es primordial, en relación al derecho a la protección de los datos de carácter personal, y en miras de garantizar la privacidad y la intimidad de las personas, que se actualice la normativa en torno a las implicaciones del Big Data en salud. No sólo hacemos referencia a las normas españolas, sino también en el ámbito de la UE, que según hemos hecho referencia en el Capítulo I de la Segunda Parte de ésta Tesis, el RGPD no ha abordado estos temas que son de evidente existencia, y más aún lo serán dentro de un año, cuando el RGPD entre en vigencia.

Protección de Datos. Disponible en Internet: <http://oiprodat.com/2014/07/25/aspectos-a-considerar-en-relacion-al-big-data/> [Consulta: 10 enero 2017].

789 MIRALLES LÓPEZ, R., op. cit.

790 Ibídem.

791 PARRA CALDERÓN, C. L. "Big data en sanidad en España: la oportunidad de una estrategia nacional". *Gaceta Sanitaria*. Vol. 30, núm. 1, enero-febrero 2017, p. 5.

(ii) Otra preocupación radica en las dificultades técnicas que supondrá el almacenamiento de semejante magnitud de datos. Evidentemente estos datos han de poder almacenarse en un determinado soporte, servidor, etc. Y este mismo reto conlleva implícito otro, que es la seguridad de ese almacenamiento, que el lugar físico donde se encuentre, cuente con una infraestructura que haga inviable su acceso, robo, *hackeo*, o cualquier injerencia.

(iii) Así también, consideramos un desafío la elaboración de algoritmos matemáticos capaces de procesar la información del Big Data, para que la misma esté siempre disponible en tiempo real -característica primordial del Big Data-, y que no existan quiebres o interrupciones del sistema o inconvenientes relacionados con los ordenadores.

(iv) Otro peligro que entraña el Big Data en salud, es el riesgo de asumir conclusiones erróneas como absolutamente ciertas, porque el Big Data, tal y como hemos explicado, trabaja con un sistema basado en las probabilidades haciendo correlaciones de datos, pero evidentemente no puede analizar la causa de los factores de esos datos que analiza, por tanto, esto podría derivar en la inseguridad que pueda conllevar tomar decisiones automatizadas sin la intervención del factor humano.

(v) Finalmente, es importante señalar otra amenaza que consideramos preocupante y que implica conocer exactamente quién tendrá acceso a la información del Big Data, ¿el médico de cabecera?, ¿el médico privado, su secretaria? Evidentemente es muy significativo este punto, porque esa “llave” de acceso a nuestros datos sensibles puede caer en manos que no sepamos quiénes son, para qué quieren nuestros datos y qué pueden hacer con ellos.

3.1. La anonimización versus la re-identificación. La anonimización no garantiza la privacidad de los datos personales.

Para adentrarnos en éste epígrafe, resulta conveniente explicar brevemente en qué consiste la anonimización de los datos, para luego comentar la posible re-identificación de la persona a partir de sus datos anonimizados, y acabar demostrando que, la privacidad de los datos personales no puede estar garantizada desde nuestro punto de

vista, con los medios tecnológicos de los que hoy se disponen.

La anonimización[792] implica la falta de identificación de una persona en relación con alguno de sus datos personales. Básicamente se logra la anonimización de los datos realizando dos pasos. En primer lugar, se intentan eliminar de los datos los rasgos que los hacen personales y por tanto susceptibles de identificar a una persona, por ejemplo, el nombre, DNI, dirección, etc. En segundo lugar, se intentan eliminar aquellos datos que pudieran dar origen a la identificación de la persona en un contexto determinado, por ejemplo, el número de ingreso hospitalario, número de habitación del paciente que está ingresado en un hospital, etc. Ésta anonimización de los datos personales aseguraba la privacidad de la persona[793].

Nuestro ordenamiento jurídico no hace mención expresa a la anonimización de los datos, pero sí a lo que denomina "disociación de los datos", que según ha entendido la AEPD tiene correlación[794]. El RD 1720/2007, define el procedimiento de disociación, estableciendo que es *"todo tratamiento de datos personales que permita la obtención de datos disociados"*[795]. Del mismo modo, la LOPD establece que el procedimiento de disociación es *"todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable"*[796]. Ésta definición se complementa con la de persona identificable, que según el RD 1720/2007, es *"toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante*

[792] La legislación española carece de una definición y una regulación específica sobre los datos anónimos o sobre su anonimización. La referencia más aproximada a este concepto podemos encontrarla en la Directiva 95/46/EU que en el Considerando (26) manifiesta que: *"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".*

[793] Para profundizar más el tema, véase: GIL GONZÁLEZ, E., op. cit., p. 83.

[794] Informe jurídico de la AEPD 207/2008. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2008-0207_Consecuencias-de-la-creaci-oo-n-de-una-base-de-datos-m-ee-dicos-anonimizada.pdf> [Consulta: 10 noviembre 2016].

[795] Artículo 5.p), del RD 1720/2007.

[796] Artículo 3.f), de la LOPD.

cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados"[797].

También cabe hacer referencia en este punto, a las estipulaciones que contiene la Ley 14/2007, de Investigación Biomédica[798], porque resulta muy ilustrativa sobre las definiciones a las que nos referimos. Al respecto, señala la Ley[799] que:

> Muestra biológica anonimizada o irreversiblemente disociada: muestra que no puede asociarse a una persona identificada o identificable por haberse destruido el nexo con toda información que identifique al sujeto, o porque dicha asociación exige un esfuerzo no razonable.
>
> Muestra biológica no identificable o anónima: muestra recogida sin un nexo con una persona identificada o identificable de la que, consiguientemente, no se conoce la procedencia y es imposible trazar el origen.
>
> Muestra biológica codificada o reversiblemente disociada: muestra no asociada a una persona identificada o identificable por haberse sustituido o desligado la información que identifica a esa persona utilizando un código que permita la operación inversa.

Consecuentemente, la diferencia respecto a los datos personales o datos anonimizados es sustancial desde el punto de vista jurídico. Los datos personales, gozan de la protección legal de la Directiva 95/46/CE, de la LOPD y del Reglamento RD 1720/2007, y, por el contrario, los datos anonimizados, escapan a ese paraguas jurídico, porque no están contemplados en la normativa. Y para que pudieran correlacionarse la disociación de los datos y la anonimización, tal y como ha entendido la AEPD[800], a fin de recibir la misma protección legal, sería necesario una interpretación de la Jurisprudencia en este sentido. Por tanto, si los datos son anonimizados y a través de ellos no se puede identificar a la persona a la que pertenecen, quedan fuera de la aplicación del ámbito legal por cuanto no son considerados datos personales. Y ello, en base a lo preceptuado en el Artículo 3 de la LOPD que manifiesta que será de aplicación a *"cualquier información concerniente a personas físicas identificadas o identificables"*[801].

---

[797] Artículo 5.o), del RD 1720/2007.

[798] Ley 14/2007, de 3 de julio, de Investigación Biomédica (BOE núm. 159, 4.07.2007).

[799] Ibídem, Artículo 3, p), q), r).

[800] Informe jurídico de la AEPD 207/2008, op. cit.

[801] Artículo 3. a), de la LOPD.

En éste sentido se ha pronunciado la AEPD[802], al entender que las iniciales del nombre y apellidos, un código o número de anonimización, el número de identificación fiscal, el número de afiliación al Sistema Público de Salud, el número de HC, no constituyen un sistema adecuado para disociar los datos personales, por lo tanto, si la persona resulta identificable, sí que se aplicará la LOPD[803]. Sin embargo, si de la anonimización o de la disociación de los datos, no se puede identificar a la persona, entonces no resultará aplicable la LOPD.

Sin embargo, a pesar de este proceso de anonimización, la realidad es diferente y ello en virtud de la aparición de las nuevas tecnologías, cada vez más utilizadas por la sociedad y en todos los sectores. Dado los avances tecnológicos, la re-identificación de la persona es viable. Con el fenómeno Big Data, los datos pueden ser objeto de re-identificación de la persona a la que pertenecen, a pesar de haber sido anonimizados[804].

En éste sentido, MIRALLES LÓPEZ[805] explica que:

> Los datos personales pueden estar presentes de dos maneras, una de tipo indirecto, cuando en origen los datos eran de carácter personal, y han sido sometidos a tratamientos de disociación -aparentemente dejan de ser datos personales, pero existe el riesgo de re-identificación-, y por tanto, a priori, los resultados de su tratamiento no aplican a personas concretas identificadas o identificables, o bien de manera directa, cuando el tratamiento "big data" se lleva a cabo directamente sobre datos personales.

Sostenemos que las personas pueden ser re-identificadas, porque al existir datos dispersos, variados y que individualmente no revelen la identidad de una persona,

---

[802] Véase al respecto: Informe jurídico 0624/2009 de la AEPD. Disponible en Internet: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2009-0624_Publicaci-oo-n-en-revista-de-foto-ganadora-de-concurso-con-im-aa-genes-de-personas.-No-necesidad-de-consentimiento.pdf> [Consulta: 18 septiembre 2016].;

[803] Vid. Informe jurídico 0533/2008 de la AEPD. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2008-0533_Aplicaci-oo-n-de-la-LOPD-en-ensayos-cl-ii-nicos.pdf> [Consulta: 18 septiembre 2016].; Informe jurídico 0654/2009 de la AEPD. Disponible en Internet: < https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2009-0654_Identificaci-oo-n-del-paciente-a-traves-de-c-oo-digo-num-ee-rico-no-constituye-un-supuesto-de-disociaci-oo-n.pdf> [Consulta: 18 septiembre 2016].

[804] Vid. GIL GONZÁLEZ, E., op. cit., p. 83

[805] MIRALLES LÓPEZ, R., op. cit.

dentro de lo que denominamos Big Data, esos datos se correlacionan y pueden volver a revelar una identidad que había sido previamente anonimizada. En éste sentido, se ha pronunciado FERRER[806], explicando que estaba demostrado que se podía re-identificar a una persona a partir de cuatro datos aleatorios de la misma. También la doctrina a través de LLÀCER, CASADO, y BUISAN[807], advierte sobre el riesgo de la re-identificación al señalar que:

> Hasta ahora, la premisa de la anonimización del dato ha representado la garantía que permitía cumplir con las regulaciones de protección de datos personales existentes. El problema radica en que, actualmente, está acreditado que la anonimización no garantiza la privacidad de los datos personales, puesto que mediante técnicas de ingeniería informática es posible volver a conectar los datos con la persona a quien pertenecen.

Asimismo, las autoras LLÀCER, CASADO, y BUISAN[808] manifiestan que, a través de los medios tecnológicos existentes, es posible la re-identificación de una persona a partir de los datos de un *dataset* (base de datos) sobre el cual se han aplicado técnicas de anonimización.

Al respecto, y tal y como viene advirtiendo la UE a través del Grupo de Trabajo del Artículo 29, la des-anonimización y la re-identificación resultan posibles empleando medios técnicos adecuados[809]. Por ello, desde la UE, se pone de relieve que es una

---

[806] Para profundizar más al respecto, véase: FERRER, S. (29.01.2015) Cuatro datos son suficientes para relacionarte con tu tarjeta de crédito. El Confidencial. Disponible en Internet: <http://www.elconfidencial.com/tecnologia/2015-01-29/cuatro-datos-son-suficientes-para-relacionarte-con-tu-tarjeta-de-credito_651827/> [Consulta: 8 febrero 2017].

[807] LLÀCER MATACÁS, Mª R.; CASADO, M.; BUISAN ESPELETA, L. (coord.)., op. cit., p. 33.

[808] Ibídem, pp. 34-35.

[809] *Opinion 06/2013 on open data and public sector information ('PSI') reuse* (Opinión 06/2013 sobre la información abierta y la reutilización de la información del sector público), del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 5 de junio de 2013, 1021/00/EN (WP 207). Disponible en Internet (versión en inglés): <https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjK1_rqwsvRAhXBaxQKHWkQDWkQFggdMAA&url=http%3A%2F%2Fec.europa.eu%2Fjustice%2Fdataprotection%2Farticle29%2Fdocumentation%2Fopinionrecommendation%2Ffiles%2F2013%2Fwp207_en.pdf&usg=AFQjCNEIJ2W02C_cQfEtHvVaTO1R3em8Jw&bvm=bv.144224172,d.bGs> [Consulta: 8 agosto 2016].; Dictamen 05/2014 sobre técnicas de anonimización, del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 10 de marzo de 1014, 0829/14/ES (WP 216). Disponible en Internet: <https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi8joqTxcvRAhUI0RQKHT9xCF0QFggcMAA&url=http%3A%2F%2Fec.europa.eu%2Fjustice%2Fdatap

tarea difícil decidir qué nivel de agregación puede ser apropiado y qué técnicas específicas de anonimización utilizar y destacan al respecto dos conclusiones: por un lado, si la agregación y la anonimización no se llevan a cabo de manera efectiva, esto conlleva el riesgo de que los individuos puedan ser re-identificados a partir de estos conjuntos de datos; y por otro lado, enfatizan en que una vez que los datos sean publicados públicamente para su reutilización, no habrá control sobre quién puede acceder a los datos. La probabilidad de que "cualquier otra persona" disponga de los medios y utilice esos medios para volver a identificar a los interesados aumentará de manera muy significativa[810].

Por lo tanto, una forma sencilla de anonimizar el Big Data consiste en eliminar cualquier dato de índole personal como nombres, direcciones o números de teléfono. De esta forma, esta información se transforma en un mero conjunto de datos. Sin embargo, una base de datos sin nombres personales o direcciones no garantiza su anonimato, ni asegura que pueda ser compartida al público o a terceras pares sin riesgo. Es por ello, que las medidas de anonimización deben ser encriptadas o más estrictas y tecnológicas para impedir la re-identificación de la persona.

---

rotection%2Farticle29%2Fdocumentation%2Fopinionrecommendation%2Ffiles%2F2014%2Fwp216_es.pdf&usg=AFQjCNErX--8_aKrEFUrFMCBB_dsG1Fu2g> [Consulta: 8 agosto 2016].

[810] El Grupo de Trabajo del Artículo 29 hace una distinción entre los “datos anónimos”, puesto que no se consideran datos personales y los “datos anonimizados” que son datos que han sido manipulados utilizando diversas técnicas para mitigar los riesgos de volver a identificar a las personas afectadas, pero no han alcanzado el umbral establecido en la letra a) del Artículo 2 y en el considerando 26 de la Directiva 95/46/EC. Las leyes de protección de datos por lo general no permiten que los organismos del sector público divulguen públicamente datos personales recopilados para otra finalidad, por lo general administrativa. Por lo tanto, en estos casos, su reutilización como parte de las iniciativas de reutilización de PSI tampoco es posible. En lugar de datos personales, suelen ser datos estadísticos derivados de datos personales que son y que deberían - en principio - estar disponibles para su reutilización. Esta es la solución más eficaz para minimizar los riesgos de la divulgación involuntaria de datos personales, según el WP 29. Estos conjuntos de datos anónimos y agregados no deben permitir la re-identificación de los individuos y, por lo tanto, no deben contener datos personales. Hasta la fecha, las iniciativas de reutilización de PSI lanzadas por organismos del sector público a través de "portales de datos abiertos" u otras plataformas tienden a hacer disponible datos agregados y anónimos para su reutilización, en lugar de datos personales como tales. Este enfoque es ciertamente más seguro y debería ser alentado, según argumenta el Grupo de Trabajo. Vid. *Opinion 06/2013 on open data and public sector information ('PSI') reuse* (Opinión 06/2013 sobre la información abierta y la reutilización de la información del sector público), del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 5 de junio de 2013, 1021/00/EN (WP 207), op. cit.

En el informe del Grupo de trabajo del Artículo 29[811] explica la posibilidad de que a partir de datos personales se pueden re-identificar a las personas, debido a su naturaleza única, los perfiles de datos genéticos constituyen un ejemplo de datos personales que están en riesgo de ser identificados si tan solo se utiliza la técnica de eliminación de la identidad del donante. Diversos estudios científicos ya han demostrado que, al combinar los recursos genéticos disponibles para el público (por ejemplo, registros genealógicos, obituarios y resultados de consultas en motores de búsqueda) y los metadatos sobre donantes de ADN (fecha de donación, edad o lugar de residencia), se puede revelar la identidad de determinadas personas, aunque el ADN se haya donado de forma "anónima".

Señala el Grupo de Trabajo del Artículo 29, que para que un dato sea verdaderamente anónimo ha de ser completamente irreversible su identificación. Para lograr esto y dado el riesgo residual que siempre va a existir al aplicar una técnica de anonimización, en la Opinión 05/2014 sobre Técnicas de Anonimización de Datos Personales, se enuncian distintas posibles técnicas a fin de anonimizar los datos personales[812]:

(i) Se recomienda al encargado de la anonimización que se encargue de forma regular de identificar, supervisar y controlar los riesgos, tanto actuales como nuevos; y evaluar si los controles que existen son suficientes.

(ii) El responsable del tratamiento deberá respetar siempre los derechos de los interesados y las libertades fundamentales.

(iii) En el caso de que existiesen normas legales, éstas deberán estar formuladas de una manera tecnológicamente neutra, teniendo en cuenta el potencial desarrollo de la tecnología de la información.

---

[811] Vid. *Opinion 06/2013 on open data and public sector information ('PSI') reuse* (Opinión 06/2013 sobre la información abierta y la reutilización de la información del sector público), del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 5 de junio de 2013, 1021/00/EN (WP 207), op. cit.

[812] Dictamen 05/2014 sobre técnicas de anonimización, del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 10 de marzo de 1014, 0829/14/ES (WP 216). Disponible en Internet: <https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi8joqTxcvRAhUI0RQKHT9xCF0QFggcMAA&url=http%3A%2F%2Fec.europa.eu%2Fjustice%2Fdataprotection%2Farticle29%2Fdocumentation%2Fopinionrecommendation%2Ffiles%2F2014%2Fwp216_es.pdf&usg=AFQjCNErX--8_aKrEFUrFMCBB_dsG1Fu2g> [Consulta: 8 agosto 2016].

Al respecto de la Opinión 5/2014 del WP 29 a la que hemos hecho referencia *ut supra*, y coincidiendo con GIL GONZÁLEZ[813], parece que hay una contradicción, porque *"Por un lado la opinión reconoce que existe un riesgo de reidentificación residual incluso después de aplicar las técnicas de anonimización. Pero, por otro lado, la Opinión también señala que la Directiva ordena que la anonimización sea irreversible".*

Asimismo, el Grupo de Trabajo del Artículo 29, expresó que debe tenerse la máxima precaución para garantizar que los conjuntos de datos a revelar no deban incluir datos que puedan ser re-identificados por medios que razonablemente puedan ser utilizados por cualquier persona, incluyendo posibles reutilizadores, pero también otras partes que puedan tener interés en obtener los datos[814]. Es decir, un dato será anónimo cuando no sea posible su vinculación con la persona a la que hubiera identificado el dato, teniendo en cuenta que el riesgo de identificación puede aumentar con el tiempo.

Por tanto, y atendiendo a la inexistencia actual de garantías reales desde el ámbito legal, en la misma línea de pensamiento que LLÀCER, CASADO, y BUISAN[815], quienes explican que:

> Desde el momento en que el propio anonimato deviene incierto es perentorio encontrar una base que legitime el análisis de datos personales de salud a gran escala. De no ser así, se abre la puerta a usos no deseados de esos datos ya que su titular, habiendo dado su consentimiento para determinadas acciones en el ámbito sanitario y de investigación, en realidad pierde el control y queda desprotegido pues -con una falsa concepción de la protección de datos y del secreto profesional- desconoce que sus datos pueden haber sido utilizados o cedidos para otros fines, ni deseados ni efectivamente consentidos.

[813] GIL GONZÁLEZ, E., op. cit., pp. 86-87.

[814] *Opinion 06/2013 on open data and public sector information ('PSI') reuse* (Opinión 06/2013 sobre la información abierta y la reutilización de la información del sector público), del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 5 de junio de 2013, 1021/00/EN (WP 207), op. cit.

[815] LLÀCER MATACÁS, Mª R.; CASADO, M.; BUISAN ESPELETA, L. (coord.)., op. cit., p. 35. Las autoras ponen el énfasis en que la re-identificación de la persona puede hacerse por los valores particulares que pueden tomar ciertos datos, hasta ahora considerados no personales; como un código postal, la fecha de nacimiento y el sexo; pero partiendo de estos datos es posible re-identificar a la gran mayoría de las personas de una base de datos.

4. Nuevos retos frente al Big Data.

4.1. Recopilación y gestión de los datos.

Según hemos comentado al inicio de éste Capítulo, Big Data refiere al conjunto de datos e información tan grandes y tan complejos que hace muy difícil su procesamiento utilizando herramientas de gestión de bases de datos convencionales. La cuestión, según JOYANES AGUILAR y POYATOS DÍAZ[816], es cómo acceder, distribuir y utilizar esta vasta cantidad de datos "no estructurados". Los pacientes, las clínicas, los hospitales tienen cantidades masivas de datos clínicos, en formatos escritos en papel o electrónicos pero que permanecen sin utilizar por la dificultad e imposibilidad material de "digerirlos" de forma efectiva, por muy buenos deseos que pueda tener el equipo sanitario.

Evidentemente la compilación de los datos existentes de cada paciente, implicará una larga y complicada labor. Nos referimos a que en términos temporales será larga porque al tratarse de datos no estructurados (recetas médicas, radiografías, resultados de pruebas diagnósticas de centros médicos privados, etc.), no están en un único sitio físico, por tanto la recopilación de toda esta información resultará complicada, no sólo porque los pacientes deberían reunirla y entregarla a un centro de salud para que ellos la gestionen, sino porque nos encontraremos en la tesitura de que muchos pacientes no guardan el resultado de pruebas médicas, radiografías, etc., que antes eran entregadas directamente al paciente. Además de ello, puntualizamos que esta labor será complicada, porque estos datos desestructurados hay que procesarlos con la tecnología adecuada para recopilarlos en los formatos idóneos a fin de que los mismos resulten útiles para luego poder gestionarlos, y en este punto nos encontraremos con la necesidad de convertir esos datos no estructurados y provenientes de diversos formatos a un lenguaje tecnológico capaz de poder procesar y analizar dichos datos. Al igual que hace décadas con la aparición de los ordenadores existían los *"data entry"* que eran informáticos que se dedicaban a volcar la información del papel a los ordenares, ahora necesitaremos un sistema similar para que recabe todos los datos y los vuelque en lo que denominamos Big Data. Este proceso, además de ser largo y complicado, puede en algunos casos devenir imposible, y ello si los datos no estructurados resultan dañados, ilegibles o imposibles de incorporar a un *dataset* (base de datos).

[816] JOYANES AGUILAR, L.; POYATOS DÍAZ, J. M., op. cit.

En base a ello, vislumbramos un gran reto en el ámbito sanitario: almacenar e interpretar la información para que sea útil en la detección de enfermedades. De hecho, más del el 80% de los datos de salud no se encuentran estructurados[817] y se almacenan de forma diferente, según sean pruebas de laboratorio, de imagen o transcripciones médicas, etc.

Las propiedades, los retos y los asuntos relevantes que caracterizan la aplicación de los Big Data en biomedicina son la gran variedad en la naturaleza de los datos y la alta velocidad de proceso requerida; retos relacionados con la veracidad de los datos, con los flujos de trabajo, con los métodos computacionales, con la extracción de información significativa, con el intercambio de datos y con la necesidad de expertos en el uso de estas tecnologías. Son relevantes asuntos relacionados con la reutilización de datos, con el riesgo de falso descubrimiento de conocimiento y con la privacidad[818].

El verdadero problema es que la información necesaria para evaluar correctamente el riesgo del paciente y determinar el mejor tratamiento está disponible en las notas del médico, pero sin las herramientas apropiadas el conocimiento sigue sin estar disponible, y por tanto sin uso. Cada día que pasa disponemos de mayores volúmenes de información, además de en nuestros centros también y sobre todo a través de la red; toda esta nueva información debe hallar un sistema para ser monitorizada, procesada, cribada y aprovechada en beneficio de la formación de nuestros médicos y por tanto también y sobre todo en beneficio del paciente[819].

---

[817] SIEMENS. Big data in the healthcare industry. Increasingly used data-driven care protocols will change healthcare delivery systems globally (Big Data en la industria de asistencia médica. Los protocolos de cuidado cada vez más usados conducidos por datos cambiarán sistemas de entrega de asistencia médica a escala mundial) (05.08.2015). Disponible en Internet: (versión en inglés): <https://www.healthcare.siemens.com/magazine/mso-big-data-and-healthcare-1.html> [Consulta: 14 noviembre 2016].

[818] Vid. BARÓ E.; DEGOUL S.; BEUSCART R.; CHAZARD E., op. cit. En éste sentido PARRA CALDERÓN es optimista: *"Estamos frente a una oportunidad histórica para aunar voluntades, políticas y tecnologías en una estrategia nacional. En este sentido, es procedente desarrollar una estrategia inicial en el ámbito de la investigación biomédica, donde los retos son tremendos pero los posibles beneficios de una explotación masiva de la información digital disponible en el Sistema Nacional de Salud son evidentes, alineando esfuerzos de las comunidades autónomas.* PARRA CALDERÓN, C. L., op. cit.

[819] PLANAS, J., op. cit.

Respecto a estos nuevos retos, en Estados Unidos, la Casa Blanca emitió un informe que explicaba la promesa del entonces presidente Obama de destinar 200 millones de dólares a I + D en el ámbito del Big Data. El informe detalla que el dinero servirá para mejorar en gran medida las herramientas y técnicas necesarias para acceder, organizar y extraer descubrimientos de los enormes volúmenes de datos digitales, y destaca que la utilización del Big Data promete transformar la capacidad para el descubrimiento científico, el medio ambiente y la investigación biomédica, educación y seguridad nacional[820].

Asimismo destaca el informe que el Big Data mejorará los principales medios científicos y tecnológicos de gestión, análisis, visualización y extracción de información útil, de grandes y diversos conjuntos de datos, lo que propiciará el aceleramiento del descubrimiento científico y conducirá a nuevos campos de investigación que de otro modo no serían posibles, fundamentalmente en la imagen, molecular, celular, electrofisiológico, químico, comportamiento, epidemiológico, clínico, y otros conjuntos de datos relacionados con la salud y la enfermedad[821].

4.2. Protección de la intimidad y privacidad frente al avance tecnológico.

Otro de los grandes retos jurídicos es combinar el derecho a la intimidad y privacidad de la persona con la innovación tecnológica necesaria para la implantación del Big Data y

---

[820] El informe explica la iniciativa del gobierno de Estados Unidos de invertir en Investigación y Desarrollo de Big Data para avanzar el estado de la técnica de las tecnologías básicas necesarias para recopilar, almacenar, preservar, administrar, analizar y compartir enormes cantidades de datos. También aprovechar estas tecnologías para acelerar el ritmo de descubrimiento en la ciencia y la ingeniería, fortalecer la seguridad nacional y transformar la enseñanza y el aprendizaje, así como expandir la mano de obra necesaria para desarrollar y utilizar las tecnologías de Big Data. También prevé el informe alentar a las Universidades a desarrollar programas interdisciplinarios de posgrado para preparar a la próxima generación de científicos e ingenieros de datos. Office of Science and Technology Policy. Executive Office of the President. (20.03.2012) *Obama administration* unveils "Big Data" initiative: announces $200 million in new R&D investments (La Oficina del Presidente Obama anuncia la iniciativa de 200 millones de dólares en I+D en Big Data). Estados Unidos. Disponible en Internet (versión en inglés): <https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiXemAocnRAhVJwBQKHd4zCYkQFggcMAA&url=https%3A%2F%2Fwww.whitehouse.gov%2Fsites%2Fdefault%2Ffiles%2Fmicrosites%2Fostp%2Fbig_data_press_release_final_2.pdf&usg=AFQjCNGDfomg7zyDTyUq77ngGpFF282yYA&sig2=KC0mFF8-mZ7fC1g7PbiQtQ> [Consulta: 14 octubre 2016].

[821] Ibídem.

la posible re-identificación de sus datos para fines distintos. Al respecto, SOLER[822] manifiesta que *"es evidente que la privacidad y la seguridad del ciudadano es un valor que debemos proteger",* pero reconocido este extremo se plantea las siguientes cuestiones: *"¿podría ser que pretendamos protegerle con tanto ahínco que al final lo que conseguimos es protegerle de la innovación y la mejora de su propio estado de salud?"*

Frente a la pregunta que plantea SOLER[823], desde el Reino Unido se ha sostenido que la utilización del Big Data en salud deviene un imperativo moral, y ello, según KELSEY[824], es porque el sistema de salud ha de salvar vidas y esta consideración debe prevalecer sobre cualquier otra. Evidentemente esta perspectiva tuvo una fuerte oposición por parte de grupos garantistas para con la privacidad de la información. Sin embargo, en Cataluña, la Agencia de Calidad y Evaluación Sanitarias de Catalunya (AQuAS), compartiendo este pensamiento, ha promovido el proyecto VISC+, con el objetivo último de mejorar la calidad de la atención sanitaria prestada a la ciudadanía[825]. Para hacerlo, VISC+ relacionará la información de salud que se genera en Cataluña de una manera totalmente anonimizada y segura, con el fin de impulsar y facilitar la investigación y la innovación en ciencias de la salud.

Ésta primera experiencia importante de Big Data en Cataluña sobre información de pacientes VISC+, que está comenzando su recorrido para uso científico, ha sido

---

[822] SOLER, I., op. cit.

[823] Ibídem.

[824] Tim Kelsey, es Director del England's National Health Service (NHS) y fue pionero en la justificación de la utilización del Big Data en salud, afirmando que el uso del Big Data en salud era esencialmente "un imperativo moral". Esta afirmación la realizó en el contexto del relanzamiento del programa care.data que tiene como objetivo el impulso de la recolección y análisis de los datos en salud digital y que tuvo una fuerte oposición en primera instancia por parte de grupos garantistas para con la privacidad de la información. Vid. KELSEY, T. (13.01.2015) NHS boss claims patient data collection is "moraly right" (Director del England's National Health Service (NHS) (El Director del Servicio Nacional de Salud NHS demanda que la recolección de datos del paciente sea "un derecho moral"). [Blog post]. Blog It Pro. Disponible en Internet (versión en inglés): <http://www.itpro.co.uk/public-sector/23844/nhs-boss-claims-patient-data-collection-is-morally-right> [Consulta: 13 febrero 2017].

[825] ARGIMON, J. M. (26.02.2015) El proyecto VISC+ es una oportunidad para la mejora de la calidad de la atención sanitaria. [Blog post]. Blog de la Agencia de Calidad y Evaluación Sanitarias de Catalunya (AQuAS). Disponible en Internet: <http://blog.aquas.cat/2015/02/26/el-proyecto-visc-es-una-oportunidad-para-la-mejora-de-la-calidad-de-la-atencion-sanitaria/?lang=es> [Consulta: 18 enero 2017].

cuestionado desde el sector doctrinario por LLÀCER, CASADO, y BUISAN[826], quienes advierten que, si bien las bases de datos de las que se nutre este proyecto conllevan la existencia de ficheros de los que dispone el sistema sanitario público catalán, y por tanto rige la LOPD y su Reglamento, *"esta regulación no resulta suficiente ya que su aplicación ha sido superada por la nueva tecnología Big Data y no evita usos indebidos y discriminatorios"*[827].

Frente a estas dudas, y con el fin de garantizar la seguridad de los datos, la Agencia de Calidad y Evaluación Sanitarias de Catalunya[828] aseguró que seguirá el protocolo de anonimización del organismo independiente *Data Protection Working Party,* aplicándose la normativa de manera muy estricta para dar las máximas garantías de seguridad. Por ello, aunque se trate de datos anonimizados, la Agencia de Calidad y Evaluación Sanitarias de Catalunya, aplicará la normativa como si se tratara de datos personales.

Desde luego, y como suele ocurrir con las nuevas tecnologías, se han generado dudas y desconfianza. Fundamentalmente los temores se basan en la posible venta de datos, pérdida de privacidad, de interés de lucro económico, de opacidad o ambigüedad a la hora de recopilar y tratar tal volumen de datos, y también existen dudas sobre un posible interés desde el sector privado (farmacéuticas y aseguradoras) para favorecer que éstas hagan aún más ganancias[829].

---

[826] LLÀCER MATACÁS, Mª R.; CASADO, M.; BUISAN ESPELETA, L. (coord.)., op. cit., pp. 36 y ss.

[827] Las autoras LLÀCER, CASADO, y BUISAN cuestionan la legitimidad del proyecto en relación con el consentimiento del paciente, manifestando que: "el proyecto VISC+, habiendo sido aprobado por un mero «Acuerdo de gobierno», no cuenta con habilitación legal suficiente para la reutilización de datos sanitarios, ya que las leyes de sanidad solo legitiman para tratar los datos de los pacientes con fines directamente asistenciales, investigadores u organizativos. El segundo tipo de legitimación, la voluntaria, proviene siempre del consentimiento expreso del paciente y es la que se precisa para tratar datos con fines estrictamente privados, es decir, sin interés público evidente; este consentimiento es el que se requiere para utilizar los datos de los usuarios en el desarrollo de las industrias sanitarias, farmacéuticas y de biotecnología, o la promoción y comercialización de sus productos. Consideración especial merecen los datos genéticos por la complejidad que supone su titularidad compartida por un núcleo familiar". Ibídem, p. 40.

[828] ARGIMON, J. M., op. cit.

[829] Ibídem.

4.3. Acceso al Big Data sanitario.

Finalmente, y tal como señalábamos *ut supra*, consideramos preocupante y primordial determinar quién y en qué circunstancias puede acceder a nuestra información de salud contenida y almacenada en el Big Data.

Teniendo en cuenta que todos los datos de carácter personal se concentrarán en un único lugar, el Big Data, y siendo que nuestros datos sensibles y más íntimos estarán en este nuevo entorno tecnológico, debemos conocer previamente cómo funciona el acceso y la posible modificación de éstos datos si hay imprecisiones, o incluso su cancelación. Los conocidos como derechos ARCO en la LOPD, a los que hemos hecho referencia en la Primera parte de ésta Tesis.

Se deberá determinar si es el paciente el que tiene la clave de acceso para que sus datos puedan ser accedidos, o, por el contrario, si es el entorno médico-sanitario el que tenga tal acceso, pero en dichas circunstancias cabrá matizar dese el punto de vista legal, cuáles son esas limitaciones de acceso y uso, y quiénes son las personas facultadas o "habilitadas" para acceder al Big Data sanitario del paciente y modificar dicha información.

Probablemente, y dado el imperante avance tecnológico, lo más útil resulte que nosotros mismos podamos hacer uso de nuestra huella digital o tarjeta sanitaria con chip inteligente, para acceder a la información médica que nos vincula, cuando nos encontremos en un hospital, en una clínica o en una consulta privada.

Conclusión.

Consideramos ciertamente que el Big Data contribuirá en el futuro a mejorar la prevención de las enfermedades, su diagnóstico, también el tratamiento del paciente, a la vez que se reducen costes sanitarios y se agiliza la gestión.

La sanidad es uno de los sectores que mayor cantidad de datos genera. En el futuro sin duda los datos seguirán acumulándose e incrementado de forma progresiva y su recopilación en las herramientas que actualmente se disponen (papel, registros, radiografías, escaners, etc.), devendrá obsoleta y también difícil de almacenar y gestionar.

Por ello, será necesario contar con herramientas tecnológicas que hagan posible la recopilación, almacenamiento y tratamiento de todos los datos y a la vez que la seguridad de los datos personales de los pacientes quede garantizada, tanto desde el punto de vista tecnológico impidiendo la re-identificación de la persona, como desde el punto de vista legal, dotando de mayores garantías jurídicas a los datos de salud en este novedoso, incipiente pero inevitable entorno tecnológico.

Conclusiones

Tras centrar conceptualmente las nociones de datos de salud e historia clínica, fenómenos muy vinculados a la actual coyuntura social y en particular desde la perspectiva jurídica de su protección frente a los avances tecnológicos; ante la inminente implementación del Big Data en el sector sanitario y con la próxima entrada en vigencia en mayo del año 2018 del Reglamento General de Protección de Datos, hemos podido comprobar cómo los actuales modelos normativos existentes en materia de protección de datos tanto en la UE como en España, no siempre son compatibles con el respeto y las garantías de la privacidad e intimidad del individuo. El análisis jurídico ha sido realizado desde la perspectiva del derecho español, con los matices autonómicos y la clara influencia comunitaria. Después de analizar los conceptos en torno a los datos de carácter sensible y la incorporación de éstos datos en la historia clínica digital, hemos detallado la protección legal de la que gozan tales derechos en nuestro ordenamiento en la Primera Parte de éste estudio, para luego comparar con la legislación europea que deberá implementarse en los próximos años, en la Segunda Parte de este trabajo, haciendo especial referencia al Big Data en salud, y de todo ello, podemos extraer las siguientes conclusiones:

Primera. Los avances tecnológicos hacen que nos preguntemos cómo se han de actualizar las normas vigentes a fin de evitar intromisiones en nuestros datos más personales, y dentro de éstos datos, a los que deben recibir una especial protección por su carácter sensible, los datos de salud. La protección de los datos de carácter personal resulta una tarea ardua desde el punto de vista jurídico. Sostenemos esto, porque los datos y la información que ellos contienen sobre las personas, están en constante movimiento y evolución a la par de las nuevas tecnologías, por tanto, la normativa siempre va a ir por detrás de los avances tecnológicos que prosperan a un ritmo vertiginoso. Antes nos preocupábamos por la información sanitaria contenida en las historias clínicas, luego por la información de salud que contienen nuestros propios dispositivos móviles a través de las apps, el futuro se basa en los relojes que serán capaces de almacenar y gestionar información y lo preocupante de ello es el Big Data sanitario que recoge toda esta información y aún no está claro cómo se almacena, dónde, qué derecho le es aplicable y sobre todo qué uso se le dará a tan sensible información.

Segunda. La implementación de la historia clínica digital supondrá un avance significativo para la atención sanitaria, dotándola de mayor agilidad, eficacia y seguridad. También reviste singular importancia la receta electrónica, que facilitará a los ciudadanos la posibilidad de retirar los medicamentos con su simple presentación en una farmacia situada en una Comunidad Autónoma distinta a aquella en la que se haya prescrito el fármaco. Pero ante éste tráfico de datos, se hace necesario fijar medidas más rigurosas respecto a la seguridad de éstos datos, al acceso a los mismos y al uso que de los mismos se realice. La Ley de Autonomía del Paciente debe actualizarse y contemplar extremos que han sido denunciados por la doctrina, y que ésta autora comparte, entre ellos, determinar el plazo de conservación de las historias clínicas, que tiene su razón de ser en las finalidades judiciales de ésta documentación, ya que los plazos para según qué procesos son dispares. Otro inconveniente a resaltar es la falta de claridad respecto a la propiedad de la historia clínica, lo que condiciona el grado y la extensión de la protección de los datos de acceso del paciente. También deberá ampliarse la regulación sobre el consentimiento informado, en los términos que expusimos en éste trabajo. Asimismo, se deberá resolver si prevalece el derecho de cancelación de los datos contenidos en la historia clínica sobre posibles responsabilidades derivadas de la práctica médica y, por tanto, de la imposibilidad que conllevaría su destrucción. En el mismo sentido, cabe establecer mecanismos seguros para garantizar que los datos contenidos en la historia clínica digital no puedan ser alterados por medios tecnológicos, destruidos, robados o utilizados para fines diferentes para lo que fueren consentidos, entre otras observaciones que hemos realizado en los Capítulos III y IV. Las Comunidades Autónomas han dado respuestas a algunos de estos problemas, pero de manera dispar. Ante la falta de previsión de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, del Real Decreto de la Ley Orgánica de Protección de Datos 1720/2007, de 21 de diciembre, y de la Ley 41/2002, de 14 de noviembre, básica reguladora de la Autonomía del Paciente, ha sido la Agencia Española de Protección de Datos la que ha dado respuesta a través de sus informes y resoluciones a las múltiples consultas en torno a la protección de los datos sensibles y a las dudas que su tratamiento, acopio y transmisión suscitan.

Tercera. En base a todas estas consideraciones, en ésta Tesis se defiende la necesidad de la concepción de una nueva rama del derecho: el Derecho Sanitario. El derecho a la salud, donde éste quedaría incorporado, posee un espectro demasiado amplio que toca la rama del derecho civil, administrativo, laboral, penal y constitucional y eso conlleva a que su regulación sea muy dispersa e ineficiente. Por ello, sostenemos

que es cada vez más notorio el requerimiento de independizar al derecho sanitario y convertirlo en una nueva rama del derecho, aportando esta Tesis argumentos para alcanzar este objetivo.

Cuarta. Tratar grandes cantidades de datos con fines de investigación científica -biomédica-, asistencia sanitaria y tratamiento médico es una tarea compleja dada la dificultad de anonimizar toda la información. En este sentido, creemos conveniente que además de la protección que reciben los titulares de los datos, los profesionales e intervinientes en los mismos, deberían estar sujetos a una confidencialidad mucho más rigurosa y específica al igual que el secreto del médico hacia sus pacientes. También deberán regularse mecanismos que impidan la re-identificación de los datos anonimizados evitando obstáculos en la utilización de datos sensibles y facilitando la investigación médico-científica. La tendencia legislativa es elevar los estándares de protección, así, en la última reforma del Código Penal que data del año 2015 se ha podido vislumbrar este hecho a través del aumento de la penalidad en materia de vulneración y revelación de secretos de datos sensibles y por tanto altamente protegidos por el derecho, como hemos tenido ocasión de exponer en la Primera Parte de ésta Tesis. En este sentido el TS ha cambiado radicalmente la tendencia jurisprudencial, llegando hasta el punto de manifestar que hoy en día cualquier persona sabe cuáles son sus límites en el entorno de una cultura digital. Por ello la justicia aplica en el caso de vulneración de datos sensibles el dolo de consecuencias necesarias y no un dolo específico. También los Códigos Éticos y Deontológicos de las profesiones sanitarias son cada vez más rigurosos en éste aspecto.

Quinta. La labor normativa llevada a cabo por el legislador europeo en materia de protección de datos a través del Reglamento General de Protección de Datos, ha tenido por objetivo adoptar un marco coherente y homogéneo en la materia, para los Estados miembros. Dicha armonización legislativa ha resultado insuficiente para solucionar los problemas jurídicos inherentes a la protección de datos y aún más, respecto a los datos de salud. Tras el análisis de la legislación existente en materia de protección de datos de carácter sensible, se sigue echando en falta una norma específica que regule la singularidad y especificidad del dato sanitario de carácter personal a fin de que puedan evitarse las lagunas que actualmente presenta la normativa vigente. Asimismo, por el carácter tan especial de este tipo de datos, referidos a la salud y a la genética de los individuos, su regulación normativa ha de ajustarse estrictamente a las exigencias del especial nivel de seguridad que su protección merece, y para ello, se hace necesaria la modificación de la LOPD para adaptarla al Reglamento, teniendo en cuenta

mecanismos estrictos y eficaces que doten de seguridad jurídica la recopilación, el tratamiento, y el intercambio de datos sensibles. Además, se deberá abogar por una conceptualización más concreta de lo que engloba o no un dato de salud, para dotarle de mayores garantías.

Y en éste sentido, como hemos puesto de manifiesto en la Segunda Parte de éste trabajo, consideramos que el legislador europeo ha desperdiciado una buena oportunidad normativa que será el Reglamento General para legislar sobre el Big Data, el *Cloud Computing*, el Internet de las cosas o *BioTech,* todo ellos con aplicación en el ámbito de los datos sanitarios. También hemos de reconocer el peligro que puede entrañar que se deposite mayor responsabilidad en los responsables y en el encargado del tratamiento de los datos, a quienes se les encarga la valoración y la apreciación en relación con los riesgos que puede conllevar los datos que deben tratar. Por lo tanto, el margen de decisión que recae en estas personas es altamente destacable, lo que en muchos casos se escapará a una actividad controladora que se pueda ejercitar sobre éstos responsables.

Sexta. Consideramos que puede ser muy conveniente la creación de un Tribunal especializado en juzgar todos los asuntos que se susciten a nivel internacional con respecto a la protección de datos. De ésta manera tendría los conocimientos específicos, sería de aplicación directa y se evitarían muchos cauces largos y costosos para dirimir cualquier controversia en la materia.

En conclusión, destacar que en los últimos años la protección de datos ha revolucionado distintas áreas jurídicas, y diversos sectores, no sólo el legal y el sanitario, sino el empresarial en sus diferentes vertientes. Éste fenómeno preocupa a la población que cada vez toma más conciencia de los datos personales que proporciona cotidianamente, pero también al sector público y privado en relación con la aplicación de las técnicas de privacidad, con el cumplimiento de la normativa, con la debida custodia de los datos y el incipiente Big Data con los riesgos que entraña, requiriéndose una normativa específica y adecuada en un futuro próximo.

Bibliografía

a) Manuales generales y monografías de referencia.

AA.VV. *Calidad en la asistencia sanitaria*. Instituto Europeo de Salud y Bienestar Social, Madrid, 1999.

- *La gestión del proceso asistencial: impacto de los sistemas de información médica.* MSC, Madrid, 2000.
- *Libro blanco para la mejora de los servicios públicos. Una nueva Administración al servicio de los ciudadanos.* MAP, Madrid, 2000.
- *La salud y los derechos humanos. Aspectos éticos y morales.* Consejo de Europa, Washington, 1996.
- *Derecho médico. Tratado de Derecho sanitario.* Colex, Madrid, 2001.
- *La reforma del Sistema Nacional de Salud.* Marcial Pons, Madrid, 2004.

ABELLÁN-GARCÍA SÁNCHEZ, F. "Perspectiva del derecho a la información, a la intimidad y a la protección de datos en un sistema de notificación y registro de sucesos adversos", en LARIOS RISCO, D. (Coordinador). *Error sanitario y seguridad de pacientes. Bases jurídicas para un registro de sucesos adversos en el Sistema Nacional de Salud.* Comares, Granada, 2009.

ABELLÁN, F; GARCÍA DÍAZ, A. *Acceso a la historia clínica con fines de investigación. Estado de la cuestión y Controversias.* Informe del Experto Nº 12, Fundación Salud 2000, 2015.

ABELLÁN-GARCÍA SÁNCHEZ, F., et. al. *Libertad de conciencia y salud. Guía de casos prácticos.* Comares, Granada, 2008.

ABERASTURI GORRIÑO, U. *La Protección de Datos en la Sanidad.* Thomson Reuters Aranzadi, Navarra, 2013.

ADSUARA VARELA, B. "El consentimiento"*,* en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016.

Agencia de Protección de Datos de la Comunidad de Madrid (APDCM). *Guía de protección de datos personales para Servicios Sanitarios Públicos.* Thomson-Civitas, Madrid, 2004.

- *Protección de datos personales para Servicios Sanitarios Públicos.* Thomson-Civitas, Madrid, 2008.
- *Repertorio de Legislación y Jurisprudencia sobre Protección de Datos.* Thomson-Civitas, Madrid, 2004.
- *Memoria del III Premio a las Mejores Prácticas Europeas en materia de Protección de Datos.* Thomson-Civitas, Madrid, 2007.

Agencia Española de Protección de Datos (AEPD). *Procedings of the first European Congress on Data Protection. Madrid, 29-31 March 2006.* Fundación BBVA, Bilbao, 2008.

AGÚNDEZ LERÍA, I. *Artículo 8. Principios relativos a la calidad de los datos. Protección de datos. Comentarios al Reglamento.* Lex Nova, Valladolid, 2008.

ALMUZARA ALAMAIDA, C. (Coordinadora). *Estudio práctico sobre la protección de datos de carácter persona.* Lex Nova, 2ª Edición, Valladolid, 2007.

ALONSO OLEA, M.; FANEGO CASTILLO, F. *Comentario a la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.* Thomson Civitas, Madrid, 2003.

ÁLVAREZ CARO, M. *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital,* Reus, Madrid, 2015.

ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M. *La defensa de la intimidad de los ciudadanos y la tecnología informática*. Aranzadi, Pamplona, 1999.

- *La historia clínica: custodia y propiedad.* I Jornadas de Protección de Datos Sanitarios en la Comunidad de Madrid, Fundación Mapfre Medicina y APDCM, Madrid, 2000.

ÁLVAREZ CIVANTOS, O. *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades.* 3ª edición, Auren, Granada, 2008.

ÁLVAREZ GUISASOLA, F. J. "Visión desde Castilla y León. Jornadas del I y II Encuentro Interautonómico sobre protección jurídica del paciente como consumidor", en TOMILLO URBINA, J.; CAYÓN DE LAS CUEVAS, J. (directores). *La Protección Jurídica del Paciente como Consumidor.* Aranzadi, Navarra, 2010.

ÁLVAREZ HERNANDO, J. *Guía Práctica sobre Protección de Datos. Cuestiones y Formularios.* Lex Nova, Valladolid, 2011.

ÁLVAREZ-RIGAUDIAS, C. "Tratamiento de Datos de Salud", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016.

APARICIO SALOM, J. *Estudio sobre la Ley Orgánica de Protección de Datos de carácter personal.* 3ª Edición, Aranzadi-Thomson Reuters, Navarra, 2009.

- *Estudio sobre la Protección de Datos.* 4ª Edición, Thomson Reuters Aranzadi, Pamplona, 2013.
- "Título II. Principios de la Protección de Datos. Artículo 4", en Troncoso Reigada, A. *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Civitas, Madrid, 2010.

ARCOS VIEIRA, Mª L. *Responsabilidad sanitaria por incumplimiento del deber de información del paciente.* Thomson-Aranzadi, Navarra, 2007.

ARENAS RAMIRO, M. *El derecho fundamental a la protección de datos personales en Europa.* Tirant lo Blanch, Valencia, 2006.

ARIAS POU, M. "Definiciones a efectos del Reglamento General de Protección de Datos", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016.

ATELA BILBAO, A.; GARAY IASI, J. "Ley 41/2002 de derechos del paciente, avances, deficiencias y problemática", en GONZÁLEZ SALINAS, P.; LIZARRAGA BONELLI, E. (coordinadores). *Autonomía del paciente, información e historia clínica (estudios sobre la Ley 41/2002, de 14 de noviembre).* Thomson Civitas, Madrid, 2004.

BAYO DELGADO, J. "Derecho comunitario sobre protección de datos"*,* en GÓMEZ MARTÍNEZ, C. (Director). *Derecho a la intimidad y nuevas tecnologías.* Consejo General del Poder Judicial, Madrid, 2004.

BERROCAL LANZAOT, A. I. "El valor de la autonomía del paciente en la Ley 41/2002, de 14 de noviembre, reguladora de los derechos y deberes de los pacientes", en CIENFUEGOS SALGADO, D. (Coord.). *Estudios en homenaje a Marcia Muñoz de Alba Medrano.* Bioderecho, tecnología, salud y derecho genómico. Universidad Nacional Autónoma de México, 2006.

BLAS ORBÁN, C. *El equilibrio en la relación médico – paciente.* Bosch, Barcelona, 2006.

CÁLIZ CÁLIZ, R., et. al. *El derecho a la protección de datos en la historia clínica y en la receta electrónica.* Aranzadi-AEPD-Thomson Reuters, Navarra, 2009.

CANTERO RIVAS, R. "La historia clínica: naturaleza y régimen jurídico", en CÁLIZ CÁLIZ, R., et al. *El derecho a la protección de datos en la historia clínica y en la receta electrónica.* Aranzadi-AEPD-Thomson Reuters, Navarra, 2009.

- *El acceso de los pacientes y sus allegados a los datos personales contenidos en la historia clínica*, en *Historia clínica electrónica, confidencialidad y protección de la información*. *Experiencias en gestión sanitaria.* Escola Galega de Administración Sanitaria, FEGAS, 2008.

CARDONA RUBERT, Mª B. *Derechos de acceso, rectificación, cancelación y oposición en el nuevo reglamento de desarrollo de LOPD.* Tirant lo Blanch, Valencia, 2008.

CARNICERO GIMÉNEZ DE AZCÁRATE, J. "Protección de datos y receta electrónica", en PÉREZ GÓMEZ, J. M. *El Derecho a la Protección de Datos en la historia clínica y la receta electrónica.* Thomson Reuters, Madrid, 2009.

CODÓN HERRERA, A. "La historia clínica: concepto, normativa, titularidad y jurisprudencia", en GONZÁLEZ SALINAS, P.; LIZARRAGA BONELLI, E. (coordinadores). *Autonomía del paciente, información e historia clínica (estudios sobre la Ley 41/2002, de 14 de noviembre).* Thomson Civitas, Madrid, 2004.

CORBELLA DUCH, J. *Manual de Derecho Sanitario.* Atelier, Barcelona, 2006.

COUDERT, F. "Tratamiento de datos especialmente protegidos", en ALMUZARA ALAMAIDA, C. (Coordinadora). *Estudio práctico sobre la protección de datos de carácter personal.* Lex Nova, 2ª Edición, Valladolid, 2007.

CRIADO DEL RIO, T.; SEOANE PRADO, J. *Aspectos Médico-legales de la Historia Clínica*. Colex, Madrid,1999.

DAVARA RODRÍGUEZ, M. A. *La Protección de datos en Europa: principios, derechos y procedimiento*. Grupo Asnef Equifax, Madrid, 1998.

DEL CASTILLO VÁZQUEZ, I. C. *Protección de datos: cuestiones constitucionales y administrativas: (el derecho a saber y la obligación de callar).* Thomson-Civitas, Navarra, 2007.

DEL PESO NAVARRO, E., et al. *Nuevo Reglamento de Protección de Datos de carácter personal. Medidas de Seguridad.* Díaz de Santos, Madrid, 2008.

DEL PESO NAVARRO, E.; RAMOS GONZÁLEZ, M. A.; DEL PESO RUIZ, M. *Documento de seguridad.* Díaz de Santos, Madrid, 2004.

DÍAZ MÉNDEZ, N. "Historia clínica. Titularidad, acceso, uso y conservación", en ABEL LLUCH, X. (Director). *El juez Civil ante la investigación biomédica.* Cuadernos de Derecho Judicial. Año 2004-X, Consejo General del Poder Judicial, Madrid, 2005.

DIETRICH PLAZA, C. "Datos genéticos y protección de datos personales", en BUISÁN, L.; SÁNCHEZ URRUTIA, A. (coordinadoras). *Intimidad, confidencialidad y protección de datos de salud.* Thomson Reuters, Navarra, 2011.

DOMÍNGUEZ LUELMO, A. *Derecho sanitario y responsabilidad médica. Comentarios a la Ley 41/2002 de 14 de noviembre, sobre derechos del paciente, información y documentación clínica.* 2ª Edición, Lex Nova, Valladolid, 2007.

EGUSQUIZA BALMASEDA, Mª Á. *Protección de datos: Intimidad y salud.* Aranzadi, Navarra, 2009.

ETREROS HUERTA, J. J. "Historia clínica electrónica", en AA.VV. *El derecho a la protección de datos en la historia clínica y la receta electrónica.* Aranzadi-AEPD, Pamplona, 2009.

FERNÁNDEZ CONTE, J.; LEÓN BRUGOS, D. "Antecedentes y proceso de reforma sobre protección de Datos en la Unión Europea", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016.

FERNÁNDEZ HIERRO, J. M. (Coordinador). *La historia clínica.* Comares, Granada, 2002.

FERNÁNDEZ-SAMANIEGO, J.; FERNÁNDEZ-LONGORIA, P. "El Derecho a la Portabilidad de los Datos", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016.

GALÁN CORTÉS, J. C. *El Consentimiento informado del usuario de los servicios sanitarios.* Colex. Madrid, 1997.

- *Aspectos legales de la relación clínica.* Jarpyo Editores, Madrid, 2000.

GARCÍA MEXÍA, P. "La singular naturaleza jurídica del Reglamento General de Protección de Datos de la UE. Sus efectos en el acervo nacional sobre protección de datos", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016.

GARRIDO CORDOBERA, L. M.; BUSTO LAGO, J. M. *Los riesgos del desarrollo en una visión comparada. Derecho argentino y Derecho español.* Reus, Madrid, 2010.

GARRIGA DOMÍNGUEZ, A. *Tratamiento de datos personales y derechos fundamentales.* 2ª Edición, Dykinson, Madrid, 2009.

GIL GONZÁLEZ, E. *Big data, privacidad y protección de datos.* Agencia Española de Protección de Datos, Madrid 2016.

GÓMEZ JARA, M.; GÓMEZ MARICHALAR, N. *Consultas en Psiquiatría Legal*. Atelier. Barcelona, 2009.

GÓMEZ NAVAJAS, J. *La protección de datos personales.* Thomson-Civitas, Navarra, 2005.

GÓMEZ PAVÓN, P. *Tratamientos médicos: su responsabilidad penal y civil.* 2da. Edición, Bosch, Barcelona, 2004.

GÓMEZ PIQUERAS, C. "La historia clínica. Aspectos conflictivos resueltos por la Agencia Española de Protección de Datos", en LESMES SERRANO, C., et al. *El derecho a la protección de datos en la historia clínica y en la receta electrónica.* Aranzadi-AEPD-Thomson Reuters, Navarra, 2009.

GÓMEZ RIVERO, Mª C. *La protección penal de los datos sanitarios. Especial referencia al secreto profesional médico.* Comares, Granada, 2007.

GÓMEZ SÁNCHEZ, Y. *Derecho Constitucional Europeo: Derechos y Libertades.* Sanz y Torres, Madrid, 2008.

GONZÁLEZ SALINAS, P.; LIZARRAGA BONELLI, E. (coordinadores) *Autonomía del paciente, información e historia clínica (estudios sobre la Ley 41/2002, de 14 de noviembre).* Thomson Civitas, Madrid, 2004.

GONZÁLEZ SALINAS, P. “El alcance del carácter básico de la ley reguladora de la autonomía del paciente y su influencia en las leyes autonómicas sobre la misma materia”, en GONZÁLEZ SALINAS, P.; LIZARRAGA BONELLI, E. (coordinadores). *Autonomía del paciente, información e historia clínica (estudios sobre la Ley 41/2002, de 14 de noviembre).* Thomson Civitas, Madrid, 2004.

GONZÁLEZ-VARAS IBÁÑEZ, A. *Derecho y conciencia en las profesiones sanitarias.* Dykinson, Madrid, 2009.

GRIMALT SERVERA, P. “Deberes y responsabilidad en materia de protección de datos”, en CAVANILLAS MÚGICA, S. (Coordinador). *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar.* Editorial Comares, Granada, 2005.

HERRÁN ORTIZ, A. I. *El derecho a la protección de datos personales en la sociedad de información.* Universidad de Deusto, Instituto de Derechos Humanos, Bilbao, 2003.

JIMENA QUESADA, L. “La tutela constitucional de la salud: Entre el consentimiento informado y la información consentida”, en GARCÍA RUIZ, Y., et al. *La salud: intimidad y libertades informadas.* Tirant lo Blanch, Valencia, 2006.

LAÍN ENTRALGO, P. *La historia clínica.* 3ª Edición, Triacasela, Madrid, 1998.

LEÓN ALONSO, M. *La Protección constitucional de la salud.* La Ley, Madrid, 2010.

LESMES SERRANO, C. (Coordinador). *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia.* Lex Nova, Valladolid, 2008.

LESMES SERRANO, C. “Prologo”, en CÁLIZ CÁLIZ, R., et al., *El derecho a la protección de datos en la historia clínica y en la receta electrónica*. Aranzadi-AEPD-Thomson Reuters, Navarra, 2009.

LOMAS HERNÁNDEZ, V. “La protección del paciente en la reciente legislación sanitaria”, en TOMILLO URBINA, J.; CAYÓN DE LAS CUEVAS, J. (directores). *La Protección Jurídica del Paciente como Consumidor.* Aranzadi, Navarra, 2010.

LÓPEZ CALVO, J. *Comentarios al Reglamento Europeo de Protección de Datos.* Sepin, Madrid, 2017.

LLÀCER MATACÁS, Mª R.; CASADO, M.; BUISAN ESPELETA, L. (coord.). *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública.* Observatori de Bioètica i Dret, Universidad de Barcelona Publicacions i Edicion. Barcelona, 2015.

MARTÍ MERCADAL, J. A.; BUISÁN ESPELETA, L. *El secreto profesional en la medicina.* Espasa Calpe, Madrid, 1988.

MARTÍN MATEO, R. *Bioética y derecho.* Ariel, Barcelona, 1987.

MARTÍNEZ AGUADO, L. "Aspectos éticos de la historia clínica", en FERNÁNDEZ HIERRO, J. M. (Coordinador). *La historia clínica.* Comares, Granada, 2002.

MARTÍNEZ-CALCERRADA, L. *Derecho Médico. Volumen I. Derecho Médico General y Especial.* Tecnos, Madrid, 1986.

MARTÍNEZ MARTÍNEZ, R. (coordinador). *Protección de Datos. Comentarios al Reglamento de desarrollo de la LOPD.* Tirant lo Blanch, Valencia, 2009.

- *Una aproximación crítica a la autodeterminación informativa.* Civitas, Madrid, 2004.

MÉJICA GARCÍA, J. M. *La historia Clínica: estatuto básico y propuesta de regulación.* Edisofer S.L, Madrid, 2002.

MÉJICA, J.; DÍEZ, J. R. *El Estatuto del Paciente. A través de la nueva legislación sanitaria estatal.* Thomson-Civitas, Navarra, 2006.

MÉNDEZ BAIGES, V.; SILVEIRA GORSKI, H. C. *Bioética y derecho.* Editorial UOC, Barcelona, 2007.

MESSÍA DE LA CERDA BALLESTEROS, J. A. *La cesión o comunicación de datos de carácter personal.* Thomson Civitas, Madrid, 2003.

MORALES PRATS, F. "El Código Penal y la protección de datos personales". *Jornadas sobre el Derecho Español de la protección de datos personales.* Agencia de Protección de Datos, Madrid, 1996.

MORENO VERNIS, M. "Documentación clínica: organización, custodia y acceso", en FERNÁNDEZ HIERRO, J. M. (Coordinador). *La historia clínica.* Comares, Granada, 2002.

MURILLO DE LA CUEVA, P. L. *La construcción del derecho a la autodeterminación informática y las garantías para su efectividad.* Fundación Coloquio Jurídico Europeo, Madrid, 2009.

- *La publicidad de los archivos judiciales y la confidencialidad de los datos sanitarios. VII Congreso Nacional de Derecho Sanitario, octubre, 2000.* Editorial Fundación Mapfre Maedicina, Madrid, 2001.

NAVALPOTRO NAVALPOTRO, Y. "Antecedentes de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)", en ALMUZARA ALAMAIDA, C. (Coordinadora) *Estudio práctico sobre la protección de datos de carácter personal.* Lex Nova, 2ª Edición, Valladolid, 2007.

PALOMAR OLMEDA, A.; GONZÁLEZ ESPEJO, P. (Directores). *Comentario al Reglamento de desarrollo de la Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal (aprobado por RD 1720/2007, de 21 de diciembre).* Thomson-Civitas, Navarra, 2008.

PENDÁS, B.; BASELGA, P. *Derecho a la intimidad / SAMUEL WARREN, LOUIS BRANDEIS*. (Traducción). Civitas, Madrid, 1995.

PÉREZ GÓMEZ, J. Mª. "Protección de datos personales en salud en materia de información sanitaria", en GÓMEZ PIQUERAS, C., et al. *Protección de datos e investigación médica.* Aranzadi-AEPD-Thomson Reuters, Navarra, 2009.

PÉREZ GÓMEZ, J. M. "La protección de los datos de salud", en RALLO LOMBARTE, A.; GARCÍA MAHAMUT, R. *Hacia un Nuevo Derecho Europeo de Protección de Datos*. Tirant lo Blanch, Valencia, 2015.

PIÑAR MAÑAS, J. L. *Legislación de Protección de Datos*. Iustel, Madrid 2011.

- "El derecho fundamental a la protección de datos personales", en *Protección de datos de carácter personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos celebrado del 2 al 6 de junio de 2003.* La Antigua, Guatemala, Tirant lo Blanch, Valencia, 2006.
- *Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio.* Fundación Alternativas, Madrid, 2009.
- *Transparencia, acceso a la información y protección de datos.* Reus, Madrid, 2014.
- "Introducción. Hacia un nuevo modelo europeo de Protección de Datos", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016.
- "Objeto del Reglamento", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016.
- "Concepto de datos de carácter personal", en TRONCOSO REIGADA, A. *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Thomson-Civitas, Pamplona, 2010.
- *¿Existe la privacidad? Inauguración Curso Académico 2008-2009.* CEU Ediciones, Universidad CEU San Pablo, Madrid, 2008.

PUENTE ESCOBAR, A. "Legitimación para el tratamiento", en MARTÍNEZ MARTÍNEZ, R. (coordinador). *Protección de Datos. Comentarios al Reglamento de desarrollo de la LOPD.* Tirant lo Blanch, Valencia, 2009.

- *Consentimiento del afectado y deber de información.* Tirant lo Blanch, Valencia, 2009.

PUYOL MONTERO, J. "Los principios del Derecho a la Protección de Datos", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016.

RALLO LOMBARTE, A. *El derecho al olvido en internet: Google versus España*. Centro de Estudios Políticos y Constitucionales, 2014.

RALLO LOMBARTE, A.; GARCÍA MAHAMUT, R. *Hacia un Nuevo Derecho Europeo de Protección de Datos*. Tirant lo Blanch, Valencia, 2015.

REMOLINA, N. *Recolección internacional de datos: un reto del mundo post-internet.* AEPD, Madrid, 2015.

RIPOL CARULLA, S. "Aplicación territorial del Reglamento", en PIÑAR MAÑAS, J. L. (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad.* Reus, Madrid, 2016.

RIPOL CARULLA, S.(ed.); BACARIA MARTRUS, J.(coord.). *Estudios de protección de datos de carácter personal en el ámbito de la salud.* APDCAT Agencia Catalana de Protección de Datos. Marcial Pons, 2006.

RIVAS VALLEJO, P.; GARCÍA VALVERDE, M. (Directoras). *Derecho y Medicina. Cuestiones jurídicas para profesionales de la salud.* Aranzadi, Navarra, 2009.

RODRÍGUEZ IZQUIERDO, R. "Los derechos y obligaciones de los pacientes", en RIVAS VALLEJO, P.; GARCÍA VALVERDE, M. (Directoras). *Derecho y Medicina. Cuestiones jurídicas para profesionales de la salud.* Aranzadi, Navarra, 2009.

RODRÍGUEZ IZQUIERDO, R. "La información sanitaria y la historia clínica", en RIVAS VALLEJO, P.; GARCÍA VALVERDE, M. (Directoras). *Derecho y Medicina. Cuestiones jurídicas para profesionales de la salud.* Aranzadi, Navarra, 2009.

ROMEO CASABONA, C. M. "Persona identificada o identificable, el afectado o interesado y el procedimiento de disociación en la protección de datos de carácter personal", en TRONCOSO REIGADA, A. *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Thomson-Civitas, Pamplona, 2010.

SÁIZ PEÑA, C. A. "La notificación de brechas de seguridad", en RALLO LOMBARTE, A.; GARCÍA MAHAMUT, R. *Hacia un Nuevo Derecho Europeo de Protección de Datos*. Tirant lo Blanch, Valencia, 2015.

SAMPRÓN LÓPEZ, D. *Los derechos del paciente a través de la información y la historia clínica.* Edisofer, Madrid, 2002.

SÁNCHEZ CARAZO, C. *La intimidad y el secreto médico.* Díaz de Santos, Madrid 2000.

SÁNCHEZ-CARO, J.; ABELLÁN, F. *Derechos y deberes de los pacientes. Ley 41/2002 de 14 de noviembre: consentimiento informado, historia clínica, intimidad e instrucciones previas.* Comares, Granada, 2003.

- *La Historia Clínica.* Fundación salud 2000. Granada, 2000.
- *Telemedicina y protección de datos sanitarios. Aspectos legales y éticos.* Comares, Granada 2002.
- *Datos de salud y datos genéticos. Su protección en la Unión Europea y en España.* Comares, Granda, 2004.
- *Derechos del médico en la relación clínica.* Comares, Granada, 2006.

- *Enfermería y Paciente. Cuestiones prácticas de Bioética y Derecho Sanitario.* Comares, Granada, 2007.

SANCHEZ-CARO, J. "El consentimiento previo a la intervención y la protección de los incapaces", en ROMEO CASABONA, C. M. *El Convenio de derechos Humanos y Biomedicina. Su entrada en vigor en el ordenamiento jurídico español.* Comares, Granada, 2002.

SÁNCHEZ GONZÁLEZ, M. A. *Intimidad y confidencialidad: su concepto e importancia.* I Jornadas de Protección de Datos sanitarios en la Comunidad de Madrid, Mapfre, Madrid, 2000.

SÁNCHEZ PATRÓN, J. M. "El régimen jurídico europeo aplicable a la confidencialidad de los datos relativos a la salud de las personas", en GARCÍA RUIZ, Y., et al. *La salud: intimidad y libertades informadas.* Tirant lo Blanch, Valencia, 2006.

SANTAMARÍA RAMOS, F. J. *El encargado independiente. Figura clave para un nuevo Derecho de protección de datos.* La Ley grupo Wolters Kluwer, Madrid, 2011.

SANTOS GARCÍA, D. *Nociones generales de La Ley Orgánica de Protección de Datos.* Tecnos, Madrid, 2005.

SANZ CALVO, L. *Artículo 4. Calidad de los datos. La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia.* Lex Nova, Valladolid, 2007.

SIMÓN CASTELLANO, P. *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*. Bosch, Barcelona, 2015.

- *El régimen constitucional del derecho al olvido digital.* Tirant lo Blanch, Valencia 2012.

SUÁREZ RUBIO, S. Mª. *Constitución y privacidad sanitaria.* Tirant lo Blanch, Valencia, 2015.

TAJADURA TEJADA, J.: "La protección de la salud (art. 43 CE)", en TAJADURA TEJADA, J. (COORDINADOR). *Los principios rectores de la política social y económica.* Editorial Biblioteca Nueva, Madrid, 2004.

TÉLLEZ AGUILERA, A. *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores.* Edisofer, Madrid, 2002.

TOMÁS MALLÉN, B. "Transparencia y protección de datos", en RALLO LOMBARTE, A.; GARCÍA MAHAMUT, R. *Hacia un Nuevo Derecho Europeo de Protección de Datos.* Tirant lo Blanch, Valencia, 2015.

TOMILLO URBINA, J.; CAYÓN DE LAS CUEVAS, J. (directores). *La Protección Jurídica del Paciente como Consumido.* Aranzadi, Navarra, 2010.

TRONCOSO REIGADA, A. *Regulatory Development of the LOPD, en Agencia Española de Protección de Datos (AEPD): Procedings of the first European Congress on Data Protection. Madrid, 29-31 March*

2006 (Desarrollo Regulatorio de la LOPD en la Agencia Española de Protección de Datos (AEPD): Procedimientos del Primer Congreso Europeo sobre Protección de Datos). Fundación BBVA, Bilbao, 2008.

- (Director) *Transparencia Administrativa y Protección de Datos Personales. V Encuentro entre Agencias Autonómicas de Protección de Datos.* Thomson Civitas, Madrid, 2008.
- *La protección de los datos personales. En busca del equilibrio.* Tirant lo Blanch, Vol. 1, Valencia, 2010.
- "Título II. Principios de la Protección de Datos. Artículo 4", en TRONCOSO REIGADA, A. *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Civitas, Madrid, 2010.

VÁZQUEZ BARROS, S. *Responsabilidad Civil de los Médicos. Doctrina, Legislación básica, Jurisprudencia, Formularios y Bibliografía.* Tirant lo Blanch, Valencia, 2009.

WESTIN, A. *Privacy and Freedom.* Editorial Atheneum, New York, 1967.

YUGUERO DEL MORAL, L. *La implantación de los derechos del paciente.* Eunsa, Navarra, 2004.

b) Artículos doctrinales en revistas.

ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M. "La aplicación de la firma electrónica y la protección de datos relativos a la salud". *Revista Actualidad Informática Aranzadi*. Núm. 39, abril, 2001, pp. 4-5.

AMAYA RICO, V. "El deber médico de información: un derecho humano fundamental". *Revista La Ley*. Tomo I, Año 2002, pp. 1831-1832.

ARIAS POU, M. "Cumplir la normativa sobre protección de datos en el entorno laboral". *Revista de Estudios Locales.* Núm. 113, septiembre, 2008, pp. 1-19. Disponible en internet: http://www.navarra.es/NR/rdonlyres/DCF7A5483551481C8CE46CBD251352BC/162689/3CumplimientoNormativaEntornoLaboral.pdf [Consulta: 10 julio 2016].

AULLÓ CHAVES, M.; PELAYO PARDOS, S. "La historia clínica", en DE LORENZO Y MONTERO, R. (Coordinador General) "Plan de formación en responsabilidad legal profesional". *Unidad didáctica núm. 1*. Madrid. Edicomplet. Asociación Española de Derecho Sanitario. 1997, p. 10.

BAZÁN, V. "El Hábeas Data y el Derecho de Autodeterminación Informativa en Perspectiva de Derecho Comparado". *Estudios Constitucionales*. Año 3, núm. 2, Chile, 2005, pp. 85-139. Disponible en Internet: <http://studylib.es/doc/7019100/el-h%C3%A1beas-data-yelderechodeautodeterminaci%C3%B3ninformat> [Consulta: 10 de septiembre de 2016].

BROGGI TRÍAS, M. A.; MEJÓN BERGÉS, R. "Las «anotaciones subjetivas» en la historia clínica". *Revista de Medicina Clínica*. Vol. 122, núm. 7, febrero 2004, p. 279. Disponible en Internet: <http://www.elsevier.es/es-revista-medicina-clinica-2-articulo-las-anotaciones-subjetivas-historia-clinica-13058386> [Consulta: 22 octubre 2016].

CANTERO RIVAS, R. "Cuestiones relativas a la historia clínica". *La Ley: revista jurídica española de doctrina, jurisprudencia y bibliografía*. Núm. 5, 1996, pp. 1421-1428.

CASADO, M. "Ética, Derecho y deontología profesional*". Derecho y Salud*. Vol. 6, núm. 1, 1998, p. 34.

CASTELLANO ARROYO, M. "Problemática de la historia clínica*". Actas del seminario Conjunto sobre Información y Documentación clínica*. Consejo General del Poder Judicial y Ministerio de Sanidad y Consumo, Madrid 22 y 23 de septiembre de 1997, vol. I, Madrid, 1998, pp. 45-90.

DAVARA RODRÍGUEZ, M. A. "Big Data". *El consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal.* Núm. 15-16, 2013, pp. 1552-1558.

DE ANGEL YAGÜEZ, R. "Problemas legales de la historia clínica en el marco hospitalario". *La Ley*. Vol. I, 1997, p. 1019.

- "Información y Documentación Clínica". *Actas del Seminario Conjunto sobre información y documentación clínica celebrado en Madrid los días 22 y 23 de septiembre de 1997*. Vol. I. Consejo General del Poder Judicial, Ministerio de Sanidad y Consumo, Madrid, 1997, pp. 111 a 121.

DE LORENZO SÁNCHEZ, A. "¿De quién son propiedad las historias clínicas?" *Deontología, Derecho y Medicina*. Colegio Oficial de Médicos, Madrid, 1977, pp. 497 y ss.

DE LORENZO Y MONTERO, R. "¿Qué se entiende por dato de salud?". *Revista Redacción Médica*. 21.06.2007, núm. 585, Año III.

- (Coordinador General) "Plan de formación en responsabilidad legal profesional". *Unidad didáctica núm. 1*. Madrid. Edicomplet. Asociación Española de Derecho Sanitario. 1997, p. 10.

DEL PESO NAVARRO, E. "La protección y la seguridad de los datos automatizados de carácter médico". *Informática y Derecho: Revista iberoamericana de derecho informático*. Núm. 12-15, 1996, pp. 903-914.

ESTEBAN GONZALO, S. "Sistema de información del Sistema Nacional de Salud". *Revista Índice*. Instituto de Información Sanitaria. Enero 2007, pp. 6-8. Disponible en internet: <http://www.revistaindice.com/numero20/p6.pdf> [Consulta: 10 julio 2016].

FRIED, C. "Privacy". *Yale Law Jurnal*, Estados Unidos, 1968, p. 483.

FOMBELLA POSADA, Mª. J.; CEREIJO QUINTEIRO, Mª. J. "Historia de la Historia Clínica". *Galicia Clínica, Sociedade Galega de Medicina Interna.* Núm. 73, 2012, pp. 21-26. Disponible en Internet: <https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=0ahUKEwiA04TkktvRAhVGPRQKHS5XBa0QFgg3MAQ&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F4056927.pdf&usg=AFQjCNHnSXyVWkqJ61TH75IJErfg63tcVQ&sig2=_fDnnOGKIMwGBxj2E8Ek3g> [Consulta: 29 octubre 2016].

GALLEGO RIESTRA, S. "Historia Clínica Electrónica y derecho a la autonomía del paciente: un conflicto de intereses". *Papeles Médicos*. Vol. 23, núm. 1, año 2014, pp. 7-19.

- "Derecho a la confidencialidad y acceso a la Historia Clínica". *Revista Clínica del Hospital Central de Asturias.* Núm. 2, julio-septiembre, 1996, pp. 4-7.

GALLEGO RIESTRA, S.; HINOJAL FONSECA, R.; RODRIGUEZ GETINO, J. A. "Los derechos de los pacientes: problemática práctica". *Medicina Clínica.* Núm. 100, 1993, pp. 538-541.

GARCÍA HERNÁNDEZ, T.; MARZO MARTÍNEZ, B. "La propiedad de la historia clínica". *La Ley: revista jurídica española de doctrina, jurisprudencia y bibliografía*. Núm. 5, 1996, pp. 1629-1631.

GINSBERG, J., et al. "*Detecting influenza epidemics using search engine query data*" (Detección de epidemias de influencia utilizando datos de consulta de los motores de búsqueda). *Revista Nature*. Vol. 457, 19.02.2009. Disponible en Internet: <http://www.nature.com/nature/journal/v457/n7232/full/nature07634.html> [Consulta: 9 enero 2017].

Grupo de Expertos en Información y Documentación Clínica. "Informe final". *Revista Calidad Asistencial 1999.* Núm. 14, Madrid, 1997, pp. 76-87.

GUTIÉRREZ CALVO, M., "Problemas jurídicos derivados de la aplicación del principio de calidad del dato por parte de las Administraciones Públicas". *REDUR.* Núm. II, diciembre 2013, pp. 169-198. Disponible en Internet: <http://www.unirioja.es/dptos/dd/redur/numero11/gutierrez.pdf> [Consulta: 10 julio 2016].

HEREDERO HIGUERAS, M. "La Protección de datos de salud informatizados en la Ley Orgánica 5/1992, de 29 de octubre". *Derecho y Salud*. Núm. 1, enero-junio 1994, pp. 17-28.

IRABURU ELIZONDO, M. "La Historia Clínica informatizada". *Derecho y Salud*. Vol. 17, Extraordinario XVII Congreso, Madrid, 2009, pp. 118-120.

LAFARGA I TAVER, J. L. "Problemas legales asociados al tratamiento informático de la historia clínica: la responsabilidad médica en el tratamiento de datos". *Derecho y Salud*. Vol. 7, núm. 2, julio-diciembre 1999, pp. 43-48.

LUNA, A.; OSUNA, E. "Problemas médico-legales en el almacenamiento y custodia de la historia clínica". *Medicina Clínica*. Vol. 88, núm. 2, 1987, pp. 631-632.

MARTÍN BERNAL, J. M. “Tratamiento jurídico de la historia clínica. Tema para un debate”. *Actualidad Administrativa*. Núm. 27, 6 al 12 de julio de 1998, pp. 581-599.

MORALES PRATS, F. “Derecho a la intimidad versus tratamiento de datos sanitarios”. *Derecho y Salud*. Vol. 9, núm. 2, julio-diciembre 2001, pp. 114-124.

MARTÍNEZ-PEREDA RODRÍGUEZ, J. M. “La Protección penal del secreto médico en el derecho español”. *Actualidad Laboral*. Núm. 20. Semana del 4 al 10 de marzo, 1996.

MURILLO DE LA CUEVA, P. L. “El derecho a la autodeterminación informativa y la protección de datos personales”. *Cuadernos de Derecho*. Núm. 20, 2008, pp. 43-58.

- “La protección de los datos de carácter personal en el horizonte de 2010”. *Anuario de la Facultad de Derecho*. Núm. 2, 2009, pp. 131-142.
- “Perspectivas del derecho a la autodeterminación informativa”. *Revista de Internet, Derecho y Política*. Núm. 5, 2007, pp. 18-32.

ORTIZ DE ELGUEA, P. “Historia Clínica: su regulación en la legislación sanitaria y en la protección de datos de carácter personal”. *Derecho y Salud*. Vol. 17, Extraordinario XVII Congreso sobre Derecho y Salud, Pamplona, noviembre 200, p. 124.

PARRA CALDERÓN, C. L. “Big data en sanidad en España: la oportunidad de una estrategia nacional”. *Gaceta Sanitaria*. Vol. 30, núm. 1, enero-febrero 2017, p. 5.

PIÑAR MAÑAS, J. L. “La Protección de Datos en el ámbito Sanitario”. *El Médico.* Anuario 2004, pp. 42-44.

PORTERO LAZCANO, G. “Historia clínica: problemática sobre la propiedad”. *Revista Latinoamericana de Derecho Médico y Medicina Lega*l. Núm. 6, junio 2002, pp. 81-88.

PRIETO ANDRÉS, A. “La nueva Directiva europea sobre el tratamiento de los datos personales y la protección de la intimidad en el sector de las telecomunicaciones”. *La Ley*. Año XXIII, núm. 5620, 26.09.2002, pp. 1-3.

PUYOL MONTERO, J. “UNA aproximación a Big Data”. *Revista de Derecho UNED*. Núm. 14, 2014, pp. 471-506.

RODA GARCÍA, L.; GALÁN CORTÉS, J. L. “Las historias clínicas y su incorporación a los expedientes judiciales”. *Actualidad del Derecho Sanitario*. Núm. 33, 1997.

RODRÍGUEZ MARTÍN, J., et al. “Consentimiento Informado. ¿Un dilema ético o legal?” *Revista Argentina de Cirugía*. Núm. 77, 1999, pp. 229-241.

ROMEO CASABONA, C. M.; CASTELLANO ARROYO, M. "La intimidad del paciente desde la perspectiva del secreto médico y del acceso a la historia clínica". *Derecho y Salud*. Vol. 1, núm. 1, julio-diciembre 1993, p. 5-17.

SÁIZ PEÑA, C. A. "Uno de los mayores retos en el entorno digital: el Big Data". *Actualidad jurídica Aranzadi.* Núm. 874, 2013, p. 14.

SAIZ RAMOS M.; LARIOS RISCO D. "El derecho de acceso a la historia clínica por el paciente: propuesta para la reserva de anotaciones subjetivas". *Derecho y Salud*. Vol. 18, núm. 1. Enero-junio 2009, pp. 21-41.

SÁNCHEZ BRAVO, A. "La regulación de los datos sensibles en la LORTAD". *ID*. Núm. 6-7, UNED, 1994, pp. 117-132.

SÁNCHEZ-CARO, J. "La Ley de Protección de Datos e innovaciones tecnológicas farmacéuticas". *Revista de Administración Sanitaria.* Vol. V, núm. 19, julio-septiembre 2001.

- "El consentimiento informado ante el derecho: una nueva cultura". *Revista calidad asistencial*. Vol. 14, núm. 2, 1999, pp. 128-144.

SÁNCHEZ JORDÁN, M. E. "Algunas cuestiones relativas al derecho de información y al deber de secreto profesional en un supuesto de responsabilidad médica". *Derecho y Salud*. Vol. 10, núm. 2, julio-diciembre 2002, pp. 162 y ss.

SOLOVE, D. J. "Understanding Privacy". *USA Hardvard University Press.* Estados Unidos, 2008, p. 2.

SUBIRÀ, C.; PRADELL DE MONTAGUT, A. "La receta electrónica en España". *Revista Garrigues Abogados y asesores Tributarios*. Barcelona, 2003, pp. 1-5.

TRONCOSO REIGADA, A. "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional". *Cuadernos de Derecho Público*. Núm. 19-20, mayo-diciembre, 2003, pp. 231-334.

- "La confidencialidad de la historia clínica". *Cuadernos de Derecho Público*. Núm. 27, enero-abril 2006, pp. 45-143. Disponible en Internet: <http://revistasonline.inap.es/index.php?journal=CDP&page=article&op=viewFile&path%5B%5D=775&path%5B%5D=830> [Consulta: 26 noviembre 2016].

WARREN, S. D.; BRANDEIS, L. D. "The right to privacy". *Harvard Law Review*. Vol. IV, núm. 5, 1890, pp. 193 y ss.

c) Legislación consultada.

1.Legislación española

Normativa estatal

- Constitución Española de 27 de diciembre de 1978, modificada por reforma de 27 de agosto de 1992 (BOE núm. 207, 28.08.1992).

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común (BOE núm. 236, 2.10.2015).

- Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN (BOE núm. 242, 9.10.2007).

- Ley 14/2007, de 3 de julio, de Investigación Biomédica (BOE núm. 159, 4.07.2007).

- Ley 29/2006, de 29 de julio, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios (BOE núm. 178, 27.07.2006).

- Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias (BOE núm. 280, 22.11.2003).

- Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud (BOE núm. 128, 29.05.2003).

- 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 (BOE núm. 274, 15.11.2002).

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE núm. 298, 14.12.1999).

- Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (BOE núm. 262, 31.10.1992, derogada).

- Ley 12/1989, de 9 de mayo de la Función Estadística Pública (BOE núm. 112, 11.05.1989).

- Ley 14/1986, de 25 de abril, General de Sanidad (BOE núm. 102, 29.04.1986).

- 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 (BOE núm. 98, 24.04.2012).

- Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud (BOE núm. 225, 16.11.2010).

- 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 (BOE núm. 17, 19.01.2008).

- Decreto 2296/2004, de 10 de diciembre, por el que se aprueba el Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración (BOE núm. 314, 30.12.2004).

- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (BOE núm. 151, 25.06.1999, derogado).

Normativa Autonómica

- Ley 21/2000, de Cataluña, sobre los derechos de información relativos a la salud, la autonomía del paciente y la documentación clínica (BOE núm. 29, 2.02.2001).

- Ley 12/1983, de 14 de julio, de administración institucional de la sanidad, y de la asistencia y los servicios sociales de Cataluña (DOGC núm. 345, 15.07.1983).

- Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos (BOE núm. 115, 14.05.2002).

- Ley 15/1990, de 9 de julio, de Ordenación Sanitaria de Cataluña (DOGC núm. 1324, 30.07.1990).

- Estatuto de Autonomía de Cataluña (BOE núm.172, 20.07.2006).

- Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos (DOGC núm. 3835, 4.03.2003).

- Decreto 159/2007, de 24 de julio, por el que se regula la receta electrónica y la tramitación telemática de la prestación farmacéutica a cargo del Servicio Catalán de Salud (DOGC núm. 4934, 26.07.2007).
- Ley 8/1997, de 26 de junio, de Ordenación sanitaria de Euskadi (BOE núm. 9, 11.01.2012).

- Decreto 45/1998, de 17 de marzo, por el que se establece el contenido y se regula la valoración, conservación y expurgo de los documentos del Registro de Actividades Clínicas de los Servicios de Urgencias de los Hospitales y de las Historias Clínicas Hospitalarias, de la Comunidad Autónoma del País Vasco (BOPV núm. 67, 8.04.1998).

- Decreto 272/1986 de 25 de noviembre por el que se regula el uso de la Historia Clínica de los Centros Hospitalarios de la Comunidad Autónoma del País Vasco (BOPV núm. 242, 6.12.1986).

- 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 (BOPV núm. 44, 4.03.2004).

- Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica (BOPV núm. 65, 29.03.2012).

- Ley 8/1997, de 26 de junio, de Ordenación sanitaria de Euskadi (BOE núm. 9, 11.01.2012).

- Decreto 45/1998, de 17 de marzo, por el que se establece el contenido y se regula la valoración, conservación y expurgo de los documentos del Registro de Actividades Clínicas de los Servicios de Urgencias de los Hospitales y de las Historias Clínicas Hospitalarias (BOPV núm. 67, 8.04.1998).

- Ley 3/2001, de 28 de mayo, reguladora del consentimiento informado y de la historia clínica de los pacientes, de Galicia (BOE núm. 158, 3.07.2001).

- Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid. (BOE núm. 245, 12.10. 2001).

- Ley 1/2003, de 28 de enero, de derechos e información al paciente de la Comunidad Valenciana (DOCV núm. 4430, 31.01.2003).

- Decreto 56/1988, de 25 de abril, del Consell de la Generalitat Valenciana (DOCV núm. 817, 4.05.1988).

- Ley 3/2003, de 6 de febrero, de Ordenación Sanitaria de la Comunidad Valenciana (BOE núm. 55, 5.03.2003).

- Orden de 17 de febrero de 1994, de la Conselleria de Sanitat i Consum, por la que se regula la confidencialidad y custodia de los datos médicos de los servicios médicos de empresa (DOCV núm. 2227, 13.03.1994).

- Orden de 14 de septiembre de 2001, de la Conselleria de Sanidad, por la que se normalizan los documentos básicos de la historia clínica hospitalaria de la Comunidad Valenciana y se regula su conservación (DOGV núm. 4111, 22.10.2001).

- Ley 6/2002, de 15 de abril, de Salud de Aragón (BOE núm. 121, 21.05.2002).

- Decreto 19/2015, de 24 de febrero, del Gobierno de Aragón, por el que se crea el Registro de solicitudes de acceso a la información pública y el fichero de datos de carácter personal "Solicitantes de acceso a la información pública" (BOA núm. 43, 4.03.2015)

- Ley 8/2003, de 8 de abril, sobre derechos y deberes de las personas en relación con la salud, Comunidad Autónoma de Castilla y León (BOE núm. 103, 30.04.2003).

- Decreto 101/2005 de 22 de diciembre, por el que se regula la historia clínica, de Castilla y León (BOCyL núm. 249, 28.12.2005).

- Ley 3/2005, de 8 de julio, de información sanitaria y autonomía del paciente, Comunidad Autónoma de Extremadura (BOE núm. 186, 5.08.2005).

- Ley 2/2002, de 17 de abril, de Salud, de la Comunidad Autónoma de La Rioja (BOR núm. 49, 23.04.2002).

- Ley 10/2001, de 28 de junio, de Salud de Extremadura (DOE núm. 76, 3.07.2001).

- Decreto 93/2009, de 24 de abril, por el que se regula la implantación de la receta electrónica en el ámbito del Sistema Sanitario Público de Extremadura (DOE núm. 82, 30.04.2009).

- Ley 7/2011, de 23 de marzo, de salud pública de Extremadura (DOE núm. 59, 25.03.2011).

- Ley Foral 11/2002, de 6 de mayo, sobre los derechos del paciente a las voluntades anticipadas, a la información y a la documentación clínica de Navarra (BON núm. 58, 13.05.2002).

- Ley 4/1994, de 26 de julio, de Salud de Murcia (BOE núm. 243, 11.10.1994).

- Ley 1/1992, de 2 de julio, del Servicio de Salud del Principado de Asturias (BOE núm. 211, 2.09.1992).

- Ley 2/1998, de 15 de junio de Salud de Andalucía (BOE núm. 185, 4.08.1998).

- Ley 5/2003, de 4 de abril, de salud de las Illes Balears (BOE núm.110, 8.05.2003).

- Ley 7/2002, de 10 de diciembre, de Ordenación Sanitaria de Cantabria (BOCT núm. 242, 18.12.2002).

- Decreto 29/2009, de 5 de febrero, por el que se regula el uso y acceso a la historia clínica electrónica en Galicia (DOG núm. 34, 18.02.2009).

- Decreto 206/2008, de 28 de agosto, de receta electrónica, de Galicia (DOG núm. 181, 18.11.2008).

- Decreto 24/2011, de 12 de abril, de la documentación sanitaria en Castilla- La Mancha (BOCM núm. 74, 15.04.2011).

- Decreto 181/2007, de 19 de junio, por el que se regula la receta médica electrónica, de Andalucía (BOJA núm. 123, 22.06.2007).

- Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid (BOCM núm. 306, 26.12.2001).

2. Legislación europea

- Declaración para la promoción de los derechos de los pacientes en Europa. Consulta Europea sobre los Derechos de los pacientes. Ámsterdam, 28-30 de marzo de 1994. Organización Mundial de la Salud (EUR/ICP/HLE 121, 28.06.1994).

- Carta de los Derechos Fundamentales de la Unión Europea, de 18 de diciembre de 2000 (DOCE C 364, 18.12.2000).

- Tratado de Funcionamiento de la Unión Europea (DOUE C 83, 30.03.2010).

- Declaración de Ginebra, adoptada por la 2ª Asamblea General de la AMM, Ginebra, Suiza, septiembre 1948 y enmendada por la 22ª Asamblea Médica Mundial, Sydney, Australia, agosto 1968 y la 35ª Asamblea Médica Mundial, Venecia, Italia, octubre 1983 y la 46ª Asamblea General de la AMM, Estocolmo, Suecia, septiembre 1994.

- Programa de Estocolmo (DO C 115, 4.05.2010).

- Plan de Acción por el que se aplica el Programa de Estocolmo (Comunicación COM (2010) 171 final 20.04.2010).

- 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 (BOE núm. 243, 10.10.1979).

- Resolución 22/1973, de 20 de noviembre, del Consejo de Europa sobre regulación jurídica de los ficheros electrónicos en el sector privado.

- Resolución 29/74, de 29 de noviembre de 1974, para establecer las pautas ordenadoras del sector público de la informática.

Consejo de Europa:

- Convenio sobre la Ciberdelincuencia, Budapest, de 23 de noviembre de 2001. Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 (BOE núm. 226, 17.11.2010, pp. 78847-78896).

- Convenio Nº 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 el 27 de enero de 1984 (BOE núm. 274, 15.12.1985, pp. 36000-36004).

- Protocolo adicional de convenio Nº 108, del Consejo de Europa, para la protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos, Estrasburgo, a 8 de noviembre de 2001. Instrumento de Ratificación del Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, hecho en Estrasburgo el 8 de noviembre de 2001 (BOE núm. 228, 20.09.2010, pp. 79619-79624).

- Convenio para la Protección de los Derechos Humanos y de la Dignidad del Ser Humano con Respecto a las Aplicaciones de la Biología y de la Medicina, hecho en Oviedo el 4 de abril de 1997. Instrumento de Ratificación del Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina), hecho en Oviedo el 4 de abril de 1997 (BOE núm. 251, 20.10.1999, pp. 36825-36830).

- Recomendación (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. Disponible en Internet: <http://www.bioeticaweb.com/recomendaciasn-nao-r-97-5-de-13-de-febrero-de-1997-del-comitac-de-ministros-del-consejo-de-europa-a-los-estados-miembros-sobre-protecciasn-de-datos-macdicos/> [Consulta: 2 septiembre 2016].

- Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, de 4 de noviembre de 1950. 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 (BOE núm. 243, 10.10.1979, pp. 23564-23579)

Reglamentos

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DOUE L 119, 4.05.2016, pp. 1-88).

- Reglamento (UE) Nº 611/2013 de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas (DOUE L 173, de 26.06.2013, pp. 2-8).

- Decisión del Consejo, de 13 de septiembre de 2004 por la que se adoptan las normas de desarrollo del Reglamento (CE) Nº 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DOUE L 296, 21.09.2004, pp. 16-22).

- Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DOUE L 8, 12.01.2001, pp. 1-22).

Directivas

- 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 (DOUE L 281, 23.11.1995, pp. 31-50).

- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (DOUE L 201, 31.07.2002, pp. 37-47).

- Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88, 4.4.2011, p. 45).

- Directiva 93/13/CE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores (DO L 95, 21.4.1993, p. 29).

- Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo (DOUE L 218, 14.08.2013, pp. 8-14).

3. Legislación internacional (Convenios internacionales)

- Declaración Universal de los Derechos del Hombre, declaración adoptada en París por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), de 10 de diciembre de 1948.

- Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, de 4 de noviembre de 1950, ratificado por España el 26.09.1979 (BOE núm. 243, 10.10.1979).

- Pacto Internacional de Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966, en vigor desde 3.01.1976 (BOE núm. 103, 30.04.1977) (17,18,26). Disponible en Internet: <http://www.ohchr.org/SP/ProfessionalInterest/Pages/CESCR.aspx> [Consulta: 2 septiembre 2016].

- Declaración de Helsinki de la Asociación Médica Mundial de 1964 (Adoptada por la 18ª Asamblea Médica Mundial, Helsinki, Finlandia, junio de 1964 y enmendada por la 29 Asamblea Médica Mundial, Tokio, Japón, octubre de 1975, la 35Asamblea Médica Mundial, Venecia, Italia, octubre de 1983 y la 41 Asamblea Médica Mundial, Hong Kong, septiembre de 1989). Disponible en Internet: <http://www.wma.net/es/30publications/10policies/b3/17c_es.pdf> [Consulta: 2 septiembre 2016].

- Declaración Internacional sobre los datos genéticos humanos, adoptada por unanimidad en la Conferencia General de la UNESCO el 16 de octubre de 2003. Disponible en Internet: <http://portal.unesco.org/es/ev.php-URL_ID=17720&URL_DO=DO_TOPIC&URL_SECTION=201.html> [Consulta: 18 septiembre 2016].

- Declaración Universal sobre el Genoma Humano y los Derechos Humanos, 28 de abril de 1977. Disponible en Internet: <http://portal.unesco.org/es/ev.php-URL_ID=13177&URL_DO=DO_TOPIC&URL_SECTION=201.html> [Consulta: 18 septiembre 2016].

- Convenio de Asturias de Bioética, firmado por España el 4 de abril de 1997, en Oviedo. Entró en vigor el 1 de enero de 2000 (BOE núm. 251, 20.10.1999).

- Ley 25.326 de Argentina, sobre Protección de datos personales, de 4 de octubre de 2000.

d) Códigos éticos.

Internacional

- Código Internacional de Ética Médica, adoptado por la 3ª Asamblea General de la AMM, Londres, Inglaterra, octubre 1949 y enmendado por la 22ª Asamblea Médica Mundial, Sydney, Australia, agosto 1968 y la 35ª Asamblea Médica Mundial, Venecia, Italia, octubre 1983. Asociación Médica Mundial (WMA, en inglés). Disponible en Internet: <http://www.wma.net/es/30publications/10policies/c8/> [Consulta: 6 agosto 2016].

- Declaración de Ginebra, adoptada por la 2ª Asamblea General de la AMM, Ginebra, Suiza, septiembre 1948 y enmendada por la 22ª Asamblea Médica Mundial, Sydney, Australia, agosto 1968 y la 35ª Asamblea Médica Mundial, Venecia, Italia, octubre 1983 y la 46ª Asamblea General de la AMM, Estocolmo, Suecia, septiembre 1994. Asociación Médica Mundial. Disponible en Internet: <http://www.wma.net/es/30publications/10policies/g1/WMA_DECLARACIONDEGINEBRA_A4_ESP.pdf> [Consulta: 6 agosto 2016].

Nacional

- Código de Ética y Deontología Médica de 1999. Éste Código se encuentra vigente con respecto a aquellas disposiciones que no contradigan al CDOMCE del 2011, op. cit. Disponible en Internet: <http://www.cgcom.es/sites/default/files/codigo_deontologia_medica.pdf> [Consulta: 22 noviembre 2016].

- Código de Deontología Médica. Guía de ética médica. Organización Colegial Médica de España de 2011. Disponible en Internet: <http://www.cgcom.es/sites/default/files/codigo_deontologia_medica_1.pdf> [Consulta: 15 julio 2015].

- Código Tipo de Tratamiento de Datos de Carácter Personal para Odontólogos y Estomatólogos de España. Diciembre 2009. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/common/pdfs/codigo_tipo_cnsejo_estomat_odont_dic_2009.pdf> [Consulta: 15 julio 2015]

- Código Deontológico de la Enfermería Española, de 14 de julio de 1989, aprobado por la Resolución Nº 32/1989 del Consejo General de Enfermería Disponible en Internet: <http://www.codem.es/codigo-deontologico> [Consulta: 16 julio 2015].

- Codi de Deontologia. 1997. Consell de Col·legis de Metges de Catalunya. Disponible en Internet: <https://www.comb.cat/cat/colegi/docs/codi_deontologic.pdf> [Consulta: 16 julio 2015].

e) Jurisprudencia consultada.

- STC 73/1982, de 2 de diciembre (BOE núm. 312, 29.12.1882).
- STC 32/1983, de 28 de abril (BOE núm. 117, 17.05.1983).
- STC 110/1984, de 26 de noviembre (BOE núm. 305, Suplemento, 21.12.1984).
- STC 53/1985 de 11 de abril (BOE núm. 119, 18.05.1985).
- STC 89/1987, de 3 de junio (BOE núm. 151, 25.06.1987).
- STC 231/1988, de 2 de diciembre (BOE núm. 307, 23.12.1988).
- STC120/1990, de 27 de junio (BOE núm. 181, 30.06.1990).
- STC137/1990, de 19 de julio (BOE núm. 181, 30.07.1990).
- STC 197/1991, de 17 de octubre (BOE núm. 274, 15.11.1991).
- STC 254/1993, de 20 de julio de 1993 (BOE núm. 197, 18.8.1993).
- STC 57/1994, de 28 de febrero (BOE núm. 71, 24.03.1994).
- STC 143/1994, de 9 de mayo de 1994 (BOE núm. 140, 13.05.1994).
- STC 215/1994, de 14 de julio (BOE núm. 197, 18.08.1994).
- STC 35/1996, de 11 de marzo (BOE núm. 93, 17.04.1996).
- STC 207/1996, de 16 de diciembre (BOE núm. 19, 22.01.1997).
- STC 94/1998, de 4 de mayo de 1998 (BOE núm. 137, Suplemento, 9.06.1998).
- STC 231/1998, de 1 de diciembre (BOE núm. 312, 30.12.1998).
- STC 134/1999, de 15 de julio (BOE núm. 197, Suplemento, 18.08.1999).
- STC 144/1999, de 22 de julio (BOE núm. 204, Suplemento, 26.08.1999).
- STC 202/1999, de 8 de noviembre de 1999 (BOE núm. 300, Suplemento, 16.12.1999).
- STC 115/2000, de 10 de mayo (BOE núm. 136, 7.06.2000).
- STC 290/2000, de 30 de noviembre de 2000 (BOE núm. 4, 4.01.2001).
- STC 292/2000, de 30 de noviembre de 2000 (BOE núm. 4, Suplemento, 4.01.2001).
- STC 156/2001, de 2 de julio (BOE núm. 178, 26.07.2001).
- STC 127/2003, de 30 de junio (BOE núm. 181, 30.07.2003).
- STC 196/2004, de 15 de noviembre (BOE núm. 306, 21.12.2004).
- STS de 28 diciembre de 1998, RJ 1998\10155.
- STS de 19 abril de 1999, RJ 1999\2588
- STS 12 de enero de 2001, RJ 2001\3
- STS 533/2008, 19 de septiembre de 2008. Recurso 10066/2008 (Roj: STS 4779/2008 – ECLI: ES:TS:2008:4779).
- STS 1328/2009, de 30 de diciembre de 2009. Recurso 1142/2009 (Roj: STS 8457/2009 – ECLI: ES:TS:2009:9457).
- STS 1624/2016, de 12 de abril de 2016. Recurso 618/2014 (Roj: STS 1624/2016 - ECLI:ES:TS:2016:1624).

- STS 1427/2016, de 8 de abril de 2016. Recurso 2050/2014 (Roj: STS 1427/2016 – ECLI:ES:TS:2016:1427).
- SAN, de 11 de marzo de 2013, Recurso 510/2011 (Roj: SAN 1133/2013 ECLI: ES:AN:2013:1133).
- SAN, de 29 de diciembre de 2014, Recurso 725/2010 (Roj: SAN 5129/2014 ECLI:ES:AN:2014:5129).
- Sentencia TEDH, 28.05.1985, Caso Abdulaziz, Cabales y Balkandali contra Reino Unido.
- Sentencia TEDH, 21.06.1988, Caso Berrehab contra Países Bajos.
- STJUE, 19 de mayo de 2009 (Asunto Comisión / Italia C-531/06 Nº 44/2009). ECLI:EU:C:2009:316.
- STJUE, 19 de mayo de 2009 (Asuntos acumulados C-171/07 y C-172/07). ECLI:EU:C:2009:315.
- STJUE de 13 de mayo de 2014 (Asunto Google, C-131/12). ECLI:EU:C:2014:317.

f) Informes jurídicos, recomendaciones y resoluciones de la Agencia Española de Protección de Datos.

- Informe jurídico de la AEPD 0153/2014. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdf_destacados/2014-0153_C-aa-maras-panor-aa-micas._Inexistencia-de-datos.pdf> [Consulta: 18 septiembre 2016].

- Informe jurídico de la AEPD 0034/2010. Disponible en Internet: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2010-0034_El-n-uu-mero-de-finca-registral-es-un-dato-identificable.pdf> [Consulta: 18 septiembre 2016].

- Informe jurídico de la AEPD 0624/2009. Disponible en Internet: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2009-0624_Publicaci-oo-n-en-revista-de-foto-ganadora-de-concurso-con-im-aa-genes-de-personas.-No-necesidad-de-consentimiento.pdf> [Consulta: 18 septiembre 2016].

- Informe jurídico de la AEPD 0654/2009. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2009-0654_Identificaci-oo-n-del-paciente-a-traves-de-c-oo-digo-num-ee-rico-no-constituye-un-supuesto-de-disociaci-oo-n.pdf> [Consulta: 18 septiembre 2016].

- Informe jurídico de la AEPD 0533/2008. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplica

cion/common/pdfs/2008-0533_Aplicaci-oo-n-de-la-LOPD-en-ensayos-cl-ii-nicos.pdf> [Consulta: 18 septiembre 2016].

- Informe jurídico de la AEPD 0488/2008. Disponible en Internet: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/common/pdfs/2008-0488_Tratamiento-y-Cesi-oo-n-de-datos-de-salud-con-finalidad-desconocida.pdf> [Consulta: 18 septiembre 2016].

- Informe jurídico de la AEPD 207/2008. Disponible en Internet: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2008-0207_Consecuencias-de-la-creaci-oo-n-de-una-base-de-datos-m-ee-dicos-anonimizada.pdf [Consulta: 10 noviembre 2016].

- Informe jurídico de la AEPD 285/2006. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2006-0285_N-uu-mero-de-tel-ee-fono-y-concepto-de-dato-personal.pdf> [Consulta: 18 septiembre 2016].

- Informe jurídico de la AEPD 327/2002. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP.pdf> [Consulta: 11 de septiembre de 2016].

- Informe jurídico de la AEPD 2001/0000, sobre el Tratamiento de los Datos de Salud. Disponible en Internet: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/index-ides-idphp.phpf> [Consulta: 13 agosto 2016].

- Resolución de la AEPD Nº: R/00646/2015 Procedimiento Nº TD/01846/2014. Disponible en Internet: <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php> [Consulta: 11 agosto 2016].

- Resolución de la AEPD Nº: R/00853/2015 Procedimiento Nº TD/01671/2014 Disponible en Internet: <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php> [Consulta: 11 agosto 2016].

- Resolución de la AEPD R/01239/2015 Procedimiento Nº TD/01997/2014; Disponible en Internet: <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php> [Consulta: 11 agosto 2016].

- Resolución de la AEPD Nº R/01119/2015 Procedimiento Nº TD/01955/2014; Disponible en Internet: <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php> [Consulta: 11 agosto 2016].

- Resolución de la AEPD Nº R/00555/2015 Procedimiento Nº TD/01533/2014; Disponible en Internet: <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php> [Consulta: 11 agosto 2016].

- Resolución de la AEPD Nº R/00741/2015 Procedimiento Nº TD/01843/2014); Disponible en Internet: <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php> [Consulta: 11 agosto 2016].

- Resolución de la AEPD Nº R/00633/2004, Procedimiento Nº TD/00218/2004. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/resultados-ides-idphp.php> [Consulta: 24 octubre 2016].

- Conclusiones y recomendaciones de la AEPD, 18.10.2002. Disponible en Internet: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/recomendaciones_concursos_tv.pdf> [Consulta: 11 de septiembre de 2016].

- Contribución de la Agencia Española de Protección de Datos a la consulta de la Comisión sobre un enfoque global de la protección de datos personales en la Unión Europea. Disponible en Internet: <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/aepd_dpa_es.pdf pdf> [Consulta: 17 septiembre 2015].

g) Informes jurídicos del Grupo de Trabajo sobre Protección de Datos del Artículo 29 de la Directiva 95/46/CE.

- Directrices sobre el derecho a la portabilidad de los datos, del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 13 de diciembre de 2016, 16/EN (GT 242). Disponible en Internet: <https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricesportabilidad.pdf> [Consulta: 8 agosto 2016].

- Grupo de Trabajo del Artículo 29. ANNEX. Health data in apps and devices (datos de salud en apps y dispositivos). 5 de febrero de 2015. Disponible en Internet: <http://ec.europa.eu/justice/data-protection/article29/documentation/otherdocument/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf> [Consulta: 8 agosto 2016].

- *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario*

Costeja González" C-131/12 (Criterios comunes para aplicar la sentencia sobre el "derecho al olvido"), del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 26 de noviembre de 2014, 14/EN. Disponible en Internet (versión en inglés): <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf> [Consulta: 10 agosto 2016].

- Dictamen 05/2014 sobre técnicas de anonimización, del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 10 de marzo de 1014, 0829/14/ES (WP 216). Disponible en Internet: <https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi8joqTxcvRAhUI0RQKHT9xCF0QFggcMAA&url=http%3A%2F%2Fec.europa.eu%2Fjustice%2Fdataprotection%2Farticle29%2Fdocumentation%2Fopinionrecommendation%2Ffiles%2F2014%2Fwp216_es.pdf&usg=AFQjCNErX--8_aKrEFUrFMCBB_dsG1Fu2g> [Consulta: 8 agosto 2016].

- *Opinion 06/2013 on open data and public sector information ('PSI') reuse* (Opinión 06/2013 sobre la información abierta y la reutilización de la información del sector público), del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 5 de junio de 2013, 1021/00/EN (WP 207). Disponible en Internet (versión en inglés): <https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjK1_rqwsvRAhXBaxQKHWkQDWkQFggdMAA&url=http%3A%2F%2Fec.europa.eu%2Fjustice%2Fdataprotection%2Farticle29%2Fdocumentation%2Fopinionrecommendation%2Ffiles%2F2013%2Fwp207_en.pdf&usg=AFQjCNEIJ2W02C_cQfEtHvVaTO1R3em8Jw&bvm=bv.144224172,d.bGs> [Consulta: 8 agosto 2016].

- Dictamen 15/2011 sobre la definición del consentimiento, del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 13 de julio de 2011, 01197/11/ES (WP 187). Disponible en Internet: <http://ec.europa.eu/justice/dataprotection/article29/documentation/opinionrecommendation/files/2011/wp187_es.pdf> [Consulta: 8 agosto 2016].

- Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 16 de febrero de 2010, 00264/10/ES (WP 169). Disponible en Internet: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf> [Consulta: 8 agosto 2016].

- Dictamen 2/2010 sobre la publicidad del comportamiento en línea, del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 22 de junio de 2010, 00909/10/ES (GT 171). Disponible en Internet: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_es.pdf> [Consulta: 8 agosto 2016].

- Dictamen 02/2010 sobre el principio de responsabilidad, del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 13 de julio de 2010, 00062/10/ES (GT 173). Disponible en Internet:

<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_es.pdf> [Consulta: 8 agosto 2016].

- Dictamen 08/2010 sobre el Derecho aplicable, del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 16 de diciembre de 2010, 0836-02/10/ES (WP 179). Disponible en Internet: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf> [Consulta: 8 agosto 2016].

- *Join contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data «The Future of Privacy»* (Contribución conjunta a la Consulta de la Comisión Europea sobre el marco legal para el derecho fundamental a protección de datos personales «El futuro de la intimidad»), del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 1 de diciembre de 2009, 02356/09/EN (WP 168). Disponible en Internet (versión en inglés): <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf> [Consulta: 8 agosto 2016].

- Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 15 de febrero de 2007, 00323/07/ES (WP 131). Disponible en Internet: <https://www.apda.ad/system/files/wp131_es.pdf> [Consulta: 26 noviembre 2016].

- Dictamen 4/2007 sobre el concepto de datos personales, del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. 20 de junio 2007, 01248/07/ES (WP 136). Disponible en Internet: <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm> [Consulta: 11 de septiembre de 2016].

h) Congresos, Ponencias, Jornadas.

BARRANCO ORTEGA, V. (22.10.2009) "La Tarjeta Sanitaria. Base de Datos población protegida SNS". Ponencia presentada en el 3er Foro sobre el Sistema de Información del SNS, Ministerio de Sanidad y Política Social, Madrid, 2009. <http://www.msps.es/estadEstudios/estadisticas/sisInfSanSNS/3ForoSISNS/docs/VictorBarranco_ponencia3Foro.pdf> [Consulta: 29 noviembre 2016].

BELTRÁN AGUIRRE, J. L. (27.06.2012). La Protección de los datos personales relacionados con la salud. Ponencia presentada en el Defensor del Pueblo de Navarra, junio de 2012, Navarra. Disponible en Internet: <http://www.navarra.es/NR/rdonlyres/517A4434-9C3B-442E-8651-61A7AE0490AD/226320/pdps.pdf> [Consulta: 7 julio 2015].

FREIXES SANJUÁN, T. “Las principales construcciones jurisprudenciales del Tribunal Europeo de Derechos Humanos. El standard mínimo exigible a los sistemas internos de derechos en Europa”. Proyecto DGICYT "Integración europea y derechos fundamentales: Integración de la jurisprudencia del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea en las sentencias del Tribunal Constitucional" (PB93-0851). Disponible en Internet: <http://personal.us.es/juanbonilla/contenido/CM/TRIBUNAL%20EUROPEO%20DE%20DERECHOS%20HUMANOS/JURISPRUDENCIA%20TEDH/PRINCIPALES%20CRITERIOS%20JURISPRUDENCIALES%20DEL%20TEDH.pdf> [Consulta: 18 septiembre 2016].

GÓMEZ PIQUERAS, C. (25 de febrero de 2008). *Contenido, usos y finalidad de la Historia Clínica.* Ponencia presentada en Antigua. Disponible en Internet: <https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjen5mwze7RAhWCWxQKHSvvAfYQFggjMAE&url=http%3A%2F%2Fwww.redipd.es%2Factividades%2Fseminarios_2008%2Fcommon%2Fponencia3_250208.pdf&usg=AFQjCNFUyIAv25hsp2c2PYdy3k6VNkG6HA> [Consulta: 29 octubre 2016].

HERNÁNDEZ MEDRANO, I. (29.11.2016) En la 3ª Jornada “Hacia un sistema sanitario basado en la creación de valor: La era de los datos, nuevo paradigma en la financiación de fármacos innovadores”, celebrada el en Madrid. El Médico Interactivo. Disponible en Internet: <http://www.elmedicointeractivo.com/articulo/noticias/big-data-supone-cambio-paradigma-extraer-conclusiones-y-tomar-decisiones/20161129173258107417.html> [Consulta: 13 enero 2017].

MUÑOZ MONTALVO, J. F. (22.10.2009) “La interoperabilidad: el nodo central del Sistema Nacional de Salud”. Ponencia presentada en el 3er Foro sobre el Sistema de Información del Sistema Nacional de Salud, celebrado el 22 de octubre de 2009, Ministerio de Sanidad y Política Social, Madrid, 2009. Disponible en Internet: <http://www.msps.es/estadEstudios/estadisticas/sisInfSanSNS/3ForoSISNS/docs/JuanFernando_ponencia3Foro.pdf> [Consulta: 29 noviembre 2016].

SALCEDO, A. (30.06.2016) El delicte de revelació de secrets: especial menció a l’aportació de documents en procediments judicials. Ponencia celebrada en el marco del 1r Congrés de l’Advocacia de Barcelona, celebrado el 30 de junio de 2016, ICAB, Barcelona. Disponible en Internet: <www.congresadvocaciabcn.cat> [Consulta: 1 julio 2016].

SISO MARTÍN, J. “Responsabilidad profesional en secreto médico”, en Ponencia del Master en valoración médica de la incapacidad laboral y dependencia. Tema 2, Universidad de Alcalá, Disponible en Internet: <http://www.juansiso.es/Almacen/SECRETO%20MEDICO%20-%20RESPONSABILIDAD%20PROFESIONAL.pdf> [Consulta: 23 marzo 2017].

i) Tesis Doctorales.

GUZMÁN GARCÍA, M. Á. *El derecho fundamental a la protección de datos personales en México: Análisis desde la influencia del ordenamiento jurídico español.* Tesis doctoral inédita. Universidad Complutense de Madrid. Facultad de Derecho. Madrid, 2013, p. 208. Disponible en Internet: **<**http://eprints.ucm.es/22817/1/T34727.pdf**>** [Consulta: 10 julio 2016].

SABARTÉS FORTUNY, R. (2013) *Historia Clínica Electrónica en un Departamento de Obstetricia, Ginecología y Reproducción: desarrollo e implementación. Factores Clave* (Tesis Doctoral). Universidad Autónoma de Barcelona, Facultad de Medicina, Barcelona, España, 2013, pp. 22 y ss. Disponible en internet: <http://www.tdx.cat/bitstream/handle/10803/117304/rsf1de1.pdf?sequence=1> [Consulta: 28 noviembre 2016].

SUÑÉ LLINÁS, E. La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina. Tesis presentada en la Universidad Complutense de Madrid, Madrid, 2013. Disponible en Internet: <http://eprints.ucm.es/22832/1/T34731.pdf> [Consulta: 17 septiembre 2016].

j) Blogs, noticias periodísticas y recursos de Internet.

ANTÓN BOIX, Mª C. La Protección de Datos. [Blog post]. Blog Revista de la Salud Mental, Sección Salud Mental, Implicaciones Legales y Forenses. Disponible en Internet: <http://www.saludmental.info/Secciones/Juridica/2008/proteccion-datos-feb08.html> [Consulta: 18 septiembre 2016].

ARGIMON, J. M. (26.02.2015) El proyecto VISC+ es una oportunidad para la mejora de la calidad de la atención sanitaria. [Blog post]. Blog de la Agencia de Calidad y Evaluación Sanitarias de Catalunya (AQuAS). Disponible en Internet: <http://blog.aquas.cat/2015/02/26/el-proyecto-visc-es-una-oportunidad-para-la-mejora-de-la-calidad-de-la-atencion-sanitaria/?lang=es> [Consulta: 18 enero 2017].

BARÓ E.; DEGOUL S.; BEUSCART R.; CHAZARD E. (2.06.2015) Toward a literature-driven definition of big data in healthcare. [Blog post]. Blog BioMed Research International, Universidad de Lille, Francia, 2015, p. 639021. Disponible en Internet (versión en inglés): <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4468280/> [Consulta: 10 enero 2017].

BUTARELLI, G. Conclusiones del Dictamen del Supervisor Europeo de Protección de Datos, sobre el cumplimiento efectivo de la legislación en la economía de la sociedad digital (DOUE C 463/8, 13.12.2016) Disponible en Internet: <https://edps.europa.eu/sites/edp/files/publication/17-01-13_big_data_ex_summ_es.pdf> [Consulta: 2 abril 2017].

CÁRCAR BENITO, J. E. (julio 2016) El Big Data en la organización sanitaria: nuevos tiempos y nuevos cambios. Un estudio previo. [Blog post]. Blog Federación Española de Sociología (FES). Disponible en

Internet: <http://www.fessociologia.com/files/congress/12/papers/5342.pdf#page=3&zoom=auto,-185,685> [Consulta: 23 enero 2017].

CORTÉS, E. (6.10.2015) Los tres candados que una empresa debe poner sobre los dados especialmente protegidos. [Blog post]. Blog Sage. Disponible en Internet: <http://blog.sage.es/economia-empresa/que-son-los-datos-especialmente-protegidos-en-proteccion-de-datos/> [Consulta: 18 septiembre 2016].

DE CASTRO VILA, C.; RUBIO MONTAÑÉS, M. L.; ALADID VILLAR, C. (mayo, 2015) Ética y acceso a datos clínicos desde los servicios de inspección y evaluación médicas. [Blog post]. Blog Formación Médica Continuada en Atención Primaria (FMC). Disponible en Internet: <http://www.fmc.es/es/tica-acceso-datos-clinicos-desde/articulo/90429633/#.WNzrXY4IFuU> [Consulta: 11 noviembre 2016].

FERRER, S. (29.01.2015) Cuatro datos son suficientes para relacionarte con tu tarjeta de crédito. *El Confidencial*. Disponible en Internet: <http://www.elconfidencial.com/tecnologia/2015-01-29/cuatro-datos-son-suficientes-para-relacionarte-con-tu-tarjeta-de-credito_651827/> [Consulta: 8 febrero 2017].

FUNDACIÓN ROCK HEALTH. (1.10.2012) Big Data *in digital health* (Big Data en salud digital). [Blog post]. Blog Rock Healt. Disponible en Internet (versión en inglés): <http://es.slideshare.net/RockHealth/rock-report-big-data> [Consulta: 10 enero 2017].

GIMÉNEZ, D. La historia clínica: Aspectos Éticos y Legales. [Blog post]. Blog Geosalud. Disponible en Internet: <http://geosalud.com/malpraxis/historiaclinica.htm> [Consulta: 22 octubre 2016].

Informe Anual del Sistema Nacional de Salud 2015, publicado por el Ministerio de Sanidad, Servicios Sociales e Igualdad. Disponible en Internet: <https://www.msssi.gob.es/estadEstudios/estadisticas/sisInfSanSNS/tablasEstadisticas/Inf_Anual_SNS_2015.1.pdf > [Consulta: 2 diciembre 2016].

JOYANES AGUILAR, L.; Poyatos Díaz, J. M. (2013) Big Data y el sector de la salud: el futuro de la sanidad. [Blog post]. Blog Juan Miguel Poyatos. The power of costumer connection. Disponible en Internet: <http://poyatosdiaz.com/index.php/big-data-y-el-sector-de-la-salud-el-futuro-de-la-sanidad> [Consulta: 14 noviembre 2016].

KELSEY, T. (13.01.2015) NHS boss claims patient data collection is “moraly right” (Director del England's National Health Service (NHS) (El Director del Servicio Nacional de Salud NHS demanda que la recolección de datos del paciente sea "un derecho moral”). [Blog post]. Blog It Pro. Disponible en Internet (versión en inglés): <http://www.itpro.co.uk/public-sector/23844/nhs-boss-claims-patient-data-collection-is-morally-right> [Consulta: 13 febrero 2017].

KENNETH, N. C.; MAYER-SCHOENBERGER, V. (May/June) The Rise of Big Data. How It´s Changing the Way We Think About the World (El auge del Big Data. Cómo está cambiando la manera en la que

pensamos el mundo). [Blog post]. Blog Foregin Affars. Disponible en Internet: (versión en inglés): <https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data> [Consulta: 8 enero 2017].

LOGICALIS. (11.05.2014) Big Data: el futuro del sector de la salud. [Blog post]. Blog sobre *Business Intelligence*. Disponible en Internet: <http://www.lantares.com/blog/big-data-el-futuro-del-sector-de-la-salud> [Consulta: 13 enero 2017].

LOGICALIS. (25.08.2014) Atención médica personalizada: Big Data y el futuro de la medicina. [Blog post]. Blog sobre *Business Intelligence*. Disponible en Internet: <http://www.lantares.com/blog/atencion-medica-personalizada-big-data-y-el-futuro-de-la-medicina> [Consulta: 13 enero 2017].

LÓPEZ LÓPEZ, V. (4.05.2015) Big data sanitario: el acelerador del conocimiento y la decisión clínica. [Blog post]. Blog A un clic de las TIC. Disponible en Internet: <http://aunclicdelastic.blogthinkbig.com/big-data-sanitario-el-acelerador-del-conocimiento-y-la-decision-clinica/> [Consulta: 12 enero 2017].

LUNA, A. G. (22.11.2014) Los datos de tu salud que recopilan los dispositivos, un negocio para las empresas. [Blog post]. Blog El Confidencial, 22-11-2014. Disponible en Internet: <http://www.elconfidencial.com/tecnologia/2014-11-22/tus-datos-de-salud-que-recopilanlosdispositivosunnegocio-para-las-empresas_500297/> [Consulta: 13 febrero 2017].

MCKINSEY GLOBAL INSTITUTE - MANYIKA J., et al. (Mayo 2011). Big Data: The next frontier for innovation, competition, and productivity (La siguiente frontera para innovación, competición, y productividad). [Blog post]. Blog Digital McKinsey. Disponible en Internet (versión en inglés): <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation> [Consulta: 10 enero 2017].

MIRALLES LÓPEZ, R. (25.07.2014) Aspectos a considerar en relación al Big Data. [Blog post]. Blog Observatorio Iberoamericano de Protección de Datos. Disponible en Internet: <http://oiprodat.com/2014/07/25/aspectos-a-considerar-en-relacion-al-big-data/> [Consulta: 10 enero 2017].

Office of Science and Technology Policy. Executive Office of the President. (20.03.2012) *Obama administration* unveils “Big Data” initiative: announces $200 million in new R&D investments (La Oficina del Presidente Obama anuncia la iniciativa de 200 millones de dólares en I+D en Big Data). Estados Unidos. Disponible en Internet (versión en inglés): <https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiXemAocnRAhVJwBQKHd4zCYkQFggcMAA&url=https%3A%2F%2Fwww.whitehouse.gov%2Fsites%2Fdefault%2Ffiles%2Fmicrosites%2Fostp%2Fbig_data_press_release_final_2.pdf&usg=AFQjCNGDfomg7zyDTyUq77ngGpFF282yYA&sig2=KC0mFF8-mZ7fC1g7PbiQtQ> [Consulta: 14 octubre 2016].

PLANAS, J. (2015) La próxima revolución en el sector sanitario. [Blog post]. Blog del Dr. Jorge Planas. Disponible en Internet: <http://www.clinicaplanas.com/jorge-planas/2012/10/29/la-proxima-revolucion-en-el-sector-sanitario/> [Consulta: 13 febrero 2017].

Proyecto HCDSNS Historia Clínica Digital del Sistema Nacional de Salud, *Informe de Situación de enero de 2017*. Publicado por el Ministerio de Sanidad, Servicios Sociales e Igualdad. Disponible en Internet:
<http://www.msssi.gob.es/profesionales/hcdsns/contenidoDoc/Inf_Sit_HCDSNS_Enero2017.pdf>
[Consulta: 12 enero 2017].

RODRIGO LARRUCEA, C. (14.04.2016) Mhealth y Bigdata en sanidad. [Blog post]. Blog Derecho y salud no van siempre de la mano. Disponible en Internet: <https://carmenrodrigodelarrucea.wordpress.com/2016/04/14/mhealth-y-bigdata-en-sanidad/#more-793> [Consulta: 11 febrero 2017].

SÁNCHEZ GARCÍA, J. J. (3.03.2015) La privacidad de los datos de salud en la era digital. [Blog post]. Blog A un click de las TIC, blogthinkbig.com. Disponible en Internet: <aunclicdelastic.blogthinkbig.com/la-privacidad-de-los-datos-de-salud-en-la-era-digital/> [Consulta: 13 febrero 2017].

SIEMENS. Big data in the healthcare industry. Increasingly used data-driven care protocols will change healthcare delivery systems globally (Big Data en la industria de asistencia médica. Los protocolos de cuidado cada vez más usados conducidos por datos cambiarán sistemas de entrega de asistencia médica a escala mundial) (05.08.2015). Disponible en Internet: (versión en inglés): <https://www.healthcare.siemens.com/magazine/mso-big-data-and-healthcare-1.html> [Consulta: 14 noviembre 2016].

SOLER, I. (23.02.2016) Entre el imperativo moral y el Big Data sanitario. El Periódico. Disponible en Internet: <http://www.elperiodico.com/es/noticias/mas-valor/impertativo-moral-gran-hermano-sanitario-4917353> [Consulta: 18 enero 2017].

VALENCIA, E. (28.09.2016) ¿Qué es el Real World Evidence y para qué sirve? [Blog post]. Blog Singular Data & Analytics. Disponible en Internet: <https://data.sngular.team/es/art/63/real-world-evidence-definicion-y-beneficios> [Consulta: 18 enero 2017].

k) Otros documentos de la Unión Europea.

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Un enfoque global de la protección de los datos personales en la Unión Europea. Bruselas, 4.11.2010 COM (2010) 609 final. Disponible en Internet:

<http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_es.pdf> [Consulta: 17 septiembre 2015].

Comunicado de Prensa de la Comisión Europea: El acuerdo sobre la reforma de la protección de datos promovida por la Comisión reforzará el mercado único digital (15.12.2015) Disponible en Internet: <http://europa.eu/rapid/press-release_IP-15-6321_es.htm> [Consulta: 3 enero 2016].

Conclusiones del Abogado General del Tribunal de Justicia, Sr. NIILO JÄÄSKINEN, en el Asunto C-131/12: Google Spain, S.L. y Google Inc. / Agencia Española de Protección de Datos, M. C. G (Conclusiones ECLI:EU:C:2013:424 de 25.05.2013) <http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=19636> [Consulta: 19 noviembre 2015].

Dictamen del Supervisor Europeo de Protección de Datos, sobre el cumplimiento efectivo de la legislación en la economía de la sociedad digital (DOUE C 463/8, 13.12.2016) Disponible en Internet: <https://edps.europa.eu/sites/edp/files/publication/17-01-13_big_data_ex_summ_es.pdf> [Consulta: 2 abril 2017].

Eurobarómetro especial (EB) 359, *Data Protection and Electronic Identity in the EU* (Protección de datos e identidad electrónica en la UE). Fecha de publicación: junio 2011: Disponible en internet (versión en inglés): <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> [Consulta: 17 de septiembre 2015].

Eurobarómetro especial (EB) 404, *European citizens' digital health literacy* (La alfabetización digital de la salud de los ciudadanos europeos). Fecha de publicación: noviembre 2014. <https://open-data.europa.eu/es/data/dataset/S1073_79_4_404> [Consulta: 17 septiembre 2015].

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos), (Comunicación COM (2012) 11 final 25.01.2012). Disponible en Internet: <https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjlrPzE0IrTAhVMtBQKHR9uAmkQFggsMAE&url=http%3A%2F%2Fwww.europarl.europa.eu%2FRegData%2Fdocs_autres_institutions%2Fcommission_europeenne%2Fcom%2F2012%2F0011%2FCOM_COM(2012)0011_EN.pdf&usg=AFQjCNG0VBRS36IGUTt_C2F00diCYC9lyw> [Consulta: 6 abril 2015].

"Umbrella Agreement" (Acuerdo Marco), firmado entre UE y Estados Unidos. 2.06.2016. Disponible en Internet: <http://www.consilium.europa.eu/de/press/press-releases/2016/06/02-umbrella-agreement/> [Consulta: 2 abril 2017].

Abreviaturas

AEPD	Agencia Española de Protección de Datos
APDCAT	Agencia Catalana de Protección de Datos
APDCM	Agencia de Protección de Datos de la Comunidad de Madrid
CDOMCE	Código Deontológico de la Organización Médica Colegial de España de 2011
CE	Constitución Española
CEDH	Carta Europea de Derechos Humanos
Convenio 108	Convenio Nº 108, del Consejo de Europa, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal
Convenio de Oviedo	Convenio de Asturias de Bioética, firmado por España el 4 de abril de 1997, en Oviedo
CP	Código Penal
Directiva 95/46/CE	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
HC	Historia clínica
HCD	Historia clínica digital
LAP	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
LGS	Ley 14/1986, de 25 de abril, General de Sanidad
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
LSG	Ley 14/1986, de 25 de abril, General de Sanidad.
OMS	Organización Mundial de la Salud
RD 1720/2007	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.
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
SAN	Sentencia de la Audiencia Nacional
SEPD	Supervisor Europeo de Protección de Datos
STC	Sentencia el Tribunal Constitucional
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
STS	Sentencia del Tribunal Supremo
TC	Tribunal Constitucional
TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnologías de información y comunicación
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
UE	Unión Europea

Índice de Anexos

ANEXO I

CONJUNTO DE DATOS DEL INFORME CLÍNICO DE ALTA

Variable	Formato	Valores	Aclaraciones	CM/R[1]
DATOS DEL DOCUMENTO				
Tipo de documento	Texto	Informe Clínico de Alta		CM
Fecha de firma	dd/mm/aaaa	Libre	Es común a ambos pies de firma del informe	CM
Fecha de Ingreso	dd/mm/aaaa	Libre		CM
Fecha de alta	dd/mm/aaaa	Libre		CM
Nombre Responsable 1	Texto	Libre (nombre+2 apellidos)	Es parte del primer pie de firma del informe	CM
Categoría profesional 1	Texto	Médico Residente Facultativo Especialista de Área Jefe de Sección Jefe de Servicio		CM
Nombre Responsable 2	Texto	Libre (nombre+2 apellidos)	Es parte del segundo pie de firma, que suele supervisar al primer firmante	CM
Categoría profesional 2	Texto	Facultativo Especialista de Área Jefe de Sección Jefe de Servicio		
Servicio	Texto	Según normativa en vigor en cada momento.	Actualmente: clasificación de Servicios del CMBD/SIFCO	CM
Unidad	Texto	Libre		CM
DATOS DE LA INSTITUCIÓN EMISORA				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL .Gerencia Regional de Salud de Castilla y León. DdS-GC. Departament de Salut de la Generalitat de Catalunya SES. Servicio Extremeño de Salud. SERGAS. Servizo Galego de Saúde. INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears. RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud SNS-O. Servicio Navarro de Salud-OSASUNBIDEA. Agència Valenciana de Salut OSAKIDETZA-Servicio Vasco de Salud.		CM
Denominación del provisor de servicios	Texto +Logo	Libre		R
Denominación del Centro	Texto + Logo	CNH y posteriormente RECESS cuando esté disponible+texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura	CM
Dirección Del Centro				
Tipo de vía	Texto	CNH y posteriormente RECESS cuando esté disponible+texto libre		CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			CM
Teléfono	Texto			CM
Dirección Web/Correo electrónico	Texto	Libre	Se incluirá la dirección Web sólo si contiene información de interés para el usuario	R

[1] Se puede clasificar cada campo según se considere que su presencia es esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debe formar parte del conjunto mínimo del SNS (CM) o por el contrario es aconsejable su presencia pero no imprescindible como parte del conjunto mínimo de datos (R)

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[1]
DATOS DEL PACIENTE				
Nombre	Texto	Dato que figure en la BD de la TSI de la CA		CM
Primer Apellido	Texto			CM
Segundo Apellido	Texto			CM
Fecha nacimiento	dd/mm/aaaa			CM
Sexo	Texto		H/M	CM
DNI/T.Residencia/Pasaporte	Texto			R
NASS	Texto			CM
CIP de C Autónoma	Texto			CM
Código SNS	Texto			R
CIP Europeo	Texto		Se reserva este espacio en previsión de que, en el futuro, exista un código europeo/internacional de identificación.	R
Nº Historia Clínica	Texto	Libre		CM
Domicilio				
Tipo de vía	Texto	Dato que figure en la BD de la TSI de la CA		CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Piso	Texto			CM
Letra	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			
Teléfono	Texto	Dato que figure en la BD de la TSI de la CA+texto libre	Existirá texto libre para añadir un segundo número de teléfono	R
DATOS DEL PROCESO ASISTENCIAL				
Motivo del Alta	Texto	Traslado a domicilio Traslado de Servicio Traslado a otro centro hospitalario Traslado a un centro sociosanitario Alta voluntaria Fallecimiento Otros	Se incluyen las categorías correspondientes al CMBD nacional, independientemente de que los CMBD autonómicos incorporen de hecho categorías adicionales, cuyas respuestas luego se reclasifican. La categoría de respuesta fallecimiento, será recodificada a "éxitus"	CM
Motivo de Ingreso	Texto	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Tipo de ingreso	Texto	Urgente Programado		CM
Antecedentes	Texto	Libre		CM
Enfermedades familiares hereditarias Enfermedades previas Antecedentes neonatales, obstétricos y quirúrgicos Alergias Hábitos tóxicos Actuaciones preventivas (1) Medicación previa Situación funcional (2) Antecedentes sociales y profesionales	Texto	Libre	(1) Vacunaciones infantiles, del adulto, quimioprofilaxis realizadas, etc (2) Se refiere a la valoración del impacto funcional de los problemas activos o enfermedades y se podrán utilizar una o varias escalas (Escalas de dependencia, clasificación funcional de la insuficiencia cardíaca, valoraciones del grado de demencia, escalas de calidad de vida, etc.)	R
Historia Actual	Texto	Libre		CM
Exploración Física	Texto	Libre		CM
Resumen pruebas complementarias	Texto	Libre		CM
Laboratorio Imagen Otras pruebas	Texto	Libre	Se recomienda la clasificación en subapartados	R
Evolución y comentarios	Texto	Libre	En su caso, puede incluirse el protocolo quirúrgico en este apartado, así como comentarios al diagnóstico o tratamiento, valoraciones diagnósticas adicionales, describir si el ingreso psiquiátrico fue involuntario,. describir reacciones adversas a fármacos u otras sustancias utilizados en este episodio, complicaciones evolutivas de la/las enfermedades o realizar valoraciones diagnósticas o comentarios adicionales.	CM

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[1]
Diagnóstico Principal	Texto +código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Otros Diagnósticos	Texto +código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Procedimientos	Texto +código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Tratamiento	Texto	Libre		CM
Recomendaciones	Texto	Libre	Se trata de recomendaciones terapéuticas que no incluyen fármacos (oxigenoterapia, dieta, reposo o limitaciones de esfuerzo físico, etc.)	R
Fármacos	Texto +código	Libre (Especialidad+principioactivo+ dosis/unidad+ nº unidades/dosis+ intervalo de dosis+ via administración+ duración) nomenclator oficial MSPS (código nacional)/Snomed-CT	En la medida en que la implantación de las aplicaciones informáticas de HCE, que incluyen módulos de prescripción lo permitan, el texto libre, será reemplazado progresivamente por el vocabulario del catálogo de medicamentos autorizados (Nomenclator Oficial/ Snomed-CT)	R
Otras Recomendaciones	Texto	Libre	Se refiere a los planes de actuación previstos que no son propiamente medidas terapéuticas. Por ejemplo, fecha de próxima cita, conveniencia de nueva revisión, petición de pruebas, etc.	CM

ANEXO II

CONJUNTO DE DATOS DEL INFORME CLÍNICO DE CONSULTA EXTERNA

Variable	Formato	Valores	Aclaraciones	CM/R[2]
DATOS DEL DOCUMENTO				
Tipo de documento	Texto	Informe Clínico de Consulta Externa		CM
Fecha de firma	dd/mm/aaaa	Libre	Es común a ambos pies de firma del informe	CM
Fecha de Consulta	dd/mm/aaaa	Libre		CM
Nombre Responsable 1	Texto	Libre (nombre+2 apellidos)	Es parte del primer pie de firma del informe	CM
Categoría profesional 1	Texto	Médico Residente Facultativo Especialista de Área Jefe de Sección Jefe de Servicio		CM
Nombre Responsable 2	Texto	Libre (nombre+2 apellidos)	Es parte del segundo pie de firma, que suele supervisar al primer firmante	CM
Categoría profesional 2	Texto	Facultativo Especialista de Área Jefe de Sección Jefe de Servicio		CM
Servicio	Texto	Según normativa en vigor en cada momento.	Actualmente: clasificación de Servicios del CMBD/SIFCO	CM
Unidad	Texto	Libre		CM
DATOS DE LA INSTITUCIÓN EMISORA				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL .Gerencia Regional de Salud de Castilla y León. DdS-GC. Departament de Salut de la Generalitat de Catalunya SES. Servicio Extremeño de Salud. SERGAS. Servizo Galego de Saúde. INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears.		CM

[2] Se puede clasificar cada campo según se considere que su presencia es esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debe formar parte del conjunto mínimo del SNS (CM) o por el contrario es aconsejable su presencia pero no imprescindible como parte del conjunto mínimo de datos (R)

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[2]
		RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud SNS-O. Servicio Navarro de Salud-OSASUNBIDEA. Agència Valenciana de Salut OSAKIDETZA-Servicio Vasco de Salud.		
Denominación del provisor de servicios	Texto + Logo	Libre		R
Denominación del Centro	Texto + Logo	CNH y posteriormente RECESS cuando esté disponible+texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura.	CM
Dirección del centro				
Tipo de vía	Texto	CNH y posteriormente RECESS cuando esté disponible+texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura	CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			CM
Teléfono	Texto			CM
Dirección Web/Correo electrónico	Texto	Libre	Se incluirá la dirección Web sólo si contiene información de interés para el usuario	R
DATOS DEL PACIENTE				
Nombre	Texto	Dato que figure en la BD de la TSI de la CA		CM
Primer Apellido	Texto			CM
Segundo Apellido	Texto			CM
Fecha nacimiento	dd/mm/aaaa			CM
Sexo	Texto		H/M	CM
DNI/T.Residencia/Pasaporte	Texto			R
NASS	Texto			CM
CIP de C Autónoma	Texto			CM
Código SNS	Texto			R
CIP Europeo	Texto		Se reserva este espacio en previsión de que, en el futuro, exista un código europeo/internacional de identificación.	R
Nº Historia Clínica	Texto	Libre		CM
Domicilio				
Tipo de vía	Texto	Dato que figure en la BD de TSI de la CA		CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Piso	Texto			CM
Letra	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			
Teléfono	Texto	Dato que figure en la BD de la TSI de la CA+texto libre	Existirá texto libre para añadir un segundo número de teléfono	R
DATOS DEL PROCESO ASISTENCIAL				
Motivo de Consulta	Texto +código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Antecedentes	Texto	Libre	Se recomienda la clasificación en subapartados	CM
Enfermedades familiares hereditarias Enfermedades previas Antecedentes Neonatales, Obstétricos y Quirúrgicos Alergias Hábitos tóxicos Actuaciones Preventivas (1) Medicación previa			(1) Vacunaciones infantiles, del adulto, quimioprofilaxis realizadas, etc (2) Se refiere a la valoración del impacto funcional de los problemas activos o enfermedades y se podrán utilizar una o varias escalas (Escalas de dependencia, clasificación	R

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[2]
Situación funcional (2) Antecedentes sociales y profesionales			funcional de la Insuficiencia cardiaca, Valoraciones del grado de demencia, Escalas de Calidad de vida, etc..)	
Historia Actual	Texto	Libre		CM
Exploración Física	Texto	Libre		CM
Resumen pruebas complementarias	Texto	Libre		CM
Laboratorio Imagen Otras pruebas	Texto	Libre	Se recomienda la clasificación en subapartados	R
Evolución y comentarios	Texto	Libre	Se pueden realizar comentarios del seguimiento evolutivo, en el caso de que el informe no se refiera a una sola consulta sino a un periodo de seguimiento en el que se han realizado varias entrevistas clínicas. En este caso se puede incluir aquí el periodo de tiempo del que es comprensivo el informe o reseñar las fechas en las que se produjeron las consultas. También es el lugar adecuado para describir reacciones adversas a fármacos utilizados en este episodio o describir complicaciones evolutivas de la/las enfermedades, realizar valoraciones diagnósticas o comentarios adicionales	CM
Diagnóstico Principal	Texto+ código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Otros Diagnósticos	Texto+ código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Procedimientos	Texto+ código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Tratamiento	Texto	Libre		CM
Recomendaciones	Texto	Libre	Se trata de recomendaciones terapéuticas que no incluyen fármacos (oxigenoterapia, dieta, reposo o limitaciones de esfuerzo físico, etc.)	R
Fármacos	Texto +código	Libre (Especialidad+principio activo+ dosis/unidad+ nº unidades/dosis+ intervalo de dosis+ vía administración+ duración) nomenclator oficial MSPS (código nacional)/Snomed-CT	Prescripciones activas al final del período de seguimiento En la medida en que la implantación de las aplicaciones informáticas de HCE, que incluyen módulos de prescripción lo permitan, el texto libre, será reemplazado progresivamente por el vocabulario del catálogo de medicamentos autorizados (Nomenclator Oficial/ Snomed-CT)	R
Otras recomendaciones	Texto	Libre	Se refiere a los planes de actuación previstos que no son propiamente medidas terapéuticas. Por ejemplo: fecha de próxima cita, conveniencia de nueva revisión, petición de pruebas etc..	CM

ANEXO III

CONJUNTO DE DATOS DEL INFORME CLÍNICO DE URGENCIAS

Variable	Formato	Valores de referencia	Aclaraciones	CM/R[3]
DATOS DEL DOCUMENTO				
Tipo de documento	Texto	Informe Clínico de Urgencias		CM
Fecha de firma	dd/mm/aaaa	Libre	Es común a ambos pies de firma del informe	R
Fecha y hora de ingreso o de activación del recurso	dd/mm/aaaa hh:mm	Libre		CM
Fecha y hora de alta	dd/mm/aaaa hh:mm	Libre		CM

[3] Se puede clasificar cada campo según se considere que su presencia es esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debe formar parte del conjunto mínimo del SNS (CM) o por el contrario es aconsejable su presencia pero no imprescindible como parte del conjunto mínimo de datos (R)

cve: BOE-A-2010-14199

Variable	Formato	Valores de referencia	Aclaraciones	CM/R[3]
Nombre Responsable 1	Texto	Libre (nombre + 2 apellidos)	Es parte del primer pie de firma del informe	CM
Categoría profesional 1	Texto	Médico Residente Facultativo Jefe de Sección Jefe de Servicio		CM
Nombre Responsable 2		Libre (nombre + 2 apellidos)	Es parte del segundo pie de firma, que suele supervisar al primer firmante	CM
Categoría responsable 2		Facultativo Jefe de Sección Jefe de Servicio		CM
Unidad Asistencial responsable	Texto	Servicio de Urgencia Hospitalaria Servicio de Urgencia de A.Primaria SAMU Sº Urgencias + texto libre		CM
DATOS DE LA INSTITUCIÓN EMISORA				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL .Gerencia Regional de Salud de Castilla y León. DdS-GC. Departament de Salut de la Generalitat de Catalunya SES. Servicio Extremeño de Salud. SERGAS. Servizo Galego de Saúde. INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears. RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud SNS-O. Servicio Navarro de Salud-OSASUNBIDEA. Agència Valenciana de Salut OSAKIDETZA-Servicio Vasco de Salud.		CM
Denominación del provisor de servicios	Texto +logo	Libre		R
Denominación del Centro	Texto + logo	CNH para Centros de Atención Especializada. Inventario para Centros de Primaria RECESS para ambos cuando esté disponible + texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura	CM
Dirección del Centro				
Tipo de vía	Texto			CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			CM
Teléfono	Texto			CM
Dirección Web/Correo Electrónico	Texto		Se incluirá la dirección Web sólo si contiene información de interés para el usuario	R
DATOS DEL PACIENTE				
Nombre	Texto	Dato que figure en BD de la TSI de la CA		CM
Primer Apellido	Texto			CM
Segundo Apellido	Texto			CM
Fecha de nacimiento	dd/mm/aaaa			CM
Sexo	Texto		H/M	CM
DNI/T.Residencia/Pasaporte	Texto			R
NASS	Texto			CM
CIP de la C. Autónoma	Texto			CM
Código SNS	Texto			R
CIP Europeo			Se reserva este espacio en previsión de que en el futuro exista un código europeo/internacional de identificación.	R
Nº Historia Clínica	Texto	Libre		R
Domicilio				
Tipo de vía	Texto	Dato que figure en la BD de TSI de la CA		CM

cve: BOE-A-2010-14199

Variable	Formato	Valores de referencia	Aclaraciones	CM/R[3]
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Piso	Texto			CM
Letra	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			
Teléfono	Texto			R
Persona de Referencia	Texto	Libre (nombre + 2 apellidos)		R
Teléfono de Referencia	Texto	Libre		R
DATOS DEL PROCESO ASISTENCIAL				
Procedencia	Texto	Médico de Familia/Pediatra de AP Por decisión del paciente o familiar Cuerpos de Seguridad Otros Servicios de Urgencias		R
Tipo de Consulta	Texto	Enfermedad Accidente de tráfico Accidente Laboral Otros Accidentes		R
Motivo de Alta	Texto	Ingreso Traslado a domicilio Traslado de Servicio Traslado a otro centro hospitalario Traslado a un centro sociosanitario Alta voluntaria Fallecimiento Otros	Se incluyen aquellas categorías correspondientes al CMBD nacional, independientemente de que los CMBD autonómicos incorporen categorías adicionales cuyas respuestas luego se reclasifican. La categoría de respuesta *fallecimiento*, será recodificada a *éxitus*.	CM
Motivo de Consulta	Texto + código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Antecedentes	Texto	Libre		CM
Enfermedades Previas Antecedentes neonatales, obstétricos y quirúrgicos Medicación previa Alergias Situación funcional (1) Antecedentes sociales y profesionales	Texto	Libre	(1) Se refiere a la valoración del impacto funcional de los problemas activos o enfermedades, y se podrán utilizar una o varias escalas (Escalas de dependencia, clasificación funcional de la insuficiencia cardiaca, valoraciones del grado de demencia, escalas de calidad de vida, etc.)	R
Historia Actual	Texto	Libre		CM
Exploración física				CM
TA (/) FC ( )lat/min FR ( ) resp/min Temp. ( )ºC Saturación O_2 Glucemia capilar Resumen de exploración	Texto	Libre		R
Resumen de pruebas complementarias	Texto	Libre	Se recomienda la clasificación en subapartados	CM
Laboratorio Imagen Otras pruebas	Texto	Libre		R
Evolución y comentarios	Texto	Libre	En su caso pueden incluirse, además de comentarios evolutivos y del período de observación, la descripción de técnicas realizadas durante el proceso de atención. También es el lugar adecuado para describir reacciones adversas a fármacos utilizados en este episodio, complicaciones evolutivas de la/las enfermedades, realizar valoraciones diagnósticas o comentarios adicionales.	CM
Diagnóstico principal	Texto +código	Libre Código CIE 9 MC/CIE 10/CIAP2 definida/SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Otros diagnósticos	Texto +código	Libre Código CIE 9 MC/CIE 10/CIAP2 definida/SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R

cve: BOE-A-2010-14199

Variable	Formato	Valores de referencia	Aclaraciones	CM/R[3]
Procedimientos	Texto +código	Libre Código CIE 9 MC/CIE 10/CIAP2 definida/SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Tratamiento	Texto	Libre		CM
Recomendaciones	Texto	Libre	Se trata de recomendaciones terapéuticas que no incluyen fármacos (oxigenoterapia, dieta, reposo o limitaciones de esfuerzo físico, etc.)	R
Fármacos	Texto +código	Libre (Especialidad+principio activo+ dosis/unidad+ nº unidades/dosis+ intervalo de dosis+ via administración+ duración) nomenclator oficial MSPS (código nacional)/Snomed-CT	Prescripciones activas. En la medida en que la implantación de las aplicaciones informáticas de HCE, que incluyen módulos de prescripción lo permitan, el texto libre, será reemplazado progresivamente por el vocabulario del catálogo de medicamentos autorizados (Nomenclator Oficial/ Snomed-CT)	R
Otras recomendaciones	Texto	Libre	Se refiere a los planes de actuación previstos que no son propiamente medidas terapéuticas. Por ejemplo: fecha de próxima cita, conveniencia de nueva revisión, petición de pruebas, etc.	CM

ANEXO IV

CONJUNTO DE DATOS DEL INFORME CLÍNICO DE ATENCIÓN PRIMARIA

Variable	Formato	Valores	Aclaraciones	CM/R[4]
DATOS DEL DOCUMENTO				
Tipo de documento	Texto	Informe Clínico de Atención Primaria		CM
Fecha de firma	dd/mm/aaaa	Libre	Fecha en la cual se emite el informe. Es común a ambos pies de firma.	CM
Fecha inicio periodo	dd/mm/aaaa	Libre	Fecha en la que se inicia el periodo de seguimiento en el que se inscriben los diferentes episodios y actuaciones que se describen.	CM
Fecha fin periodo	dd/mm/aaaa	Libre	Fecha en la que finaliza el periodo de seguimiento en el que se inscriben los diferentes episodios y actuaciones que se describen.	CM
Nombre Responsable 1	Texto	Libre (nombre + 2 apellidos)	Es parte del primer pie de firma del informe	CM
Categoría profesional 1	Texto	Médico Residente Médico de Familia Pediatra de AP Texto Libre		CM
Nombre Responsable 2	Texto	Libre (nombre + 2 apellidos)	Es parte del segundo pie de firma, que suele supervisar el primer firmante	CM
Categoría responsable 2	Texto	Médico de Familia Pediatra de AP Texto Libre		CM
DATOS DE LA INSTITUCIÓN EMISORA				
Denominación del Servicio de Salud	Texto + logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL .Gerencia Regional de Salud de Castilla y León. DdS-GC. Departament de Salut de la Generalitat de Catalunya SES. Servicio Extremeño de Salud. SERGAS.Servizo Galego de Saúde. INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears. RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud SNS-O. Servicio Navarro de Salud-OSASUNBIDEA. Agència Valenciana de Salut OSAKIDETZA-Servicio Vasco de Salud.		CM

[4] Se puede clasificar cada campo según se considere que su presencia es esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debe formar parte del conjunto mínimo del SNS (CM) o por el contrario es aconsejable su presencia pero no imprescindible como parte del conjunto mínimo de datos (R)

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[4]
Denominación del provisor de servicios	Texto +logo	Libre		R
Denominación del Centro	Texto + logo	Inventario de Centros de Atención Primaria y posteriormente RECESS cuando esté disponible + texto libre		CM
Dirección del Centro				
Tipo de vía	Texto	Inventario de Centros de Atención Primaria y posteriormente RECESS cuando esté disponible + texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura	CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Piso	Texto			CM
Letra	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			CM
Teléfono	Texto			CM
Dirección Web/Correo Electrónico	Texto	Libre	Se incluirá la dirección Web sólo si contiene información de interés para el usuario	R
DATOS DEL USUARIO/PACIENTE				
Nombre	Texto	Dato que figure en BD de la TSI de la CA		CM
Primer Apellido	Texto			CM
Segundo Apellido	Texto			CM
Fecha de nacimiento	dd/mm/aaaa			CM
Sexo	Texto		H/M	CM
DNI/T.Residencia/Pasaporte	Texto			R
NASS	Texto			CM
CIP de la C. Autónoma	Texto			CM
Código SNS	Texto			R
CIP Europeo			Se reserva este espacio en previsión de que en el futuro, exista un código europeo/internacional de identificación	R
Nº Historia Clínica	Texto	Libre		CM
Domicilio				
Tipo de vía	Texto	Dato que figure en la BD de TSI de la CA		CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Piso	Texto			CM
Letra	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			
Teléfono	Texto			R
Persona de Referencia	Texto	Libre (nombre + 2 apellidos)	Se trata de la persona que representa los intereses del paciente.	R
Teléfono de Referencia	Texto	Libre		R
DATOS DE SALUD				
Antecedentes	Texto	Libre	Se recomienda su clasificación en subapartados	CM
Enfermedades familiares hereditarias Enfermedades previas Antecedentes neonatales, obstétricos y quirúrgicos Alergias Hábitos tóxicos Actuaciones preventivas (1) Medicación previa Situación funcional (2) Antecedentes sociales y profesionales			(1) Vacunaciones infantiles, del adulto, quimioprofilaxis realizadas, etc (2) Se refiere a la valoración del impacto funcional de los problemas activos o enfermedades y se podrán utilizar una o varias escalas (Escalas de dependencia, clasificación funcional de la insuficiencia cardíaca, valoraciones del grado de demencia, escalas de calidad de vida, etc.)	R
Resumen pruebas complementarias	Texto	Libre		CM
Laboratorio Imagen Otras pruebas	Texto	Libre	Se recomienda la clasificación en subapartados	R
Resumen de Episodios Atendidos	Texto + código	Libre Código CIE 9 MC/CIE 10/CIAP2 definida/SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[4]
Evolución y comentarios	Texto	Libre	Se pueden realizar comentarios del seguimiento evolutivo. También es el lugar adecuado para describir reacciones adversas a fármacos utilizados o describir complicaciones evolutivas de la/las enfermedades, realizar valoraciones diagnósticas o comentarios adicionales	CM
Diagnósticos	Texto + código	Libre Código CIE 9 MC/CIE 10/CIAP2 definida/SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Procedimientos	Texto + código	Libre Código CIE 9 MC/CIE 10/CIAP2 definida/SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Tratamiento	Texto	Libre	Se refiera al último tratamiento que esté activo	CM
Recomendaciones	Texto	Libre	Se trata de recomendaciones terapéuticas que no incluyen fármacos (oxigenoterapia, dieta, reposo o limitaciones de esfuerzo físico, etc.)	R
Fármacos	Texto +código	Libre (Especialidad+principio activo+ dosis/unidad+ nº unidades/dosis+ intervalo de dosis+ vía administración+ duración) nomenclator oficial MSPS (código nacional)/Snomed-CT	Prescripciones activas al final del período de seguimiento En la medida en que la implantación de las aplicaciones informáticas de HCE, que incluyen módulos de prescripción lo permitan, el texto libre, será reemplazado progresivamente por el vocabulario del catálogo de medicamentos autorizados (Nomenclator Oficial/ Snomed-CT)	CM R
Otras Recomendaciones	Texto	Libre	Se refiere a los planes de actuación previstos que no son propiamente medidas terapéuticas. Por ejemplo: fecha de próxima cita, conveniencia de una nueva revisión, petición de pruebas, etc…	R

ANEXO V

CONJUNTO DE DATOS DEL INFORME DE RESULTADOS DE PRUEBAS DE LABORATORIO

Variable	Formato	Valores	Aclaraciones	CM/R[5]
DATOS DEL DOCUMENTO				
Tipo de documento	Texto	Informe de Resultados de Pruebas de Laboratorio		CM
Fecha de firma	dd/mm/aaaa	Libre	Es común a ambos pies de firma del informe	CM
Nombre Responsable 1	Texto	Libre (nombre+2 apellidos)	Es parte del primer pie de firma del informe	CM
Categoría profesional 1	Texto	Médico Residente Facultativo Especialista de Área Farmacéutico Residente Biólogo Residente Jefe de Sección Jefe de Servicio Texto libre		CM
Nombre Responsable 2	Texto	Libre (nombre+2 apellidos)	Es parte del segundo pie de firma, que suele supervisar al primer firmante	CM
Categoría profesional 2	Texto	Facultativo Especialista de Área Jefe de Sección Jefe de Servicio Texto libre		CM
Servicio	Texto	Análisis Clínicos Anatomía Patológica Bioquímica Clínica Hematología y Hemoterapia Genética Inmunología Microbiología y parasitología	RD 1277/2003 y normativa en vigor en cada momento	CM
Unidad	Texto	Libre		CM

[5] Se puede clasificar cada campo según se considere que su presencia es esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debe formar parte del conjunto mínimo del SNS (CM) o por el contrario es aconsejable su presencia pero no imprescindible como parte del conjunto mínimo de datos (R)

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[5]
DATOS DE LA INSTITUCIÓN EMISORA				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL .Gerencia Regional de Salud de Castilla y León. DdS-GC. Departament de Salut de la Generalitat de Catalunya SES. Servicio Extremeño de Salud. SERGAS. Servizo Galego de Saúde. INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears. RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud SNS-O. Servicio Navarro de Salud-OSASUNBIDEA. Agència Valenciana de Salut OSAKIDETZA-Servicio Vasco de Salud.		CM
Denominación del provisor de servicios	Texto +Logo	Libre		R
Denominación del Centro	Texto + Logo	CNH y posteriormente RECESS cuando esté disponible+texto Libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura	CM
Dirección Del Centro				
Tipo de vía	Texto	CNH y posteriormente RECESS cuando esté disponible+texto libre		CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			CM
Teléfono	Texto			CM
Dirección Web/Correo electrónico	Texto	Libre	Se incluirá la dirección Web sólo si contiene información de interés para el usuario	R
DATOS DEL PACIENTE				
Nombre	Texto	Dato que figure en la BD de la TSI de la CA		CM
Primer Apellido	Texto			CM
Segundo Apellido	Texto			CM
Fecha nacimiento	dd/mm/aaaa			CM
Sexo	Texto		H/M	CM
DNI/T. Residencia/Pasaporte	Texto			R
NASS	Texto			CM
CIP de C Autónoma	Texto			CM
Código SNS	Texto			R
CIP Europeo	Texto		Se reserva este espacio en previsión de que, en el futuro, exista un código europeo/internacional de identificación.	R
Nº Historia Clínica	Texto	Libre		CM
Nº Cama / Nº Consulta	Texto	Libre		R
DATOS DEL SOLICITANTE				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL .Gerencia Regional de Salud de Castilla y León. DdS-GC. Departament de Salut de la Generalitat de Catalunya SES. Servicio Extremeño de Salud. SERGAS. Servizo Galego de Saúde INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears.		CM

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[5]
		RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud SNS-O. Servicio Navarro de Salud-OSASUNBIDEA. Agència Valenciana de Salut OSAKIDETZA-Servicio Vasco de Salud.		
Denominación del provisor de servicios	Texto +Logo	Libre		R
Denominación del Centro	Texto + Logo	CNH[6] y posteriormente RECESS[7] cuando esté disponible+texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura	CM
Servicio	Texto	Según normativa en vigor en cada momento	Actualmente clasificación de Servicios del CMBD/SIFCO	CM
Unidad	Texto	Libre		CM
Nombre del solicitante	Texto	Libre (nombre+2 apellidos)		CM
Categoría profesional	Texto	Médico Residente Facultativo Especialista de Área Jefe de Sección Jefe de Servicio Médico de Familia Pediatra de AP Texto libre		CM
DATOS DEL PROCESO ASISTENCIAL				
DATOS DE LA MUESTRA				
Fecha de toma de muestra	dd/mm/aaaa	Libre		CM
Número de muestra	Texto	Libre		CM
Tipo de muestra	Texto + Código	Libre Bioquímica: LOINC Hematología: LOINC Inmunología: LOINC Genética: LOINC Microbiología: Vocabulario local a partir de LOINC A. Patológica: Snomed-CT		CM R
Grupo de determinación	Texto	Bioquímica general Sistemático orina Hormonas Marcadores tumorales Niveles de fármacos y tóxicos Gasometría Hematología Hemostasia (Coagulación) Hemoterapia Hematología-Coagulación: Pruebas especiales Inmunología - Alergia Microbiología Genética Anatomía Patológica - Biopsias Anatomía Patológica – Citologías	<u>Bioquímica General</u> • *Metabolitos (ej. glucosa, urea, creatinina, etc.)* • *Enzimas (AST, ALT, LDH, etc)* • *Iones (Na, K, Cl, Ca, P, Mg, etc)* • *Otras proteínas (Marcadores cardiacos, etc.)* • *Líquidos Biológicos* • *Espermiogramas y estudios semen* • *Estudios en heces* • *Elementos traza (Cu, Se, etc)* • *Proteínas (Transferrina, Ceruloplasmina, Complemento,etc.)* • *Electroforesis de proteínas* • *Inmunofijacion / Inmunosubstracción* • *Inmunoglobulinas y Cadenas ligeras* <u>Sistemático orina</u> • *Urianálisis* • *Sedimento* <u>Hormonas</u> • *Hormonas* • *Vitaminas* • *Otros inmunoensayos relacionados (ej PAPPA)* <u>Marcadores tumorales</u> • *Marcadores tumorales séricos* • *Patología Molecular enfermedades neoplásicas hematológicas*	CM

[6] CNH: Catálogo Nacional de Hospitales
[7] RECESS: Registro General de Establecimientos, Centros y Servicios Sanitarios del MSPS.

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[5]
			• *Patología Molecular enfermedades neoplásicas, tumores sólidos* *Niveles de fármacos y tóxicos* • *Monitorización de Fármacos* • *Detección Drogas de abuso* • *Detección de otros tóxicos (metales pesados, tóxicos laborales, etc.)* • *Farmacogenómica* *Gasometría* *Hematología* • Hematimetría manual y automatizada (incluye el Hemograma , el diferencial leucocitario automatizado y manual, la morfología eritrocitaria, la VSG , la viscosidad plasmática, etc..) *Hemostasia (coagulación)* • Pruebas de Hemostasia básicas (Tiempo de Protrombina, Tiempo de Tromboplastina Parcial Activada y Fibrinógeno) *Hemoterapia* • *Estudios de Inmunohematología (detección de Anticuerpos irregulares)* • *Pruebas de compatibilidad transfusional* *Hematología-Coagulación: Pruebas especiales* • *Citoquímica, Citometría, Citogenética y Biología Molecular de sangre periférica y médula ósea (incluye todos los marcadores diagnósticos)* • *Aspirado medular y Biopsia de Médula Ósea (incluye todos los estudios de médula ósea)* • *Estudios de Eritropatología* • *Pruebas para estudio de Diátesis Hemorrágicas* • *Pruebas para estudio de Trombosis* • *Biología Molecular de alteraciones congénitas o adquiridas de la Hemostasia* *Inmunología - Alergia* • *Autoinmunidad* • *Inmunoquímica* • *Histocompatibilidad* • *Inmunobiología* *Microbiología* • *Bacteriología* • *Virología* • *Parasitología* • *Micología* • *Serología infecciosa* • *Biología molecular infecciosa* *Genética* • *Citogenética* • *Patología/Genética molecular* *Anatomía Patológica – Biopsias* • *Biopsias y piezas quirúrgicas* • *Inmunohistoquímica* • *Anatomía Patológica molecular* • *Microscopía electrónica* • *Citometría de flujo*	

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[5]
			Anatomía Patológica – Citologías • *Citologías y PAAF* • *Inmunocitoquímica* • *Anatomía Patológica molecular* • *Microscopía electrónica* • *Colometría de flujo*	
Modelo TIPO A			Este modelo puede recoger todos aquellos resultados de pruebas diagnósticas que se expresan con una denominación de determinación, un resultado (generalmente expresado en cifras), las unidades de medida utilizadas y un rango de valores de referencia que se toman como estándar de normalidad. Ej. Bioquímica sangre.	
Determinación	Texto	Libre		CM
Resultado	Texto	Libre		CM
Unidades	Texto	Libre		CM
Rango	Texto	Libre		CM
Comentarios	Texto	Libre		R
Modelo TIPO B			Este modelo puede recoger todos aquellos resultados de pruebas diagnósticas que requieran una descripción y una conclusión en texto libre. Ej. Estudio de médula ósea.	
Determinación	Texto	Libre		CM
Técnica	Texto			CM
Descripción	Texto	Libre		CM
Conclusión	Texto+ Código	Libre SNOMED		CM R

ANEXO VI

CONJUNTO DE DATOS DEL INFORME DE RESULTADOS DE PRUEBAS DE IMAGEN

Variable	Formato	Valores	Aclaraciones	CM/R[8]
DATOS DEL DOCUMENTO				
Tipo de documento	Texto	Informe de resultados de pruebas de imagen		CM
Fecha de firma	dd/mm/aaaa	Libre	Es común a ambos pies de firma del informe	CM
Nombre Responsable 1	Texto	Libre (nombre+2 apellidos)	Es parte del primer pie de firma del informe	CM
Categoría profesional 1	Texto	Médico Residente Facultativo Especialista de Área Jefe de Sección Jefe de Servicio		CM
Nombre Responsable 2	Texto	Libre (nombre+2 apellidos)	Es parte del segundo pie de firma, que suele supervisar al primer firmante	CM
Categoría profesional 2	Texto	Facultativo Especialista de Área Jefe de Sección Jefe de Servicio		CM
Servicio	Texto	Radiodiagnóstico Medicina Nuclear		CM
Unidad	Texto	Libre		CM

[8] Se puede clasificar cada campo según se considere que su presencia es esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debe formar parte del conjunto mínimo del SNS (CM) o por el contrario es aconsejable su presencia pero no imprescindible como parte del conjunto mínimo de datos (R)

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[8]
DATOS DE LA INSTITUCIÓN EMISORA				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL .Gerencia Regional de Salud de Castilla y León. DdS-GC. Departament de Salut de la Generalitat de Catalunya SES. Servicio Extremeño de Salud. SERGAS. Servizo Galego de Saúde. INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears. RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud SNS-O. Servicio Navarro de Salud-OSASUNBIDEA. Agència Valenciana de Salut OSAKIDETZA-Servicio Vasco de Salud.		CM
Denominación del provisor de servicios	Texto +Logo	Libre		R
Denominación del Centro	Texto + Logo	CNH y posteriormente RECESS cuando esté disponible+texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura	CM
Dirección Del Centro				
Tipo de vía	Texto	CNH y posteriormente RECESS cuando esté disponible+texto libre		CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			CM
Teléfono	Texto			CM
Dirección Web/Correo electrónico	Texto	Libre	Se incluirá la dirección Web sólo si contiene información de interés para el usuario	R
DATOS DEL PACIENTE				
Nombre	Texto	Dato que figure en la BD de la TSI de la CA		CM
Primer Apellido	Texto			CM
Segundo Apellido	Texto			CM
Fecha nacimiento	dd/mm/aaaa			CM
Sexo	Texto		H/M	CM
DNI/T. Residencia/Pasaporte	Texto			R
NASS	Texto			CM
CIP de C Autónoma	Texto			CM
Código SNS	Texto			R
CIP Europeo	Texto		Se reserva este espacio en previsión de que, en el futuro, exista un código europeo/internacional de identificación	R
Nº Historia Clínica	Texto	Libre		CM
Nº Cama / Nº Consulta	Texto	Libre		R
DATOS DEL SOLICITANTE				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha.		CM

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[8]
		SACyL .Gerencia Regional de Salud de Castilla y León. DdS-GC. Departament de Salut de la Generalitat de Catalunya SES. Servicio Extremeño de Salud. SERGAS. Servizo Galego de Saúde. INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears. RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud SNS-O. Servicio Navarro de Salud-OSASUNBIDEA. Agència Valenciana de Salut OSAKIDETZA-Servicio Vasco de Salud.		
Denominación del provisor de servicios	Texto +Logo	Libre		R
Denominación del Centro	Texto + Logo	CNH[9] y posteriormente RECESS[10])cuando esté disponible+texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura	CM
Servicio	Texto	Según normativa en vigor en cada momento	Actualmente clasificación de Servicios del CMBD/SIFCO	CM
Unidad	Texto	Libre		CM
Nombre del solicitante	Texto	Libre (nombre+2 apellidos)		CM
Categoría profesional	Texto	Médico Residente Facultativo Especialista de Área Jefe de Sección Jefe de Servicio Médico de Familia Facultativo Pediatra de AP Texto Libre		CM
DATOS DEL PROCESO ASISTENCIAL				
Información Clínica	Texto	Libre	Reflejará el mismo contenido que el volante de petición de la exploración. Es el lugar para detallar los datos clínicos que justifican la realización de la prueba y establecen las sospechas diagnósticas	CM
Exploración	Texto + Código (cadena numérica+ cadena de texto)	Libre Catálogo SERAM en vigor Catálogo SEMN en vigor		CM R
Fecha de Exploración	dd/mm/aaaa	Libre		CM
Descripción de la exploración	Texto	Libre	Es una descripción detallada de la exploración realizada, en la que podrán concretarse además: . Prioridad (normal, urgente) . Medios de contraste (tipo, dosis y velocidad de inyección . Reacciones adversas . Otros incidentes (falta de colaboración, ansiedad, claustrofobia…) y abordaje de los mismos. . Limitaciones técnicas . Exploración con la que se compara y fecha de la misma	R
Hallazgos	Texto	Libre	Es una descripción detallada de los hallazgos, en la que podrán concretarse además: . Hallazgos negativos	CM

[9] CNH: Catálogo Nacional de Hospitales
[10] RECESS: Registro General de Establecimientos, Centros y Servicios Sanitarios del MSPS.

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[8]
			. Comparación con estudios previos . Limitaciones diagnósticas	
Diagnóstico	Texto + Código	Libre Cadena de texto (Nombre del catálogo utilizado) + Código asignado		CM R
Recomendaciones	Texto	Libre	Es el lugar para recoger: Cuidados o tratamientos que se deben seguir después de la realización de la exploración diagnóstica o intervencionista. Indicación de otras exploraciones que se deben realizar para completar el estudio del paciente o el plazo en el que se debe realizar un control de la exploración	CM

ANEXO VII

CONJUNTO DE DATOS DEL INFORME DE CUIDADOS DE ENFERMERÍA

Variable	Formato	Valores	Aclaraciones	CM/R [11]
DATOS DEL DOCUMENTO				
Tipo de documento	Texto	Informe de Cuidados de Enfermería		CM
Fecha de firma	dd/mm/aaaa	Libre	Es común a ambos pies de firma del informe	CM
Fecha Valoración de Enfermería	dd/mm/aaaa	Libre		CM
Fecha Alta de Enfermería/Fecha de Derivación Enfermera	dd/mm/aaaa	Libre		CM
Enfermera Responsable 1	Texto	Libre (nombre+2 apellidos)	Es parte del primer pie de firma del informe	CM
Categoría profesional Enfermera Responsable 1	Texto	Enfermera Enfermera Especialista Enfermera Residente (EIR)		CM
Enfermera Responsable 2	Texto	Libre (nombre+2 apellidos)	Es parte del segundo pie de firma, que suele supervisar al primer firmante	CM
Categoría profesional Enfermera Responsable 2	Texto	Enfermera Enfermera Especialista		CM
Dispositivo Asistencial	Texto	Centro de Salud Hospital Urgencias Hospitalarias Urgencias Extrahospitalarias Centro Sociosanitario Otros		CM
DATOS DE LA INSTITUCIÓN EMISORA				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL .Gerencia Regional de Salud de Castilla y León. DdS-GC. Departament de Salut de la Generalitat de Catalunya SES. Servicio Extremeño de Salud. SERGAS.Servizo Galego de Saúde. INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears. RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud SNS-O. Servicio Navarro de Salud-		CM

[11] Se puede clasificar cada campo según se considere que su presencia es esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debe formar parte del conjunto mínimo del SNS (CM) o por el contrario es aconsejable su presencia pero no imprescindible como parte del conjunto mínimo de datos (R)

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R [11]
		OSASUNBIDEA. Agència Valenciana de Salut OSAKIDETZA-Servicio Vasco de Salud.		
Denominación del provisor de servicios	Texto +Logo	Libre		R
Denominación del Centro	Texto + Logo	CNH[12] para Centros de Atención Especializada, Inventario para Centros de Primaria y posteriormente RECESS[13] cuando esté disponible + texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura	CM
Dirección Del Centro				
Tipo de vía	Texto	CNH y posteriormente RECESS cuando esté disponible+texto libre		CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			CM
Teléfono	Texto			CM
Dirección Web/Correo electrónico	Texto	Libre	Se incluirá la dirección Web sólo si contiene información de interés para el usuario	R
DATOS DEL PACIENTE				
Nombre	Texto	Dato que figure en la BD de la TSI de la CA		CM
Primer Apellido	Texto			CM
Segundo Apellido	Texto			CM
Fecha nacimiento	dd/mm/aaaa			CM
Sexo	Texto		H/M	CM
DNI/T.Residencia/Pasaporte	Texto			R
NASS	Texto			CM
CIP de C Autónoma	Texto			CM
Código SNS	Texto			R
CIP Europeo	Texto		Se reserva este espacio en previsión de que, en el futuro, exista un código europeo/internacional de identificación.	R
Nº Historia Clínica	Texto	Libre		CM
Domicilio				
Tipo de vía	Texto	Dato que figure en la BD de la TSI de la CA		CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Piso	Texto			CM
Letra	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
Teléfono	Texto	Dato que figure en la BD de la TSI de la CA+texto libre	Existirá texto libre para añadir un segundo número de teléfono	R
Persona de Referencia	Texto	Libre (nombre + 2 apellidos)	Se trata de la persona que representa los intereses del paciente.	CM
Teléfono de Referencia	Texto	Libre		CM
DATOS DEL PROCESO ASISTENCIAL				
Causas que generan la actuación enfermera	Texto	Libre		CM
Motivo de Alta/Derivación Enfermera	Texto	Ingreso Traslado a domicilio Traslado de Servicio Traslado a centro hospitalario Traslado a un centro sociosanitario Alta voluntaria Fallecimiento Otros		CM

[12] CNH: Catálogo Nacional de Hospitales
[13] RECESS: Registro General de Establecimientos, Centros y Servicios Sanitarios del MSPS.

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R [11]
Antecedentes y entorno	Texto	Libre	Destacar solamente la información relevante	CM
Enfermedades Previas Intervenciones quirúrgicas Tratamientos farmacológicos Alergias Actuaciones preventivas (1) Factores personales, familiares, sociales, culturales y laborales destacables (2).	Texto	Libre	(1) Vacunaciones y su estado (2) El conjunto de factores reseñados se refiere a aquellos elementos (personales, familiares, sociales o profesionales) que, formando parte de su entorno, pueden influir o condicionar la evolución de su estado de salud. Tienen cabida también aquellos acontecimientos puntuales (pérdida de familiar, evento laboral,...) que puedan influir en su respuesta ante diferentes situaciones de salud.	R
Diagnósticos Enfermeros resueltos	Texto + código	Literal NANDA +Código NANDA	Se trata de destacar aquellos diagnósticos, ya resueltos, que puedan resultar de interés para prever posteriores apariciones	CM R
Protocolos asistenciales en los que está incluido	Texto	Libre	Tienen cabida todos los procesos asistenciales y programas de salud en los que se encuentre incluido, tanto programas preventivos como de seguimiento, rehabilitación o educación sanitaria entre otros. Así como la relación de problemas interdependientes y/o de colaboración si fuera el caso.	CM
Valoración activa	Texto	Libre		CM
Modelo de referencia utilizado Resultados destacables	Texto	Libre	Deberá reflejarse la información relativa a la valoración enfermera más reciente. Se recomienda especificar otras escalas o tests aplicados y ajenos al modelo utilizado en la valoración general.	CM CM
Diagnósticos Enfermeros activos	Texto + código	Literal NANDA + Código NANDA	Aquellos diagnósticos presentes en el momento de la elaboración del informe, tanto reales como potenciales	CM R
Resultados de Enfermería	Texto + código	Literal NOC + Código NOC	Aquellos resultados seleccionados para identificar la evolución del paciente, como resultado de las intervenciones planificadas	CM R
Intervenciones de Enfermería	Texto + código	Literal NIC +Código NIC	Las intervenciones que se están llevando a cabo en el momento de elaboración del informe	CM R
Cuidador principal	Texto	Libre (nombre + 2 apellidos) + Vinculación con el usuario	Deberá indicarse tanto el nombre como la relación que tiene con él (familiar, cuidador externo…)	CM R
Información complementaria/Observaciones	Texto	Libre	Puede incluirse información relativa a la presencia de catéteres, prótesis, dietas especiales, así como destacar algún aspecto de especial relevancia relativo a la aplicación de las intervenciones activas.	R

ANEXO VIII

CONJUNTO DE DATOS DE LA HISTORIA CLÍNICA RESUMIDA

Variable	Formato	Valores	Aclaraciones	CM/R[14]	Volcado de Datos [15]	Acceso[16]
DATOS DEL DOCUMENTO						
Tipo de documento	Texto	Historia Clínica Resumida		CM	A	P/C
Fecha de creación	dd/mm/aaaa	Libre		CM	A	P/C
Fecha de última actualización	dd/mm/aaaa	Libre	La fecha en la que fue modificado alguno de los componentes del registro por última vez	CM	A	P/C

[14] Se puede clasificar cada campo según se considere que su presencia es esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debe formar parte del conjunto mínimo del SNS (CM), o por el contrario es aconsejable su presencia, pero no imprescindible como parte del conjunto mínimo de datos (R).
[15] Los datos de los campos de la Historia Clínica Resumida deben alimentarse de forma automática **A**, a partir de la historia de salud digital, excepto un número muy reducido de ellos que tendrá que alimentar manualmente **M** el profesional, en aquellos casos en que éste lo considere conveniente.
[16] El campo puede estar accesible, según la naturaleza de su contenido (anotaciones subjetivas o datos objetivos), a los profesionales P o al ciudadano C

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[14]	Volcado de Datos [15]	Acceso[16]
DATOS DE LA INSTITUCIÓN EMISORA						
Denominación del Servicio de Salud	Texto + logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL .Gerencia Regional de Salud de Castilla y León. DdS-GC. Departament de Salut de la Generalitat de Catalunya SES. Servicio Extremeño de Salud. SERGAS.Servizo Galego de Saúde INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears. RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud SNS-O. Servicio Navarro de Salud-OSASUNBIDEA. Agència Valenciana de Salut OSAKIDETZA-Servicio Vasco de Salud.		CM	A	P/C
Denominación del provisor de servicios	Texto+logo	Libre		R		
DATOS DEL USUARIO/PACIENTE						
Nombre	Texto	Dato que figure en BD de TSI de la CA		CM	A	P/C
Primer Apellido	Texto			CM	A	P/C
Segundo Apellido	Texto			CM	A	P/C
Fecha de nacimiento	dd/mm/aaaa			CM	A	P/C
Sexo	Texto		H/M	CM	A	P/C
DNI/T.Residencia/Pasaporte	Texto			R	A	P/C
NASS	Texto			CM	A	P/C
CIP de C. Autónoma	Texto			CM	A	P/C
Código SNS	Texto			R	A	P/C
CIP Europeo			Se reserva este espacio en previsión de que en el futuro, exista un código europeo/internacional de identificación.	R	A	P/C
Nº Historia Clínica	Texto	Libre		CM	A	P/C
Tipo de vía	Texto	Dato que figure en la BD de TSI de la CA		CM	A	P/C
Nombre de la vía	Texto			CM	A	P/C
Número de la vía	Texto			CM	A	P/C
Piso	Texto			CM	A	P/C
Letra	Texto			CM	A	P/C
Código Postal	Texto			CM	A	P/C
Municipio	Texto			CM	A	P/C
Provincia	Texto			CM	A	P/C
Teléfono	Texto			R	A	P/C
Persona de referencia	Texto	Libre (nombre + 2 apellidos)	Se trata de la persona que representa los intereses del paciente.	R	A/M	P/C
Teléfono de referencia	Texto	Libre		R	A/M	P/C
Cuidador Principal	Texto	Libre (nombre + 2 apellidos)		R	A/M	P/C
DATOS DE SALUD						
Existe información reservada por decisión del paciente	Botón s/n	SI NO	Este campo informa al profesional de que existe algún dato clínico que no figura en la HC por decisión del propio paciente.	CM	A	P/C
Existe documento de instrucciones previas	Botón s/n	SI NO	Informa al profesional de que existe este documento que esta disponible en el Registro de Últimas Voluntades.	CM	A/M	P/C

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[14]	Volcado de Datos [15]	Acceso[16]
Está incluido en protocolo de investigación clínica	Botón s/n	SI NO	Informa de la inclusión en un protocolo de investigación en la fecha de última actualización.	R	M	P/C
Alergias	Texto	Libre		CM	A	P/C
Vacunaciones	Texto	Libre		CM	A	P/C
Problemas Resueltos, Cerrados o Inactivos	Texto	Fecha + Texto Libre	Se especificará la fecha de cierre y el motivo	R	A	P/C
Problemas y Episodios Activos	Texto + Código	Fecha + Texto libre Sistema de Codificación CIE 9 MC/CIE 10/CIAP 2 Definida/SNOMED-CT	Los que figuren en la historia a la fecha de última actualización. Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS	CM R	A	P/C
Tratamiento	Texto	Libre		CM		P/C
Recomendaciones	Texto	Libre	Se trata de recomendaciones terapéuticas que no incluyen fármacos (oxigenoterapia, dieta, limitaciones de esfuerzo físico, etc.)	CM	A	P/C
Fármacos	Texto +código	Libre (Especialidad+principio activo+ dosis/unidad+ nº unidades/dosis+ intervalo de dosis+ via administración+ duración) nomenclator oficial MSPS (código nacional)/Snomed-CT	Prescripciones activas a la fecha de actualización. En la medida en que la implantación de las aplicaciones informáticas de HCE, que incluyen módulos de prescripción lo permitan, el texto libre, será reemplazado progresivamente por el vocabulario del catálogo de medicamentos autorizados (Nomenclator Oficial/ Snomed-CT)	CM	A	P/C
Diagnósticos Enfermeros activos	Texto + Código	Literal NANDA +Código NANDA	Los que figuren en la historia a la fecha de última actualización	CM R	A	P/C
Resultados de Enfermería	Texto + Código	Literal NOC +Código NOC	Aquellos resultados seleccionados para identificar la evolución del paciente, como resultado de las intervenciones planificadas Los que figuren en la historia a la fecha de última actualización	CM R	A	P/C
Intervenciones de Enfermería	Texto + código	Literal NIC +Código NIC	Los que figuren en la historia a la fecha de última actualización	CM R	A	P/C
ALERTAS	Texto	Libre	Su contenido deben ser advertencias clave de carácter objetivo que por su especial trascendencia deban ser resaltadas para ser tenidas en cuenta por cualquier profesional que deba prestar atención (Ej: Angioedema desencadenado por IECAS, Dispositivo IV con reservorio)	CM	M	P/C
Observaciones Subjetivas del Profesional	Texto	Libre	La única justificación de este campo es recoger valoraciones del profesional, siempre que sean de auténtico interés para el manejo de los problemas de salud por otro profesional. Sólo deberán ser reseñadas aquellas observaciones que sean encuadrables en algunos de los siguientes apartados: • VALORACIONES SOBRE HIPÓTESIS DIAGNÓSTICAS NO DEMOSTRADAS • SOSPECHA ACERCA DE INCUMPLIMIENTOS TERAPÉUTICOS • SOSPECHA DE TRATAMIENTOS NO DECLARADOS	R	M	P

cve: BOE-A-2010-14199

Variable	Formato	Valores	Aclaraciones	CM/R[14]	Volcado de Datos [15]	Acceso[16]
			• SOSPECHA DE HÁBITOS NO RECONOCIDOS • SOSPECHA DE HABER SIDO VÍCTIMA DE MALOS TRATOS • COMPORTAMIENTOS INSÓLITOS			

ANEXO IX

LISTADO ALFABÉTICO DE ABREVIATURAS EMPLEADAS

Abreviatura empleada	Significado
BD TSI	Base de datos de tarjeta sanitaria individual
CIAP 2	Clasificación internacional en atención primaria. Versión 2
CIE9-MC	Clasificación internacional de enfermedades. Modificación clínica
CM	Conjunto mínimo
CMBD	Registro de Altas de los Hospitales Generales del Sistema Nacional de Salud
CNH	Catálogo Nacional de Hospitales
LOINC	Logical observation identifiers names and codes
MSPS	Ministerio de Sanidad y Política Social
NANDA	North American Nursing Diagnosis Association
NIC	Nursing Interventions Classification
NOC	Nursing Outcomes Classification
R	Recomendable
RECESS	Registro General de Establecimientos, Centros y Servicios Sanitarios del Ministerio de Sanidad y Política Social
SERAM	Sociedad Española de Radiología Médica
SEMN	Sociedad Española de Medicina Nuclear
SIFCO	Sistema de Información del Fondo de Cohesión del SNS
SNOMED-CT	Systematized Nomenclature of Medicine-Clinical Terms

cve: BOE-A-2010-14199