El derecho fundamental a la protección de datos de salud

Canales Gil, A.[1]

Sanid. mil. 2009; 65 (1): 23-36

INTRODUCCIÓN

El derecho fundamental a la protección de datos de carácter personal no es reconocido como tal en todos los países. Sin embargo, hay una cuestión que cada vez despierta una unanimidad más amplia. Resulta preciso proteger a la persona, respecto al desarrollo exponencial de las tecnologías de la información y las telecomunicaciones, porque la posibilidad de un tratamiento cada vez más eficaz de sus datos no puede convertirse en un fin en sí mismo y, por tanto, realizarse al margen de su consentimiento.

Actualmente aparecen, casi a diario, nuevos retos a la protección de datos personales. La Telemedicina, el uso de sistemas de Radiofrecuencias, la cada vez más potente y funcional telefonía móvil, por poner solamente tres ejemplos, son nuevos riesgos que, utilizados sin las debidas garantías, pueden invadir seriamente la esfera más íntima del individuo. Al igual que hoy, en el pasado hubo reacciones frente al uso abusivo y, por tanto, invasivo de lo que tradicionalmente se conocía como «*la Informática*» sobre la esfera de la privacidad del individuo.

La citada reacción reviste caracteres más preocupantes si la invasión de la privacidad del individuo afecta a los datos personales que afectan a las esferas más íntimas del individuo. En este sentido, se encuentran los datos que se afectan a la salud de los ciudadanos. Es tan sensible esta esfera de los datos sanitarios que, incluso, como más adelante se verá, el paciente tiene el «*derecho a no saber*» en relación a una determinada patología.

En consecuencia en el presente artículo, después de describir sintéticamente las principales características del derecho fundamental a la protección de datos de carácter personal, se pasará examen a las cuestiones más relevantes referidas a este derecho en el ámbito sectorial sanitario, entre otras, el concepto de dato de salud, el principio de consentimiento para la recogida y tratamiento de datos de salud, las medidas de seguridad aplicables, las obligaciones de custodia y conservación de las historias clínicas, el derecho de acceso a éstas y sus limitaciones, el posible acceso a la documentación clínica sin consentimiento del paciente e, incluso, en el caso de que éste hubiese fallecido, el deber de secreto de los profesionales sanitarios, el «*derecho a no saber*» que reconoce la legislación a todo paciente, y el tratamiento de los datos de salud en ensayos clínicos y estudios genéticos.

Asimismo, se pondrá especial énfasis en señalar las principales diferencias y complementariedades existentes entre algunos términos que se emplean por el Legislador en relación al derecho a la información asistencial y al derecho fundamental a la protección de datos de salud. Dentro de las primeras, el asunto más relevante será el dedicado a analizar la diferencia entre el derecho al «*consentimiento informado*», propio de las leyes de atención al paciente, y el principio de consentimiento propio del derecho fundamental citado. Entre las complementariedades entre las normativas reguladoras del derecho a la protección de datos y del derecho a la información sanitaria y atención al paciente, se examinarán algunas, como por ejemplo, la relativa al derecho de acceso a la historia clínica.

La experiencia ha demostrado que, en la mayor parte de las ocasiones, cuando los profesionales sanitarios han vulnerado el derecho a la protección de datos, lo han hecho ignorando la existencia de dicho derecho fundamental y movidos por un encomiable pero peligroso voluntarismo orientado a procurar una adecuada asistencia sanitaria de sus pacientes.

Es de desear que el presente artículo sirva para que los profesionales sanitarios, por un lado, conozcan las obligaciones que el derecho fundamental a la protección de datos les impone en el tratamiento de los datos de salud, y, por otro, diferencien dichas obligaciones de las que se derivan también para ellos del derecho a la información sanitaria y atención al paciente.

I. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL ORDENAMIENTO JURÍDICO ESPAÑOL

1. RÉGIMEN JURÍDICO VIGENTE

Hoy en día existe en nuestro país un marco jurídico regulador de la protección de datos personales, entre los que se incluyen lógicamente los relativos a la salud. Está constituido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), que entró en vigor el 14 de enero de 2000, salvo en lo que se refiere a ficheros preexistentes o a la aplicación de medidas de seguridad, y por su Reglamento de desarrollo aprobado por Real Decreto 1720/2007, de 21 de diciembre (en lo sucesivo RLOPD), que ha entrado en vigor el 19 de abril de 2008, y que suponen la trasposición a nuestro ordenamiento jurídico de la Directiva del Parlamento Europeo y del Consejo 95/46/CEE, de 24 de octubre, «*relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*»(1).

1 Tcol. Interventor. Ex-Subdirector General de Inspección y ex-Secretario General de la Agencia Española de Protección de Datos.

Recibido: 6 de agosto de 2008.
Aceptado: 13 de enero de 2009.

(1) Después de esta Directiva, «transversal», se aprobaron las siguientes que vienen a regular la protección de datos en algunos ámbitos concretos: Directiva 97/66/CE, relativa al tratamiento de los datos personales y protección a la intimidad en el sector de las telecomunicaciones; Directiva 99/93/CE, sobre firma electrónica; Directiva 00/31/CE, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior; Directiva 02/58/CE, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

2. ÁMBITO DE APLICACIÓN

La normativa de protección de datos únicamente se extiende respecto de datos relativos a personas físicas identificadas o identificables[2].

De acuerdo con lo señalado, es preciso resaltar las siguientes consideraciones:

- ➢ *«Las personas fallecidas no tienen derecho a la protección de datos de carácter personal»*, ya que, a tenor del artículo 32 del Código Civil, *«La personalidad se extingue por la muerte de las personas»*.

En relación con esta consideración, es preciso puntualizar lo siguiente que puede tener directa aplicación al ámbito sanitario:

- Las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos[3].
- La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (en lo sucesivo LAP)[4], establece un régimen especial de acceso a la historia clínica de los pacientes fallecidos al establecer que los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica a las personas vinculadas por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. Más adelante se volverá sobre este asunto.

- ➢ *«Las personas jurídicas no poseen derecho a la protección de datos de carácter personal»*[5].
- ➢ *«Para que se aplique la LOPD es preciso que exista un fichero automatizado o manual»*, es decir, que consista en un conjunto estructurado conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a sus datos personales[6].
- ➢ «Los datos de las personas físicas han de ser identificados o identificables». En relación a dicho asunto, la Directiva 95/46/CEE señala[7] *que «para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a dicha persona»*. El RLOPD, en su artículo 5.1.o), establece que «*o) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados»*.

De acuerdo con ello, los principios de la protección de datos no se aplicarán a aquellos datos respecto de los que no sea posible identificar al interesado. Más adelante se completará este análisis con algunas aplicaciones que se producen en el ámbito sanitario[8].

- ➢ *«La LOPD no se aplicará a los ficheros mantenidos por personas físicas para el ejercicio de actividades exclusivamente personales o domésticas»*[9]. Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.

3. SUJETOS OBLIGADOS

Los artículos 3.d) y g) de la LOPD y 5.1.q) e i) del RLOPD señala, como sujetos obligados en el derecho fundamental a la protección de datos, al responsable del fichero o tratamiento y al encargado de tratamiento. El primero en cuanto que es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. El encargado de tratamiento porque es la persona física o jurídica, pública o privada, u órgano administrativo que, sólo o conjuntamente con otros, trata datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. En el ámbito de los datos de salud, como luego se analizará, sería el caso del promotor (responsable del fichero) y del monitor (encargado de tratamiento) en el entorno del desarrollo de un ensayo clínico con medicamentos.

4. PRINCIPIOS GENERALES

La Directiva 95/46/CEE y, lógicamente, la LOPD que la transpone a nuestro ordenamiento jurídico reconocen que el tratamiento de datos personales ha de ajustarse a los principios de información, de consentimiento, de calidad, y de seguridad. A continuación se hace una breve síntesis de cada uno de ellos.

4.1. Principio de Información

Los artículos 5 de la LOPD y 18 del RLOPD regulan el deber de información, que incumbe a los responsables de los ficheros o tratamientos, así como el modo de acreditar su cumplimiento[10]. De acuerdo con lo señalado en dichos preceptos, cabe deducir las siguientes conclusiones:

(2) Artículos 3.a) de la LOPD y 2 y 5.1.f) del RLOPD.
(3) Artículo 2.4 del RLOPD.
(4) Artículo 18.4.
(5) Considerando 24 de la Directiva 95/46/CEE.
(6) Considerando 27 de la Directiva 95/46/CEE.
(7) Considerando 26.
(8) Por ejemplo, en el caso de las excepciones al principio de consentimiento para el tratamiento y cesión de los datos de salud.
(9) Sobre este asunto resulta especialmente interesante consultar la Sentencia del Tribunal de Justicia de las Comunidades Europeas de 6 de noviembre de 2003 (caso *«Bodil Lindqvist»*), sobre cuya doctrina no me voy a detener por exceder al contenido y extensión del presente artículo. Ver Artículo 4.a) del RLOPD.
(10) El Tribunal Constitucional, en Sentencia 292/2000, señala que dicho deber es indispensable para hacer efectiva la definición constitucional del derecho fundamental a la protección de datos personales, y señala en su Fundamento Jurídico Séptimo que *«En fin, son elementos característicos de la definición constitucional del derecho funda-*

- *«Es obligatorio que los responsables de ficheros o tratamientos procedan a informar a los interesados, previamente a la recogida de sus datos y de modo expreso, preciso e inequívoco, de los extremos a que se refiere el artículo 5.1 de la LOPD*[11]», ya que son elementos característicos del derecho fundamental a la protección de datos los derechos del afectado a consentir sobre la recogida y uso de sus datos personales.

Por ello, la habilitación para tratar los datos por parte del responsable, salvo que la misma le venga atribuida por una ley o que los datos se encuentren recogidos en fuentes accesibles al público, se basa siempre en los términos incluidos en la cláusula informativa que se le haya planteado al afectado en el momento de consentir la recogida de sus datos.

- *«Corresponde al responsable del fichero o tratamiento la obligación de probar que ha cumplimentado el deber de informar»*. Para dicho fin deberá de conservar los soportes originales, incluso por medios informáticos o telemáticos siempre que permitan acreditar que no se han alterado[12].

4.2. Principio de Consentimiento

De acuerdo con lo señalado, el tratamiento de datos personales se basa en el consentimiento del afectado, salvo que una ley lo excepcione o que los datos tratados procedan de fuentes accesibles al público.

El artículo 3.h) de la LOPD y el artículo 5.1.d) del RLOPD entienden por consentimiento del interesado «*toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen*.»

En casos muy concretos[13], no vale con la recogida del consentimiento inequívoco del interesado, sino que se requiere el consentimiento expreso, para datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, o el consentimiento expreso y por escrito, para datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias.

Por lo que se refiere a las excepciones al principio de consentimiento para el tratamiento de sus datos, el artículo 6.2 de la LOPD y el artículo 10.2 y 3 del RLOPD disponen lo siguiente:

- Dentro de los casos de excepción del principio de consentimiento, por existir habilitación legal o por tratarse del ejercicio de las funciones propias de las Administraciones Públicas en el ejercicio de sus competencias, se pueden mencionar los ámbitos fiscal[14], de la Seguridad Social[15], de Prevención de Riesgos Laborales[16], o de Prevención del Blanqueo de Capitales[17].
- En el supuesto del desarrollo de una relación contractual cuando el tratamiento de los datos sea necesario para su mantenimiento o cumplimiento. En relación con esta excepción, la Agencia Española de Protección de Datos suele conocer de casos en los que, o bien se trataron los datos del afectados sin que éste hubiese suscrito contrato alguno[18], o bien se hizo para alguna finalidad que no tiene que ver, directamente, con el mantenimiento o cumplimiento del citado contrato.
- Respecto a la excepción del consentimiento inequívoco por la vía del artículo 7.6 de la LOPD, como más adelante se abordará, la cuestión a dilucidar es hasta qué punto todas las entidades imputadas por un tratamiento sin consentimiento de datos de salud alegan que cuentan con habilitación para ello a tenor de dicho precepto. Sobre este asunto, conviene recordar que la regla general es la recogida en el artículo 7.3 de la LOPD, siendo el artículo 7.6 la excepción a dicha regla. Así lo ha manifestado la Audiencia Nacional en dos importantes Sentencias de 26 de septiembre y 12 de abril de 2002, cuando en esta última analizó el tratamiento de datos de salud para el control del absentismo laboral.

4.3. Principio de Calidad

Respecto del principio de calidad de los datos, regulado en el artículo 4,1, 2, 3, 4 y 5 de la LOPD y en el artículo 8 del RLOPD, cabe efectuar las siguientes consideraciones:

- Los datos pueden recogerse para su tratamiento siempre que sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, de modo que existe una sutil distinción entre *«finalidad de la recogida»* y *«finalidad del tratamiento»*, pues la recogida sólo puede hacerse con fines determinados, explícitos y legítimos, y el tratamiento posterior no puede hacerse de manera incompatible con dichos fines. De este modo, y de acuerdo con el artículo 1,b) de la Directiva 95/46/CEE, si la recogida se hizo con fines determinados *«cualquier uso o tratamiento con finalidad distinta es incompatible con la primera finalidad que determinó su captura por lo que, en este contexto, diferente e incompatible significan lo mismo»*[19].

---

mental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.
Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele.»

(11) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, y de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

(12) Artículo 12.3 del RLOPD.

(13) Artículo 7,2 y 3 de la LOPD.

(14) Ley 58/2003, de 17 de diciembre, General Tributaria.

(15) Real Decreto Legislativo 1/1994, de 20 de junio, por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social.

(16) Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

(17) Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales.

(18) Sentencia de la Audiencia Nacional de 18 de mayo de 2005, que ratificó la sanción impuesta en Resolución de la Agencia de 14 de marzo de 2003.

(19) √Sentencia de la Audiencia Nacional de 2 de marzo de 2005.

- ➢ Los datos del afectado deben de responder, con veracidad, a la situación actual del mismo.
- ➢ Por último, es preciso señalar que cuando los datos hayan dejado de ser necesarios para la finalidad determinada, explícita y legítima que motivó su recogida, deberán ser cancelados pero de modo que, en todo caso, se evite que nadie diferente al afectado pueda acceder a dichos datos.

Por ello, si alguno de los citados datos ya no son necesarios, deberán conservarse bloqueados, a tenor del artículo 16.3 de la LOPD y del artículo 5.1.b) del RLOPD, a expensas de la atención de las posibles responsabilidades surgidas del tratamiento, hasta que transcurran los correspondientes plazos de prescripción. Por el contrario, si algún dato ya no se encuentra supeditado a ningún plazo de esta naturaleza, no podrá, en ningún caso, ser dejado al alcance de terceros, como, por ejemplo, cuando algunos responsables los depositan en la vía pública en contenedores especiales de papel para que sean posteriormente reciclados.

Como consecuencia de lo señalado, en materia de protección de datos, la obligación de secreto de los datos de los afectados subsiste para el responsable del fichero sea cual sea el plazo de prescripción de las posibles responsabilidades surgidas del tratamiento. Nunca puede desentenderse de la confianza que depositó en él el titular de los datos, cuando decidió prestar su consentimiento para que los tratara en sus ficheros.

4.4. Principio de Seguridad

La LOPD en su artículo 9 se refiere a las medidas de seguridad que el responsable del fichero o el encargado del tratamiento han de implementar para que los datos personales sean gestionados en un entorno que impida su alteración, pérdida, tratamiento o acceso no autorizado por parte de terceros.

El RLOPD desarrolla el citado precepto de la LOPD y distingue en su regulación entre ficheros automatizados y manuales. Establece tres niveles de seguridad en función de la naturaleza de los datos sometidos a tratamiento.

Como común denominador a todos los niveles de seguridad, es preciso señalar que ha de existir el correspondiente *«Documento de Seguridad»*, en el que se recojan con carácter obligatorio las normas para el acceso a los sistemas de información del responsable o del encargado de tratamiento. Lo más importante es que este documento ha de ser un instrumento en continua evolución, de modo que responda, en todo momento, a las necesidades organizativas de la entidad o del profesional individual. Para ello, el registro de incidencias, el seguimiento de las claves de identificación y autenticación, así como de los controles de acceso, y, muy en especial, las auditorías bianuales (aplicables a partir del nivel de seguridad medio), han de contribuir a mantener actualizado el *«Documento de Seguridad»*.

Por tanto, la cuestión a dilucidar, a mi juicio, es la siguiente: *«¿Pueden existir "fugas de datos" a pesar de existir el correspondiente "Documento de Seguridad"?»*. Indudablemente puede haberlas, y no solamente cuando exista un *«Documento de Seguridad»* inadecuado. En este último caso, con más razón, si el citado *«Documento de Seguridad»* no es capaz de describir y controlar los flujos de información necesarios para delimitar un correcto funcionamiento de la organización. Piénsese, por ejemplo, en un centro hospitalario en el que cualquiera que presta servicios en el mismo pudiese acceder al archivo de historias clínicas y consultar cualquier documento incluido en ellas. En este caso, la falta de medidas de seguridad responde a un *«problema organizativo»*, que, sin duda, de probarse daría lugar a la declaración de alguna infracción en materia de protección de datos.

Sin embargo puede existir un *«Documento de Seguridad»* magníficamente concebido, actualizado y gestionado, y, no obstante, las *«fugas de datos»* también pueden producirse. Aquí el problema no es organizativo sino *«personal»*, motivado porque el usuario no ha atendido a sus obligaciones, bien intencionalmente, bien de una manera negligente. Respecto al primer comportamiento nada debe añadirse. Se trata de un usuario que, por una motivación externa a su tarea, decide provocar tales *«fugas de datos»*. El orden penal, laboral o estatutario, si se trata de un funcionario, establecerá, en su caso, las consecuencias de su comportamiento. El caso de la negligencia del usuario que puede provocar *«fugas de datos»*, es en el que ha de ponerse especial atención para que, en la medida de lo posible, no se produzca. Para ello, el usuario ha de comprender e interiorizar, en una palabra «*concienciarse*», que las *«claves de identificación y autenticación»* son el único instrumento a través del cual queda a salvo la correcta ejecución de las tareas que tenga encomendadas. La no actualización de ellas, su conocimiento por terceras personas (que no sea el responsable del fichero, el responsable de seguridad o el administrador del sistema), o el no bloqueo del terminal cuando se abandona el puesto de trabajo, pueden dar lugar a vulneraciones de la normativa de protección de datos que, además, no se pueden remediar ya que el sistema informático identifica, sin duda alguna, cuál fue el código de usuario desde el cual se produjo el acceso indebido.

Deben extremarse, por tanto, dichos controles a pesar de que, esté probado, el ser humano tiene mayor inclinación a la *«comodidad»* sobre la *«seguridad»* en el manejo de los sistemas de información. Por ello, sabedores de todo lo señalado, el usuario debe huir, por negligencia, de cualquier comportamiento que pueda causar *«fugas de datos personales»*, máxime cuando, además, las consecuencias penales, laborales y estatutarias, también pueden concurrir en el presente supuesto.

5. DERECHOS DE LOS INTERESADOS

Además de los principios señalados, la LOPD reconoce a favor de los interesados, cuyos datos están siendo tratados por los responsables de ficheros o tratamientos, una serie de derechos, de naturaleza personalísima aunque pueden ejercitarse a través de representación voluntaria[20], con el fin de que puedan conocer, rectificar, cancelar o, en su caso, oponerse a dichos tratamientos.

5.1. Derecho de acceso

El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso,

[20] Artículos 15 a 17 de la LOPD y 23 del RLOPD.

se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos[21]. En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento[22].

5.2. Derecho de rectificación

El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos[23].

5.3. Derecho de cancelación

El ejercicio del derecho de cancelación[24] dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos[25], sin perjuicio del deber de bloqueo.

En este sentido, la cancelación[26] es el procedimiento por el que el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

5.4. Derecho de oposición

El derecho de oposición[27] es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

- Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario[28].
- Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, cualquiera que sea la empresa responsable de su creación[29].
- Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal[30].

II. LA PROTECCIÓN DE DATOS DE SALUD

1. INTRODUCCIÓN

En el ámbito sanitario confluye la aplicación de leyes que imponen determinadas obligaciones a los profesionales sanitarios. Dentro de éstas, la LOPD presenta unas claras especialidades sobre el resto de normas en cuanto que establece dos tipos de obligaciones, unas «*positivas*» o «*de hacer*» y otras «*negativas*» o «*de no hacer*», y que, en todo caso, han de ser respetadas tanto por los responsables de ficheros o tratamientos como por los profesionales sanitarios que tratan los datos de los pacientes. Dichas obligaciones se formulan en la LOPD de la siguiente manera:

- Las primeras (que se han denominado «*positivas*» o «*de hacer*») se concretan en una serie de obligaciones de hacer que se han de implementar por parte de los responsables de los ficheros o tratamientos. En unos casos, se habrá de actuar antes de la creación del fichero, y, en otros, a lo largo del proceso del tratamiento de los datos relativos a la salud de los interesados. Dentro de las obligaciones que hay que desarrollar antes de creación del fichero, se encuentra la relativa a la obligación de notificación[31] a la Agencia Española de Protección de Datos o a las agencias de protección de datos autonómicas[32], en el caso de que dicha notificación afecte a ficheros que sean competencia de esas autoridades de control[33].

De entre las obligaciones «*positivas*» o «*de hacer*», aunque todas ellas son igualmente exigibles, sin embargo la que reviste mayor trascendencia, por la naturaleza especialmente protegida de los datos de salud, es la relativa a las medidas de seguridad que se han de implementar en un fichero que contenga datos de salud. En este sentido, la LOPD[34] se refiere a las necesarias medidas de seguridad que han de implementar los responsables del fichero y, en su caso, encargados de tratamiento, para evitar que terceros no autorizados accedan a los datos de salud, remitiéndose a la vía reglamentaria para fijar los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de la citada Ley Orgánica. El

[21] Artículos 15.1 de la LOPD y 27 del RLOPD.
[22] A tenor del artículo 28.1 del RLOPD, para hacer efectivo este derecho se podrá utilizar la visualización en pantalla, el medio escrito, copia o fotocopia remitida por correo, certificado o no, la telecopia, el correo electrónico u otros sistemas de comunicaciones electrónicas, o cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.
[23] Artículos 4.3 y 4, y 16.2 de la LOPD, y 31 a 33 del RLOPD.
[24] Artículos 16.3 de la LOPD y 31.2 del RLOPD.
[25] Artículo 16.2 de la LOPD.
[26] Artículo 5.1.b) del RLOPD.
[27] Artículos 6.4, 17 y 30.4 de la LOPD y 34 a 36 del RLOPD.
[28] Artículo 6.4 de la LOPD.
[29] Artículo 30.4 de la LOPD.
[30] Artículo 13.2 de la LOPD
.
[31] En este sentido los responsables de los ficheros o tratamientos han de haber desplegado una serie de actuaciones en orden a concretar la identificación del responsable del fichero, la identificación del fichero, las finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, los procedimiento y procedencia de los datos, las categorías de los datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad exigibles, las cesiones previstas, las transferencias internacionales de datos previstas, y, en su caso, la identificación del encargado del tratamiento.
[32] Decreto 40/2004, de 18 marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos de la Comunidad de Madrid. Decreto 48/2003, de 20 febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos. Ley 2/2004, de 25 febrero, de regulación de Ficheros de Datos de Carácter Personal de Titularidad Pública y de creación de la Agencia Vasca de Protección de Datos.
[33] Ficheros públicos autonómicos y locales en cada comunidad autónoma.
[34] Artículo 9.

RLOPD establece que deberán implementarse las medidas de seguridad de nivel alto[35] para los ficheros o tratamientos de datos concernientes a la salud, sin perjuicio de que se pueden aplicar las de nivel básico en los siguientes casos:

- Cuando los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros, o cuando se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad[36].
- Cuando los datos de salud se refieran 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[37].

➢ En cuanto a las denominadas obligaciones «*negativas*» o «*de no hacer*», se refieren a situaciones en las que el responsable del fichero o del tratamiento se ha de abstener de actuar si ello conlleva una conculcación de los principios que inspiran el sistema jurídico que garantiza el respeto del derecho fundamental a la protección de datos. En este sentido, los responsables deben de actuar, en todo momento, dentro del ámbito del consentimiento expreso otorgado por los titulares de los datos de salud, o de la habilitación legal que les permite tratarlos sin el consentimiento de éstos. En relación a dichos datos, la LOPD, como ya se ha analizado al tratar el principio de consentimiento, ha procedido a incluirlos dentro una regulación especial, más garantista, que califica como «*datos especialmente protegidos*», ya que se trata de datos que afectan a las esferas más íntimas de la persona.

Junto a la LOPD existen otras leyes, las de autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica[38], que disciplinan parte del quehacer diario de los profesionales sanitarios. En la mayoría de las ocasiones, siguiendo la terminología ya utilizada para la LOPD, las obligaciones que estas normas imponen son de naturaleza «*negativa*» o «*de no hacer*», es decir, de prohibición de determinados comportamientos por parte de los profesionales[39]. En otros casos, aunque existe una obligación «*positiva*» o «*de hacer*»[40] el profesional está obligado a desplegar una conducta activa ante el paciente, sin embargo normalmente dicho comportamiento se circunscribe al ámbito de la estricta relación profesional entre ambos, transcendiendo solamente al ámbito de la protección de datos desde el punto de vista de la integración de determinada documentación escrita, que en su caso haya que formalizar, dentro de la historia clínica del paciente.

Por último, es preciso señalar que cada una de las leyes sectoriales sanitarias, que disciplinan la autonomía del paciente y los derechos y obligaciones en materia de información y documentación clínica, tienen el rango de ley ordinaria y, como tales, establecen en sus respectivos articulados, porque no podría ser de otra manera a tenor del principio de jerarquía normativa, que lo señalado en las mismas respecto del acceso y conservación a la documentación clínica se rige por lo previsto en la LOPD.

2. CONCEPTO DE «DATO DE SALUD»

A pesar de la claridad con la que la LOPD incardina los datos de salud dentro de los «*datos especialmente protegidos*», ni en dicha norma ni en la legislación sectorial sanitaria se encuentra una definición de lo que se ha de entender como «*dato de salud*». Únicamente se recoge desde hace poco tiempo, desde el 19 de abril de 2008 fecha en que se produce la entrada en vigor del RLOPD[41], una definición de dato de carácter personal relacionado con la salud referida a las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

En dicho precepto se ha recogido el común denominador de las diferentes definiciones que se habían acuñado en las normas internacionales[42] y que, ya desde mediados del siglo pasado, habían señalado que el «*dato de salud*» debía de ser objeto de especial protección. En este sentido, la Recomendación (97) 5, del Comité de Ministros del Consejo de Europa, de 13 de febrero de 1997, relativa a la «*Protección de Datos Médicos*», señalaba que la expresión «*datos médicos*» abarcaba todos los datos de carácter personal relativos a la salud de una persona, y comprende los datos que manifiesta y estrechamente se relacionen con la salud y las informaciones genéticas.

Además de las definiciones normativas señaladas que formularon un concepto extensivo del concepto de «*dato de salud*», el Tribunal de Justicia de las Comunidades Europeas tuvo oportunidad de pronunciarse sobre el concepto de «*dato de salud*» en la Sentencia de 6 de noviembre de 2003[43]. Como cuestión prejudicial cuarta, el Tribunal Sueco planteaba, en relación a la aplicación de la Directiva 95/46/CE, si *«¿Constituye un dato relativo a la salud que, con arreglo al artículo 8, apartado 1, no puede ser objeto de tratamiento la divulgación en una página web de la circunstancia de que un compañero de trabajo, designado por su nombre, se ha lesionado el pie y está en situación de baja parcial?»*. En relación a dicho asunto, el Tribunal señaló que, teniendo en cuenta el objeto de la Direc-

(35) Artículo 81.3.a).
(36) Artículo 81.5.
(37) Artículo 81.6.
(38) Utilizamos el título que emplea la Ley 41/2002, aunque existen diferentes normas autonómicas que se refieren, por ejemplo, a los «*derechos y deberes de la personas en relación con la salud*» en la Ley de Castilla y León 8/2003, de 8 abril, a la «*Información sanitaria y autonomía del paciente*» en la Ley de Extremadura 3/2005, de 8 julio, o al «*consentimiento informado y de la historia clínica de los pacientes*» en la Ley de Galicia 3/2001, de 28 mayo.
(39) Por ejemplo, en cuanto al deber de secreto en relación a los datos relativos a la salud que conozcan en razón de sus cometidos asistenciales.
(40) En relación, por ejemplo, al derecho del paciente a recibir una información precisa, clara y completa sobre la que fundar su consentimiento informado para someterse a la realización de cualquier procedimiento diagnóstico o terapéutico.
(41) Artículo 5.1.g).
(42) En ese sentido, la Carta Magna de la Organización Mundial de la Salud ha definido la salud como «*el estado de completo bienestar físico, mental o social, y no solamente la ausencia de afecciones o enfermedades*». Por su parte, el Apartado 45 de la Memoria Explicativa del citado Convenio 108 del Consejo de Europa, considera que dentro de la noción de «*datos de carácter personal relativos a la salud*» se incluyen *«las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo»*, pudiendo tratarse, por tanto, de informaciones relativas a una persona con buena salud, enferma e, incluso, fallecida. Añade el citado apartado que estos datos comprenden también los referidos al «*abuso del alcohol o al consumo de drogas*».
(43) Caso *Bodil Lindqvist*, que decidió una decisión prejudicial sobre interpretación de la Directiva 95/46/CEE planteada por el Tribunal Sueco encargado de juzgar los hechos relatados en la citada sentencia.

tiva, es preciso dar una interpretación amplia a la expresión «*dato relativos a la salud*», empleada en el artículo 8.1, de modo que comprenda la *«información relativa a todos los aspectos, tanto físicos como psíquicos, de la salud de una persona»*.

Por tanto, el concepto de «*dato de salud*» ha de entenderse, como expresa el RLOPD, en sentido amplio, es decir, incluyendo en el mismo *«cualquier información que haga referencia a una afección o enfermedad, a un estado de completo bienestar tanto físico como psíquico, así como a cualquier otro aspecto que afecte o pueda afectar, de modo directo o indirecto, a la salud de una persona»*. De este modo, se incluyen, por ejemplo, las patologías, las pruebas que expresen un estado de salud bueno o malo de la persona[44], incluso si ha fallecido, y aquellos que se refieran, por ejemplo, a estudios genéticos, a situaciones de abuso del alcohol o relativas al consumo de drogas, a valoración de minusvalías, donación y recepción de gametos y preembriones en procesos de reproducción asistida, y a procesos de extracción y trasplante de órganos.

3. PRINCIPIO DE INFORMACIÓN

Ya se ha señalado que al responsable del fichero o tratamiento le corresponde el deber de información en el momento de la recogida de los datos. Este deber es preciso cumplimentarlo aún en el caso de que el responsable pase a tratar los datos sin necesidad de contar con el consentimiento del interesado. Por ello, en el caso de los datos de salud, por su especial naturaleza, dicho deber debe de ser observado, si cabe, aún con más rigor.

La prueba del cumplimiento del citado deber corresponde al responsable del fichero o tratamiento, motivo por el cual dicha prueba no podría obtenerse a través de una mera información verbal. Por tal motivo, la manera de cumplir con el citado deber, cuando los datos se recogen de los propios interesados, debería hacerse del siguiente modo:

- ➢ Por medio de una cláusula informativa que se incluirá en los impresos previstos para recogida de los datos. De implementarse este procedimiento, lo congruente sería acreditar que el interesado ha quedado informado de los términos a que se refiere la LOPD[45] mediante la estampación de su firma.
- ➢ A través de la colocación de tablones informativos. En estos casos, los carteles anunciadores deberán cumplir con las siguientes condiciones:
  - Que resulten claramente visibles por parte de los interesados quedando así garantizado que los mismos han podido tener perfecto conocimiento de la información exigible.
  - Que el formato permita que los interesados puedan acceder con claridad a la información que se les facilita.
  - Que la información facilitada cumple lo señalado en el artículo 5.1 de la LOPD. Sobre este particular es preciso tener presente lo señalado en la normativa sobre autonomía del paciente y los derechos y obligaciones en materia de información y documentación clínica, ya que en la misma se establecen claramente, como más adelante se verá, los supuestos en los que podrá accederse a los datos de salud contenidos en la historia clínica.

4. PRINCIPIO DE CONSENTIMIENTO

4.1. Consentimiento expreso y consentimiento informado

Como ya se ha señalado, la LOPD[46] requiere que los datos de salud, al pertenecer al grupo de los «*datos especialmente protegidos*», sean recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. Es decir, como principio general, cabe afirmar que los datos de salud solamente podrán ser tratados cuando el interesado consienta expresamente, salvo que la ley, bien la propia LOPD u otra ley sectorial en atención a un bien jurídico prevalente, autorice dicho tratamiento sin necesidad de haber contado previamente con el consentimiento de éste.

En cuanto a la naturaleza jurídica del consentimiento necesario para el tratamiento de los datos de salud, a diferencia de lo que se prevé en la LOPD[47] para los datos referentes a ideología, afiliación sindical, religión y creencias[48], es preciso observar que la Ley exige que sea expreso[49], inequívoco[50], específico e informado[51], resultando de capital importancia ésta última ya que sin esta característica difícilmente la declaración de voluntad podrá llegar a ser inequívoca y específica.

En el caso de los menores de edad[52], la obtención del consentimiento expreso en materia de protección de datos, previa implementación de un procedimiento que garantice que se ha comprobado de modo efectivo la edad del menor, se efectuará de la siguiente manera:

- Si el menor es mayor de catorce años, el responsable del fichero o del tratamiento podrá obtener el consentimiento de aquél salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad[53].
- Si es menor de catorce años, el responsable del fichero o del tratamiento deberá requerir el consentimiento de los padres, tutores o representantes legales. En este caso, deberá articularse un procedimiento que garantice que se ha comprobado de modo efectivo la autenticidad del consentimiento prestado por éstos.

(44) De una persona sana o enferma.
(45) Artículo 5.1.
(46) Artículo 7.3.
(47) Artículo 7.2.
(48) Artículo 7.2 dispone que para tales datos el consentimiento ha de ser emitido de forma expresa y por escrito.
(49) Artículo 7.3.
(50) Artículo 6.1.
(51) Artículo 3.h).
(52) Artículo 13 del RLOPD.
(53) Por ejemplo, a tenor del artículo 5.3 de la Ley del Parlamento Andaluz 1/2007, de 16 de marzo, por el que se regula la investigación en reproducción celular con finalidad exclusivamente terapéutica, se exige, para donar óvulos y células somáticas, mayoría de edad y plena capacidad de obrar, salvo en el caso de los menores o incapacitados en los que se requerirá el consentimiento de sus representantes legales.

Por su parte, como ya se ha adelantado, las normas que se han denominado de autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, establecen una serie de reglas especiales para la prestación del consentimiento informado en caso de minoría de edad. Dichas normas, vaya por delante, nada tienen que ver con la normativa de protección de datos de carácter personal a la que se ha hecho referencia en relación al RLOPD.

Así, en la Ley 41/2002, de 14 de noviembre, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica[54] (en lo sucesivo LAP), se establece que habrá de otorgarse el consentimiento informado por representación, en el caso de que el menor no sea capaz ni intelectual ni emocionalmente de comprender el alcance de una intervención, distinguiendo estos supuestos:

- Si el menor tiene cumplidos los doce años, el representante legal antes de manifestarse sobre el consentimiento escuchará la opinión del menor.
- Si se trate de menores emancipados o mayores de dieciséis años, que no estuviesen incapaces o incapacitados, no cabe la prestación del consentimiento informado por representación. En estos casos, cuando la intervención conlleve grave riesgo, según el criterio facultativo, los padres serán informados y su opinión será tenida en cuenta para la toma de la decisión correspondiente.

Lo señalado sirva de ejemplo para no confundir conceptos semánticamente iguales que aparecen recogidos en leyes que se aplican a los profesionales sanitarios, y que, al analizar su contenido jurídico se observa que el mismo es completamente dispar. En tal sentido, no deben confundirse los conceptos de «*consentimiento expreso, inequívoco, específico e informado*», del que habla la LOPD[55] como ya se ha analizado, con el de «*consentimiento informado*» a que se refieren las leyes ya citadas sobre autonomía del paciente y derechos y obligaciones en materia de información y documentación clínica. Se trata, eso sí, de dos consentimientos compatibles entre sí, pero mientras que el primero se refiere, en general, a la habilitación necesaria para el tratamiento de los datos de salud del interesado, salvo que exista habilitación legal que exonere de recabar dicho consentimiento, el segundo persigue obtener la conformidad libre, voluntaria y consciente del paciente después de que el profesional sanitario le haya informado adecuadamente sobre las alternativas y posibilidades de curación de una concreta patología o enfermedad.

4.2. Excepciones al principio de consentimiento

De acuerdo con lo señalado en el epígrafe anterior, tampoco tendrán nada que ver las excepciones relativas al «*consentimiento expreso, inequívoco, específico e informado*» exigido por la LOPD, con las que afectan al «*consentimiento informado*» regulado en las normas de autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Entrando en el análisis de la normativa de protección de datos y de la legislación sectorial sanitaria que la complementa, solamente podrá excepcionarse el consentimiento para tratar datos de salud cuando una norma con rango de ley, en atención a un bien jurídico prevalerte, así lo recoja expresamente. Por lo tanto, de acuerdo con lo señalado, los supuestos en los cuales el Legislador[56] ha entendido que es posible tratar los datos de salud de los pacientes, sin necesidad de tener que contar con su previo consentimiento expreso, son los siguientes:

a) Respecto al tratamiento de los datos de salud.

- ➢ Cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias que les atribuyen una norma con rango de ley o una norma de derecho comunitario[57].
- ➢ 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[58].

En el caso de que sea necesario acceder a la historia clínica del paciente desde otro centro en el cual estuviese recibiendo asistencia sanitaria, se deberá facilitar el acceso cuando sea solicitada por el facultativo responsable de esa asistencia, siempre que cuente con la autorización expresa del paciente. No obstante, si la asistencia se produce en una situación de urgencia, en la que el paciente no pueda prestar su consentimiento, se podrá facilitar el acceso a la historia clínica si el profesional sanitario justifica debidamente la necesidad asistencial que requiere el uso de esa documentación.

Cuando el acceso a la historia clínica del paciente se haya de facilitar para salvaguardar el interés vital de otra persona, el responsable del fichero deberá adoptar las medidas precisas para que se garantice el anonimato del propio paciente (procedimiento de disociación)[59].

- ➢ Cuando el tratamiento de los datos de salud 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 se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto[60]. En relación a este supuesto la legislación sanitaria sectorial complementa la regulación de la siguiente manera:
  - Podrán acceder a la historia clínica del paciente los profesionales asistenciales que realizan el diagnóstico o el tratamiento del paciente, como instrumento fundamental para su adecuada asistencia[61]. Si no concurre tal situación, es

[54] Artículo 9.3.c).
[55] Artículos 3.h), 6.1, y 7.3.
[56] Recogidos en la LOPD y que el resto de leyes sobre autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica han de respetar.
[57] Artículo 10.3.a) del RLOPD.
[58] Artículos 6.2, y 7.6, párrafo segundo de la LOPD y 10.3.c) del RLOPD.
[59] Artículos 3.f) y 11.6 de la LOPD, y 5.1.p) del RLOPD.
[60] Artículos 7.6.párrafo primero de la LOPD y 10.3.c) del RLOPD.
[61] Artículo 16.1 LAP y, por ejemplo, artículo 13,1 del Decreto 101/2005, de 22 de noviembre, por el que se regula la historia clínica en la Comunidad Autónoma de Castilla y León.

decir, si el acceso se realiza por un profesional sanitario que no está vinculado al diagnóstico del titular de los datos, no podrá producirse el acceso a la historia clínica.

– Dentro de la gestión de servicios sanitarios, el personal sanitario que ejerza funciones de inspección, evaluación, acreditación y planificación, podrá acceder a las historias clínicas exclusivamente para el ejercicio de sus competencias[62]. En este caso también se incluirán las actuaciones previas que deban practicar los inspectores médicos de la Administración de la Seguridad Social.

b) Respecto a la cesión de los datos de salud[63].

- ➢ Cuando sea necesaria para solucionar una urgencia que requiera acceder a un fichero. En este caso, existe obligación de preservar los datos de identificación personal del paciente, salvo que éste autorice lo contrario.
- ➢ Cuando sea precisa para realizar estudios epidemiológicos en los términos previstos en la legislación sobre sanidad estatal o autonómica. En este caso, se podrá acceder a la historia clínica de un paciente, pero con la obligación de preservar su anonimato, de modo que se separen los datos de identificación personal del paciente de los de carácter clínico-asistencial, salvo que el propio paciente consienta no separarlos[64].
- ➢ Con fines históricos, científicos o estadísticos en cuyo caso el acceso a la historia clínica del paciente se realizará, como en el supuesto anterior, preservando su anonimato salvo que el propio paciente consienta que sean conocidos por terceros[65]. En este sentido, la normativa sanitaria establece que se podrá acceder a la historia clínica del paciente en las citadas condiciones cuando el mismo se deba a fines de salud pública, de investigación o de docencia[66].
- ➢ Cuando la comunicación sea practicada a instancia de jueces o tribunales en el ejercicio de las funciones que legalmente tienen atribuidas[67]. A tal efecto, bastará con que la autoridad judicial lo solicite en la correspondiente resolución. Sobre este caso, se deberá de dar acceso a la historia clínica del paciente en los términos en los que se haya manifestado el juez o tribunal correspondiente[68], de lo contrario se corre el riesgo de contradecir el artículo 118 de la Constitución. Sin embargo, el responsable de la custodia clínica deberá ceñir el acceso a lo solicitado por la autoridad judicial de modo que, salvo que lo que se solicite sea toda la historia clínica, no será posible que ante una petición de información parcial el citado responsable atienda el requerimiento remitiendo la totalidad de la información contenida en la historia clínica. En caso de duda sobre los términos de la resolución judicial, el responsable deberá pedir aclaración sobre el contenido concreto de la historia clínica que se le está solicitando.
- ➢ Cuando se produzca, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud[69] cuando se realice para la atención sanitaria de las personas[70]. En este sentido, se deberá de dar acceso a la historia clínica, siempre que el profesional sanitario así lo requiera, con motivo que el paciente se encuentre recibiendo asistencia en otro centro[71].

Sin perjuicio de las cesiones señaladas, las instituciones y los centros sanitarios así como los profesionales correspondientes, podrán proceder al tratamiento de datos de salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con la legislación estatal o autonómica sobre sanidad[72]. Como ejemplo de lo señalado, los auxiliares administrativos podrán acceder a los datos de salud de los pacientes, pero solamente cuando sea necesario para desarrollar las funciones que tuviesen encomendadas[73].

5. DEBER DE SECRETO

En los supuestos analizados, los responsables de los ficheros o de los tratamientos y el profesional sanitario, que intervenga en cualquier fase del tratamiento de los datos de salud, han de respetar el deber de secreto respecto de cualquiera de los que puedan haber conocido en el desarrollo de sus cometidos, incluso después de haber cesado en su relación con los citados responsables. En tal sentido se manifiesta la LOPD[74] y se recoge en el resto de normas que, tanto a nivel general como autonómico, han regulado la autonomía del paciente y los derechos y obligaciones en materia de información y documentación clínica.

6. PRINCIPIO DE CALIDAD

Lo señalado en el epígrafe 4.3 del presente artículo, respecto al principio de calidad de los datos personales, resulta plenamente aplicable a los datos relativos a la salud. De esta manera, los citados datos podrán recogerse para su tratamiento siempre que sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, deberán responder, con veracidad, a la situación actual de su titular, y, cuando hayan dejado de ser necesarios para la finalidad determinada, explícita y legítima que motivó su recogida, deberán ser cancelados de modo que, en todo caso, se evite que ningún tercero pueda acceder a dichos datos. Por lo tanto, en relación a dichos extremos, resulta obligada la remisión a lo señalado en el mencionado epígrafe de este artículo.

(62) Artículo 16.4 de la LAP y, por ejemplo, artículo 17.3 del Decreto 101/2005, de 22 de noviembre, por el que se regula la historia clínica en la Comunidad Autónoma de Castilla y León.
(63) Artículo 11.2.f) de la LOPD.
(64)
(65) Artículo 11.2.e) de la LOPD.
(66) Artículo 16.3 de la LAP y, por ejemplo, artículo 17.2 del Decreto 101/2005, de 22 de noviembre, por el que se regula la historia clínica en la Comunidad Autónoma de Castilla y León.
(67) Artículo 11.2.d) de la LOPD.
(68) Artículo 16.3 de la LAP y, por ejemplo, artículo 17.1 del Decreto 101/2005, de 22 de noviembre, por el que se regula la historia clínica en la Comunidad Autónoma de Castilla y León.
(69) Artículo 10.5.párrafo final del RLOPD.
(70) Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
(71) Artículo 13.3, párrafo primero, del Decreto 101/2005, de 22 de noviembre, por el que se regula la historia clínica en la Comunidad Autónoma de Castilla y León.
(72) Artículo 8 de la LOPD.
(73) Artículos 7.6 y 8 de la LOPD, y 16.4 de la LAP.
(74) Artículo 10.

El análisis de dicho principio tiene, en relación al tratamiento o a la cesión de datos de salud, una característica que debe ser recordada. Hace referencia a que la información, por vía de excepción al principio de consentimiento, ha de ser proporcional a la finalidad perseguida en cada caso. Como consecuencia de lo señalado, es preciso concretar qué parte de la documentación clínica será necesario facilitar para cada caso concreto, de modo que se traten o cedan los datos que estrictamente sean necesarios en función de los fines que están recogidos en cada una de las habilitaciones legales que resulten aplicables.

7. MEDIDAS DE SEGURIDAD APLICABLES A LOS DATOS DE SALUD

En el presente artículo ya se ha señalado que, aunque los datos de salud son datos especialmente protegidos y están sometidos a medidas de seguridad de nivel alto, sin embargo será posible la aplicación de medidas de seguridad de nivel básico en determinados casos. El RLOPD incorpora esta importantísima novedad que, sin duda, va a facilitar el tratamiento de datos porque define las medidas de seguridad que debían aplicarse en los casos en que en los ficheros se incluyesen datos especialmente protegidos pero cuyo tratamiento tuviese relación con la gestión de pagos o con el cumplimiento de deberes públicos. De este modo se superaba el principio general de que un dato de salud, por ser especialmente protegido, elevaba el nivel de seguridad de todo el fichero por lo que debían adoptarse necesariamente las medidas de nivel alto. Pues bien, a partir de ahora con la entrada en vigor del RLOPD el 19 de abril de 2008, la situación cambia notablemente.

Por lo tanto, ha de deducirse una nueva conclusión no conocida hasta ahora: Los datos de salud, dependiendo de las circunstancias que rodeen su tratamiento, exigirán la aplicación de los siguientes niveles de medidas de seguridad recogidos en la normativa de protección de datos:

- ➢ En general, se aplicarán las medidas de nivel alto[75].
- ➢ Se aplicarán las de nivel básico:
  - – En el caso de que los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros[76].
  - – Cuando se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad[77]. Este podría ser el caso de un fichero en el que se recogiese simplemente el dato de que un interesado es fumador, sin más referencia ni a sus hábitos de consumo de tabaco ni a otros que permitieran determinarlo.
  - – Por último, en el caso de que los datos de salud se refieran 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, se aplicarán las de nivel básico[78].

Respecto a las medidas de seguridad son muchos los extremos que merecerían atención, pero ello excede en mucho al objeto del presente artículo. No obstante, desde el punto de vista del profesional sanitario, que interviene en cualquier fase del tratamiento de los datos de salud, los aspectos más significativos son los siguientes:

- – Deberá de cumplir el correspondiente Documento de Seguridad, que deberá de ser elaborado por el responsable del fichero o tratamiento, ya que en el mismo se recogerán las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
- – Deberán de tener acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. A tal efecto, el responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
- – Velará porque el sistema de identificación y autenticación con el que accedan a los ficheros no sea conocido por terceros Esta obligación es aún más importante en el caso general de que el fichero con datos de salud tenga que respetar el nivel de medidas de seguridad de nivel alto, ya que en este supuesto se guarda la información que permite identificar quién fue el usuario que practicó el registro accedido. El usuario será entonces el responsable de demostrar que el acceso fue necesario para desarrollar las funciones que tuviera encomendadas.

Por lo que se refiere a la normativa sanitaria, que regula la autonomía del paciente y los derechos y obligaciones en materia de información y documentación clínica, se establece que son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas para la conservación de los ficheros que contienen datos de carácter personal y, en general, por la LOPD[79]. En este sentido, dichas medidas permitirán, por ejemplo, no sólo evaluar que los datos no se han destruido sino que, aún conservándose durante largos períodos de tiempo, se han utilizado únicamente para las finalidades que legalmente la justifican y si se han producido accesos no autorizados.

8. DERECHO DE ACCESO A LA HISTORIA CLÍNICA

El derecho de acceso a la historia clínica se encuentra particularmente influido por la regulación que realiza la LAP, motivo por el que hay que prestar especial atención a lo señalado en ella[80]. La citada Ley regula el derecho de acceso desde los siguientes dos puntos de vista:

- – Desde el derecho de acceso a toda la información que posea el responsable de la custodia clínica, de tal modo que si trata otros datos personales del interesado que no figuran en ella,

[75] Artículo 81.3.a) del RLOPD.
[76] Artículo 81.5..a) del RLOPD
[77] Artículo 81.5.b) del RLOPD.
[78] Artículo 81.6 del RLOPD.
[79] Artículo 17.6 de la LAP.
[80] Artículo 18 de la LAP.

también deberá atender su ejercicio e incluir dichos datos en la información que le facilite.

– Desde el derecho a obtener copia de los datos que figuran en su historia clínica. En relación a dicha cuestión se pueden plantear las siguientes situaciones:

  • Atendiendo al contenido que en cada caso sea exigible respecto a la historia clínica, a tenor de lo previsto en la LAP y en el resto de normativa autonómica que regula la autonomía del paciente y los derechos y obligaciones en materia de información y documentación clínica, puede suceder que el derecho de acceso tuviera como finalidad obtener copia de algunas de las pruebas practicadas en el proceso asistencial. En tal caso, pueden plantearse estos supuestos:
    - Que las copias de las mencionadas pruebas no figuren en la historia clínica pero sí los informes derivados de las mismas. En este caso, si el contenido mínimo de la historia clínica hace referencia a los citados informes, bastará con facilitar el acceso respecto de éstos para entender perfectamente atendido el derecho de acceso a la historia clínica.
    - Que las copias sí figuren en la historia clínica además de los correspondientes informes, en cuyo caso se facilitará copia de ambos soportes.
    - Que el contenido mínimo de la historia clínica se refiera no solamente a los citados informes sino también a las copias de las pruebas en las que se sustenta, en cuyo caso habría, primero, que completar la historia clínica para, después, proceder a atender el derecho de acceso.
  • También puede suceder que el titular de los datos de salud solicite en el ejercicio del derecho de acceso que se le entregue la documentación original que obra incluida en su historia clínica. En tal caso, el derecho de acceso se atenderá correctamente facilitando solamente la copia de los datos que figuran en su historia clínica.
  • Por último, si el interesado solicita conocer el acceso a los medicamentos que se le han suministrado habrá de facilitársele dicha información, ya que la denominación de los mismos no se encuentra incluida en las excepciones al deber de informar que se establecen en la LAP[81].

Desde el punto de vista de la legitimación para el ejercicio del derecho de acceso, los datos de salud incluidos en la historia clínica pertenecen al paciente. Por este motivo y, como regla general, será el único legitimado para poder acceder a dichos datos, bien por sí mismo o a través de representante, salvo que se trate de alguno de los supuestos, que ya se han analizado, y que permiten con la habilitación legal suficiente que los datos sean tratados o cedidos sin necesidad de tener que contar con el previo consentimiento de su titular.

Como ya se ha señalado, la regulación del derecho de acceso desde el punto de vista de la protección de datos se encuentra recogida en la LOPD y en su normativa de desarrollo, sin embargo, cuando se trata de datos de salud, sus previsiones deben integrarse con las de la LAP y con las especialidades previstas la normativa autonómica. En referencia al derecho de acceso en el ámbito sanitario, habrá que distinguir los siguientes supuestos:

➢ Derecho de acceso ejercitado por el propio interesado[82]: En tal supuesto es preciso tener en cuenta que el ejercicio del derecho de acceso no tiene carácter ilimitado, sino que ha de respetar las siguientes reglas:

  – El citado derecho podrá ser ejercitado por el paciente o por aquel que actúe en su representación, siempre que ésta quede debidamente acreditada.
  – El derecho de acceso no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en la historia clínica recogidos en interés terapéutico del paciente.
  – Tampoco podrá ejercerse en contra de la voluntad del profesional sanitario, que puede oponerse a que se dé acceso a las anotaciones subjetivas que puedan obrar en la historia clínica del paciente. En este sentido, conviene aclarar dos cuestiones:
    • En el derecho de acceso que ejerza el titular de los datos hay obligación de darle a conocer la existencia o no de anotaciones subjetivas.
    • La titularidad del derecho a la reserva de las anotaciones subjetivas corresponde a los profesionales sanitarios que hubiesen participado en su elaboración. Por tanto, habrán de ser estos profesionales los que lo ejerzan y no las entidades en las que aquellos presten sus servicios.

➢ Derecho de acceso ejercitado por alguna persona distinta al interesado, en cuyo caso es preciso distinguir los siguientes casos:
  – Que el interesado viva y el ejercicio del derecho de acceso sea planteado por una persona que actúa como representante legal de aquel[83]. En tal supuesto se facilitará el acceso a dicho representante legal siempre que en el poder se contemple específicamente un apoderamiento específico para tal finalidad.
  – Que el interesado viva y el ejercicio del derecho de acceso sea planteado por una persona que no actúa como representante legal de aquel. En este caso, el acceso debe ser denegado sin más trámites.
  – Que el interesado hubiese fallecido ejercitándose el derecho de acceso por una persona que pudiese demostrar que tuvo una relación familiar o de hecho, en tal caso solamente se podrá facilitar el acceso si es que el fallecido no hubiese dejado por escrito su voluntad de que no se permitiera el acceso a su historia clínica.
    Si, no obstante, se necesita acceder a dicha documentación clínica por motivo de la atención de una urgencia de un tercero se podrá realizar a pesar de existir prohibición expresa al efecto, siempre que se tomen medidas para asegurar el anonimato del paciente fallecido.

[81] Artículo 118.3.
[82] Artículo 18.3 de la LAP.
[83] Artículo 18.2 de la LAP.

Lo señalado con anterioridad, no es impedimento para que, antes de facilitar el acceso, el responsable de la custodia de la historia clínica deba de solicitar del profesional sanitario que atendió al fallecido si ejercita o no su derecho de reserva sobre las anotaciones subjetivas que pudieran existir en la misma.

En todo caso, el acceso se practicará con respeto a la intimidad del fallecido y al principio de proporcionalidad, de modo que se facilite solamente respecto de los datos que sean pertinentes en función de la finalidad que se persiga.

– Que el interesado hubiese fallecido ejercitándose el derecho de acceso por una persona que no pudiese probar que había mantenido con el interesado una relación familiar o de hecho, en cuyo caso no se podrá facilitar dicha información.

➢ Respecto al derecho de acceso a la historia clínica en el caso de la minoría de edad, se puede plantear el asunto de en qué casos pueden los titulares de la patria potestad estar habilitados para acceder a la historia clínica del menor aportando solamente, por ejemplo, una fotocopia del libro de familia. Este asunto tiene relación directa con el de la capacidad que tienen los menores de edad para prestar consentimiento, y que ya ha sido tratado anteriormente[84]. De acuerdo con dicha capacidad, cabe la diferenciación de los siguientes supuestos:

– Si el menor es mayor de catorce años tiene capacidad suficiente al disponer de madurez suficiente para ejercitar el derecho de acceso, por lo que no es necesario que exista representación legal por parte de los titulares de la patria potestad. De este modo, si la madre o el padre de un mayor de catorce años ejercita el derecho de acceso a la información contenida en la historia clínica de su hijo o hija éste deberá ser rechazado. Se exceptúan de esta regla los siguientes casos:
  • Cuando el acceso fuese solicitado por el menor como titular de los datos.
  • Cuando el menor se encontrase previamente incapacitado.
– Cuando el menor no supere los catorce años, al no considerársele legalmente con madurez suficiente, la entrega de los datos existentes en la historia clínica a los titulares de la patria potestad podría hacerse sin exigir que previamente el menor hubiera conferido representación suficiente para ello.

9. DERECHO DE RECTIFICACIÓN

El derecho de rectificación ofrece perfiles específicos cuando se ejerce sobre la información contenida en la historia clínica. Esta situación se produce porque el paciente puede instar la rectificación de una información que se encuentra avalada por la participación de un profesional sanitario. En estos casos, para que tal rectificación pueda practicarse, debe de estar avalada por la existencia de un informe diferente emitido por otro profesional sanitario. Ello conlleva la necesidad de instar los procedimientos que la normativa de aplicación contemple para la revisión de los diagnósticos médicos por error en su determinación, agravación o mejoría, con aportación de las pruebas adecuadas al efecto que los propios facultativos haya resuelto que son precisas[85].

10. TRATAMIENTO DE DATOS GENÉTICOS

Como ya se ha señalado, los datos genéticos son datos personales relativos a la salud de las personas, menos en el caso, por ejemplo, de un fichero en el que se recojan datos de vestigios hallados en el escenario de un determinado hecho en el que, al no saber a qué personas pertenecen, no es un fichero relativo a datos de una persona identificada ni identificable por lo que no es le aplicaría la LOPD. En el momento en que se pudiera identificar al titular de alguna de las muestras recogidas, esos datos sí pasarían a ser datos de carácter personal.

Los datos genéticos serán, además, datos de salud tanto si los efectos del análisis de ADN son codificantes o expresivos como no codificantes, ya que si bien es posible que del resultado del análisis no se derivan directamente datos de salud, dichos resultados vienen a conformar la huella genética de una persona y por tanto se encuentran directamente relacionados con su salud. Por tanto, la expresión «*datos genéticos*» se refiere a todos los datos, de cualquier tipo, relacionados con los caracteres hereditarios de un individuo o que, vinculados a dichos caracteres compongan el patrimonio de un grupo de individuos emparentados[86].

Los datos genéticos que se incluyan en un fichero de carácter personal procederán de pruebas realizadas voluntariamente por los interesados, o de personas desaparecidas, toda vez que el objetivo del tratamiento será, precisamente, asociar la muestra genética con una determinada persona desaparecida a fin de lograr su identificación futura. En relación con este tipo de datos es preciso comentar los siguientes aspectos:

– Es necesario respetar estrictamente, como en el resto de los datos de salud, el deber de secreto de modo que ningún tercero al interesado, aunque fuese la familia más allegada, pueda conocer por el centro sanitario o por el propio profesional sanitario que se ha llevado a cabo un análisis de carácter genético.
– El centro sanitario o el profesional sanitario, a la vista de los resultados obtenidos en la prueba genética del interesado, no deberán dirigirse de oficio a los otros miembros de su familia biológica con el fin de proponerles la realización de unas pruebas genéticas, porque no cuentan con el consentimiento del interesado y porque los familiares tienen, respecto del derecho a la información asistencial, el «*derecho a no saber*» sobre todo en casos en los que el perfil genético que se le puede comunicar puede ser el del posible desarrollo de una enfermedad que pueda no tener actualmente curación[87].

[84] Artículo 13 del RLOPD.

[85] Podría ser la existencia de un contrainforme médico que contradijera lo recogido en otro informe sobre la misma patología y que se encontrara incluido en la correspondiente historia clínica.

[86] Recomendación (97) 5 del Comité de Ministros del Consejo de Europa.

[87] Sería el caso de que a través de una prueba genética se conociese que en una determinada familia biológica existen portadores de un gen responsable de una enfermedad incurable. De comunicarlo de oficio el profesional sanitario al resto de los miembros podría crear en éstos un estado de ansiedad permanente sin que, por el contrario, hubiese representado una ventaja directa pues no se dispone de remedio para esa enfermedad.

Como ya se ha adelantado en este artículo, los avances en materia de investigación genética han abierto un debate muy interesante y, a la vez bastante inquietante, sobre sus posibles utilidades. Por este motivo todos los instrumentos internacionales recientemente publicados se han decantado por prohibir de hecho cualquier discriminación entre personas físicas basada en datos genéticos[88]. Llegaron a producirse casos en los que algunas personas decidían no someterse a «*pruebas genéticas de diagnóstico*», que por lo tanto eran necesarias para aclarar las causas de una enfermedad con manifiestos síntomas clínicos, porque temían que sus empleadores y las compañías de seguros pudieran acceder a las mismas. Fue la reiteración de este temor en los ciudadanos lo que provocó que en los Estados Unidos se adoptara la Ley Federal de no discriminación por la información genética. El asunto venía provocado porque habían surgido algunas voces muy interesadas en aprobar la posibilidad de que, antes de suscribir una póliza de seguro (de vida o de enfermedad) o de contratar a un trabajador/a, la entidad de seguros o el empresario pudieran obligar a la persona a someterse a un análisis de esa naturaleza. El mercado reclamaba interesadamente incorporar las funcionalidades de los avances en esta materia a su negocio.

En relación a los datos genéticos, el Grupo del artículo 29 de la Directiva 95/46/CEE de Protección de Datos[89], extraordinariamente preocupado por el asunto, formuló las siguientes pautas de actuación:

- La humanidad no debe reconducirse sólo a características genéticas, a su mapa genético que, en cualquier caso, no constituyen la explicación universal definitiva de la vida humana. Por tanto, una de las primeras garantías que condicionan la utilización de los datos genéticos debe ser evitar asignar a estos datos un valor explicativo universal.
- Los datos genéticos han de recogerse para finalidades determinadas, explícitas y legítimas, y no tratarse posteriormente de modo incompatible con los fines para los cuales fueron recogidos.
- Los datos han de ser adecuados, pertinentes y no excesivos en relación a los fines para los que se recaben y para los que se traten posteriormente[90].
- Respecto de la posible incidencia de las pruebas genéticas en el mundo laboral, hasta la fecha no se han obtenido datos concluyentes sobre la pertinencia y fiabilidad de las mismas en dicho contexto por lo que su valor predictivo sigue siendo dudoso. Por lo tanto, no cabe permitir la discriminación de las personas sobre una información que desvela un gran margen de probabilidad y, además, cuando para el desarrollo de futuras enfermedades influyen otros factores externos, como pueden ser los medioambientales.
- Lo mismo cabe señalar respecto a la utilización de los datos genéticos en el ámbito de los seguros. Solamente podrá autorizarse en casos excepcionales explícitamente previstos por la Ley. De lo contrario, la utilización de los datos genéticos podría generar una discriminación contra el asegurado o los miembros de su familia biológica, ya que tendrían que abonar primas desorbitadas o resultar inasegurables sobre la base de un riesgo de enfermedad que cabe la posibilidad de que nunca se declarara.
- Por lo que se refiere a la recogida y registro de datos genéticos con fines de investigación, lo que se conoce con el nombre de «*biobancos*», y, en especial, a los principios de información, consentimiento y calidad, lo más adecuado sería, como regla general, establecer la obligación de aplicar prácticas de anonimización, salvo en lo relativo al desarrollo de ensayos clínicos en los que el promotor y el investigador deben conocer, en determinadas circunstancias que a continuación se analizarán, la identidad del titular de dichos datos.

11. TRATAMIENTO DE DATOS EN ENSAYOS CLÍNICOS CON MEDICAMENTOS

El genoma humano está compuesto por nucleótidos de los que prácticamente su totalidad están situados de la misma manera en el ser humano. Ello permite afirmar nuestra identidad como especie biológica independiente. Pero acontece que, en torno al 1 por ciento de los mencionados nucleótidos, presentan un poliformismo genético que es el que motiva la necesidad de estudiar la propensión a padecer determinadas enfermedades y de analizar la respuesta a la administración de determinados medicamentos. Cuando el poliformismo genético afecta al nucleótido único aparecen las disciplinas de la Farmacogenética y de la Farmacogenómica. La primera analiza los aspectos genéticos relacionados con la variabilidad de la respuesta a los medicamentos en individuos o poblaciones. Por su parte, la Farmacogenómica se ocupa del estudio sistemático de todo el genoma en relación con el proceso de descubrimiento y desarrollo de nuevos medicamentos.

En cualquiera de las dos disciplinas señaladas, se desarrollan los ensayos clínicos con medicamentos que tienen una importante implicación con al tema de la protección de datos de carácter personal. La norma que regula los citados ensayos es el Real Decreto 223/2004, de 8 de febrero, y prevé que en su desarrollo intervengan, además del sujeto que decide someterse al ensayo clínico, los siguientes agentes:

- ➢ Promotor, que será el responsable del inicio, gestión y/o financiación del ensayo clínico. Desde el punto de vista de la LOPD actuará como responsable del fichero ya que decidirá sobre la finalidad, contenido y uso del tratamiento.
- ➢ Monitor, que será el profesional elegido por el promotor para el seguimiento directo de la realización del ensayo, sirviendo de vínculo entre aquél y el investigador o equipo de investigación. A tenor de la LOPD será un encargado de tratamiento que actuará bajo las instrucciones del promotor.
- ➢ La organización de investigación del contrato, que estará constituida por la persona física o jurídica contratada por el promotor para realizar funciones o deberes de éste en rela-

[88] Carta de los Derechos Fundamentales de la Unión Europea, en su artículo 21, Convenio sobre los Derechos Humanos y la Biomedicina adoptado en Oviedo el 4 de abril de 1997, en su artículo 11, y Declaración Universal sobre el Genoma Humano y los Derechos Humanos de la Unesco de 16 de noviembre de 1999, en su artículo 6.

[89] Documento de trabajo sobre datos genéticos adoptado el 17 de marzo de 2004.

[90] Por ejemplo, se declaró desproporcionada la intención de crear un fichero con muestras genéticas para identificar a los recién nacidos por medio de pruebas de ADN, ya que puede conseguirse el mismo resultado de impedir la identificación madre-hijo con otros medios tales como la utilización de pulseras de identidad o la toma de huellas plantares.

ción al ensayo clínico. Al igual que en el caso del monitor su papel, desde el punto de vista de la protección de datos, será el de un encargado de tratamiento.

- ➢ Investigador o equipo de investigación, dirigido por un profesional sanitario que actuará como investigador principal, que será el médico o la persona que ejerce una profesión reconocida para llevar a cabo investigaciones en el seno de un centro sanitario, en razón de su formación científica y de su experiencia en la atención sanitaria requerida. Su responsabilidad es la realización práctica del contrato y por ello, desde el punto de vista de la LOPD, el centro sanitario en el que se desarrolle el ensayo clínico asumirá el papel de responsable del fichero.
- ➢ Comité Ético de Investigación Clínica que se configura como el organismo independiente, formado por profesionales sanitarios y no sanitarios, encargado de velar por la protección de los derechos, seguridad y bienestar de las personas que participan en el ensayo. Su papel, a tenor de la LOPD, sería el de un usuario, que podría entrar a conocer los datos sin necesidad de contar con el consentimiento de los sujetos sometidos al ensayo clínico, en virtud de habilitación legal.

De acuerdo con el señalado y en relación al esquema de agentes que intervienen en el desarrollo de un ensayo clínico, la posición habitual de un profesional sanitario será la de investigador recayendo en el mismo, a tenor de la normativa de protección de datos, las siguientes funciones:

- La recogida del consentimiento del sujeto sometido al ensayo clínico, tanto del «*consentimiento informado*» propio de la normativa de autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, como del «*consentimiento expreso, inequívoco, específico e informado*» exigido por la LOPD. En relación a este último, aparte de los extremos generales a que se ha de referir el deber de información[91], en la experiencia práctica de los ensayos clínicos resulta habitual que los datos se recaben en varios países a la vez y que la información haya de ser objeto de transferencia internacional de datos al promotor que puede estar en un país que cuente o no con un nivel adecuado de protección. Extremos como éste, deberán de ser objeto de consentimiento expreso por parte de las personas que deciden participar en el ensayo clínico.
- Crea, notifica y registra el fichero en el que se recogerán los datos correspondientes a las personas que se van a someter al ensayo clínico. La previsión del entorno global del desarrollo del ensayo clínico, en el que lo normal suele ser que se produzcan transferencias internacionales de datos, deberá incluirse en la notificación de los ficheros que el investigador remita al registro de protección de datos que corresponda[92].
- Se responsabiliza de la veracidad de los datos que transmite al promotor,
- Velará por la confidencialidad de la información que se refiera a las personas que participan en el ensayo.

Desde el punto de vista del investigador no cabe duda de que existe un fichero con datos personales. Ahora bien existen dudas sobre si, al tener que transmitir la información al promotor y al monitor de manera disociada, solamente existe el citado fichero, no resultando de aplicación la LOPD al fichero del promotor al no contener datos relativos a personas identificadas o identificables. Respecto de este asunto, y sin perjuicio de que cada ensayo clínico deba de ser analizado en particular, puede afirmarse que las funciones que se encomiendan al promotor le han de permitir, en determinadas circunstancias, llegar a conocer la identidad de los sujetos sometidos al ensayo clínico. Por ejemplo, al promotor le corresponde la responsabilidad de comunicar a las autoridades sanitarias, a los investigadores y al Comité Ético de Investigación Clínica las sospechas de reacciones adversas graves e inesperadas. Por lo tanto, en estos casos resulta obligado identificar a los sujetos sometidos al ensayo clínico en cuyo caso el fichero del cual es responsable el promotor estará sometido a la LOPD. Asimismo, la necesidad de contar con la identificación de las personas sometidas al ensayo puede venir motivada por la contratación de un seguro de responsabilidad civil que responda de los daños y perjuicios que pudieran padecer dichas personas por actividades del promotor, del monitor, del investigador principal y de sus colaboradores, o, en su caso, del hospital o centro donde se llevan a cabo el ensayo.

[91] Artículo 5.1 de la LOPD.

[92] Registro General de Protección de Datos en el ámbito de la Agencia Española de Protección de Datos, o los registros de los órganos de control en materia de protección de datos que se hayan creado en las comunidades autónomas.