La protección de datos relativos a la salud y la historia clínica en la normativa española y europea

Data Protection Health and Medical History in Spanish and European Regulations

Ana Isabel Berrocal Lanzarot
Profesora Contratada Doctora de Derecho Civil. UCM

Resumen

La Constitución Española en su artículo 18, además de, consagrar como derecho fundamental el derecho a la intimidad personal y familiar, hace referencia, asimismo, en su apartado cuarto al derecho de protección de datos de carácter personal, cuando alude al uso de la informática en relación con el derecho al honor y la intimidad personal de los ciudadanos. Dentro de este derecho a la protección de datos de carácter personal ocupa un lugar destacado los datos relativos a la salud; y dentro de éstos, los datos genéticos, como datos sensibles, y que son objeto de una protección reforzada. Su uso, acceso, y cesión a terceros requieren el consentimiento expreso del interesado, salvo supuestos de urgencia o para realizar estudios epidemiológicos según los términos establecidos en la legislación sanitaria estatal y autonómica.

En todo caso, las instituciones y centros sanitarios públicos y privados y los profesionales correspondientes pueden proceder al tratamiento de los datos personales relativos a la salud de las personas que acudan ellos, y sólo en el ámbito relativo al ejercicio de sus funciones. Los documentos referidos a los procesos asistenciales de cada paciente como la historia clínica, en la que se incorporará la información que, se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente resulta, igualmente, necesario garantizar su seguridad, su correcta conservación y la recuperación de la información que se contiene en ella, pudiendo acceder sólo los profesionales asistenciales del centro que, realizan el diagnóstico o el tratamiento del paciente, como instrumento fundamental para su adecuada asistencia, e igualmente, el personal de administración y gestión de los centros sanitarios en lo relacionado con sus propias funciones. Sobre tales bases, el presente estudio se va a centrar en el análisis de los datos relativos a la salud, y en

Fecha de recepción del artículo
Octubre de 2011
Fecha de aceptación del artículo
Octubre de 2011

especial, en los datos genéticos, y al uso y acceso de la historia clínica tanto en la normativa general relativa a la protección de datos como la autonómica y europea existente en relación con la materia; y, de forma más específica en la legislación sanitaria.

Palabras claves

Datos de la salud, datos genéticos, datos personales, consentimiento, acceso, uso, cesión, historia clínica, diagnóstico, tratamiento, profesionales sanitarios.

Summary

The Spanish Constitution in his article 18, besides, to dedicate as fundamental right the right to the personal and familiar intimacy, refers, likewise, in his fourth paragraph to the protection right of information of personal character, when it alludes to the use of the computer science in relation with the right to the honor and the personal intimacy of the citizens. Inside this right to the protection of information of personal character an outstanding place occupies the information relative to the health; and inside these, the genetic information, as sensitive information, and that are an object of a reinforced protection. His use, access, and transfer to third parties need the express assent of the interested party, except suppositions of urgency or to realize epidemiological studies according to the terms established in the sanitary state and autonomous legislation.

In any case, the institutions and sanitary public and private centers and the corresponding professionals can proceed to the treatment of the personal information relative to the health of the persons who come they, and only in the area relative to the exercise of his functions. The documents referred to the welfare processes of every patient as the clinical history, in which there will join the information that, is considered to be transcendental for the knowledge veracious and updated of the bill of health of the patient it turns out, equally, necessary to guarantee his safety, his correct conservation and the recovery of the information that controls itself in her, being able to accede only the welfare professionals of the center that, they realize the diagnosis or the treatment of the patient, as fundamental instrument for his suitable assistance, and equally, the personnel of administration and management of the sanitary centers in the related thing to his own functions. On such bases, the present study is going to centre on the analysis of the information relative to the health, and especially, on the genetic information, and to the use and access of the clinical history so much on the general regulation relative to the protection of information as autonomous and existing European on relation with the matter; and, of more specific form in the sanitary legislation.

Key words

Information of the health, genetic information, personal information, assent, access, use, transfer, clinical history, diagnosis, treatment, sanitary professionals..

Sumario

I. Consideraciones previas. Normativa nacional y europea sobre tratamiento y protección de datos personales.

II. Los datos de la salud como categoría de datos de carácter personal.

III. Confidencialidad y medidas de seguridad en el tratamiento de los datos de la salud.

IV. Datos genéticos como datos de la salud.

I. Consideraciones previas. Normativa nacional y europea sobre tratamiento y protección de datos personales

En el artículo 18.1 de la Constitución Española se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen, cuya protección frente a intromisiones ilegítimas tiene su plasmación jurídica en la Ley Orgánica 1/1982, de 5 de mayo de Protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Asimismo, en su apartado 4 se señala 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». Si en un principio, la protección de datos venía siendo considerada como parte del derecho a la intimidad y privacidad, a través del concepto de «derecho a la autodeterminación informativa». Así, el Tribunal Constitucional, en varias sentencias, relacionaba el derecho a la protección de datos de carácter personal con el derecho a la intimidad, y, para ello proclamaba el reconocimiento global de este derecho en cuanto «abarque su defensa frente a las intromisiones que por cualquier medio pueda realizarse en ese ámbito reservado de vida». Con posterioridad, el derecho fundamental de protección de datos fue considerado como un derecho autónomo e independiente del derecho a la intimidad, superando así el concepto de «derecho de autodeterminación informativa». Lo que tuvo lugar con la sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. De forma que, el derecho de protección de datos tras la citada resolución, adquirió un ámbito de aplicación más amplio que, el del derecho a la intimidad[1]. En este contexto, desarrollando el citado apartado 4 del artículo 18, se publicó primero la Ley Orgánica 5/1992, de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de carácter personal, en cuya Exposición de Motivos se establecía que «su finalidad es hacer frente a los riesgos que para los derechos fundamentales puede suponer el acopio y tratamiento de datos por medios informáticos». Partiendo de esta base, su articulado se desarrollaba estableciendo, en primer lugar unas disposiciones generales relativas al objeto, ámbito de aplicación y definiciones; para luego referirse a los principios de la protección de datos, los derechos de las personas, las disposiciones sectoriales, distinguiendo los ficheros de titularidad pública y privada, el movimiento internacional de datos, la Agencia de Protección de Datos, para terminar con las infracciones y sanciones a quienes vulnerasen el derecho fundamental a la protección de datos. Esta Ley ha sido derogada por la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de carácter personal (en adelante LOPD), tras varios años de proceso legislativo lento y denso, y orientada principalmente a resolver las divergencias que, existían entre la antigua Ley y la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la cual debía haber sido traspuesta al ordenamiento español en un período de tres años desde su adopción. Esta Ley tiene una estructura sistemática muy similar a la contenida en la antigua Ley,

1. En este sentido, el Tribunal Supremo, Sala de lo Contencioso-Administrativo, sección 3ª, de 15 de abril de 2002 (RJ 2002/4689), en su *Fundamento de Derecho Cinco* precisa que: «A partir del artículo 18.4 de la Constitución Española queda incorporado a nuestro Ordenamiento un nuevo derecho fundamental (de «libertad informática»), lo denomina el Tribunal Constitucional en sus sentencias 254/1993, de 20 de julio (RTC 1993/254), 94/1998, de 4 de mayo (RTC 1998/94), 202/1999, de 8 de noviembre (RTC 1999/202), y 292/2000, de 30 de noviembre), en el que el bien jurídico garantizado es el de la libertad o autodeterminación informativa, que consiste en el control que corresponde a la persona sobre la información que le concierne personalmente, sea íntima o no, para preservar, de este modo y en último extremo, la propia identidad, dignidad y libertad»; la sentencia del Tribunal Superior de Justicia de Murcia, Sala de lo Contencioso-Administrativo, sección 2ª, de 29 de abril de 2004 (RJCA 2004/749), que señala en su *Fundamento de Derecho Cuarto*: «la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el artículo 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplio como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre (RTC 1987/170, F.4), como el derecho al honor, citado expresamente en el artículo 18.4, e igualmente, en expresión bien amplia del propio artículo 18.4 CE, al pleno ejercicio de los derechos de la persona.

si bien, introduce y regula algunos conceptos nuevos como la definición de las obligaciones y responsabilidades de la figura del Encargado de tratamiento o el derecho de oposición al tratamiento de datos del que gozan los interesados, y establece un régimen sancionador en tres niveles de infracciones, leves, graves, y muy graves, estipulando también tres niveles de sanciones económicas al efecto, las cuales van desde los 601,01 hasta los 601.012,10 euros. No obstante, esta norma ha sido muy criticada por contemplar un panorama legislativo ambiguo e incompleto que da lugar a muchas interpretaciones y, a una situación de inseguridad jurídica para aquellos responsables de ficheros que, tienen que cumplir con las obligaciones estipuladas en el texto. En su Disposición Transitoria Tercera, además de derogar la anterior Ley, establece que, hasta que no se lleve a cabo el desarrollo reglamentario *«continuarán en vigor, con su propio rango, las normas reglamentarias existentes, y, en especial, los Reales Decretos 428/1993, de 26 de marzo, 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se oponga a la presente Ley»*. Tras un proceso legislativo que duró más de dos años, finalmente, se aprobó el Reglamento de desarrollo de la LOPD (Real Decreto 1720/2007, de 21 de diciembre), si bien, no se limita a ser un desarrollo de dicha norma, sino que se ha aprovechado para regular en el mismo determinadas cuestiones que, desde la entrada en vigor de la LOPD, suscitaron dudas interpretativas y prácticas. En efecto, esta norma reglamentaria nace con vocación de desarrollar no sólo los mandatos contenidos en la LOPD, sino también aquellos otros aspectos, que tras la entrada en vigor de la citada Ley, se había demostrado que, precisaban de un mayor desarrollo normativo, y respecto de los cuales la experiencia ha requerido un cierto grado de precisión que, dote de seguridad al sistema. Cabe destacar que, uno de los objetivos del nuevo desarrollo reglamentario es reforzar la idea de protección de los derechos de los titulares de los datos con la exigencia de cumplimiento de algunos de los requisitos, que se imponen para poder llevar a cabo el tratamiento de datos personales. Entre ellos, cabe destacar los siguientes:

a) Forma de recabar el consentimiento tácito y el consentimiento para fines distinto a los directamente relacionados con la relación contractual (principalmente, para fines comerciales);

b) Conservación por el Responsable del Fichero de un medio de prueba que permita acreditar el cumplimiento del deber de información;

c) Flexibilización de la forma de ejercer los derechos de acceso, rectificación, cancelación y oposición (ARCO).

Además de las anteriores novedades, cabe destacar, asimismo, las siguientes:

a) Modificación de la tipología de datos, y /o ficheros y los niveles de seguridad correspondientes a los mismos;

b) Regulación complementaria de los tratamientos con fines de publicidad y prospección comercial, así como de los ficheros de solvencia patrimonial y de crédito;

c) Regulación de las medidas de seguridad respecto de los ficheros no automatizados (soporte papel);

d) Regulación detallada de los Códigos Tipo;

e) Regulación de diferentes procedimientos tramitados

El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales, y sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado»; y, la sentencia del Tribunal Superior de Justicia de Galicia, Sala de lo Contencioso-Administrativo, sección 1ª, de 16 de enero de 2008 (RJCA 2008/700).
Por su parte, la sentencia del Tribunal Constitucional, Sala 2ª, de 8 de noviembre de 1999 (RTC 1999/202), pone de manifiesto que, la libertad informática es el derecho a controlar el uso de los datos relativos a la propia persona inserta en un programa informático «habeas data», y comprende entre otros, la oposición del ciudadano a que determinados datos sean utilizados para fines distintos de aquél que justificó su obtención.

por la Agencia Española de Protección de Datos; y

f) Se completa la regulación de las relaciones del encargado del tratamiento de los datos, con referencia a la subcontratación, conservación de datos, y las medidas de seguridad que, deben ser aportadas por el encargado del tratamiento.

Con posterioridad a esta normativa, se dicta la Ley 34/2002, de 11 de Julio se Servicio de la Sociedad de la Información y de Comercio Electrónico (LSSI) que, regula en su Título III, el régimen jurídico de las comunicaciones comerciales realizadas por vía electrónica, y establece en su artículo 19 que *«las comunicaciones comerciales y las ofertas promocionales se regirá, además de por la presente Ley, por su normativa propia y la vigente en materia comercial y de publicidad»*, y, que *«en todo caso, será de aplicación la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de carácter personal, y su normativa de desarrollo, en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales»*.

Esta LSSI hace una remisión empresa a la LOPD y su normativa de desarrollo en los que se refiere al tratamiento de los datos personales necesario para llevar a cabo la realización de comunicaciones comerciales por vía electrónica. En particular, en la LSSI se regulan los siguientes aspectos relativos a tales comunicaciones:

a) Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación equivalentes;

b) Derechos de los destinatarios del servicio; y,

c) Información exigida sobre las comunicaciones, ofertas promocionales, y concursos.

De forma adicional, con motivo de la reforma de la LSSI, llevada a cabo por la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, y de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, se atribuyó a la Agencia Española de Protección de Datos la competencia para sancionar el envió de comunicaciones comerciales por vía electrónica u otros medios de comunicación electrónica equivalente a destinatarios que, no hayan autorizado su remisión o se hayan opuesto a las mismas.

Precisamente, el Capítulo III, del Título III de la Ley General de Telecomunicaciones se dedica a la regulación del secreto de las comunicaciones y protección de datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas. Para ello el legislador regula en su articulado de forma genérica algunos principios como:

1. La interceptación de las comunicaciones electrónicas por los servicios técnicos;

2. El cifrado en las redes y servicios de comunicaciones electrónicas;

3. El secreto de las comunicaciones;

4. La protección de datos de carácter personal;

5. La redes de comunicaciones electrónicas en el interior de los edificios; y,

6. Los derechos de los usuarios.

En desarrollo de esta Ley General de Telecomunicaciones, en el Título V del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, se regula la protección de los datos personales en la explotación de redes y en la prestación de los servicios de comunicaciones electrónicas disponibles al público. En este sentido, los artículos 61 a 82 contenidos en el citado Título vienen a regular, entre otros aspectos: los datos personales sobre el tráfico y la facturación; las guías de servicios de comunicaciones electrónicas disponibles al público; la protección de datos personales en la facturación desglosada; las llamadas no solicitadas para fines de venta; prestación de los servicios de elaboración de guías de abonados y de consulta telefónica sobre número de abonado; datos de localización distintos de los de tráfico; y, la protección de datos personales en los servicios avanzados de telefonía.

Finalmente, como respuesta a la necesidad de adaptar el marco legal al desarrollo experimentado por las tecnologías de la información, se aprueba la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas, y a las redes públicas de telecomunicaciones. Con esta Ley, además de posibilitar la transposición a nuestro ordenamiento jurídico de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, se regula la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultades siempre que, les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

Para tal fin se establece la obligación genérica, para quienes son operadores de telefonía fija o móvil, acceso a Internet o telefonía y correo electrónico por Internet (prestadores de estos servicios), de registrar y conservar de forma sistemática y durante un plazo de 12 meses, determinada información asociada a dichos servicios (entre otros, datos relativos al origen u destino de la comunicación, así como identificación de la fecha, hora, duración y tipo de comunicación).

En el ámbito autonómico, hay que mencionar, la Ley 8/2001, de 13 de julio de protección de datos de carácter personal en la Comunidad de Madrid; la Ley 2/2004, de 25 de febrero de regulación de Ficheros de Datos de carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos; el Decreto 104/2008, de 22 de julio sobre protección de datos de carácter personal en la Junta de Comunidades de Castilla-La Mancha; el Decreto 29/2009, de 5 de febrero de la Comunidad Autónoma de Galicia por el que se regula el uso y acceso a la historia clínica electrónica; y, la Ley 32/2010, de 1 de octubre de normas reguladoras de la Autoridad catalana de Protección de Datos.

En el contexto europeo, hay que hacer referencia al Convenio, número 108, del Consejo de Europa de 28 de enero de 1981, para la Protección de personas con respecto al tratamiento automatizado de datos de carácter perso-

nal y su Protocolo Adicional de 8 de noviembre de 2001. Se trata de uno de los documentos más importantes que, se han publicado en materia de protección de datos personales, pues, supone uno de los primeros y mayores impulsos a nivel internacional en la regulación de los derechos de las personas físicas en el tratamiento automatizado de sus datos de carácter personal. Mediante la firma de este Convenio, los Estados firmantes adquieren, en virtud del artículo 4.2 el compromiso de tomar «en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo». Precisamente, el objetivo de este 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 respeto al tratamiento automatizado de los daros de carácter personal correspondientes a dicha persona».

En este Convenio se define como dato de carácter personal «cualquier información relativa a una persona física identificada o identificable», definición muy similar como veremos a la que se contiene en la LOPD. Después de trascurridos algunos años desde la firma del mencionado Convenio 108, y habiéndose aprobado en España la ya derogada Ley Orgánica 5/1992, de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de carácter personal (LORTAD), se publica en 1995, la Directiva 95/46/CE que establece para los Estados miembros los principios de protección de datos que, deben regir en el ordenamiento interno de cada uno de ellos, otorgando a estos efectos un plazo de tres años para su transposición.

Sin embargo, como hemos visto, no fue hasta diciembre de 1999, cuando se aprueba la actual LOPD, en la que se transponen tales principios. De esta forma, y bajo el desarrollo de aspectos tan básicos como el respeto a la vida privada y la intimidad, así como la libre circulación de mercancías, personas, servicios y capitales establecido en el artículo 7 A del Tratado, nace esta Directiva para proteger a los individuos cuyos datos personales vayan a ser tratados tanto por Entidades Públicas como privadas. Cabe resaltar de esta Directiva que, en su Considerando 27 y a diferencia del ámbito de aplicación de la LORTAD entiende que «la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual, principio que luego adopta la propia LOPD».

El 31 de octubre de 2003 se deroga la Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones en virtud del mencionado artículo 19 de la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Tal como establece su artículo 1.2 «las disposiciones de la presente Directiva especifican y completan la Directiva 95/46/CE a los efectos mencionados en el apartado 1. Con esta norma se pretende proteger y custodiar la intimidad de los abonados y usuarios de servicios de comunicaciones electrónicas disponibles para el público en las redes de comunicaciones de la Comunidad, incluyendo también la protección de los intereses legítimos de los abonados que, sean personas jurídicas. Para ello, se concretan cuáles son los derechos de los abonados y usuarios de los servicios de comunicaciones electrónicas, así como las obligaciones y responsabilidades de los prestadores de estos servicios. En el articulado de la Directiva se regula entre otras materias:

> a) La seguridad técnica y de gestión que deben adoptar los proveedores de servicios de comunicaciones electrónicas;

b) La confidencialidad de las comunicaciones;

c) El tratamiento de datos de tráfico;

d) La facturación desglosada;

e) La presentación y restricción de la identificación de la línea de origen y la línea conectada;

f) El tratamiento de los datos de localización;

g) Las guías de los abonados; y

h) El envío de comunicaciones no solicitadas.

Esta Directiva ha sido modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009, por la que se modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) número 2004/2006, sobre la cooperación en materia de protección de consumidores.

Posteriormente, se aprueba la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, relativa a la conservación de datos generados o tratados con relación a la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, por medio de la cual se pretende armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones, con relación a la conservación de determinados datos generados o tratado por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro. Se aplica esta Directiva a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado, pero no alcanzará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada, utilizando una red de comunicación electrónica.

Finalmente, en relación a la regulación general relativa a la protección de datos personales, el Reglamento (CE) número 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 respeta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. La finalidad de este Reglamento es «garantizar tanto el respeto efectivo de las normas de protección de los derechos y las libertades fundamentales de las personas, como la libre circulación de los datos personales entre los Estados miembros y las instituciones y organismos comunitarios, en el ejercicio de sus competencias respectivas. Dentro de su articulado se regula la licitud del tratamiento de datos, los cambios en los fines del tratamiento, la transmisión de datos entre instituciones y organismos comunitarios o a otros destinatarios, el tratamiento de categorías especiales de datos, el derecho de información del interesado, los derechos del interesado, etcétera.

Las disposiciones del Reglamento, en virtud de su artículo 3.1 son de aplicación «al tratamiento de datos personales por parte de todas las instituciones y organismos comunitarios, en la medida en que dicho tratamiento se

lleve a cabo para el ejercicio de actividades que pertenecen al ámbito de aplicación del Derecho Comunitario», comprendiendo tanto los tratamientos de datos personales automatizados como los no automatizados. Asimismo, establece en su artículo 7 uno de sus principios básicos «sin perjuicio de lo dispuesto en los artículos 4, 5 y 10, los datos personales sólo se transmitirán a otras instituciones y organismos comunitarios o en el seno de dichas instituciones y organismos, si son necesarios para el ejercicio legítimo de las tareas que, pertenecen al ámbito de competencia del destinatario».

En el ámbito estricto de los datos atinentes a la salud, hay que destacar la Recomendación (97) 5, de 13 de febrero, sobre protección de datos médicos que ha venido a sustituir a la Recomendación (81) 1, de 23 de enero, sobre reglamentación aplicable a los bancos automatizados de datos médicos. Asimismo, el Convenio sobre Derechos Humanos y Biomedicina 4 de abril de 1997 (Convenio de Oviedo). Igualmente, hay que hacer referencia al Tratado de la Comunidad Económica en cuyo artículo 286.1 referido a la protección de datos personales, dispone que «a partir del 1 de enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el presente Tratado o sobre la base del mismo». Por su parte, el artículo 30.1 b) del Tratado de la Unión Europea establece que «la recogida, almacenamiento, tratamiento, análisis e intercambio de información pertinente, en particular, mediante Europol, incluida la correspondiente a informes sobre operaciones financieras sospechosas que obre en poder de servicios con funciones coercitivas, con sujeción a las disposiciones correspondientes en materia de protección de datos personales». En el proceso de implementación de este artículo, la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal establece en su artículo 6 que, el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, de datos relativos a la salud o a la vida sexual sólo se permitirá cuando sea estrictamente necesario y su Derecho nacional establezca las garantías adecuadas.

En el Tratado de Lisboa que modificó sustancialmente el Derecho originario de la Unión Europea, dando lugar a dos Tratados, el ya conocido Tratado de la Unión Europea, y el Tratado de Funcionamiento de la Unión Europea, el artículo 16 de este último (que modifica el artículo 286 del TCE), incorpora una regulación de la protección de datos personales, en cuyo apartado 1 se declara que «toda persona tiene derecho a la protección de datos de carácter personal que le conciernan», y el apartado 2 del mismo confía al Parlamento Europeo y al Consejo, la responsabilidad de esta protección, estableciendo a tal fin y 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 Europea, 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», y añade «el respeto de dichas normas estará sometido al control de autoridades independientes».

Además de las normas que se adopten en el seno del Parlamento en virtud del presente artículo, se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea que, establece que «el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente Capítulo y sobre la libre circulación de dichos datos».

En la Carta de Derechos Fundamentales, proclamada en el Consejo Europeo de Niza en el año 2000, dedica su artículo 8 a la protección de datos de carácter personal, declarando el derecho de toda persona a dicha protección. Reconoce, igualmente, el derecho de la persona a acceder a los datos que la conciernan y a su rectificación; y, se establece como principio, el tratamiento leal de los datos y, la necesidad de obtener el consentimiento de la persona afectada u otro fundamento legítimo previsto por la Ley.

En relación a datos genéticos, hay que destacar la Declaración Universal sobre Genoma Humano y los Derechos Humanos de 1997, aprobada por la XXIX Comisión de la Conferencia General de la Unesco, en París, el 11 de noviembre de 1997, y por Resolución de la Asamblea General de Naciones Unidas, de 10 de diciembre de 1998, siendo desarrolladas las previsiones de esta Declaración, por la Declaración Internacional sobre Datos Genéticos Humanos de 2003, aprobada por la XXXII Conferencia General de la UNESCO, concluida en París, el 16 de octubre de 2003.

En España, hay que mencionar la Ley 14/1986, de 14 de abril, General de Sanidad; la Ley 41/2002, de 14 de noviembre de autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica; la Ley 16/2003, de 28 de mayo de cohesión y calidad del Sistema Nacional de Salud; la Ley 44/2003, de 21 de noviembre de Ordenación de las profesiones sanitarias; la Ley 29/2006, de 26 de julio de garantías y uso racional de los medicamentos y productos sanitarios; la Ley 14/2006, de 26 de mayo sobre Técnicas de Reproducción Humana Asistida; la Ley 1472007, de 3 de julio, de Investigación biomédica; el Real Decreto 2070/1999, de 30 de diciembre regulador de las actividades de obtención y utilización clínica de órganos humanos; el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual; y, el Real Decreto 1301/2006, de 10 de noviembre, por el que se establecen las normas de calidad y seguridad para la donación, la obtención, la evaluación, el procesamiento, la preservación, el almacenamiento, y la distribución de células y tejidos humanos y se aprueba las normas de coordinación y funcionamiento para su uso en humanos.

Sobre tales bases normativas tan amplias, el presente estudio se va a centrar en el análisis de la protección de datos personales relativos a la salud, el acceso y cesión de los mismos, con especial referencia a los datos genéticos, para finalizar con el uso y acceso a la historia clínica. Por razones de espacio, destacaremos los aspectos más relevantes de la materia señaladas; todo ello, sin perjuicio de un tratamiento más extenso en otro estudio, de algún aspecto destacable de aquélla.

II. Los datos de la salud como categoría de datos de carácter personal

La LOPD española tiene, asimismo, por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor, e intimidad personal y familiar. Alcanza a los datos de carácter personal registrados en soporte físico, que los haga susceptible de tratamiento y a toda modalidad de uso posterior. Por tanto, se amplía el objeto de protección a los ficheros tanto automatizados como en soporte papel que, contengan datos personales siempre que sean susceptibles de tratamiento.

Se considera datos de carácter personal «cualquier información concerniente a personas físicas identificadas o identificables» (artículo 3 a) LOPD); o «cualquier información numérica, alfabética, gráfica, fotográfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables» (artículo 5.1 f) del Reglamento de la LOPD). Mientras que se

considera datos de carácter personal relacionados con la salud «las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas, los referidos a sus porcentajes de discapacidad y a su información genética» (artículo 5.1 g) del Reglamento de la LOPD)[2]. El conjunto de documentos que contienen datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencia recibe el nombre de historia clínica (artículo 3 de la Ley 41/2002 de Derechos de los pacientes).

Se entiende como «datos especialmente protegidos» los datos de carácter personal que hagan referencia al origen racial, a la salud, y a la vida sexual, y, se precisa que, sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente (artículo 7.3 de la LOPD). Quedan, además, expresamente prohibidos «los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual» (artículo 7.4 de la LOPD).

No obstante, se habilita al tratamiento de datos relativos a la salud «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».

Podrán, también, ser objeto de tratamiento cuando «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» (artículo 7.6 de la LOPD). Si bien, para facilitar la asistencia sanitaria ordinaria, la LOPD prevé en su artículo 8 que, sin perjuicio de lo establecido en el artículo 11 de la propia ley (que regula la comunicación y cesión de datos), «las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad».

En armonía con esta previsión, el artículo 10.5 del Reglamento de la LOPD establece que, los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica, y añade expresamente que 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».

Con estas previsiones normativas, lo que hace la LOPD es recoger la regulación contenida previamente en la Directiva 95/46/CE respecto al tratamiento de este tipo de datos que, sin embargo, de forma más tajante que en la citada Ley Orgánica, viene a considerar que, los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad del individuo no deben ser objeto de tratamiento alguno, salvo que el sujeto haya dado su consentimiento expreso. No obstante, es bien cierto que, la propia Directiva admite la posibilidad de que esta prohibición ceda en casos específicos como el tratamiento con fines relacionados con la salud, siempre que se realice por personas físicas sometidas a una obligación legal de secreto profesional, o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales. Igualmente, en la Directiva se admite la posibilidad que «cuando esté jus-

2. Este precepto se inspira en el apartado 45 de la Memoria Explicativa del Convenio número 108 del Consejo de Europa de 1981 que en la definición de «datos de carácter personal relativos a la salud» considera que 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», y, añade el citado apartado 45 que «debe entenderse que estos datos comprenden igualmente informaciones relativas al abuso de alcohol o al consumo de drogas». En este mismo sentido, la Recomendación R (97) de 13 de febrero, del Comité de Ministros del Consejo de Europa, referente a la protección de datos médicos afirma que «la expresión de 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», y, la Recomendación R (91) 15, del Comité de Ministros del Consejo de Europa, en materia de estudios epidemiológicos en el ámbito de la salud mental, hace hincapié en la necesidad de establecer las garantías necesarias para la protección de datos referentes a este tipo de trastornos.
Por su parte, el Tribunal de Justicia de las Comunidades Europeas, en la sentencia de 6 de noviembre de 2003, caso de la Sra, Lindqvist - caso C-101/01-, otorga a la expresión «datos relativos a la salud» que utiliza la Directiva 95/46/CE un contenido amplio, comprendiendo toda la información relativa a todos los aspectos de la salud de la persona, tanto físicos como psíquicos.

tificado por razones de interés público importante», se permita a los Estados hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como «la salud pública, y la protección social, particularmente en los relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y servicios en el régimen del seguro de enfermedad, la investigación científica y las estadísticas públicas; que a ellos corresponde, no obstante, prever las garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida privada de las personas» (Considerandos 33 y 34 y artículo 8).

En este contexto, llama la atención que, el artículo 7.3 de la LOPD al regular el tratamiento, entre otros, de los datos de la salud, sólo se refiera al consentimiento expreso, y no aluda a otros requisitos específicos como su prestación por escrito, como si lo hace para los datos que revelen la ideología, afiliación sindical, religión y creencia a los que se refiere el apartado segundo del mismo precepto; quizá porque se posibilita el consentimiento oral, aparte del escrito en el artículo 2.2 de la Ley 41/2002, y, porque que la propia dinámica y la práctica de numerosas aplicaciones biomédicas verían limitada su operatividad, si se requiriera el consentimiento expreso y escrito en cada una de ellas.

Ni la Ley 8/2001 de Protección de Datos de Carácter personal de la Comunidad de Madrid, ni el Decreto 104/2008, de Protección de Datos de carácter personal de la Junta de Comunidades de Castilla-La Mancha, ni la Ley 32/2010 sobre normas reguladoras de la Autoridad catalana de protección de datos hacen referencia alguna a los datos sobre la salud. Sin embargo, en la Ley 2/2004 de Ficheros de Datos de carácter personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, si alude en su artículo 2.4 al tratamiento de los datos de salud por instituciones y centros sanitarios[3]; y en el artículo 22.4 d) tipifica como infracción muy grave «recabar y tratar datos referidos al origen racial, a la salud, o a la vida sexual, cuando no lo disponga una ley o el afectado no haya consentido expresamente». Por su parte, el Decreto 29/2009, de la Comunidad Autónoma de Galicia, en su artículo 5 remite a la Ley Orgánica y a su Reglamento de desarrollo en todo lo relativo al tratamiento de datos de salud y a la posibilidad de comunicarlos a través de medios electrónicos, entre organismos, centros, servicios y establecimientos de la Consellería de Sanidad, el Servicio Gallego de Salud y el Sistema Nacional de Salud, cuando se produzcan en la atención sanitaria de las personas, tanto se realicen con medios propios o concertados.

Sobre tales bases normativas, hay que señalar que, inicialmente en la conceptuación de datos relativos a la salud, se hacía referencia en la doctrina con dicha expresión «datos de salud», a los datos personales obtenidos con ocasión de tratamientos médicos y asistencia sanitaria en general; mientras que, ahora, atendiendo a la regulación de la LOPD, se ha impulsado una ampliación en la obtención de datos relativos a la situación física y psíquica de la persona para aplicaciones diferentes del tratamiento sanitario del interesado. Por tanto, se pueden obtener datos relativos a la salud de interesado, sin que exista patología alguna que tratar. De forma que, la más acertada definición debería referirse al tipo de dato en sí mismo, y no al fin para el que se obtiene[4].

No obstante, estos datos de salud deben recibir una protección reforzada en todo caso por la información que, revelan o puede llegar a revelar y no en función del fin, objeto de tratamiento de dichos datos. Una definición amplia del dato de salud resulta en cierta forma reforzada por cómo se conceptúa la salud en la Organización Mundial de la Salud (OMS), como «un estado de completo bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades».

3. Artículo 2.4 señala que: «4. Las instituciones y centros sanitarios de carácter público y los profesionales a su servicio podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratadas en los mismos, de acuerdo con lo dispuesto en la legislación sectorial sobre sanidad, sin perjuicio de la aplicación de lo dispuesto en esta Ley en todo lo que no sea incompatible con aquella legislación».

4. En esta línea, **De Miguel Sánchez N.**, «Datos de carácter personal relativos a la salud: una obligada remisión a la normativa del sector sanitario», Comentario a la Ley Orgánica de Protección de Datos de carácter personal, director Antonio Troncoso Reigada, Civitas-Thomson Reuters, Navarra, 2010, p. 712.

En esta línea, para **Gómez Sánchez** dato de salud es «cualquier dato personal relativo a la realidad física y psicológica de un individuo y cualquier dato que se genere como consecuencia de dicha situación o de la participación del sujeto en actividad o proceso, cualquier dato obtenido en el ámbito biomédico, ya responda estrictamente a un tratamiento médico o a cualquier otra prestación que tenga que ver con su bienestar físico o psíquico, aunque la misma no responda a la necesidad de tratar una enfermedad en sentido estricto»[5].

Ha sido específicamente en el Derecho comunitario donde se ha incluido dentro de la categoría de datos sensibles, los datos de salud. En este sentido, la Directiva 95/46/CE, afirma en su artículo 8.1 que «Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad». No obstante, se flexibiliza esta regla general al posibilitarse excepciones o, porque el tratamiento queda sujeto a la autorización de una autoridad independiente. Así con respecto a las excepciones, no tiene lugar la citada prohibición cuando:

> a) El interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o;
>
> b) El tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantía adecuadas, o;
>
> c) El tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o;
>
> d) El tratamiento sea efectuado en el cursos de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o;
>
> e) El tratamiento se refiera a datos que el interesado haya hecho manifiestamente público o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial. Y, más en concreto, en el ámbito médico, no se aplicará tampoco tal prohibición cuando el tratamiento de datos 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 sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de

5. **Gómez Sánchez Y.**, «Datos de salud como datos especialmente protegidos. Comentario al artículo 7 de la Ley de Protección de Datos», Comentario a la Ley Orgánica de Protección de Datos de carácter personal, director Antonio Troncoso Reigada, Civitas-Thomson Reuters, Navarra, 2010, p. 649.

las normas establecidas por las autoridades nacionales competente, o por otra persona sujeta asimismo a un obligación equivalente de secreto.

Finalmente, los Estados miembros podrán, alegando motivos de interés púbico, establecer otras excepciones, además de las expuestas, bien mediante su legislación nacional, o bien por decisión de la autoridad de control[6]. En este sentido, el Reglamento número 45/200, considera, igualmente, como categoría especial de datos, los datos relativos a la salud, salvo que el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo cuando las normas internas de la institución o del organismo comunitario dispongan que tal prohibición no puede quedar sin efecto por el consentimiento del interesado, o que el tratamiento es necesario para cumplir las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral, en la medida en que esté autorizado por el Tratado de la Unión Europea u otros instrumentos jurídicos adoptados sobre la base del mismo, o, si fuera necesario, en la medida en que lo haya aprobado el Supervisor Europeo de Protección de Datos, con la aportación de garantías suficientes; o el tratamiento es necesario para salvaguardar los intereses esenciales del interesado o de otra persona, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento; o, el tratamiento se refiere a datos que el interesado ha hecho manifiestamente públicos; o es necesario para el reconocimiento, el ejercicio, o la defensa de un derecho o en un procedimiento judicial; o, en fin, el tratamiento lo lleva a cabo, en el curso de sus actividades legítimas y con las garantías apropiadas, un organismo sin ánimo de lucro que constituya una entidad integrada en un institución u organismo comunitario, no sujeta a la legislación nacional sobre protección de datos en virtud del artículo 4 de la Directiva 95/46/CE, con fines políticos, filosóficos, religiosos o sindicales, a condición de que el tratamiento se refiere únicamente a los miembros de dicho organismo, o a las personas que mantenga contactos regulares con él en relación con sus objetivos y que los datos no se divulguen a un tercero sin el consentimiento del interesado (artículo 10).

Asimismo, se reitera que no se aplicará tal prohibición cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médico, la prestación sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional, o por otra persona sujeta asimismo a una obligación de secreto equivalente. Por otra parte, también señala que, los tratamientos de datos que, puede suponer riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance u objetivos estarán sujetos a control previo por parte del Supervisor Europeo de Protección de Datos. Pueden suponer tales riesgos lo tratamientos de datos relativos a la salud, y los tratamientos de datos relativos a sospechas, infracciones, condenas penales o medidas de seguridad (artículo 27.2 a)).

En este contexto, cabe señalar que, bajo el término de protección de datos se hacen referencia a la protección jurídica de las personas físicas en lo que concierne al tratamiento de datos personales. El fundamento del ámbito subjetivo de aplicación de la normativa de protección de datos reside, pues, en que la protección de los datos personales se refiere a la intimidad personal y familiar, por lo que no puede trasladarse dicha protección a las empresas puestos que, éstas no gozan del citado derecho a la intimidad. De forma que, quedan fuera del ámbito de protección de la norma las personas jurídicas[7].

El artículo 1 de la LOPD señala que: *«La presente Ley Orgánica tiene por objeto garantizar y proteger en lo que concierne al tratamiento de los datos*

6. En esta línea, establece en su Considerando 34 que: «también se deberá autorizar a los Estados miembros, cuando esté justificado por razones de interés público importante, a hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como la salud pública y la protección social, particularmente en los relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, la investigación científica y las estadísticas públicas; que a ellos corresponde, no obstante, prever las garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida privada de las personas».

7. Se entiende por persona jurídica de Derecho privado para los efectos de esta Ley «la persona jurídica no comprendida en los alcances del artículo 1 del Título preliminar de la ley 27444, Ley del Procedimiento Administrativo General» (artículo 2.11 de la Ley de Protección de Datos peruana).

personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar». El Reglamento de desarrollo de la Ley refuerza lo anterior al indicar en su artículo 2.2 que: *«Este Reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, al tiempo que amplía dicha exclusión respecto de los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales»*[8].

En todo caso, conviene señalar que, la LOPD y su Reglamento no resulta ser de aplicación, a los tratamientos realizados sobre los datos contenidos en ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. Por tanto, se excluye aquellos tratamientos de datos que, se realicen en esferas domésticas, como por ejemplo, una base de datos de contactos personales almacenados en la agenda de un ordenador personal al que se le da un uso doméstico; a los tratamientos de datos sometidos a la normativa sobre protección de materias clasificadas; y, a los tratamientos establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

Asimismo, la LOPD y su Reglamento de desarrollo remite a su regulación específica, los tratamientos de datos personales relativos a ficheros regulados por la legislación electoral, los ficheros que sirvan a fines exclusivamente estadísticos y estén amparados por la legislación estatal o autonómica sobre función estadística pública; los ficheros derivados del Registro Civil y del Registro Central de penados y rebeldes; los ficheros que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del Régimen del personal de las Fuerzas Armadas; y, los ficheros procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámara por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia (artículo 2.2 y 3).

Finalmente, con relación a los datos de personas fallecidas, quedan expresamente excluidos del ámbito de aplicación de la LOPD española el tratamiento de los mismos, con la salvedad de lo previsto a los efectos de posibilitar el ejercicio de los derechos de acceso y cancelación de datos, cuando proceda. En este sentido, las personas vinculadas al fallecido por razones familiares o análogas, podrán dirigirse a los Responsables de los Ficheros o Tratamientos, con la finalidad de notificar el óbito, debiendo aportar documentación acreditativa suficiente (por ejemplo, acta de defunción), y solicitar la cancelación de datos, cuando haya lugar a ello. Respecto a la protección de datos de los empresarios individuales, la LOPD lo incluye dentro de su ámbito de aplicación.

De forma que, alcanza tanto al tratamiento de los datos de tales empresarios referidos a su esfera privada, como pese a no ser posible deslindar inicialmente, si dichos datos corresponden a la esfera profesional o personal del empresario, analizando el supuesto concreto, se determina que, afectan a su esfera personal. Este criterio ha sido expresamente recogido en el artículo 2.3 del Reglamento de desarrollo de la LOPD al señalar que: *«los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal»*.

Por otra parte, para el tratamiento de los datos personales debe mediar el consentimiento de su titular. El artículo 3 h) de la LOPD española define consentimiento del interesado como *«toda manifestación de voluntad, libre,*

8. El artículo 3 a) de la LOPD define datos de carácter personal: «Cualquier información concerniente a personas físicas identificadas o identificables»; y, el artículo 5.1 f) del Reglamento de la LOPD como «Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables».

inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen». Esta misma definición se reitera en el artículo 5 d) del Reglamento de la LOPD.

Este consentimiento se convierte en el eje central de la regulación en materia de protección de datos, que otorga al interesado la potestad para determinar el tratamiento de los datos referidos a su persona (artículo 6 de la LOPD y artículos 13 a 17 del Reglamento de la LOPD)[9]; y debe ser previo, informado[10], expreso e inequívoco para que la recogida de sus datos sea lícita, lo que dotará de legitimidad al tratamiento posterior de los datos. Se posibilita, además del consentimiento expreso, el consentimiento tácito.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que, concurran en el tratamiento o serie de tratamientos (artículos 12.1 del Reglamento de la LOPD). En todo caso, el término «consentimiento inequívoco» representa un concepto jurídico indeterminado en el que se incluyen tres tipos de manifestaciones atendiendo a la normativa española: a) El consentimiento expreso para el tratamiento de los datos relativos a la salud, origen racial y vida sexual; b) El consentimiento expreso y por escrito, para el tratamiento de datos de ideología, afiliación sindical, religión y creencias; c) El consentimiento tácito para el tratamiento de la mayoría de los datos personales[11]. En relación a este último caso, se exige para que pueda entender recabado tal consentimiento de forma lícita y, adecuadamente: 1. Cumplir con el deber de información y ofrecer al titular de los datos un plazo de treinta días para manifestar su negativa al tratamiento. Se deberá facilitar al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considera ajustado al Reglamento de la LOPD los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido; 2. Conocer si la comunicación enviada (por ejemplo, a través de correo postal o correo electrónico) ha sido objeto de devolución por cualquier causa. Si la comunicación no ha llegado al interesado, el Responsable del Fichero no podrá tratar los datos personales (artículo 14.2 y 4 del Reglamento de la LOPD). En todo caso, corresponde a aquél probar la existencia del consentimiento inequívoco del afectado, que no podrá presumirse.

Si el Responsable del Tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que, no guardan relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que, manifieste expresamente su negativa al tratamiento o comunicación de datos (artículo 15.1 del Reglamento de la LOPD).

Cuando se trate de datos sensibles, el consentimiento para su tratamiento deberá efectuarse, además, por escrito. De no mediar el consentimiento del titular, sólo podrá proceder al tratamiento de tales datos cuando la Ley lo autorice, siempre que con ello se atienda a motivos de interés público.

Ahora bien, para que el interesado consienta debe estar debidamente informado, para poder decidir acerca del tratamiento a aplicar (artículo 5 de la Ley 41/2002). Parece que, en materia de datos relativos a la salud no cabe un consentimiento tácito, pues, debe ser expreso, entendiendo por tal «aquel que se obtiene de una declaración inequívoca por parte del interesado que acepta o rechaza la cesión y uso de sus datos» (sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, sección 1ª, de 24 de marzo de 2006)[12] . Además ha de ser específico, pues, el afectado ha de consentir

9. *Vid.*, la sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, sección 1ª, de 15 de octubre de 2004 (RJCA 2005/687) cesión datos sin consentimiento del interesado; la sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, sección 1ª, de 31 de enero de 2008 (RJCA 2008/10); la sentencia del Tribunal Constitucional, Sala 2ª, de 29 de junio de 2009 (RTC 2009/159); la sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, sección 1ª, de 9 de julio de 2009 (JUR 2009/390576); la sentencia del Tribunal Superior de Justicia del País Vasco, Sala de lo Contencioso-Administrativo, sección 3ª, de 30 de noviembre de 2009 (RJCA 2010/351); la sentencia del Tribunal Supremo, Sala Contencioso-Administrativo, sección 6ª, 23 de febrero de 2011 (RJ 2011/1533); y, la sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, sección 1ª, de 16 de junio de 2011 (RJCA 2011/512).

10. Debe ir precedido de la correspondiente información, *vid*., la sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, sección 1ª, de 21 de septiembre de 2005 (JUR 2005/262828).

11. La sentencia de la Audiencia Nacional, sección 1ª, de 30 de junio de 2004, establece que la concurrencia del consentimiento inequívoco del afectado que exige el artículo 6.1 de la LOPD, en el supuesto de que el interesado niegue haberlo otorgado, debería acreditarse por quien realiza el tratamiento, a través de los medios previstos legalmente. Por su parte, la sentencia de la Audiencia Nacional, sección 1ª, de 1 de febrero de 2006, considera la prueba indiciaria como medio para acreditar el consentimiento; y, la sentencia de la Audiencia Nacional, sección 1ª, de 25 de octubre de 2005, viene a exigir que quien

realiza el tratamiento de los datos, debe poder acreditar que ha obtenido el consentimiento del afectado; consentimiento que debe ser prestado previa la información contenida en el artículo 5 de la LOPD, y siendo, por tanto, el emisor del consentimiento, consciente de lo que hace.

12. En el mismo sentencia, la sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, sección 1ª, de 23 de noviembre de 2006 (RJCA 2006902).

con respecto a una situación concreta y bien definida. De forma que, corresponde al responsable del tratamiento de los datos, probar en todos los casos, que obtuvo el consentimiento expreso del interesado, y que ese consentimiento vino precedido de una información exacta. En todo caso, consentir la recogida y el tratamiento de datos personales, no implica en modo alguno consentir su cesión a terceros, pues, no pueden usarse los datos de carácter personal para finalidades distintas e incompatibles con aquellas para las que los datos hubieran sido recogidos (artículo 4.2 de la LOPD). De forma que, una nueva posesión y uso requerirán el consentimiento del interesado. Así lo exige la propia LOPD en su artículo 11.1 cuando precisa que los datos de carácter personal sólo podrán ser comunicados a un tercero para el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado; y añade, en su apartado tercero, «será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilita al interesado no le permita conocer la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretende comunicar». O como dispone el Tribunal Constitucional en si sentencia 292/2000, de 30 de noviembre «el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de éstos, pues, solo así será eficaz su derecho a consentir, en cuando facultad esencial de su derecho a controlar y disponer de sus datos personales. Para lo que no basta que conozca, que tal cesión es posible según la disposición que ha creado o modificado el fichero, sino también las circunstancias de cada cesión concreta».

En este contexto, tampoco habrá consentimiento eficaz, cuando el tercero maneje los datos, superando o excediéndose del ámbito de autorización concedida, o como manifiesta el Tribunal Constitucional en sentencia 196/2004, 15 de noviembre (citada por la sentencia 159/2009, de 29 de junio), «se subviertan los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida».

En cuanto a la posibilidad que se contiene en la LOPD de que por razones de interés general, se permita que los datos puedan ser recabados, tratados y cedidos sin contar con el consentimiento del afectado (artículo 7.3), el Tribunal Constitucional de nuevo ha precisado en la citada sentencia 292/2000, que «las posibles limitaciones del derecho fundamental a la intimidad personal deberán estar fundadas en una previsión legal que tenga justificación constitucional, sea proporcionada y que exprese con precisión todos y cada uno de los presupuestos materiales de la medida limitadora».

Por su parte, las excepciones a lo previsto en el artículo 7.3 de la LOPD, donde se contiene los requisitos que la propia Ley exige para recabar, tratar o ceder datos de carácter personal que hagan referencia a la salud, se contienen en el artículo 7.6 «cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente al secreto», o «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», viene a reproducir prácticamente lo dispuesto en el artículo 8.3 de la Directiva 95/46/CE. Al respecto, el Documento de Trabajo sobre Protección de datos del artículo 29 (00323/07/ES WP 131), en relación con el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos, adoptado el 15 de febrero de 2007, señala que:

1. Esta excepción cubre solamente el tratamiento de datos personales para el propósito específico de proporcionar servicios relativos a la salud de carácter preventivo, de diagnóstico, terapéutico o de convalecencia y a efectos de la gestión de estos servicios sanitarios, como por ejemplo, la facturación, contabilidad o estadísticas. No cubre, por tanto, el tratamiento posterior que no sea necesario para la prestación directa de tales servicios, como la investigación médica, el reembolso de gastos por un seguro de enfermedad, o la interposición de demandadas pecuniarias;

2. Además, el tratamiento de datos personales contemplado en el artículo 8.3 deberá ser necesario para los fines específicos contenidos en la letra a);

3. El tratamiento de datos sensibles debe ser realizado por un profesional sanitario o por otra persona sujeta, asimismo al secreto (médico) profesional o a una obligación equivalente al secreto[13].

El propio artículo 6.2 de la LOPD señala que, nos será preciso el consentimiento cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de la presente Ley. Entendiendo por interés vital la realización de intervenciones sanitarias que sean necesarias para preservar la salud de la persona[14]. **Troncoso Reigada** entiende que la referencia al «interés vital» se justifica en la vertiente objetiva del derecho a la vida que anima toda gestión asistencial y que prevalecerá sobre el derecho a la intimidad y a la protección de datos personales[15]. Asimismo, **Arruego** manifiesta que sería tres elementos los que identificarían este tipo de situaciones de «interés vital»: la gravedad, al existir un riesgo cierto de que la integridad o la vida del individuo sufra un menoscabo; la urgencia, pues, dicho riesgo impone una intervención médica perentoria; y la imposibilidad de que el paciente manifieste su voluntad con relación a la intervención sanitaria que, precisa[16] .

En cuanto a lo previsto en el artículo 8 de la LOPD, relativo a la posibilidad de comunicar a un tercero sin el previo consentimiento del interesado los datos de carácter personal relativos a su salud, cuando ello sea necesario ante una urgencia o para realizar un estudio epidemiológico en los términos establecidos en la Ley estatal o autonómica relativa a la materia (apartado f) del artículo 11 de la LOPD), «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». El artículo 10.5 párrafo segundo del Reglamento de la LOPD precisa sobre lo dispuesto en el citado artículo 8 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»*.

De forma que, atendiendo a la normativa expuesta, podemos concluir que, la regla general para la recogida y tratamiento de los datos de la salud, es la que exige el consentimiento libre, inequívoco, previo, informado, expreso y por escrito de los afectados, si bien este consentimiento no será necesario, cuando el interesado haya prestado su consentimiento expreso para ello (artículo 7.3); o cuando la Ley lo permita por razones de interés público (artículo 7.3); en los casos previstos en el artículo 7.6; en los supuestos contem-

13. Tomada la referencia, **López Ulla, J.M.**, «El consentimiento del afectado en el tratamiento de datos relativos a la salud», *Comentario a la Ley Orgánica de Protección de Datos de carácter personal, director Antonio Troncoso Reigada*, Civitas-Thomson Reuters, Navarra, 2010, pp. 681-682.

14. **Collado García-Lajara L.**, Protección de datos de carácter personal, Comares, Granada 2000, p. 21 critica la imprecisión del término «interés vital», manifestando que se trata de un concepto jurídico indeterminado que, deberá concretarse en cada caso por la justicia administrativa. El Grupo de Trabajo sobre la Protección de Datos del artículo 29, señala en su *Documento de Trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME)*, adoptado el 15 de febrero de 2007, p. 10, señala con relación al término «interés vital del interesado» que, «el tratamiento debe referirse a intereses individuales esenciales del interesado o de otra persona, y debe -en el contexto médico- ser necesario para un tratamiento médico dirigido a salvar la vida en una circunstancia en que el interesado no esté en condiciones de expresar sus intenciones. Por consiguiente, esta excepción sólo puede aplicarse a un pequeño número de casos de tratamiento y no puede utilizarse en absoluto para justificar el tratamiento de datos médicos personales con fines distintos del tratamiento del interesado, como por ejemplo, realizar investigaciones médicas generales que sólo darán resultados en el futuro». *Vid.*, la sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, sección 1ª, de 23 de noviembre de 2006 (RJCA 2006/902).

15. **Troncoso Reigada A.**, «La protección de datos sanitarios: la

plados en el artículo 11 respecto a la cesión; y, finalmente, cuando la comunicación tenga lugar entre organismos, centros y servicios del sistema Nacional de Salud en los términos previstos en el artículo 8 de la LOPD y artículo 10.5 párrafo segundo del Reglamento de la LOPD.

En todo caso, conviene precisar que, el acceso a los datos relativos a la salud por parte del personal sanitario, y por ende a la historia clínica, será exclusivamente para garantizar una asistencia adecuada el paciente, y por tanto, referida sólo a ella; e, igualmente, el personal de la administración y gestión de los centros sanitarios sólo podrán acceder a tales datos en lo relacionado con sus propias funciones, salvo que aras del interés general se exija otra cosa[17].

Sobre tales bases, la Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios, alude en varias preceptos a la protección de datos personales, con especial referencia al consentimiento para el tratamiento de los mismo y su cesión. Así se ocupa de la protección de datos de carácter personal en relación con las actuaciones en el marco de la farmacovigilancia (artículo 54.2), en el que los datos de reacciones adversas detectadas en España se integrarán en las redes europeas e internacionales de farmacoviglancia, de las que España forme parte, con la garantía de protección de los datos de carácter personal exigida por la normativa vigente.

Asimismo, las autoridades sanitarias pueden llegar a suspender aquellos programas de farmacovigilancia en los que se aprecien defectos graves en los procedimientos de obtención de datos y tratamiento de la información obtenida. Si bien, dicha suspensión requerirá el previo informe favorable del comité competente en materia de seguridad de medicamente de la Agencia Española de Medicamentos y Productos Sanitarios (artículo 54.4). Como ya hiciera el artículo 85.6 de la derogada Ley de Medicamento de 1990, en el artículo 77.8 se señala que, no será necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica en soporte papel o electrónico de conformidad con lo dispuesto en los artículos 7, apartados 3 y 6; 8 y 11, apartado 2 a) de la LOPD. Las citadas actuaciones deberán tener por finalidad facilitar la asistencia médica y farmacéutica al paciente y permitir el control de la prestación farmacéutica del Sistema Nacional de Salud. Esta previsión no estaba en la derogada Ley de 1990. Finalmente, el artículo 87.5 en relación a la trazabilidad de los medicamentos dispone que la recogida y tratamiento de datos a que se refiere este artículo, deberá adecuarse a la normativa vigente en materia de seguridad y protección de datos de carácter personal, en cumplimiento de la LOPD, teniendo en consideración de responsables de sus respectivos ficheros de titularidad pública la Administración General del Estado, las Administraciones Autónomas y, en su caso, las Administraciones corporativas correspondientes.

El artículo 33.3 de la Ley 16/2003, de 28 de mayo de cohesión y calidad del Sistema Nacional de Salud remite a la LOPD en lo referente a la colaboración de las oficinas de farmacia, considera entre los criterios generales y comunes para lograr tal colaboración por medio de conciertos que, garanticen a los ciudadanos la dispensación en condiciones de igualdad efectiva en todo el territorio nacional, independientemente de la comunidad autónoma de residencia, los relativos a la gestión por medios informáticos de la información necesaria para el desempeño de tales actividades y para la colaboración con las estructuras asistenciales del Sistema Nacional de Salud. No obstante, con el fin de lograr la máxima fiabilidad de la información que, se produzca, el Ministerio de Sanidad y Consumo, previo acuerdo del Consejo Interterritorial del Sistema Nacional de Salud, establecerá la definición y normalización de datos y flujos, la selección de indicadores y los requerimientos

confidencialidad de la historia clínica», *Protección de Datos personales para servicios sanitarios públicos*, Asociación de Protección de Datos de la Comunidad de Madrid, Madrid, 2008, p. 54.

16. **Arruego G.**, «La naturaleza constitucional de la asistencia sanitaria no consentida y los denominados supuestos de «urgencia vital»», *Revista Española de Derecho Constitucional, número 82, 2008*, p. 80.

17. *Vid.*, la sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, sección 1ª, de 28 de febrero de 2003 (JUR 2005/190523); y, la sentencia del Tribunal Supremo, Sala de lo Penal, sección 1ª, de 27 de noviembre de 2007 (RJ 2007/9354). Por su parte, la sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, sección 1ª, de 30 de mayo de 2007 (RJCA 2007/448), señala que, el acceso ha de comprender los datos de base del afectado y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos, y la especificación de los concretos usos y finalidades para los que se almacenaron los datos; todos aquellos relativos a la determinación y constatación de sus lesiones, su evolución, y en su caso, las secuelas advertidas, que afectan a la salud del titular de los datos, pero no pueden incluirse como «datos base», las valoraciones o apreciaciones de índole médica sobre el encaje de las lesiones o secuelas padecidas. En esta línea, *vid.*, asimismo, la sentencia del Tribunal Supremo, Sala de lo Contencioso-Administrativo, sección 6ª, de 11 de marzo de 2011 (RJ 2011/2065).

técnicos necesarios para la integración de la información (artículo 53.3); y, asimismo, la cesión de los datos, incluso aquellos de carácter personal, estarán sujetos 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 (artículo 53.6).

También en la Ley 44/2003, de 21 de noviembre de ordenación de las profesiones sanitarias se incluyen previsiones sobre la protección de datos personales. Así, en el artículo 5 relativo a los «Principios generales de la relación entre los profesionales sanitarios y las personas atendidas por ellos», en su apartado 1 letra f) se señala que, los pacientes tiene derecho a recibir información de acuerdo con lo establecido en la Ley 41/2002, y para garantizar de forma efectiva y facilitar el ejercicio de los derechos de los pacientes, los colegios profesionales, consejos autonómicos, y consejos generales, en sus respectivos ámbitos territoriales, establecerán los registros públicos de profesionales que, de acuerdo con los requerimientos de esta ley, serán accesibles a la población y estarán a disposición de las Administraciones sanitarias. Los indicados registros, respetando los principios de confidencialidad de los datos personales contenidos en la normativa de aplicación, deberán permitir conocer el nombre, titulación, especialidad, lugar de ejercicio y los otros datos que, en esta Ley se determinan como públicos (apartado 2).

Por su parte, la Ley 41/2002, establece como criterios básicos y principios de actuación en relación con los datos biosanitarios encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y documentación clínica, el respeto a la dignidad de la persona humana, a la autonomía de su voluntad y a su intimidad (artículo 2.1); y añade que, toda actuación en el ámbito de la sanidad requiere, con carácter general, el previo consentimiento de los pacientes o usuarios. Un consentimiento que, se debe obtener después de que el paciente reciba una información adecuada y, que se hará por escrito en los supuestos previstos en la Ley (artículo 2.2.).

La Ley 14/2007, de 3 de julio de Investigación biomédica establece como principio fundamental en la realización de cualquier investigación biomédica la protección de la dignidad e identidad del ser humano con respeto a cualquier investigación que, implique intervenciones sobre seres humanos en el campo de la biomedicina, garantizándose a toda persona sin discriminación alguna el respeto a la integridad y a sus demás derechos y libertades fundamentales (artículo 2 a)). Asimismo, define consentimiento como «la manifestación de la voluntad libre y consciente válidamente emitida por una persona capaz, o por su representante autorizado, precedida de la información adecuada» (artículo 3 f)); y señala que se respetara la libre autonomía de las personas que, pueden participar en una investigación biomédica o que pueda aportar a ella sus muestras biológicas, para lo que será preciso contar con que previamente haya prestado su consentimiento expreso y escrito, una vez haya sido oportunamente informado. Igualmente, la información se prestará por escrito y comprenderá la naturaleza, importancia, implicaciones y riesgos de la investigación. De prestarse a las personas con discapacidad se hará en condiciones y formatos apropiados a sus necesidades.

En tal contexto, toda persona tiene derecho a ser informada de sus datos genéticos y otros de carácter personal que, se obtengan en el curso de una investigación biomédica según los términos en que consintió. Este mismo derecho se reconoce a la persona que haya aportado, muestras biológicas con tal finalidad, o cuando se hayan obtenido otros materiales biológicos a partir de aquéllos. En todo caso, se respetará el derecho de la persona a qué no se comuniquen tales datos, incluidos los descubrimientos inesperados que, se pudieran producir en el curso de la investigación. No obstante, cuando a criterio del facultativo responsable, esta información sea necesaria para

evitar un grave perjuicio para su salud o la de sus familiares biológicos, se informará a un familiar próximo, o a un representante, previa consulta del comité asistencial si lo hubiera. Si bien, la comunicación se limitará exclusivamente a los datos necesarios para estas finalidades.

Sobre tales bases, la cesión de datos de carácter personal a terceros ajenos a la actuación médico-asistencial, o a una investigación biomédica requerirá el consentimiento expreso y escrito del interesado. En el supuesto, que los datos obtenidos del sujeto en la investigación pudieran revelar información de carácter personal de sus familiares, tal cesión requerirá, igualmente, el consentimiento de tales personas. De todas formas, se prohíbe la utilización de los datos relativos a la salud de las personas con fines distintos de aquéllos para los que se prestó el consentimiento.

Por otra parte, en esta norma se reconoce el derecho a la protección de datos entre las funciones a ejercer por parte del Comité de ética, pues, habrá de velar por el cumplimiento de procedimientos que, permitan asegurar la trazabilidad de las muestras de origen humano (artículo 12.2 d)); y, asimismo, procederá al seguimiento del cumplimiento del deber de informar a los participantes en la investigación biomédica sobre aquella información, valga la redundancia, relevante acerca su participación en la investigación, siendo aquélla comunicada por escrito a los participantes, o en su caso, a sus representantes, a la mayor brevedad; debiendo dar cuenta a la autoridad competente que, dio la autorización para dicha investigación de las incidencias que observe, con el fin de que aquélla pueda adoptar las medidas que corresponda de acuerdo con lo establecido en la normativa vigente en materia de protección de datos personales (artículo 25.5).

En cuanto al tratamiento de datos de menores de edad, teniendo en cuenta el principio fundamental de «interés superior del niño», y el principio de autonomía de la persona, concretado en relación con los menores, en los diferentes grados de madurez que, tienen lugar en su desarrollo; una de las novedades del Reglamento de la LOPD es la regulación expresa del tratamiento de los datos de menores de edad y los requisitos que deben cumplirse[18]. En este sentido, como regla general, se exige contar con el consentimiento inequívoco de quienes ostenten la patria potestad o representación legal del menor (padres, tutores u otro representante legal). Asimismo, se prevé que el menor de edad pueda prestar su consentimiento por sí mismo, siempre que sea mayor de 14 años y la Ley no exija la asistencia de los titulares de la patria potestad o tutela (menor maduro); sea menor emancipado, o cuando sea parte de un contrato de trabajo, siempre que tenga entre 16 y 18 años y esté emancipado o haya obtenido el beneficio de la mayoría de edad, o tenga 16 y 18 años y obtenga el consentimiento de los padres o tutores o autorización de la persona o institución que, los tenga a su cargo. El consentimiento de los padres o tutores será necesario respecto de los menores de 14 años. Asimismo, el Responsable del Fichero deberá articular algún tipo de procedimiento que, le permita garantizar la comprobación efectiva del menor y la autenticidad del consentimiento prestado, en su caso, por los padres o representantes legales (artículo 13.1 y 4 del Reglamento de la LOPD)[19]. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en el citado artículo 13. En ningún caso, podrá recabarse del menor, datos que permitan obtener información sobre los demás miembros del grupo familiar o sobre las características de los mismos, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad, y dirección del padre, madre o tutor con la única finalidad de recabar la autorización

18. Inspirada esta regulación tal vez en la Ley Orgánica 1/1996, de 15 de enero de Protección Jurídica del Menor, en donde expresamente se establece que los menores gozarán de los derechos que les reconocen la Constitución y los Tratados Internacionales, especialmente la Convención de Derechos del Niño de las Naciones Unidas y se les reconoce el derecho a ser oídos, cuando tengan suficiente juicio.

19. Toda vez que estos datos hoy en día se recaban por Internet, la prueba del consentimiento y de la edad resulta en la práctica extremadamente difícil, pero como dice **Fernández López J.M.**, «Algunas reflexiones sobre los aspectos generales que regula el reglamento de desarrollo de la LOPD», *Revista Española de Protección de Datos, núm. 3, julio-diciembre 2007*, pp. 35-64, «esta regulación servirá de llamada de atención a desaprensivos que obtienen datos en circunstancias dudosas de menores por este medio y de los padres para que no hagan dejación de sus obligaciones a la hora de permitir navegar por Internet a sus hijos de forma descontrolada».

prevista en el mencionado apartado 1 del artículo 13 (artículo 13.2).

En la Ley 14/2007 de Investigación biomédica, el consentimiento se otorgará por representación cuando la persona esté incapacitada o sea menor de edad, siempre y cuando no existan otras alternativas para la investigación. La prestación de tal consentimiento por representación será proporcional a la investigación a desarrollar, y se efectuará con respeto a la dignidad de la persona y en beneficio de su salud. En todo caso, las personas incapacitadas, y los menores de edad participarán en la investigación en la medida de lo posible y según su edad y capacidad en la toma de decisiones a lo largo de tal investigación (artículo 4.2).

Junto a la regla general consistente en que para la recogida y tratamiento de los datos personales se necesita contar con el consentimiento inequívoco del interesado, el artículo 6.2 de la LOPD hace una enumeración taxativa de los supuestos en los que no se requerirá el consentimiento del interesado para el tratamiento de sus datos personales. Así se entiende que éste no será preciso: a) Cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, que les atribuya una norma con rango de ley o una norma de derecho comunitario; b) Cuando se recaben con ocasión de la celebración de un contrato o precontrato o de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento; c) Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7.6 de la LOPD; d) Cuando el tratamiento esté autorizado en una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los siguientes supuestos: 1. El tratamiento sea necesario para que el Responsable del Tratamiento cumpla un deber que le imponga una de dichas normas; 2. El tratamiento tenga por objeto la satisfacción de un interés legítimo del Responsable del Tratamiento, amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades de los interesados. De igual modo, el legislador español ha querido otorgar una protección especial al tratamiento de una categoría de datos, al considerar que afectan a la esfera más sensible de la persona, pues, se refieren a la ideología, religión, creencia, afiliación sindical, origen racial, vida sexual y salud. Así en el artículo 7 de la LOPD se establece la necesidad de obtener el consentimiento expreso para tratar estos datos. Por su parte, el tratamiento de los datos relativos a la salud puede tener lugar sin el consentimiento del interesado, cuando se realicen con objeto de prestar atención sanitaria y el tratamiento sea realizado por un profesional sanitario sujeto al deber de secreto profesional, o por persona sujeta a una obligación equivalente a tal deber de secreto. En este sentido, se expresa el artículo 8 de la LOPD.

Con relación a la recogida y solicitud de consentimiento para el tratamiento de datos personales relativos al tráfico, facturación o localización propios de la prestación de servicios de telecomunicaciones y de comunicaciones electrónicas, así como su revocación, se habrá de someter a lo establecido en la normativa específica y en lo que no resulte contrario a los establecido en el Reglamento de la LOPD (artículo 16 del citado Reglamento).

Finalmente, es de destacar que el consentimiento otorgado por el interesado puede ser revocado en cualquier momento sin efectos retroactivos observando los requisitos previstos para su otorgamiento (artículo 6.3 de la LOPD). A tal fin, se deberá facilitar al interesado un medio sencillo y gratuito a través del cual puede revocar el consentimiento o manifestar su oposición al tratamiento, siendo de aplicación lo dispuesto a propósito de la forma de recabar el consentimiento, así 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 (artículo 17.1 del Reglamento de la LOPD). En este sentido, no se considera conformes a la LOPD, los medios que el Responsable establezca para que el interesado pueda manifestar su negativa al tratamiento mediante el envío de cartas certificadas o envíos semejantes, y la utilización de servicios de telecomunicaciones, que impliquen una tarificación adicional al afectado, o cualesquiera otros medios que, supongan un coste adicional al interesado (artículo 17.1 párrafo segundo del Reglamento de la LOPD).

Una vez recibida la revocación del consentimiento, el Responsable del Fichero dispondrá del plazo de diez días para cesar en el tratamiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la LOPD. Si los datos se hubieran cedido previamente, también se deberá advertir a los cesionarios, y en el mismo plazo de tiempo, de la revocación de consentimiento solicitada. Y, por último, si el interesado hubiera solicitado la confirmación del cese en el tratamiento de los datos del Responsable del Fichero, éste deberá responder expresamente a la solicitud (artículo 17.2 y 3 del Reglamento de la LOPD).

En este sentido, la Ley 14/2007, de investigación biomédica precisa que las personas que, participen en una investigación podrán revocar su consentimiento en cualquier momento, sin perjuicio de las limitaciones que establece esta Ley; exigiéndose para ello que las personas o entidades que hayan recibido tal revocación, dispongan de las medidas necesarias para lograr que ésta sea efectiva (artículo 4.3).

III. Confidencialidad y medidas de seguridad en el tratamiento de los datos de la salud

Como hemos expuesto, nuestro Ordenamiento parte el consentimiento del interesado como base jurídica para el tratamiento de datos de carácter personal, pero en la medida que los datos relativos a la salud forman parte del reducto de privacidad, que garantiza el artículo 18.1 de la Constitución Española, podemos hablar de un derecho de confidencialidad, y más en concreto, de un derecho de confidencialidad de la historia clínica. En consecuencia, la revelación de una información relativa a la salud de un sujeto sin su previa autorización, no sólo constituye un daño a un bien constitucional como el de respeto a la dignidad de la persona, sino que puede llegar a condicionar de facto el ejercicio y disfrute de otros derechos constitucionales[20]. De ahí que, la LOPD sólo permita en su artículo 7.3 que, estos datos sean recabados, tratados y en su caso, cedidos cuando por razones de interés general así lo permita una Ley o cuando el afectado expresamente lo consienta. El carácter confidencial de esta información también se reconoce en el artículo 10.3 de la Ley 14/1986 General de Sanidad, y especialmente, en el artículo 7.1 de la Ley 41/2002, de Derecho de los pacientes. De todas formas, en aras de confidencialidad, esta misma Ley permite al paciente acceder a su historia clínica -incluso mediante representación debidamente acreditada-, si bien dicho acceso no puede ejercitarse en perjuicio de terceras personas a la confidencialidad de datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, lo cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas (artículo 18.1 y 3).

En caso de pacientes fallecidos, los centros sanitarios y los facultativos sólo facilitaran el acceso a la historia clínica de aquéllos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así lo acredite. En cualquier caso, el acceso de un tercero a la historia clínica motivado por riesgo para la salud, se limitará a los datos pertinentes. No se facilitará en todo caso, información que afecte a la

20. Vid., la sentencia del Tribunal Constitucional, Sala 1ª, de 23 de marzo de 2009 (RTC 2009/70).

intimidad del fallecido, ni a las anotaciones subjetivas de los profesionales, ni que perjudiquen a terceros (artículo 18.4).

Asimismo, el artículo 15.4 de la citada Ley, manifiesta que *«Las historias clínicas se llevarán con criterios de unidad e integración, en cada institución asistencial como mínimo, para facilitar el mejor y más oportuno conocimiento de los facultativos de los datos de un determinado paciente en cada proceso asistencial»*, añadiéndose en la Disposición Adicional Tercera como máxima para alcanzar la implantación de un sistema de compatibilidad, que éste se ha de logar mediante la actuación coordinada del Ministerio de Sanidad y las Comunidades Autónomas competentes en la materia, para evitar repeticiones innecesarias en las exploraciones y procedimientos a que se someta un mismo paciente en diversos centros asistenciales españoles; para lo cual se articularan los recursos técnicos y la historia clínica digital, como elementos de vital importancia. Para la consecución de estos objetivos de integración es fundamental el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual[21]. En él se establece el conjunto de datos básicos que han de reunir las tarjetas emitidas en soporte informático por las diferentes Administraciones sanitarias y por el Instituto Nacional de Gestión Sanitaria para las personas que, tengan acreditado su derecho a la asistencia sanitaria pública. Asimismo, se determina la asignación de un código de identificación personal del SNS, de carácter irrepetible y único a lo largo de la vida de la persona. El código se asigna por el sistema en el momento de inclusión de los datos relativos a cada ciudadano en la base de datos de la población protegida, desarrollada por el Ministerio de Sanidad, y actúa como clave de vinculación de los diferentes Códigos de identificación personal autonómicos que, cada individuo puede tener a lo largo de la vida. Este Código facilita la búsqueda de la información sanitaria de un paciente que pueda encontrarse dispersa por el SNS, a fin de que pueda ser localizada y consultada por los profesionales sanitarios para la prestación de la debida asistencia (artículo 4). De conformidad con el artículo 56 de la Ley 16/2003, de Cohesión y calidad del Sistema Nacional de Salud corresponde al Ministerio de Sanidad y Consumo la coordinación de los mecanismos de intercambio de información clínica, previamente acordados por las Comunidades Autónomas, para permitir tanto al interesado como a los profesionales que participen 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 integración de la información. El Ministerio de Sanidad y Consumo es el responsable de establecer el procedimiento que, permita el intercambio telemático de la información exigible para el ejercicio de las competencias de las Administraciones Públicas, debiendo sujetarse tal intercambio a las precisiones de la LOPD y Ley de Derechos de los pacientes. Este es precisamente el sistema en el que se basa el Plan de Calidad del SNS presentado en marzo de 2006, con relación a la implantación de la historia clínica digital del SNS[22].

En cuanto al requisito ético de la confidencialidad de la profesión médica, conviene recordar que, se estableció por primera vez en el juramento hipocrático, y fue confirmado por la Declaración de Ginebra de la Asociación Médica Mundial (1948)[23]. En todo caso, la Directiva 95/46/CE, para el caso que surja la necesidad que personal no médico trate los datos personales sensibles como son los datos de salud, deberá estar sujetos al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes (artículo 8.3).

Por su parte, la Declaración Universal sobre Genoma Humano y los Derechos Humanos de 1997 establece en su artículo 7 la obligación de respetar la confidencialidad de los datos genéticos asociados a una persona identificable, conservados o tratados con fines de investigación o con cual-

21. La Disposición Adicional única dispone que *«en la medida en que se establezcan por la Unión Europea criterios de normalización que faciliten la circulación y la mejora de la asistencia sanitaria de pacientes en el ámbito comunitario, las tarjetas sanitarias individuales del Sistema Nacional de Salud deberá adoptarse a aquéllos»*. Para lograr tales criterios de normalización en el seno de la Unión Europea, hay que destacar la Recomendación de la Comisión sobre la interoperabilidad transfronteriza de los sistemas de historias de salud electrónicas de 2 de julio de 2008; Directiva 2011/24/UE del Parlamento europeo y del Consejo de 5 de marzo de 2011 relativo a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza; y, el Proyecto de Servicios Abiertos Inteligentes *Smart Open Services* (SOS).

22. Los objetivos generales del proyecto de historia clínica digital se centra en los siguientes aspectos: 1. Garantizar 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 la salud que integran el SNS; 2. Dotar al SNS de un sistema de acceso seguro que garantice al ciudadano la confidencialidad de los datos de carácter personal relativos a su salud; 3. Garantizar a los profesionales sanitarios facultados por cada servicios de salud el acceso, y autorizados en cada caso por el paciente, el acceso a determinados conjuntos de datos de salud, generados en una Comunidad Autónoma distinta de aquella desde la que se requiere la información, siempre que el usuario o paciente demande sus servicios sanitarios desde un centro público del SNS; y, 4. Dotar al sistema de historia clínica digital de agilidad y sencillez en el acceso.

➥

quier otra finalidad, de conformidad con lo que establezca en cada caso las leyes nacionales de los distintos Estados; y añade que, sólo la Ley podrá limitar los derechos de la persona concernida a la confidencialidad de sus datos y a la obtención, de su previo o informado consentimiento para la obtención de este tipo de datos.

En el ámbito nacional, la Ley 41/2002 de Derechos de los pacientes declara que, toda persona tiene derecho a que se le 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. Y añade que, los centros sanitarios adoptarán las medidas oportunas para garantizar tales derechos, y para ello, elaborarán las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes (artículo 7). Precisamente, con relación al acceso a la historia clínica, como instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente, y, a cuyo acceso sólo pueden corresponder a los profesionales que atienden al paciente; se señala, no obstante que, si el acceso tiene lugar con fines judiciales, epidemiológicos, de investigación o de docencia, se rige por lo dispuesto en la LOPD, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación al caso; y, asimismo, obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial; de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado el consentimiento para no separarlos.

No obstante, de esta regla general se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativo con los clínicos-asistenciales, en los cuales se estará a lo que determinen los jueces y tribunales en el proceso correspondiente. En todo caso, el acceso a los datos y documentos de la historia clínica han de limitarse estrictamente a los fines específicos de cada caso (artículo 16.3).

Asimismo, esta Ley 41/2002 hay que decir que, en los términos ya reseñados, incorpora una garantía más al sistema de acceso a la historia clínica, al establecer que el personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos que se contengan en la misma en el ejercicio de sus propias funciones. Con ello se prohíbe la divulgación de cualquier información que figure en la historia clínica fuera del ámbito estrictamente necesario para la prestación del servicio y siempre que el profesional que hace uso de dicha información, sea el que tiene encomendada la asistencia o el tratamiento (artículo 16.4)[24].

Por tanto, el acceso a la historia clínica en el ámbito de un determinado centro sanitario está limitado al propio personal sanitario que preste asistencia al paciente, a fin de garantizar su adecuado diagnóstico y tratamiento; y al personal de administración y gestión, exclusivamente en lo que resulte necesario para el ejercicio de sus funciones; estando unos y otros sujetos al deber de secreto.

En esta línea, la Ley 14/2007, de 3 de julio de Investigación biomédica garantiza la protección de la intimidad personal y el tratamiento confidencial de los datos personales que, resulten de una investigación biomédica conforme a lo dispuesto en la LOPD. Las mismas garantías se aplican a las muestras biológicas que, sean fuente de información de carácter personal (artículo 5.1). En todo caso, quedará sometida al deber de secreto, cualquier persona que en el ejercicio de sus funciones en relación con una concreta actuación médico-asistencial, o con una investigación biomédica, cualquiera que sea el alcance que tenga una y otra, acceda a datos de carácter personal. Este deber persistirá aún una vez que, haya cesado la investigación o la actuación. Si no

23. El Grupo Europeo de Ética de la Ciencia de las Nuevas Tecnologías en su Dictamen para la Comisión Europea de 30 de julio de 1999 bajo la rúbrica Principios Éticos de la Sanidad en la Sociedad de la Información dispone que «la obtención y acceso a los datos sobre la salud personal está restringida a los facultativos que realizan el tratamiento médico y a aquellas terceras personas (facultativos que no realizan el tratamiento, personal sanitario y social, personal de la administración, etc.) que puedan demostrar un uso legítimo»; y que «todos los usuarios legítimos de los datos personales sobre la salud tienen una obligación de confidencialidad equivalente a la obligación profesional del secreto médico. Las excepciones a esta obligación deben limitarse y establecer por normas legales».

24. En artículo 16 de la Ley 41/2002, define la historia clínica como «instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realiza el diagnóstico o el tratamiento del paciente tiene acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia» (apartado 1). Y, añade «cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten» (apartado 2).

fuera posible publicar los resultados de una investigación sin identificar a la persona que, participó en la misma o que aportó muestras biológicas, tales resultados sólo podrán ser publicados cuando haya mediado el consentimiento expreso o previa de aquélla (artículo 5.4 y 5).

Por otra parte, la información que se ha de facilitar a los participantes en una investigación, ha de incluir el propósito, plan detallado, las molestias, y los posibles riesgos y beneficios de la investigación, y las medidas para asegurar el respeto a la vida privada y a la confidencialidad de los datos personales de acuerdo con las exigencias previstas en la legislación sobre protección de datos de carácter personal (artículo 15.2 d)).

Lo cierto es que la prohibición tajante de utilizar datos relativos a la salud de las personas con fines distintos a aquellos para los que se prestó el consentimiento y el sometimiento de cualquier persona que, tenga acceso a los datos personales en el ejercicio de sus funciones al deber de secreto, incluso después de haber cesado en la investigación, son garantías suficientes y muy valiosas en relación con el derecho de las personas a la protección de sus datos personales. Igualmente, como hemos visto, la difusión del resultado de una investigación cede ante el carácter prevalente del derecho a la protección de datos, ya que si tal publicación requiere la identificación de la persona que participó en la investigación, se ha de solicitar su consentimiento expreso y previo.

Como el artículo 87.5 de la Ley 29/2006, el artículo 8 de esta Ley exige que se respete el deber de confidencialidad y lo dispuesto en la LOPD en relación con el proceso de trazabilidad de las células, tejidos y cualquier materia biológico de origen humano. De igual manera, el artículo 42.2 requiere que, el Banco Nacional de Líneas celulares mantenga la confidencialidad de los datos y demás exigencias respecto de las actuaciones que se lleven a cabo, de acuerdo con lo establecido en la Ley 14/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida, y en la LOPD, y contempla en sus actuaciones los principios de precaución, proporcionalidad y ausencia de lucro.

Precisamente, la citada Ley 14/2006, dispone en su artículo 3.6 que todos los datos relativos a la utilización de estas técnicas deberán recogerse en la historia clínica de cada persona, que deberán ser tratadas con las debidas garantías de confidencialidad respecto a la identidad de los donantes, de los datos y condiciones de los usuarios, y de las circunstancias que concurran en el origen de los hijos así nacidos. No obstante, se tratará de mantener la máxima integración posible de la documentación clínica de la persona usuaria de las técnicas.

Por su parte, el artículo 15.1 e) garantiza la confidencialidad de los datos de los progenitores en la cesión de preembriones, y el artículo 18.3 establece la obligación de los equipos médicos de recoger en una historia clínica, custodiada con la debida protección y confidencialidad, todas las referencias sobre los donantes y usuarios, así como los consentimientos firmados para la realización de la donación o de las técnicas. Los datos contenidos en estas historias clínicas, excepto la identidad de los donantes, deberán ser puestos a disposición de la receptora y de su pareja o, de hijo nacido por estas técnicas, cuando llegue a su mayoría de edad, o de sus representantes legales, si así lo solicitan. También se contienen en esta Ley, el derecho a la confidencialidad de los donantes en relación con los datos que de los mismos deben figurar en el registro Nacional de Donantes (artículo 21.1), y se exige que, para la adopción de determinadas medidas dentro de los procedimientos sancionadores regulados en la Ley, se adopten las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los dere-

chos a la intimidad personal y familiar, y a la protección de los datos personales cuando éstos pudieran resultar afectados (artículo 24.4).

Por otra parte, el artículo 79 del Reglamento de la LOPD establece la obligación de los responsables de los tratamientos de datos o los ficheros de implantar las medias de seguridad con arreglo a lo dispuesto en el Título VIII del citado Reglamento, con independencia de cuál sea su sistema de tratamiento. Como hiciera ya la LOPD, el Reglamento hace referencia a tres niveles de seguridad, básico, medio y alto que son de aplicación cumulativa, de forma que los datos garantizados con un nivel de seguridad alto -como es el aplicable a los datos de salud-, también son receptores de medidas de seguridad de nivel medio y básico. No obstante, el artículo 81.5 rebaja el nivel de protección reforzada al nivel básico entre otros, de los datos de salud en los siguientes supuestos: a) Cuando se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros; o b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad. Además, también podrán implantarse medidas 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 todo caso, las garantías reforzadas que el denominado nivel alto de protección otorga a los datos sensibles entre los que se encuentran los datos de la salud, se refiere a ámbitos de gestión y distribución de soportes (artículo 101); a copias de respaldo y recuperación (artículo 102); registros de acceso (artículo 103); y telecomunicaciones (artículo 104). En relación con la gestión y distribución de soportes, el Reglamento establece una serie de medidas relativas al sistema de etiquetado de manera identificable para las personas autorizadas, y que no dificulten la identificación a los terceros. Asimismo, se prevén medidas de cifrado u otro mecanismo similar para asegurar que la información no sea accesible ni pueda ser manipulada durante su transporte. También se cifrarán los datos que contengan los dispositivos portátiles, cuando éstos se encuentren fuera de las instalaciones que, están bajo el control del responsable del fichero. Por último, el Reglamento aconseja evitar el tratamiento de los datos de carácter personal en dispositivo portátiles que, no permitan su cifrado. Si, con todo, hubiera de realizarse éste, deberán constar motivadamente en el documento de seguridad y se deberán adoptar las medias que tengan en cuenta los riesgos de realizar tratamientos de datos en entornos desprotegidos.

En relación a las copias de respaldo y de procedimientos de recuperación, el Reglamento establece que deberán conservar una copia de tal respaldo y procedimientos de recuperación en lugar diferente de aquel en que se encuentran los equipos informáticos que los tratan, garantizándose de este modo, la integridad y recuperación de la información, de forma que sea posible su recuperación. En cuanto a los registros de accesos que en cada intento de acceso se guardan, como mínimo la identificación del usuario, la fecha, y la hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado; si el acceso gozó, además, de una autorización también debe guardarse la información sobre ésta que, permita identificar el registro accedido.

Los mecanismos que permiten el registro de accesos deberán estar bajo el control directo del responsable de seguridad competente, y no deben permitir su desactivación ni la manipulación de los mismos. El período mínimo de conservación de los datos registrados será de dos años. La garantía en este punto se refuerza, pues, el responsable de seguridad se encargará de revi-

sar al menos una vez al mes, la información de control registrada, y elaborará al efecto un informe de las revisiones realizadas y los problemas detectados.

De todas formas, no será necesario el registro de accesos regulado en el artículo 103 cuando concurran las siguientes circunstancias: a) Que el responsable del fichero o del tratamiento sea una persona física; b) Que el responsable del fichero o del tratamiento garantice que, únicamente él tiene acceso y trata los datos personales.

Este nivel de garantía también contiene previsiones en el ámbito de las telecomunicaciones al disponer el artículo 104 del citado Reglamento que, conforme el artículo 81.3 deben implantarse las medidas de seguridad de nivel alto en la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas, y que habrá de realizarse cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice, que la información no sea inteligible ni manipulada por terceros.

IV. Datos genéticos como datos de la salud.

La Declaración Internacional Sobre Datos Genéticos Humanos de 2003, declara en su Preámbulo que «la información genética forma parte del acervo general de los datos médicos», por lo que insiste en la vinculación entre los datos genéticos y los datos de la salud.

No obstante, en la doctrina desde hace tiempo se ha considerado que, los datos genéticos ha de ser objeto de una protección y estatus especial, y ello por las características particulares que presenta la información genética y que la hacen especialmente sensible, así se destaca: a) Su carácter único o singularidad, en cuanto que todo individuo es un ser genéticamente irrepetible (salvo en el caso de gemelos monocigóticos). En consecuencia, los datos genéticos son reflejo de la propia individualidad de la persona y dan cuenta de su identidad genética única y singular; b) Es permanente e inalterable, ya que acompaña al individuo a todo lo largo de toda su vida, salvo la existencia de mutaciones genéticas espontáneas o provocadas (ingeniería genética); c) Es indestructible, pues, se halla presente prácticamente en todas las células del organismo, durante la vida e incluso después de la muerte; d) Es una información no voluntaria; e) Tiene capacidad predictiva en la medida en que, en algunos casos, permite conocer anticipadamente la aparición futura de enfermedades o de predisposiciones o susceptibilidades a enfermedades; f) Finalmente, la información genética establece la vinculación biológica del individuo con su familia, de la que también aporta información[25].

Sin embargo, en el documento elaborado por el Grupo de Experto de la Comisión Europea, bajo el título 25 Recomendación sobre las repercusiones éticas, jurídicas y sociales de los test genéticos, se intenta evitar el denominado excepcionalismo genético, pues, se considera que, no resulta correcto establecer una diferenciación entre los datos genéticos y otros datos médicos; de forma que, todos los datos médicos merecen en todo momento los mismos niveles de calidad y confidencialidad.

Por su parte, en la Recomendación número R (97) 5 del Comité de Ministros del Consejo de Europa sobre protección de datos médicos se contiene una definición de los datos genéticos como «todos los datos, cualquiera que sea su clase, relativos a las características hereditarias de un individuo o al patrón hereditario de tales características dentro de un grupo de individuos emparentados», asimismo, hace referencia a «los datos sobre cualquier información genética que el individuo porte (genes) y a los datos de la línea

25. **Abellán Sánchez F.,** Selección genética de embriones: entre la libertad reproductiva y la eugenesia, Comares, Granada, 2007, pp. 169-181; del mismo autor, «Datos genéticos y la investigación biomédica», *Comentario a la Ley Orgánica de Protección de Datos de carácter personal, director Antonio Troncoso Reigada*, Civitas-Thomson Reuters, Navarra, 2010, pp. 686-687.

genética relativos a cualquier aspecto de la salud o la enfermedad, ya se presente con caracteres identificables o no». Se señala, también que, la línea genética estará constituido por similitudes genéticas resultantes de una procreación y compartida por dos o más individuos. De manera que, define los datos médicos como «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».

En esta misma Recomendación se proclama, igualmente que, los datos genéticos recogidos y procesados para el tratamiento preventivo, el diagnóstico o el tratamiento del afectado o para la investigación científica, sólo deben emplearse para esos fines, o para permitir al afectado tomar una decisión libre e informada en estas materias. Además, se contempla la posibilidad de procesamiento de los datos genéticos con fines judiciales o de investigación criminal, siempre que sea objeto de una ley específica que, ofrezca medidas de salvaguardia adecuadas (artículo 4.8). Con igual garantía legal admite la Recomendación la recogida y procesamiento de datos genéticos en orden a predecir enfermedades en casos en que exista un interés superior (artículo 4.9).

Ni la Ley 8/2001, de Protección de Datos de la Comunidad de Madrid, ni la Ley 2/2004, de la Agencia Vasca de Protección de Datos, ni el Decreto 104/2008, de Protección de Datos de carácter personal en Castilla-La Mancha, ni la Ley 32/2010 de la Autoridad catalana de Protección de Datos hacen referencia expresa a los datos genéticos. No obstante, la Agencia Española de Protección de Datos, como las Agencias creadas en las Comunidades Autónomas de Madrid, País Vasco y Cataluña consideran que, a los datos genéticos se han de aplicar el tratamiento de datos sensibles, por lo que deben recibir las garantías reforzadas que, la propia LOPD establece para este tipo de datos.

En esta línea, el Grupo de Trabajo del artículo 29 (GT 29) sobre protección de datos personales de la Unión Europea, creado por la Directiva 95/46/CE, como órgano consultivo independiente, integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea, con funciones de Secretariado, en su Documento sobre datos genéticos de 17 de marzo de 2004, considero que «dada la importancia de los datos genéticos y su conexión con informaciones susceptibles de revelar el estado de salud o el origen étnico, es conveniente considerarlos como datos sensibles, incluyéndolos en la definición del artículo 8, párrafo 1 de la Directiva y las leyes nacionales de transposición».

Tampoco se contiene referencia expresa al derecho de protección de datos en el ámbito biomédico en el Convenio de Oviedo de 1997, simplemente, en el Capítulo IV dedicado al Genoma humano, se señala en su artículo 11 que se prohíbe cualquier tipo de discriminación de la persona a causa de su patrimonio genético; y en su artículo 12 se establece que, sólo podrá realizarse pruebas predictivas de enfermedades genéticas o que permitan identificar al sujeto como portador de un gen responsable de una enfermedad, o detectar una predisposición o una susceptibilidad genética a una enfermedad, exclusivamente para fines médicos, o de investigación médica y con un asesoramiento genético apropiado.

Por su parte, el Reglamento de la LOPD sí menciona la información genética en su artículo 5.1 g) a efecto de asimilarla a lo que el citado Reglamento denomina datos relacionados con la salud. Igualmente, en la ley 14/2007, de Investigación biomédica se equiparan los datos genéticos relacionados con la salud a los datos de salud, recibiendo las mismas garantías que éstos, sin

perjuicio dice el artículo 47 de lo establecido en la LOPD. Y se define dato genético de carácter personal como «la información sobre las características hereditarias de una persona identificada o identificable obtenida por el análisis de ácido nucleicos u otros análisis científicos»[26].

Con relación a tales datos, antes de que el sujeto preste su consentimiento, dispone esta Ley que, ha de ser informado de los datos genéticos de carácter personal que, se obtengan del análisis genético según los términos en que manifestó su voluntad, sin perjuicio del derecho de acceso reconocido en la legislación sobre protección de datos de carácter personal, que podrá suponer la revocación de la previa manifestación de voluntad libremente otorgada (artículo 49). El consentimiento deberá ser expreso y específico por escrito para la realización de un análisis genético. Si bien, para acceder al cribado genético será precisa el consentimiento explícito y por escrito del interesado. El Comité de Ética de la Investigación determinará, asimismo, los supuestos en los que el consentimiento podrá expresarse verbalmente.

En todo caso, cuando el cribado incluya enfermedades no tratables o los beneficios sean escasos inciertos, el consentimiento se obtendrá siempre por escrito. En cuanto a la obtención y análisis de muestras de personas fallecidas, se podrán llevar a cabo, siempre que pueda resultar de interés para la protección de la salud, y salvo que el fallecido lo hubiese prohibido expresamente en vida. Para ello, se ha de consultar los documentos de instrucciones previas y, en su defecto, a los familiares más próximos del fallecido. El acceso de los familiares biológicos a la información derivada del análisis genético del fallecido, se limitará a los datos genéticos pertinentes para la protección de la salud de aquéllos. La realización de análisis genéticos sobre preembriones *in vivo* y sobre embriones y fetos en el útero, requerirán el consentimiento expreso de la mujer gestante (artículo 48).

El acceso de los profesionales sanitarios del centro o establecimiento donde se conserve la historia clínica del paciente, y por tanto, los datos genéticos que consten en la misma, tiene un alcance limitado, pues, sólo tendrá lugar en la medida que sea pertinente para la asistencia que se presta al paciente (artículo 50.1). El deber de secreto del personal sanitario respecto de tales datos sólo puede exceptuarse por el consentimiento expreso y escrito del afectado (artículo 51.1); y, en el caso de análisis genético de varios miembros de una familia, los resultados se archivarán y comunicarán a cada uno de ellos de forma individualizada. En caso, de personas incapacitadas o menores se informará a los tutores o representantes legales (artículo 51.2).

La regla general para el uso de los datos genéticos es la exigencia de consentimiento expreso del afectado, salvo que los datos hayan sido previamente anonimizados (artículo 50.2)[27]. Sólo en casos excepcionales y de interés sanitario general, -que la Ley de Investigación Biomédica no precisa-, la autoridad competente previo informe favorable de la autoridad en materia de protección de datos (Agencia Española de Protección de Datos; o demás Agencias autonómicas), podrán autorizar la utilización de datos genéticos codificados, siempre asegurando que, no puedan relacionarse o asociarse con el sujeto fuente por parte de terceros (artículo 50.3).

Estos datos genéticos de carácter personal se conservarán durante un período mínimo de cinco años desde la fecha en que fueron obtenidos, transcurrido el cual el interesado podrá solicitar su cancelación. Si tal petición no tiene lugar, el responsable de los datos puede conservarlos durante el plazo que sea necesario para preservar la salud de la persona de quien procede o de terceros relacionados con ella. Con independencia de estos supuestos, los datos únicamente podrán conservarse, con fines de investigación, de forma anonimizada, sin que sea posible la identificación del sujeto fuente (artículo 52).

26. Desde esta perspectiva, el Grupo Europeo de Ética de las ciencias y de las nuevas tecnologías en su Dictamen sobre Aspectos éticos de los implantes TIC en el cuerpo humano, pone de relieve cómo la implantación de tales dispositivos en nuestro organismo le convierte en una fuente de generación de datos a los que es necesario aplicar los principios relativos a la protección de datos de carácter personal; y, el Grupo de Trabajo sobre protección de datos del artículo 29, en su Documento de Trabajo sobre Datos Genéticos adoptado el 17 de marzo de 2004, manifiesta como las muestras de ADN tomadas en el lugar de un crimen, pueden constituir una fuente de datos personales.
Vid., en torno al tratamiento de la información genética en el marco de la Ley 14/2007, de Investigación biomédica, **De Miguel Sánchez N.**, «Investigación y protección de datos de carácter personal: Una aproximación a la Ley 14/2007, de 3 de julio de Investigación Biomédica», *Revista Española de Protección de Datos, número 1, 2006,* pp. 143 y siguientes.

27. Según establece el artículo 3 c) de la Ley 14/2007, anonimización es *«el proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere. Es aplicable también a la muestra biológica».*

En relación con información relativo a la utilización de muestras biológicas, el artículo 59 de la Ley establece que, sin perjuicio de lo previsto en la legislación sobre protección de datos de carácter personal, y en particular, del artículo 45 de esta ley, antes de emitir el consentimiento para la utilización de una muestra biológica con fines de investigación biomédica que, no vaya a ser sometida a un procedimiento de anonimización, el sujeto fuente deberá ser informado por escrito, entre otros aspectos:

a) Finalidad de la investigación o línea de investigación para la cual consiente;

b) Beneficios esperados,

c) Posibles inconvenientes vinculados con la donación y obtención de la muestra, incluida la posibilidad de ser contactado con posterioridad con el fin de recabar nuevos datos u obtener otras muestras;

d) Identidad del responsable de la investigación;

e) Derecho de revocación del consentimiento y sus efectos, incluida la posibilidad de la destrucción o de la anonimización de la muestra, y de que tales efectos no se extenderán a los datos resultantes de las investigaciones que ya se hayan llevado a cabo;

f) Lugar de realización del análisis y destino de la muestra al término de la investigación: disociación, destrucción, u otras investigaciones, y que, en su caso, comportará a su vez el cumplimiento de los requerimientos previstos en la Ley. En el caso de que estos extremos no se conozcan en el momento, se establecerá el compromiso de informar sobre ello en cuanto se conozca;

g) Derecho a conocer los datos genéticos que se obtengan a partir del análisis de las muestras donadas;

h) Garantía de confidencialidad de la información obtenida, indicando la identidad de las personas que tendrán acceso a los datos de carácter personal del sujeto fuente;

i) Advertencia sobre la posibilidad de que se obtenga información relativa a su salud derivada de los análisis genéticos que se realicen sobre su muestra biológica, así como sobre su facultad de tomar una posición en relación con su comunicación;

j) Advertencia de la implicación de la información que se pudiera obtener para sus familiares, y la conveniencia de que él mismo, en su caso, transmita dicha información a aquéllos; y

k) Indicación de la posibilidad de ponerse en contacto con él/ella, para lo que podrá solicitárseles la información contenidas en los apartados a), b), c), y d) de este artículo.

En el caso que la muestra sea conservada sin anonimización, el sujeto fuente debe ser informado por escrito de las condiciones de conservación, objetivos, usos futuros, cesión a terceros y condiciones para poder retirarlas o

pedir su destrucción. No obstante, las muestras biológicas utilizadas en la investigación biomédica se conservarán únicamente en tanto sean necesarias para los fines que justificaron su recogida, salvo que el sujeto fuente haya otorgado su consentimiento explícito para otros usos posteriores (artículo 61).

En relación a los biobancos, los artículos 63 a 71 de la Ley ofrecen una regulación detallada en relación a los mismos[28]. Están sujetos por sus propios fines a la legislación sobre protección de datos de carácter personal. Precisamente en el artículo 66.2 c) entre las obligaciones que tendrá el director de un biobanco, está la de garantizar la calidad, la seguridad y la trazabilidad de los datos y muestras biológicas almacenadas y de los procedimientos asociados al funcionamiento del biobanco. Asimismo, establece la ley que el responsable del fichero deberá atender a las solicitudes del ejercicio de los derechos de acceso, rectificación, cancelación u oposición formuladas por los sujetos fuente, de conformidad con la normativa vigente en materia de protección de datos de carácter personal (artículo 66.3).

En cuanto a la cesión de muestras, deberá ir acompañada de la información clínica asociada, en cuyo caso los datos estarán protegidos según lo dispuesto en la Ley de Autonomía del Paciente, y la LOPD (artículo 69.6).

La regulación y garantías sobre obtención, información previa, consentimiento, confidencialidad, cesión, conservación de datos y muestras biológicas en la propia Ley de Investigación biomédica, serán de aplicación también a las muestras depositadas en biobancos, aunque las muestras biológicas que se incorporen a los biobancos, puedan utilizarse para cualquier investigación biomédica, de acuerdo con la Ley, cuando exista consentimiento del sujeto fuente o de sus representantes legales (artículo 70).

Una vez constituidos los biobancos deben inscribirse en la Agencia Española de Protección de Datos previamente a su también preceptiva inscripción en el Registro Nacional de Biobancos para la Investigación Biomédica, bajo la dependencia del Instituto de Salud Carlos III. La inscripción en la Agencia Española de Protección de Datos tiene efectos declarativos y no constitutivos (artículo 67).

En este contexto, nuestra Ley de Enjuiciamiento Criminal prescribe que, siempre que concurran acreditadas razones que lo justifiquen, el Juez de Instrucción puede acordar, en resolución motivada, la obtención de muestras biológicas del sospechoso que resulten indispensables para la determinación de su perfil de ADN. A tal fin, podrán decidir la práctica de aquellos actos de inspección, reconocimiento o intervención corporal que resulten adecuados a los principios de proporcionalidad y razonabilidad, lo que podrán llevarse a cabo incluso contra voluntad del afectado, por constituir una prueba esencial para investigar su participación o no en un delito (artículo 363 segundo párrafo)[29].

Por su parte, el artículo 58.2 párrafo segundo de la Ley de Investigación biomédica, contempla una excepción al consentimiento del sujeto fuente para la utilización de sus muestras cuando su obtención no sea posible o represente un esfuerzo no razonable, y siempre que cuente con el informe favorable del Comité de Ética de la Investigación del Centro, que deberá tener en cuenta como mínimo los siguientes requisitos:

a) Que se trate de una investigación de interés general;

b) Que la investigación se lleve a cabo por la misma institución que solicitó el consentimiento para la obtención de

28. Biobanco es como señala el artículo 3 d) de la Ley 14/2007 *«el establecimiento público o privado, sin ánimo de lucro, que acoge una colección de muestras biológicas concebida con fines diagnósticos o de investigación biomédica y organizada como una técnica con criterios de calidad, orden y destino».*

29. Modificado por la Disposición Final primera de la Ley Orgánica 15/2003, de 25 de noviembre de modificación del Código Penal.

las muestras;

c) Que la investigación sea menos efectiva o no sea posible sin los datos identificativos del sujeto fuente;

d) Que no conste una objeción expresa del mismo; y,

e) Que se garantice la confidencialidad de los datos de carácter personal.

Finalmente, en el ámbito internacional es importante resaltar la Declaración Internacional sobre los Datos Genéticos Humanos aprobada por la XXXII Conferencia General de la Unesco de 16 de octubre de 2003, en la que, además de fijar el principio de consentimiento informado del interesado para la obtención de sus datos genéticos, establece que los datos genéticos humanos y los datos proteómicos humanos, podrán ser tratados, utilizados y conservados solamente con los fines siguientes:

1. Diagnósticos y asistencia sanitaria, que incluye pruebas de cribado y predictivas;

2. Investigación médica y otras formas de investigación científica, comprendidos los estudios epidemiológicos, en especial, los de genética de poblaciones, así como los estudios de carácter antropológicos o arqueológicos;

3. Medicina forense y procedimientos civiles o penales u otras actuaciones legales; y,

4. Cualesquiera otros fines compatibles con la Declaración Universal sobre el Genoma Humano y los Derechos Humanos y el derecho internacional relativo a los derechos humanos (artículo 5).

Correspondencia
Departamento de Derecho Civil.
Facultad de Derecho. Universidad Complutense de Madrid
Ciudad Universitaria, s/n
28040 Madrid
aiberrocalanzarot@d.ucm.es