

LA PROTECCIÓN DE DATOS DEL USUARIO DE LA SANIDAD: DERECHO A LA INTIMIDAD Y ASISTENCIA SANITARIA.

Javier García Amez

Asesor Jurídico

Hospital Universitario Central de Asturias

Resumen: La protección de la intimidad del usuario de la Sanidad está dispersa en una pluralidad de normas, este artículo pretende analizarlas y exponerlas desde una versión crítica, ofreciendo soluciones a los posibles problemas que se han detectado.

Palabras clave: Protección de datos. Sanidad Privacidad.

Key Words: Data Protection. Health. Privacy

Dirección: javier.amez@sespa.princast.es

Finalización: 4 de marzo de 2010

1. INTRODUCCIÓN

En el campo sanitario nuevas tecnologías se están abriendo paso, contribuyendo con ello a que los poderes públicos puedan cumplir, de manera más eficaz, con el mandato que se inculca desde el artículo 43.1 de la Constitución (en adelante, CE), que establece el Derecho a la Salud de todas las personas, y que contempla una vertiente prestacional, ya que exige el establecimiento de una serie de prestaciones sanitarias en aras a lograr que todas las personas gocen de un óptimo estado de salud¹.

Consecuencia del acceso a las prestaciones sanitarias, los usuarios de las mismas revelan una serie de datos que supone una cesión de información sobre su salud para que la asistencia sea más eficaz. De este modo, cada persona va forjando desde su nacimiento un amplio y prolijo historial de informaciones médicas, puesto en peligro por el avance tecnológico². Como contrapartida del desarrollo y expansión de la informática, las personas

pág. 188. Sobre este Derecho, véase PEMAN GAVIN, J., *Derecho a la salud y asistencia sanitaria*, Publicaciones del Real Colegio de España, Bolonia, 1989

² Vid. PEREZ LUÑO, A.-E., «Biotecnologías e intimidad», PEREZ LUÑO, A.-E., *La tercera generación de Derechos Humanos*, Thomson- Aranzadi, Cizur- Menor, 2006, págs. 136-137.

¹ Vid. BERMEJO LATRE, J., «Sanidad y Administración Sanitaria», BERMEJO VERA, J. (Dir.), *Derecho Administrativo. Parte especial*. Thomson- Civitas, Madrid, 6ª Edición, 2005,

se muestran más vulnerables, más transparentes por una accesibilidad y asequibilidad del conocimiento y manejo de los datos, hábitos u actividades, algo que escapa cada vez más a su control, poniéndose en peligro derechos y libertades fundamentales³.

El constituyente español, consciente de este riesgo⁴, junto al reconocimiento en el apartado 1º del artículo 18 del derecho a la intimidad personal y familiar, añadió un apartado cuarto⁵:

“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”

Según la sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre⁶, este artículo pretende crear un Instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos. Un Instituto que además es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama *la informática*, y que se ha dado en llamar libertad informática, el derecho a controlar el uso de los mismos datos insertos en un progra-

ma⁷. En palabras del propio Tribunal Constitucional, en su sentencia 292/2000, de 30 de noviembre⁸:

“[...] el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso [...]”

Todo usuario de la Sanidad se verá protegido frente a las nuevas tecnologías por el derecho a la protección de datos, si bien, como todo derecho, no presenta un contenido ilimitado, tiene una serie de límites. En el ámbito sanitario, en determinados supuestos, con el objeto de cumplir con el mandato constitucional de velar por la salud de las personas, se hace necesaria la obtención de datos personales recogidos en historias clínicas al objeto de realizar investigaciones que se llevan a cabo mediante la elaboración y transmisión de datos personales identificados, motivo por el cual, surge un conflicto entre el derecho a la intimidad y el derecho a la salud⁹, aunque la conservación y el acceso a tales datos no sólo es necesario para garantizar la salud de la persona, también se realiza para salvaguardar el derecho de todos los ciudadanos a la tutela de su salud, de modo que el tratamiento, recogida o cesión de datos sanitarios se puede justificar, aun careciendo del consentimiento del interesado¹⁰.

2. EL DISPERSO MARCO NORMATIVO REGULADOR DE LOS DATOS SANITARIOS

El derecho a la intimidad tiene por objeto la garantía a todas las personas de un ámbito reservado de su vida respecto al conocimiento y la acción de terceros, ya sean entes públicos o privados¹¹. Se

³ Vid. GARCÍA GARNICA, M. C., «La protección de los datos relativos a la salud de los trabajadores (A propósito de la STC 202/1999, de 8 de noviembre.)», *Derecho Privado y Constitución*, núm. 14, Enero- Diciembre, 2000, pág. 135. Sobre los riesgos que suponen las nuevas tecnologías para la protección de un determinado tipo de datos sanitarios, como son los genéticos, vid. ROMEO CASABONA, C.M., «El tratamiento y la protección de los datos genéticos», MAYOR ZARAGOZA, F., y ALONSO BEDATE, C. (Coords.), *Gen- Ética*, Ariel, Barcelona, 2003, págs. 236 y 237.

⁴ La protección de la intimidad del usuario de la Sanidad ya era una tarea que se había emprendido por medio del Secreto Médico, al en este sentido, MUÑOZ MACHADO, S., «El secreto médico», *Revista de Administración Pública*, núm. 79, enero- abril, 1976, págs. 163 a 213, trabajo dentro del cual puede encontrarse un análisis de la normativa existente en el momento, así como los supuestos en los que cede y las personas que se ven afectadas al respecto.

⁵ Sobre este artículo, FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales en las Administraciones Públicas*, Thomson- Civitas, Madrid, 2003, págs. 51 a 69, y MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica a la autodeterminación informativa*, Thomson Civitas, Madrid, 2004.

⁶ Ponente, Sr. González de Campos.

⁷ Sentencias del Tribunal Constitucional 11/1998, de 13 de enero (Ponente, Sr. Ruíz Vadillo) y 94/1998, de 4 de mayo (Ponente, Sr. González de Campos).

⁸ Ponente, Sr. González de Campos.

⁹ Vid. PEREZ LUÑO, A.-E., «Biotecnologías...», *cit.*, pág. 137.

¹⁰ Vid. GARCÍA GARNICA, M.C., «La protección de los datos...», *cit.*, pág. 150.

¹¹ Sentencias del Tribunal Constitucional 231/1988, de 2 de diciembre (Ar.231. Ponente, Sr. Rubio Llorente),

trata de aquella facultad que ostenta toda persona para que determinados hechos o actuaciones de su vida permanezcan ocultos hacia el exterior, reservándose para sí misma¹². En el campo de la sanidad no es posible ofrecer una asistencia adecuada sin conocer datos, hechos y actuaciones de la persona que ésta guarda para sí misma y que forman parte de su esfera íntima, de manera que el usuario ha de abrir necesariamente su intimidad para que la prestación se lleve a cabo eficazmente. El legislador, consciente de ello, siempre que ha regulado los grandes aspectos de este campo se ha preocupado por el debido respeto a la intimidad de las personas, para que no se produzca una vulneración de la misma con el pretexto de proporcionar una asistencia sanitaria eficaz.

La primera norma que debemos de señalar, es aquella que está llamada a desarrollar el artículo 43 CE, la Ley 14/1986, de 25 de abril, General de Sanidad (en adelante, LGS). Esta norma establece un catálogo de derechos básicos de todo usuario de la Sanidad, y así, en su artículo 10, impone las siguientes obligaciones:

“1. Al respeto a su personalidad, dignidad humana e intimidad sin que pueda ser discriminado por razones de raza, de tipo social, de sexo, moral, económico, ideológico, político o sindical. [...]”

3. A la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público.”

Esta disposición será completada en el año 2002 mediante la aprobación de la Ley 41/2002, de 14 de noviembre, básica, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

197/1991, de 17 de octubre (Ar. 197. Ponente, Sr. Rodríguez-Piñero y Bravo-Ferrer), 57/1994, de 18 de febrero (Ar. 57. Ponente, Sr. González Campos), 143/1994, de 9 de mayo (Ar. 143. Ponente, Sr. Rodríguez-Piñero y Bravo-Ferrer) 207/1996, de 16 de diciembre (Ar. 207, Ponente, Sr. Gimeno Sendra), 98/2000, de 10 de abril (Ar. 98. Ponente, Sr. Garrido Falla), 156/2001, de 2 de julio (Ar. 156, Ponente, Sr. Viver Pi-Sunyer) 127/2003, de 30 de junio (Ar. 127. Ponente, Sr. Cachón Villar) y 196/2004, de 15 noviembre (Ar. 196. Ponente, Sr. Delgado Barrio) entre otras.

¹² Sobre el origen del derecho a la intimidad, *vid.* WARREN S. y BRANDEIS, L. (Traducción de Benigno Pendás y Pilar Baselga), *El Derecho a la Intimidad*, Civitas, Madrid, 1995.

(en adelante LDO)¹³, que según su artículo 1 tiene por objeto la regulación de los derechos y obligaciones de los pacientes, usuarios y profesionales de todos los centros y servicios sanitarios, ya sean públicos o privados¹⁴. DE LA TORRE FORCARDELL, señala que la LDO ha cumplido un papel fundamental en este campo, ya que partiendo del reconocimiento de los derechos de los pacientes en las relaciones clínico – asistenciales, vino a completar y adoptar las previsiones de la LGS con relación al

¹³ Sobre el contenido de esta ley resulta aconsejable el libro de PEMÁN GAVÍN, J., *Asistencia sanitaria y Sistema Nacional de Salud*, Comares, Granada, 2005, págs. 257 a 276 y SÁNCHEZ –CARO, J. y FERNÁNDEZ ABELLÁN, F., *Derechos y deberes de los pacientes*, Comares, Albolote, 2003, Un completo y correcto examen de la historia de la intervención administrativa en el campo sanitario se encuentra en MUÑOZ MACHADO, S., *La formación y la crisis de los servicios sanitarios públicos*, Alianza, Madrid, 1995.

¹⁴ De todas formas el contenido de la LDO deberá ser completado con las leyes que las Comunidades Autónomas dicten sobre la materia, ya que, de acuerdo con la distribución de competencias, éstas pueden asumir según el artículo 148.1.21ª CE, las competencias en materia de Sanidad, siempre y cuando se respete la legislación básica del Estado, tal y como se señala en el artículo 149.1.16ª CE, y que es el título competencial alegado para aprobar la LDO, que conforma lo que se puede calificar como el estatuto básico del usuario de la Sanidad. Estatuto que deberá ser completado con las leyes autonómicas, de forma que la protección de los derechos y de las obligaciones de los pacientes, la normativa aparece dispersa en varias normas, una normativa básica –de origen estatal- y una serie de normas –dictadas por las Comunidades Autónomas- que completan a la primera. Así, por ejemplo, pueden verse la Ley 1/2003, de 28 enero, de Derechos e Información al Paciente de la Comunidad Valenciana, Ley 21/2000, de 29 diciembre, de Autonomía del Paciente y Derechos de Información y Documentación Clínica de Cataluña, Ley Foral 11/2002, de 6 mayo, de Derechos del paciente a las voluntades anticipadas, a la información y a la documentación clínica de Navarra, Ley 11/2007, de 26 noviembre, reguladora del consejo genético, de protección de los derechos de las personas que se sometan a análisis genéticos y de los bancos de ADN humano en Andalucía, Ley 8/2003, de 8 abril, sobre derechos y deberes de la personas en relación con la salud de Castilla y León, Ley 3/2005, de 8 julio, de Información Sanitaria y Autonomía del Paciente de Extremadura, Ley 12/2001, de 21 diciembre, de Ordenación Sanitaria de Madrid, Ley 3/2009, de 11 mayo, de Derechos y Deberes de los Usuarios del Sistema Sanitario de Murcia, Decreto 175/1989, de 18 julio, de la Consejería de Sanidad y Consumo del Gobierno Vasco, por el que se aprueba la Carta de derechos y obligaciones de pacientes y usuarios, Orden de 28 febrero 2005, de la Consejería de Sanidad de Canarias, por la que se aprueba la Carta de los Derechos y de los Deberes de los Pacientes y Usuarios Sanitarios y se regula su difusión, Decreto 23/2007, de 1 marzo, del Consejo de Gobierno de Cantabria, sobre Derechos de la madre, el padre y el recién nacido en relación con el nacimiento en el ámbito sanitario

derecho a la intimidad, el derecho a la confidencialidad de los datos y el deber de secreto profesional, aclarando de esta manera la situación jurídica y los derechos y obligaciones de los profesionales sanitarios, de los ciudadanos y de las instituciones sanitarias¹⁵, a la vez que el artículo 7.1 establece la obligación de respeto por la confidencialidad de los datos¹⁶.

Fuera de lo que podríamos calificar normativa general sanitaria, nos encontramos normas relativas a sectores concretos, entre las cuales destacan el Real Decreto 411/1996, de 1 de marzo, por el que se regulan las actividades relativas a la utilización clínica de tejidos humanos¹⁷, Real Decreto 2070/1999, de 30 de diciembre, por el que se regulan las actividades de obtención y utilización clínica de órganos humanos y la coordinación territorial en materia de donación y trasplante de órganos y tejidos¹⁸, Real Decreto 1088/2005, de 16 de

septiembre, por el cual se establecen los requisitos técnicos y condiciones mínimas de la hemodonación y de los centros y servicios de transfusión¹⁹, 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 aprueban las normas de coordinación y funcionamiento para su uso en humanos²⁰, Real

¹⁵ Vid. DE LA TORRE FORCADELL, S., «Reflexiones sobre el acceso a la historia clínica informatizada y la protección de datos de salud», PLAZA PENADÉS, J. (Coord.), *Cuestiones actuales de Derecho y Tecnologías de la Información y la Comunicación (TICS)*, Thomson- Aranzadi, Cizur Menor, 2006, pág. 121. En igual sentido, AYERRA LAZCANO, J. M., «Regulación general de la Historia Clínica», *Derecho y Salud*, Volúm. 11, núm. 11, Enero-Junio, 2003, pág. 25.

¹⁶ La LDO en el artículo 7. 1 establece que:

“1. Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.”

¹⁷ En su artículo 3 establece que:

“1. En ningún caso podrán facilitarse ni divulgarse informaciones que permitan la identificación del donante y del receptor de tejidos humanos.

2. El donante no podrá conocer la identidad del receptor, ni el receptor la del donante, a excepción de los donantes vivos genéticamente relacionados.

3. La información relativa a donantes y receptores de tejidos humanos será recogida, tratada y custodiada en la más estricta confidencialidad, conforme a lo dispuesto en el artículo 10.3 de la Ley 14/1986, de 25 de abril, General de Sanidad, y en los artículos 7, 8 y concordantes de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal.”

¹⁸ El artículo 5 dispone que:

“1. No podrán facilitarse ni divulgarse informaciones que permitan la identificación del donante y del receptor de órganos humanos.

2. Los familiares del donante no podrán conocer la identidad del receptor, ni el receptor o sus familiares de la del donante y, en general, se evitará cualquier difusión de información que pueda relacionar directamente la extracción y el ulterior injerto o implantación. De esta limitación se excluyen los directamente interesados en el supuesto del artículo 9.

3. La información relativa a donantes y receptores de órganos humanos será recogida, tratada y custodiada en la más estricta confidencialidad, conforme a lo dispuesto en el artículo 10.3 de la Ley 14/1986, de 25 de abril, General de Sanidad, y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.”

¹⁹ Su artículo 5.1 dice lo siguiente:

“Se garantizará a los donantes de sangre la confidencialidad de toda la información facilitada al personal autorizado relacionada con su salud, de los resultados de los análisis de sus donaciones, así como de la trazabilidad futura de su donación, de acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.”

²⁰ Este derecho se recoge en el artículo 6, el cual señala que:

“1. Se garantizará a los donantes la confidencialidad de todos los datos relacionados con su salud y facilitados al personal autorizado, así como de los resultados y la trazabilidad de sus donaciones, de acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Los establecimientos de tejidos deberán adoptar, en el tratamiento de los datos relacionados con los donantes, las medidas de seguridad de nivel alto previstas en el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por el Real Decreto 994/1999, de 11 de junio.

3. Los datos de carácter personal tendrán carácter confidencial y estarán exclusivamente a disposición de los interesados, conforme a lo dispuesto en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y, en su caso, de la autoridad judicial para el ejercicio de las funciones que tiene encomendadas. Su utilización se limitará a fines asistenciales o de interés para la salud pública y será recogida y custodiada conforme a lo dispuesto en el artículo 10 de la Ley 14/1986, de 25 de abril, General de Sanidad, en la Ley 15/1999, de 13 de diciembre, y en la citada Ley 41/2002, de 14 de noviembre.

4. El deber de confidencialidad no impedirá la adopción de medidas preventivas cuando se sospeche la existencia de riesgos para la salud individual o colectiva en los términos previstos en los artículos 25 y 26 de la Ley General de Sanidad o, en su caso, conforme a lo que establece la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública, la Ley 41/2002, de 14 de noviembre, y la Ley Orgánica 15/1999, de 13 de diciembre.

5. No podrán facilitarse ni divulgarse informaciones que permitan la identificación de donantes y receptores de células

Decreto 223/2004, de 6 febrero, por el que se regula los ensayos clínicos con medicamentos²¹, la Ley 16/2006, de 26 de mayo, de Técnicas de reproducción humana asistida (en adelante, LRA)²², y la Ley Orgánica 2/2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo²³.

Con carácter general, en todas estas normas aparece recogido el derecho a la intimidad del usuario de la sanidad, si bien, con la excepción de la LDO, se limitan a un mero reconocimiento de este derecho, lo que supone el desconocimiento de los casos en los que el mismo cede o los mecanismos tendentes a conseguir una tutela efectiva frente a las vulneraciones, algo que nos obliga a tener que acudir a aquella normativa que con carácter general se preocupa de la regulación de la protec-

y tejidos humanos, ni podrán facilitarse a los donantes o sus familiares los datos identificadores de los receptores o viceversa.”

²¹ En concreto, el artículo 3.6 del mismo dispone:

“6.El tratamiento, comunicación y cesión de los datos de carácter personal de los sujetos participantes en el ensayo se ajustará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y constará expresamente en el consentimiento informado”.

²² Es en esta norma, en la que más veces aparece reconocido el derecho a la intimidad del usuario de tales técnicas, al hacerlo en los artículos 3.6 -obligación de que aquellos datos relativos a la utilización estas técnicas, sean recogidos en historias clínicas individualizadas, las cuales serán tratadas con las debidas garantías de confidencialidad respecto de la identidad de los donantes, de los datos y condiciones de los usuarios y de las circunstancias que concurran en el origen de los hijos que nazcan mediante el empleo de estas técnicas-, 5.5 -obligación de que la donación de gametos y preembriones sea anónima a la vez de que se garantice la confidencialidad de los datos sobre la identidad de los donantes por parte de los bancos de gametos, así como por parte de los registros de donantes-, 18.3 -los equipos médicos deberán de recoger en una historia clínica todas las referencias sobre los donantes y usuarios de estas técnicas, así como todas los consentimientos firmados para la realización de tales actos, la cual deberá de ser custodiada con la debida protección y confidencialidad- y 21 -imposición al Registro nacional de donantes, de que las inscripciones que se realicen en él, se efectúen con las garantías precisas de confidencialidad de los datos proporcionados-. Sobre en contenido de esta ley, COBACHO GOMEZ, J. A. e INIESTA DELGADO, J. J. (Coords.), *Comentarios a la Ley 14/2006, de 26 de mayo, sobre Técnicas de Reproducción Humana asistida*, Thomson- Aranzadi, Cizur- Menor, 2007 y LLEDO YAGUE, F., OCHOA MARIETA, C. Y MONJE BALMASEDA, O. (Coords.), *Comentarios científico-jurídicos a la ley sobre técnicas de reproducción humana asistida*, Dyckinson, Madrid, 2007.

²³ En concreto, los artículos 20 a 23 de la misma regulan el manejo de la información en este ámbito.

ción de datos de carácter personal, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), que en sus artículos 7.3 y 8 cataloga a este tipo de información como especialmente protegidos²⁴. No obstante, también ha de analizarse toda la normativa de desarrollo de la LOPD, concretada en el Real Decreto 428/1993, de 26 de marzo por el que se aprueba el Estatuto de la Agencia de Protección de Datos, Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, RPD), Instrucción 1/1998, de 19 de enero, de la Agencia Estatal de Protección de Datos (en adelante, AEPD), relativa al ejercicio de los derechos de acceso rectificación y cancelación (en adelante Instrucción, 1/1998), Instrucción 1/2000, de 1 de diciembre, relativa a las normas por las que se rigen los movimientos internacionales de datos (en adelante Instrucción, 1/2000).

De todas maneras, la Ley 14/2007, de 3 de julio, de Investigación biomédica (en adelante, LIB) ha venido a marcar un antes y un después en la protección del derecho a la intimidad en el sector, ya no de la asistencia sanitaria en sí, sino el relativo a las investigaciones biomédicas en general, pues se ocupa de regular de manera específica en el sector de las mismas este derecho, otorgando una sustantividad propia, que con anterioridad a la LIB no se daba, a la protección de un determinado tipo de información como es la genética, que en esta ley cuenta de un régimen específico y que se

²⁴ En muchas ocasiones, sobre todo en la fase de instrucción de procedimientos administrativos sancionadores o procedimientos penales, se hace necesario acceder a esta información, de modo que se crean ficheros destinados a tales fines, por lo cual a este artículo 7.3 se le debe de sumar el 7.5 LOPD, que cataloga a este tipo de datos como especialmente protegidos, no obstante, en este punto, y siguiendo a HUERGO LORA, A., *Las sanciones administrativas*, Iustel, Madrid, 2007, pág. 37, nota 25, se debe recordar que los delitos no son lo mismo que las infracciones administrativas, tal y como se desprende de la lectura de la legislación al respecto, a tales efectos, por lo que los primeros gozan de una protección más fuerte que las segundas. Igualmente, y del mismo autor, «La Constitución de 1978 y el Derecho Administrativo», en AAVV., *Homenaje a la Constitución Española: XXV aniversario*, Servicio de Publicaciones de la Universidad de Oviedo, Oviedo, 2005, págs. 34 a 36.

muestra, en principio, acorde con las específicas características de los mismos²⁵.

Hasta ahora hemos visto las normas que a nivel interno español se ocupan de regular la protección del derecho a la intimidad del usuario de la sanidad. En el ámbito internacional también existe normativa, si bien, ésta ha surgido con la preocupación de preservar no tanto el derecho a la intimidad cuanto los derechos en general de toda persona frente a los avances de la medicina y las nuevas tecnologías²⁶. De estas normas no todas cuentan con un mismo valor jurídico, y en lo que a la protección de los datos sanitarios concierne, nos encontramos un único instrumento de carácter vinculante para los Estados, pues los restantes son Declaraciones Internacionales²⁷ o Recomendaciones

²⁵ Sobre los datos genéticos en general, véanse por todos, REBOLLO DELGADO, R. y GÓMEZ SÁNCHEZ, Y., *Biomedicina y Protección de Datos*, Dyckinson, Madrid, 2008, SUÁREZ ESPINO, M. L., *El Derecho a la intimidad genética*, Marcial Pons, Madrid, 2008, ALVAREZ GONZÁLEZ, S., *Derechos fundamentales y protección de datos genéticos*, Dyckinson, Madrid, 2007, y NICOLÁS JIMÉNEZ, P., *La Protección jurídica de los datos genéticos de carácter personal*, Cátedra interuniversitaria fundación BBVA- Diputación Foral de Bizkaia de Derecho y Genoma Humano, Comares, Bilbao- Granada, 2006 y SANCHEZ-CARO, J. y ABELLÁN, F., *Datos de salud y dato genéticos*, Comares, Albolete, 2004-

²⁶ No debemos olvidar en este punto del Convenio el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, y ratificado por España el 27 de enero de 1984. El cual, según nos señala ULL PONT, E., *Derecho Público de la informática. Protección de datos de Carácter personal*. UNED, Madrid, 2ª edición, 2003, pág. 54., tiene el ambicioso proyecto de armonizar la necesidad de libre circulación de datos, con la protección de los derechos de la persona.

²⁷ Se trata de la Declaración Internacional sobre el Genoma Humano y los Derechos Humanos, aprobada por aclamación el 11 de noviembre de 1997 en la Conferencia General de la UNESCO, la Declaración Internacional sobre datos genéticos, aprobada por aclamación en la Conferencia General de la UNESCO, el 16 de octubre de 2003 (en adelante DDG) y la Declaración Internacional de la UNESCO sobre la Bioética y Derechos Humanos, aprobada por aclamación en la Conferencia General de la UNESCO de 19 de octubre de 2005. Declaraciones todas ellas que se refieren a un determinado tipo específico de datos sanitarios, los genéticos. Sobre su valor, a pesar de tratarse de una norma con un valor meramente programático, las Declaraciones de la UNESCO se han convertido a lo largo de los años en auténticos principios generales de Derecho Internacional, tal y como acertadamente ha señalado ROMEO CASABONA, C., *Los genes y sus leyes. El derecho ante en genoma humano*. Cátedra interuniversitaria fundación BBVA- Diputación Foral de Bizkaia de Derecho y Genoma Humano, Comares, Bilbao- Granada, 2002, pág. 42, Opinión también sustentada en GARCÍA AMEZ, J., «Los protección de

hacia los Estados²⁸, y que en definitiva no son más *soft law*. Esta norma es el Convenio para la protección de los Derechos Humanos y la dignidad del ser humano respecto a la aplicación de la biología y la Medicina, firmado en Oviedo el 4 de abril de 1997 (en adelante, Convenio de Oviedo), cuyo objeto, según destaca ROMEO CASABONA, consiste en lograr proteger los Derechos Humanos frente a los avances que cada día se producen en el campo de la Biomedicina, noble labor que se realiza elevando la dignidad humana al más alto rango posible²⁹. Siguiendo la tónica del artículo 8 del Convenio Europeo sobre Derechos Humanos³⁰, el artículo 10 del Convenio de Oviedo dice:

“Todos tienen el derecho al respeto a su vida privada en el ámbito de su salud”

Finalmente, también nos encontramos con el importante papel que en esta materia ha venido a jugar la Unión Europea, que a lo largo de su historia ha aprobado varias directivas cuyo centro de atención no es la intimidad sanitaria, sino la protección de datos en general, y entre las que destaca Directiva 95/46/CE, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales, y a la

los datos genéticos en España. Una mirada desde los principios generales de protección de datos de carácter personal», *Revista de Derecho y Genoma Humano/ Law and the Human Genome Review*, núm. 24, Enero-Junio, 2006, pág. 31.

²⁸ Recomendación (97) 5, del Comité de Ministros del Consejo de Europa, relativa a la protección de datos médicos. Respecto a la protección de la información genética véase las Resoluciones del Consejo Económico y Social de las Naciones Unidas sobre privacidad genética y no discriminación 2001/39, de 26 de julio de 2001, y 2003/232, de 22 de julio de 2003, y la Recomendación (2006) 4, del Comité de Ministros del Consejo de Europa sobre investigación con material biológico de origen Humano, de 13 de marzo de 2006.

²⁹ Vid. ROMEO CASABONA, C.M., «El Convenio Europeo sobre Derechos Humanos y Biomedicina: sus características y repercusiones en el Derecho Español», ROMEO CASABONA, C.M. (Ed.), *El convenio de Derechos Humanos y Biomedicina. Su entrada en vigor en el ordenamiento jurídico español*, Cátedra interuniversitaria fundación BBVA- Diputación Foral de Bizkaia, Cátedra de Derecho y Genoma Humano, Comares, Bilbao- Granada, 2002, pág. 9. Sobre la elaboración y tramitación parlamentaria de este Convenio, NICOLÁS JIMÉNEZ, P., «El Convenio de Oviedo de Derechos Humanos y Biomedicina: la génesis parlamentaria de un ambicioso proyecto del Consejo de Europa», *Revista de las Cortes Generales*, núm. 40, Marzo, 1997, págs. 129 y ss.

³⁰ Convenio para la protección de los Derechos Humanos y las libertades fundamentales, firmado en Roma el 4 de noviembre de 1950.

libre circulación de estos datos (en adelante, Directiva 95/46/CE). El contenido de ésta será analizado a lo largo de este trabajo.

Veamos ya, una vez expuesto el disperso y complicado entramado legal que regula este tipo de datos, la protección del interesado³¹.

3. LOS DATOS SANITARIOS

En su artículo 7 la LOPD califica a los datos sanitarios como *especialmente protegidos*, dejando entrever la importancia de su protección, si bien, no ofrece una definición de qué se ha de entender como tales, ya que su artículo 8 efectúa una remisión a lo que disponga la legislación específica – sea autonómica o estatal– para su tratamiento. El Consejo de Europa, en el punto 45 de la memoria que acompaña al Convenio 108, sí que define los mismos, al considerar que la noción de datos sanitarios comprende las informaciones concernientes a la salud pasada, presente y futura, física o mental del individuo, siendo posible que las informaciones provengan de una persona que goza de buena salud, enferma o fallecida, comprendiendo estos datos, igualmente, informaciones relativas al abuso de alcohol o consumo de drogas. Es decir, el concepto de dato sanitario es realmente amplio y permite incluir información variopinta sobre un sujeto determinado³².

³¹ Por interesado entiende el artículo 3.1 LOPD, toda persona física titular de los datos a que se refiere el tratamiento.

³² Este concepto ha sido ampliado por el Tribunal de Justicia de las Comunidades Europeas, quien en la sentencia de 6 de noviembre de 2003, Caso Lindqvist (Ar. 368. Ponente, Sr. Ogilvy Edward), en su punto 50, incluye dentro de este concepto la información relativa a los aspectos físicos o psíquicos de una persona. Sobre el contenido de esta sentencia, *vid.* ARENAS RAMIRO, M., «El derecho a la protección de datos personales en la jurisprudencia del TJCE», PLAZA PENADÉS, J. (Coord.), *Cuestiones...*, *cit.*, págs. 113 a 119. Una definición doctrinal, también amplia de este tipo de datos, nos la proporciona SERRANO PÉREZ M. M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Thomson-Civitas, Madrid, 2003, pág. 417, quien considera que son toda la información sensible relativa a la salud de un individuo, así como todos aquellos datos personales que es preciso recabar para completar el expediente de esta persona, y que en el campo de la medicina se recoge en lo que se denomina como historia clínica. Véase igualmente el artículo 5.1.g) RPD, que recoge una definición de dato de salud similar a la que hemos señalado.

Según el artículo 3.a) LOPD, esta información ha de versar sobre personas físicas identificadas o identificables³³. HEREDERO IGLESIAS³⁴, señala que para poder hablar de dato personal, deben concurrir dos elementos, la información y la persona a quien le concierne, pues si nos encontramos con la sola existencia de información, pero no está relacionada con una persona, a pesar de que sea un dato no será catalogada como dato de carácter personal, al encontrarnos ante lo que se denomina como dato anónimo³⁵.

Elemento fundamental en esta cuestión es la historia clínica³⁶, objeto de regulación en los artículos 14 a 19 LDO –que cuentan con la consideración de normativa básica estatal³⁷–, proporcionando una definición de la misma en el artículo 14.1:

“[...]el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con

³³ *Vid.* RIPOL CARULLA, S., «La protección de los datos médicos y genéticos en la normativa del Consejo de Europa (Parte I)», *Revista de Derecho y Genoma Humano/ Law and the Human Genome Review*, núm. 5, Julio- Diciembre, 1996, pág. 125.

³⁴ Si bien refiriéndose a la Directiva 95/46/CE, que en su artículo 2 establece este mismo concepto

³⁵ *Vid.* HEREDERO HIGUERAS, M., *La Directiva Comunitaria de Protección de los Datos de Carácter Personal*, Aranzadi, Elcano, 1997, pág. 131 y APARICIO SALOM, J., *Estudios sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Elcano, 2ª edición, 2002, pág. 49. Por su parte, el RD 1332/1994, en el artículo 1 ofrece una definición más ilustrativa y completa:

“[...]toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable[...].”

³⁶ Un estudio completo y detallado de la misma, desbordaría el presente trabajo, aunque la historia clínica ha sido estudiada ampliamente por parte de la doctrina, de modo que me remito a los trabajos de ROMEO CASABONA C.M., y CASTELLANO ARROYO, M., «La intimidad del paciente desde la perspectiva del secreto médico y el acceso a la historia clínica», *Derecho y Salud*, núm. 1, Julio, 1993; SÁNCHEZ CARAZO, C., *Protección de datos de carácter personal relativos a la salud*, Agencia de Protección de Datos, Madrid, 1999; MÉGICA GARCÍA, J., *El enfermo transparente. Futuro jurídico de la historia clínica electrónica*, Edisofer, Madrid, 2002; AYERRA LAZCANO, J. M., «Regulación...», *cit.*; RODRÍGUEZ LÓPEZ, P., *La autonomía del Paciente. Información, consentimiento y documentación clínica*, Diles, Madrid, 2004; y DE LA TORRE FORCADELL, S., «Reflexiones...», *cit.*, entre otros.

³⁷ Disposición adicional primera, la cual se basa para ello en los títulos competenciales otorgados por el artículo 149.1 CE en sus puntos 1º y 16ª.

objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro”

Siguiendo en esta punto a DE LA TORRE FORCADELL, la historia clínica es el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial, no limitándose a ser una mera narración o exposición de hechos, puesto que incluye juicios, documentos, procedimientos, informaciones y, sobre todo, el consentimiento del paciente³⁸.

Respecto a su custodia, la LDO establece en el punto segundo de este artículo 14 que cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información.

Este artículo se ha de completar con lo dispuesto en la LOPD y su normativa de desarrollo, sobre todo, en lo que concierne a las medidas de seguridad que se deben adoptar en aras a garantizar que los documentos que integran el historial clínico se conserven de modo seguro, sin que el derecho a la intimidad del usuario quede restringido, y se cumpla con los postulados del principio de seguridad, el cual será objeto de análisis posteriormente.

Respecto a su contenido, el artículo 15 señala que, además de tener como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que bajo criterio médico permitan el conocimiento veraz y actualizado del estado de salud³⁹, deberá incorporar: la información que se considere trascendental para el conocimiento veraz

³⁸ Vid. DE LA TORRE FORCADELL, S., «Reflexiones...», *cit.*, pág. 121.

³⁹ En cuanto al contenido mínimo que ha de recoger toda historia clínica, el artículo 15.2 LDO establece que recogerá: la documentación relativa a la hoja clínico-estadística, la autorización de ingreso, el informe de urgencia, la anamnesis y la exploración física, la evolución del paciente, las órdenes médicas, la hoja de interconsulta, el consentimiento informado los informes de exploraciones complementarias, de anestesia, quirófano o de registro del parto, de anatomía patológica, la evolución y planificación de cuidados de enfermería, la aplicación terapéutica de enfermería, el gráfico de constantes, y el informe clínico de alta.

y actualizado del estado de salud del paciente, estableciendo el derecho de todo usuario a que quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales realizados por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada.

4. LOS PRINCIPIOS DE PROTECCIÓN DE DATOS

GARCÍA LUENGO señala que los Principios Generales del Derecho son el principal instrumento con que cuenta el ciudadano para controlar la actividad de la Administración, a la vez que cumplen una importante labor al iluminar y dotar de sentido unitario una normativa administrativa condenada a sufrir el fenómeno de motorización legislativa⁴⁰. Se constituyen como el contenido esencial del derecho a la protección de datos, de modo que con ellos el legislador aspira a constituir un sistema preventivo de tutela de la persona respecto al tratamiento de sus datos, estableciendo un saludable equilibrio entre los avances de la sociedad de la información y el respeto a la libertad de los ciudadanos⁴¹, lo cual es realizado mediante una serie de derechos y de obligaciones que se derivan de estos principios que se recogen en la LOPD⁴². Además, los principios generales de protección de datos tienen otra importante función, son aquellos valores que la Sociedad en su conjunto entiende como dignos de tutela y que han sido recogidos en la LOPD por el legislador.

Los principios que recoge esta norma son cuatro: calidad de los datos, transparencia, consentimiento y seguridad. Ha de destacarse en este punto la gran labor llevada a cabo por parte de la Unión Europea, que ha conseguido que, todas las norma-

⁴⁰ Vid. GARCÍA LUENGO, J., *El principio de protección de la confianza en el Derecho Administrativo*, Civitas, Madrid, 2002, pág. 115, nota 1.

⁴¹ Vid. HERRÁN ORTÍZ, A., *El derecho a la protección de datos personales en la sociedad de la información*, Universidad de Deusto, Bilbao, 2003, pág. 53, y *El derecho a la intimidad en la nueva Ley Orgánica de protección de datos personales*, Dykinson, Madrid, 1999, págs. 210- 211.

⁴² Vid. GARCÍA AMEZ, J., «Los principios relativos a la protección de datos de carácter personal. Su proyección sobre los datos genéticos en España», AAVV., *16th World Congress on Medical Law. Proceedings Book, Vol. 1*, WAML, Toulouse, 2006, pág. 561 y «La protección de los datos...», *cit.*, págs. 34- 36.

tivas internas de sus Estados miembros, incorporen estos mismos principios, proporcionando un nivel de protección –de mínimos– del derecho a la protección de los datos, fruto sobre todo de la Directiva 95/46/CE, que obligó a los destinatarios a incorporar los principios que analizamos a continuación.

4.1. Principio de calidad de los datos

Es el más fundamental de todos los principios y del que se derivan más derechos para el interesado. Aparece reflejado en el artículo 4 LOPD en los siguientes términos:

“1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando resulten adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatibles el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan como veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16”

Este principio exige que se den una serie de requisitos en los datos: la existencia de un fin, y que éstos, sean adecuados, pertinentes y no excesivos con el mismo.

A) Existencia de un fin

La LOPD, en el artículo 4.1, impone la obligación de que, para poder llevar a cabo cualquier tratamiento con datos, exista un fin que lo legitime. El artículo 7.3 LOPD dispone que los datos relativos a la salud sólo se van a poder recabar, tratar o ceder, cuando medie una razón de interés general, la cual ha de venir predeterminada por medio de

una ley, con la excepción de que el interesado, de manera expresa, así lo consienta.⁴³ La importancia de la existencia de un fin es tal que a juicio de GUICHOT, sólo si se tiene constancia de la finalidad para la cual se van a utilizar los datos la sociedad podrá conocer la entidad de los tratamientos que se efectúan en nuestro país, permitiendo al interesado poder decidir de manera racional respecto a si cede o no sus datos, y posibilitándole el consentir o no una posterior cesión para tal finalidad⁴⁴.

Pero según el artículo 4.1 LOPD no va a caber cualquier tipo de fin, se exige que, éste, cumpla una serie de requisitos: ha de ser determinado, explícito, y legítimo. En caso contrario no se cumplirán los postulados del principio de calidad, y por tanto se estaría menoscabando la intimidad de la persona. En este sentido no compartimos la afirmación de APARICIO SALOM⁴⁵, para el que es suficiente la existencia de un fin genérico, que será concretado por el afectado, que podrá ejercitar sus derechos en aras a prohibir el empleo de los datos para una determinada operación. En nuestra opinión el fin debe ser determinado, pues el interesado debe conocer el mismo, ya que la existencia de un fin genérico supondría que, cada vez que se concretase, el interesado ha de ejercita sus derechos en aras a defenderse frente al mismo, lo que supondría un coste elevado para el mismo que desencadenaría una gran riesgo de lesión de derechos, al obligar al responsable del fichero a que, cada vez que concretase la finalidad, se la tuviera que comunicar al interesado al objeto de que la consienta⁴⁶.

Esta finalidad deberá estar presente durante todo el tiempo en el cual se tengan los datos. Si desaparece en cualquier momento, o pierde alguno de los requisitos señalado, el fin ya no legitimaría la

⁴³ La LGS establece una serie de supuestos en los cuales se van a poder crear ficheros que contengan datos de tipo sanitario, así, se pueden citar los artículos 8,10, 23 y 61 de la misma. Por su parte, también en la Ley Orgánica 3/1986, de 14 de abril de medidas especiales en materia de Salud Pública, la LRA, o la Ley 29/2006, de 26 de julio, de garantías y uso racional en los medicamentos, y productos sanitarios encontramos otros supuestos.

⁴⁴ Vid. GUICHOT, E., *Datos personales y Administraciones Públicas*, Thomson-Civitas, Madrid, 2005, págs. 230- 231.

⁴⁵ Vid. Estudios..., cit. pág. 112

⁴⁶ De idéntica opinión a la que en este trabajo se sustenta, SANTOS GARCÍA D., *Nociones generales de la Ley Orgánica de Protección de Datos*, Tecnos, Madrid, 2005, pág. 54.

posesión de los datos, y por tanto, lo datos se tendrían de manera ilícita.

En el campo de los ficheros públicos, éstos se han de crear por medio de una norma con rango de Ley, de forma que el principio de finalidad que se prevé en la LOPD deriva a su vez a un principio de reserva de Ley⁴⁷, lo cual, tal y como han apuntado VALERO TORRIJOS y LÓPEZ PELLICER, supone que, un incumplimiento de esta reserva, condiciona la validez de los actos administrativos que hubieren sido dictados al amparo de datos contenidos en un fichero irregular⁴⁸.

El tratamiento de los datos recogidos por las Administraciones Públicas viene subordinado a la adecuación a los fines de interés público que condicionan la actuación o ejercicio de las competencias⁴⁹, lo que enlaza con el deber constitucional de servir con objetividad a los intereses generales que se inculca a la Administración Pública, recogido en el artículo 103.1 CE, a la vez que, nuevamente,

⁴⁷ Vid. GUICHOT, E., *Datos personales...*, cit., págs. 233-234. Tampoco debemos olvidar que este requisito enlaza a su vez con el principio de legalidad que actualmente rige en nuestro ordenamiento jurídico la actuación de las Administraciones Públicas, de tal modo que las mismas para poder actuar han de estar habilitadas previamente. Sobre el principio de legalidad vid. GARCÍA DE ENTERRÍA, E., y FERNÁNDEZ-RODRÍGUEZ, T. R., *Curso de Derecho Administrativo I*, 13ª edición, Thomson-Civitas, Madrid, 2006, págs. 437 a 455 y 491-493., así como MUÑOZ MACHADO, S., *Tratado de Derecho Administrativo y Derecho Público General I*, 2ª edición, Iustel, Madrid, 2006, págs. 321 a 611.

⁴⁸ Vid. VALERO TORRIJOS, J. y LÓPEZ PELLICER, J. A., «Algunas consideraciones sobre el derecho a la protección de los datos personales en la actividad administrativa», *Revista Vasca de Administración Pública*, núm. 59, enero-abril, 2001, pág. 271. Sobre la validez de los actos administrativos, véanse las obras BOCANEGRA SIERRA, R., *Lecciones sobre el acto administrativo*, Thomson-Civitas, Madrid, 3ª edición, 2006, págs. 115 a 147 y 175 a 205, y *La teoría del acto administrativo*, Iustel, Madrid, 2005, págs. 79 a 98 y 167 a 200; GARCÍA LUENGO, J., *La nulidad de pleno derecho de los actos administrativos*, Civitas, Madrid, 2002, y «Los supuestos de nulidad de pleno derecho establecidos al margen de la Ley de Procedimiento Común», *Revista de Administración Pública*, núm. 159, 2002, págs. 137 a 172; y el comentario al título IV de la Ley de Procedimiento Común, realizado por BARREIRO DIAZ, J. M^a., en MILLÁN CALENTI, R. A. (Coord.), *La Ley 30/1992 comentada por Letrados de la Xunta de Galicia*, Asociación profesional de Letrados de la Xunta de Galicia, Santiago de Compostela, 2006, págs. 246 a 265 y FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales...*, cit., pág. 465-470.

⁴⁹ Vid. VALERO TORRIJOS, J. y LÓPEZ PELLICER, J.A. , «Algunas consideraciones...», cit., pág. 267.

hemos de traer a colación el artículo 43.1 CE, que tal y como señalábamos anteriormente, exige que los poderes públicos lleven a cabo actuaciones conducentes a proporcionar el mayor bienestar posible en lo que a la Salud de las personas respecta.

Respecto a la finalidad la LOPD incurre, y así lo ha constatado a su vez la doctrina⁵⁰, en un incumplimiento del Derecho Comunitario⁵¹, generado como consecuencia de una deficiente transposición de la Directiva 95/46/CE. La LOPD establece en el artículo 4.2 la prohibición de todos aquellos usos que resulten *incompatibles* con la finalidad prevista, de tal forma que está permitiendo aquellos que sean *distintos* pero *compatibles* con la misma, mientras que la directiva prohíbe todo uso *distinto*, sea compatible o no. El mantenimiento de tal disposición supone que el titular del fichero puede emplear los datos que se contienen en el mismo para cualquier finalidad, siempre que, ésta, se muestre compatible con el uso para el cual fue creado, llegándose a situaciones en las cuales se emplean datos para finalidades totalmente distintas de aquellas para las cuales se recogieron pero compatibles con éstas⁵². De *lege ferenda* sería necesario, sobre todo en un ámbito tan peligroso como es la información sanitaria, establecer que los usos que se pueden efectuar con los mismos, única y exclusivamente son aquellos para los que

⁵⁰ Vid. GUICHOT, E., *Datos personales...* cit., págs. 231 a 234; HERRÁN ORTÍZ, A., *El derecho a la intimidad...*cit., págs. 212 a 215; SERRANO PÉREZ, M. M., *El derecho fundamental...*, cit., págs. 439 a 442; GARCÍA AMEZ, J., «La protección de los datos...», cit., págs. 37- 38.; GARRIAGA DOMÍNGUEZ, A., *Tratamiento de Datos Personales y Derechos Fundamentales*, Dykinson, Madrid, 2004, págs. 78 a 80.

⁵¹ Sobre el derecho a ser resarcido por los daños ocasionados por este incumplimiento del Derecho Comunitario, NICOLÁS LUCAS A., «La incidencia en la práctica española del principio de responsabilidad patrimonial por incumplimiento del derecho comunitario», *Revista de Administración Pública*, núm. 168, 2005, págs. 351- 380.

⁵² Vid. FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales...*, cit., pág. 231, ofrece una justificación de la causa última por la que se ha optado por esta redacción «debe tenerse en cuenta que la finalidad primordial de este inciso del artículo 4.2 LOPDP fue, precisamente, el de no introducir excesivo rigor en la destinación de los datos personales en consonancia con el dictado literal de la DPD, con lo que de la *voluntas legislatoris* se deriva un decisivo ánimo a favor de una interpretación estricta de la incompatibilidad que, aunque inicialmente pensada en relación con actividades empresariales, no parece existir obstáculo alguno, antes bien, para extender la actuación administrativa.»

se recabaron, tal y como establece en este punto el artículo 5.4 LIB, si bien, el ámbito de aplicación de la misma se ve limitado al sector de las investigaciones biomédicas y no el asistencial en general.

No obstante, de la jurisprudencia de nuestro Tribunal Constitucional, se puede llegar a la conclusión de que, los datos, única y exclusivamente se van a poder emplear para aquella finalidad para la cual fueron recabados, según se puede extraer de la lectura de las sentencias del Tribunal Constitucional 94/1998, de 4 de mayo⁵³, 202/1999, de 8 de noviembre⁵⁴, y 11/1998, de 13 de enero⁵⁵, algo que también ha sido señalado por parte de la doctrina, la cual señala que necesariamente deberá existir una correlación entre la obtención de los datos y aquella finalidad para la cual fueron recabados^{56 57}.

⁵³ Ar. 94. Ponente, Sr. González Campos.

⁵⁴ Ar. 202. Ponente, Sr. Cachón Villar.

⁵⁵ Ar.11. Ponente, Sr. Ruiz Vadillo. Esta sentencia señala en su fundamento jurídico 5º:

“y aquí se utilizó un dato sensible, que habría sido proporcionado con una determinada finalidad, para otra radicalmente distinta, con menoscabo del legítimo derecho de libertad sindical”

⁵⁶ Vid. REBOLLO DELGADO, L., *Derechos fundamentales y protección de datos*. Dykinson, Madrid 2004, pág. 146.

⁵⁷ La Audiencia Nacional se ha opuesto a esta interpretación que venimos sosteniendo. En la sentencia de 11 de febrero de 2004 (Ar. 441, Ponente, Sr. Teso Gamella.) pretende salvar la inconstitucionalidad del artículo 4.2 LOPD. El tribunal se basa en para ello en una interpretación sistemática del mismo, y así en su fundamento 4º viene a decir que:

“[...] En relación con la interpretación de la expresión «finalidades incompatibles» que establece el artículo 4.2 de la Ley Orgánica 15/1999, esta Sala no puede compartir el criterio que postula la recurrente, pues aunque el artículo 4.2 de la Ley 15/99, en contraposición con el artículo 4.2 de la Ley 5/92, ya no se refiere a «finalidades distintas», sino a «finalidades incompatibles», revelando una ampliación de la posibilidad de utilización de los datos, sin embargo la interpretación sistemática del precepto y la ambigüedad del término «finalidades incompatibles» avalan la interpretación realizada en el acto administrativo impugnado. En efecto, según el diccionario de la Real Academia «incompatibilidad» significa «repugnancia que tiene una cosa para unirse con otra, o de dos o más personas entre sí», por tanto, una interpretación literal ampararía el uso de los datos para cualquier fin abriendo una gama indefinida e ilimitada de finalidades, pues es muy difícil imaginar usos que produzcan la repugnancia que evoca la incompatibilidad, por lo que « hemos declarado en Sentencia de 8 de febrero de 2002. Teniendo en cuenta, además, que semejante interpretación conduce al absurdo y como tal ha de rechazarse», como dicho término se introduce en el Ley de 1999, como ha declarado la doctrina, por una traducción poco precisa del artículo 6 de la Directiva 46/1995, de 24 de octubre [...]”

B) Los datos han de Pertinentes.

Que los datos sean pertinentes significa que éstos deberán estar relacionados con el fin para el que se recogieron, no debiendo exceder de la finalidad perseguida, de modo que se va a crear una relación entre ésta y la información recabada. Relación que conlleva la prohibición de recabar más datos que aquellos que sean estrictamente necesarios para dicha actuación, a pesar de que lo puedan ser para actuaciones futuras. Es decir, se trata de una obligación que, salvo mediación de consentimiento del interesado, o habilitación legal, no permite incluir dentro de un fichero datos que no sean necesarios para atender la finalidad para la cual ha sido autorizado⁵⁸. Este artículo 4.1 LOPD se desglosa en tres requisitos: adecuación, pertinencia en sentido estricto y datos no excesivos⁵⁹.

La adecuación, se trata de aquella obligación que tiene el responsable del fichero de asegurar al interesado de que los datos se ajustan a las estrictas necesidades que quiere satisfacer, la cuales, han de estar íntimamente ligadas a la finalidad del tratamiento. Por su parte, pertinencia, en sentido estricto, es nuevamente una obligación para el responsable, y que va a manifestarse en el compromiso que éste adquiere de que los datos se van a someter a los usos y al objeto para el cual se recogieron, y que sean necesarios para alcanzar los fines que se han propuesto⁶⁰. Respecto a la exigencia de no ser excesivos, consiste en no poder recoger más datos que aquellos que sirvan para cumplir los fines para los cuales fueron recabados⁶¹.

En definitiva, supone que la persona no podrá exigir al interesado que revele información sobre su salud que no sirva para cumplir con el fin para el cual está recabando sus datos, que en este caso sería el prestar una asistencia sanitaria al interesado.

C) Los datos han de ser veraces y exactos

Son requisitos establecidos en los puntos 3º y 4º de este artículo 4, que se materializan en que los datos recogidos en un fichero, deben ser veraces y exactos.

⁵⁸ Vid. APARICIO SALOM, J., *Estudios...*, cit., pág. 109.

⁵⁹ Vid. SANTOS GARCÍA, D., *Nociones...*, cit., pág. 53.

⁶⁰ *Ibidem*, pág. 53.

⁶¹ *Ibidem*, pág. 54.

La veracidad de los datos es definida por ESPINAR VICENTE como la perfecta correspondencia entre el discurso que marcan los hechos y aquel que es transmitido al receptor de la información, y supone que, el responsable del fichero, deberá asegurarse de que aquellos datos que se encuentran recogidos en su fichero se adecuan a la realidad, y en caso de que no sea así se exige, *ex lege*, la cancelación de oficio de aquellos datos que resulten inexactos o incompletos, o proceder a su sustitución o rectificación⁶².

La sentencia del Tribunal Constitucional 105/1990, de 6 de junio⁶³, afirma que la veracidad, implica que el informador ha de tener un especial deber de comprobar la veracidad de los hechos que expone mediante las oportunas averiguaciones, empleando para ello la diligencia exigible a un profesional. La sala de lo Contencioso-Administrativo de la Audiencia Nacional, en sentencia de 19 de abril de 2002⁶⁴, ha venido a señalar que este principio se traduce en la necesidad de exigir una especial diligencia a las entidades gestoras de los datos, las cuales deberán mantenerlos al día y de conformidad con el principio de calidad de los datos.

ALVAREZ- CIENFUEGOS añade que, este deber, exige una identidad con la situación real de la persona, de manera que se deberá respetar la exactitud y actualización de los datos, de tal forma que se refleje la situación actual del afectado⁶⁵.

Las consecuencias del incumplimiento de tales deberes son la entrada en juego del artículo 16 LOPD, o lo que es lo mismo, los derechos de rectificación y de cancelación.

D) Los datos han de ser leales

Es un requisito aplicable a la recogida. Consiste en la exigencia de que, en el momento en el cual se pretende recabar datos del interesado, la persona que quiere hacerlo debe realizarlo sin que medie engaño alguno o falsedades por su parte, de mane-

ra que la propia LOPD en su artículo 4.7 prohíbe que se utilicen para la recolección de datos medios fraudulentos, desleales o ilícitos.

4.2. Principio de Transparencia.

Este principio -también denominado como de publicidad⁶⁶- aparece recogido en el artículo 5 LOPD. El interesado deberá ser informado, con carácter previo y por parte de la persona que solicita los mismos, de modo expreso, preciso e inequívoco, de una serie de cuestiones: la existencia del fichero o tratamiento de datos, finalidad de la recogida y los destinatarios de la información, el carácter optativo y obligatorio de las preguntas, las consecuencias de la obtención de los datos, de la negativa a suministrarlos y la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.

Puede suceder que la persona pretenda obtener los datos por medio de Internet, impresos o cuestionarios, aquí la obligación de informar no cesa, según se puede observar en el artículo 5.2 LOPD. Tampoco en aquellos casos en los cuales la información no ha sido recabada del interesado, puesto que, de acuerdo con el artículo 5.4 LOPD, se le ha de informar de manera expresa e inequívoca de las cuestiones anteriores por parte del responsable

⁶⁶ La importancia de este principio ha sido destacada por HERRÁN ORTIZ. A., *El derecho a la intimidad...*, cit., pág. 215, la cual señala que es uno de los pilares fundamentales en la protección de datos, ya que el interesado no alcanzaría a conocer de qué tiene que protegerse, o qué derechos debe ejercitar en tanto no conozca la realidad de sus datos personales y el tratamiento al que están sometidos. Por su parte, VILLAVERDE MENÉNDEZ, I., «Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993», *Revista Española de Derecho Constitucional*, núm. 41, Mayo- Agosto, 1994, págs. 207, 210, 217 y 223, señala la estrecha relación que guarda el derecho a estar informado sobre las cuestiones que actualmente se recogen en el artículo 5.2 LOPD con el derecho a la intimidad, pues el derecho a la intimidad se configura como un derecho de defensa que no se reduce únicamente a impedir que terceros accedan a un ámbito considerado como íntimo, sino que también faculta para que la persona que ha cedido una determinada información impida que, quien la tiene, la haga pública, de tal modo que para poder ejercitar sus derechos debe estar informado en todo momento sobre los datos que posee una persona determinada, de modo que si no lo está, se vulneraría el derecho a la intimidad del artículo 18.º CE. Sobre esta Sentencia del Tribunal Constitucional, consúltese a su vez, FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales...*, cit., págs. 69- 83.

⁶² Vid. ESPINAR VICENTE, J. M., «La primacía del derecho a la información sobre la intimidad y el honor», GARCÍA SAN MIGUEL, L., *Estudios sobre el derecho a la intimidad*. Tecnos, Madrid, 1992, pág. 65.

⁶³ Ar. 105. Ponente, Sr. López Guerra.

⁶⁴ Ar. 143504. Ponente, Sr. Buisán García.

⁶⁵ Vid. ALVAREZ-CIENFUEGOS SUAREZ, J. M., *La defensa de la intimidad de los Ciudadanos y la Tecnología Informática*, Aranzadi, Elcano, 1999, pág. 31.

del fichero en un plazo de tres meses, que se contará desde el momento en el cual se procede a registrar los datos, si bien se exceptúan los casos en los cuales se ha informado al interesado con anterioridad de tal operación de tratamiento de datos.

Excepciones al deber de información se recogen en el punto 5 de este artículo 5. En primer lugar, cuando los datos proceden de fuentes accesibles al público y se destinan a la actividad de publicidad comercial. En este caso se impone la obligación de informar, en cada comunicación que se dirija al interesado, del origen de los datos, identidad del responsable del tratamiento y los derechos que le asisten. Respecto a este tipo de datos, LEGUINA VILLA los define como libres o no sensibles, encontrándose recogidos en documentos abiertos o accesibles de modo permanente a la disponibilidad de cualquier persona sin necesidad de acreditar derecho o interés jurídico que justifique el acceso a dicha información⁶⁷. La catalogación en los artículos 7 y 8 LOPD de los datos sanitarios como especialmente protegidos pretende impedir que estén en estas fuentes accesibles al público. No obstante, la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud, en su artículo 53 establece una serie de información referente a la salud accesible al público en general⁶⁸.

⁶⁷ Vid. LEGUINA VILLA, J., «Libertad informática y datos accesibles al público», *Justicia Administrativa*, núm. 4, Julio, 1999, pág. 7.

⁶⁸ En este artículo se regula lo que se conoce como “Sistema de Información Sanitaria”, el cual estará a disposición de sus usuarios, que serán las Administraciones públicas sanitarias, los gestores y profesionales de la sanidad y los ciudadanos, en los términos de acceso y difusión que se acuerden en el Consejo Interterritorial del Sistema Nacional de Salud. En lo que a su contenido respecta, contendrá información sobre las prestaciones y la cartera de servicios en atención sanitaria pública y privada, e incorporará, como datos básicos, los relativos a población protegida, recursos humanos y materiales, actividad desarrollada, farmacia y productos sanitarios, financiación y resultados obtenidos, así como las expectativas y opinión de los ciudadanos, todo ello desde un enfoque de atención integral a la salud, marcándose para ello una serie de objetivos, de tal modo que para las Autoridades sanitarias, la información favorecerá el desarrollo de políticas y la toma de decisiones, dándoles información actualizada y comparativa de la situación y evolución del Sistema Nacional de Salud; en el caso de los profesionales sanitarios, la información irá dirigida a mejorar sus conocimientos y aptitudes clínicas. Incluirá directorios, resultados de estudios, evaluaciones de medicamentos, productos sanitarios y tecnologías, análisis de buenas prácticas, guías clínicas, recomendaciones y recogida

La segunda excepción versa sobre la información referente al carácter optativo u obligatorio de las preguntas, las consecuencias de la obtención de los datos y de la negativa a suministrarlos y la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición, lo cual no será necesaria siempre que de su contenido se deduzca claramente de la naturaleza de los datos personales que se solicitan o las circunstancias en que se recaban.

4.3. Principio de Consentimiento.

El artículo 6 LOPD establece el principio de consentimiento, que junto con la calidad de los datos constituyen los principales soportes de la normativa de protección de datos. Este artículo señala que:

“El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa”

A renglón seguido, y de manera específica para el campo sanitario, el artículo 7.3 LOPD impone la obligación, salvo que una norma con rango de ley diga lo contrario, de obtener el consentimiento para realizar cualquier operación con datos, reforzando la importancia del consentimiento para la LOPD, y configurándose como el principio fundamental que preside la normativa sobre protección de este tipo de datos, tal y como se desprende también de la lectura de la legislación española de

de sugerencias; respecto a los ciudadanos, contendrá información sobre sus derechos y deberes y los riesgos para la salud, facilitará la toma de decisiones sobre su estilo de vida, prácticas de autocuidado y utilización de los servicios sanitarios y ofrecerá la posibilidad de formular sugerencias de los aspectos mencionados; por último, para las organizaciones y asociaciones en el ámbito sanitario, contendrá información sobre las asociaciones de pacientes y familiares, de organizaciones no gubernamentales que actúen en el ámbito sanitario y de sociedades científicas, con la finalidad de promover la participación de la sociedad civil en el Sistema Nacional de Salud. Sobre el sistema de información sanitaria, vid. PALOMAR OLMEDA, A., «Servicio de información y tarjeta sanitaria en el marco de la nueva regulación de las relaciones interadministrativas en materia de sanidad», PAREJO ALFONSO, L., VAQUER CABALLERÍA, M., y PALOMAR OLEDA, A. (Coords.), *La reforma del Sistema Nacional de Salud: cohesión, calidad y estatutos profesionales*, Marcial Pons, Madrid, 2004, págs. 167 a 214.

protección de datos⁶⁹, concretamente los artículos 5, 6, 7, 11, 16 y 44 LOPD y 2, 4, 7, 8, 16 LDO. Es pues que, como señala HERRÁN ORTÍZ, el derecho a consentir el tratamiento de los datos estructura y organiza la autodeterminación informativa, o lo que es igual, la facultad de los interesados de establecer y decidir sobre el tratamiento de la información que les concierne⁷⁰.

La LOPD define en su artículo 3.h) el consentimiento:

“[...]toda manifestación de voluntad, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le conciernen.”

De la lectura de este precepto, podemos extraer la conclusión que, para poder hablar de la existencia de consentimiento, el mismo ha de presentar una serie de notas: inequívoco, específico y lo más fundamental de todo, informado⁷¹ y revocable⁷².

Respecto a la forma en la cual se ha de emitir, nada dice al respecto la LOPD, con la excepción de aquellos datos que revelen ideología, afiliación sindical, religión y creencias. En tales casos, tal y como ordena el artículo 7.2 LOPD, se ha de realizar por escrito. Salvo para estos supuestos, entre los cuales no se encuentran los datos sanitarios, el

consentimiento se podrá realizar bien verbalmente bien por escrito, si bien, esta afirmación ha de ser matizada. En varias ocasiones, para obtener tal tipo de datos se hace necesaria la realización de una serie de pruebas tendentes a obtener información sobre la salud de una persona, actuaciones que conllevan intervenciones quirúrgicas, procedimientos diagnósticos y terapéuticos invasores, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente – por ejemplo biopsias, amniocentesis, etcétera-. En tales supuestos, según el artículo 8.2 LDO, el consentimiento ha de ser por escrito⁷³.

Siguiendo con las notas del consentimiento, no se exige que éste sea personal. La LDO, en su artículo 5.1, facilita que pueda ser emitido por parte de otras personas, en la medida en que permite hacerlo a personas vinculadas al paciente, bien por razones de parentesco o por razones de hecho –es decir amigos, compañero sentimental, pareja de hecho, etcétera-, siempre que el paciente lo hubiese autorizado de manera expresa o tácita.

Existe un supuesto en el artículo 5.3 LDO en el que se permite prescindir del consentimiento, cuando el paciente, según el criterio del médico que le asiste, carezca de capacidad para entender la información a causa de su estado físico o psíquico, la información se pondrá en conocimiento de las personas vinculadas a él por razones familiares o de hecho. Es decir, cuando carezca de la capacidad necesaria para entender el acto que está realizando, quedando en tal caso a la discreción del médico que asiste al paciente que se declare o no incapaz para prestar el consentimiento esta persona. En tal caso, el tratamiento o recogida de los datos debe autorizarse por parte de los familiares del paciente o de una persona que esté vinculada al enfermo por

⁶⁹ Crítico con la regulación del consentimiento para este tipo de datos se muestra FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales...*, cit., págs. 287-291.

⁷⁰ Vid. HERRÁN ORTÍZ, A., *El derecho a la intimidad...*, cit. pág. 220. Por su parte, RIPOL CARULLA, S., «La protección...», cit., pág. 127. justifica la exigencia del consentimiento en la estrecha relación de confianza existente entre el médico y el paciente.

⁷¹ Este último requisito enlaza con el principio que anteriormente analizábamos de Transparencia o publicidad en el tratamiento, así se considera que un consentimiento es informado cuando el interesado ha recibido toda la información que se recoge en el artículo 5.1 LOPD y que anteriormente comentábamos.

⁷² Vid. RIPOL CARULLA, S., «La protección de los datos médicos y genéticos en la normativa del Consejo de Europa (Parte II)», *Revista de Derecho y Genoma Humano/ Law and the Human Genome Review*, núm. 6, Enero - Junio, 1997, pág., 117., señala que la propia exigencia de un consentimiento libre, viene a incluir de manera implícita, la posibilidad de que una vez otorgado, el sujeto titular de los datos pueda retirar su consentimiento o modifique las condiciones para las cuales lo prestó. En idéntico sentido, CONDE ORTIZ, C., *La protección de datos personales: Un derecho autónomo con base en los conceptos de intimidad y privacidad*, Dykinson – Universidad de Cádiz, Madrid, 2005, pág. 96, quien añade que no se hace necesario el aducir una “justa causa” para ello.

⁷³ Artículo que recoge un derecho de vital importancia en el ámbito sanitario, el consentimiento informado, y que supone la obligación para el facultativo de proporcionar al usuario una serie de información sobre el acto que pretende realizar, al objeto de que éste pueda emitir con el mayor conocimiento posible su consentimiento hacia el mismo. Según el artículo 10 LDO de modo comprensible se debe de proporcionar la siguiente información: las consecuencias relevantes o de importancia que la intervención origina con seguridad, los riesgos relacionados con las circunstancias personales o profesionales del paciente; los riesgos probables en condiciones normales, conforme a la experiencia y al estado de la ciencia o directamente relacionados con el tipo de intervención; y las contraindicaciones que se pueden dar.

razones de hecho, si bien, el incapaz, fuera cual fuese la causa de su incapacidad, no pierde el derecho a la información asistencial, a pesar de que quién está autorizando sea el representante legal, tal y como se dice en el artículo 5.2 LDO⁷⁴.

Esta regla general del consentimiento presenta una serie de excepciones recogidas en el artículo 6.2 LOPD, que en su interior alberga una serie de supuestos en los cuales se prescinde del consentimiento del afectado para el tratamiento de los datos, si bien, no impide, siempre que una ley no disponga lo contrario, que el interesado se oponga al tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal caso, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

El primer supuesto es aquel en el que los datos se recogen para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias⁷⁵. En estos casos, justificados en la persona que aparece como titular del fichero y no en la finalidad del mismo, el único límite que establece la LOPD es que el tratamiento sirva, exclusivamente para el ejercicio de las funciones propias de las Administraciones, y que han de estar incluidas dentro de su marco competencial⁷⁶. El supuesto más claro en el campo de los datos sanitarios es el relativo a los ficheros de enfermos de VIH, y en los cuales son incluidos todas aquellas personas a las que se les diagnostica tal enfermedad, con independencia de que consientan o no tal acto; su regulación, en lo que a nivel estatal se

refiere, viene dado por el Real Decreto 2210/1995, de 28 de diciembre, por el cual se crea la Red de Vigilancia Epidemiológica⁷⁷. Otro supuesto viene establecido en la Ley Orgánica 3/1986, de 29 de abril, de Medidas especiales en materia de Salud Pública, concretamente sus artículos 2 y 3⁷⁸.

El siguiente supuesto del artículo 6.2 LOPD es cuando el tratamiento tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, LOPD. Es decir, cuando éste se muestre como necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También se prevé que puedan ser objeto de tratamiento cuando el mismo sea necesario para salvaguardar el interés vital del afectado o de otra

⁷⁴ Así el artículo 33 de esta norma establece que:

“La fuente de información de casos serán los médicos tanto del sector público como privado, que diagnostiquen al enfermo, quienes, *de forma inmediata al diagnóstico y obligatoriamente*, lo notificarán al Registro de SIDA de la Comunidad Autónoma, en el cuestionario unitario y homogéneo que a tal efecto suministrará dicho Registro.” (La cursiva es nuestra)

A nivel autonómico se han creado una serie de registros, si bien el más polémico ha sido el establecido por el Principado de Asturias, mediante Resolución de 7 de enero de 1999, de la Consejería de Servicios Sociales, cuya legalidad ha sido reafirmada por el Tribunal Superior de Justicia de la Comunidad Autónoma del Principado de Asturias, en sentencia de 15 de septiembre de 2005 (Ar. RJCA 2007/330, Ponente, Sr. Buján Álvarez). Sobre el derecho a la intimidad en este tema, *Vid. SOLA RECHE, E., «Algunos problemas relativos al derecho a la intimidad del paciente VIH+», Derecho y Salud*, volúm. 3, núm. 1, enero- junio, 1995, págs. 77 a 88. Sobre la Red de Vigilancia Epidemiológica, CIERCO SEIRA, C., *Administración Pública y salud colectiva*, Comares, Granada, 2006, págs. 58-74.

⁷⁵ Estos artículos señalan que:

“Artículo 2. Las autoridades sanitarias competentes podrán adoptar medidas de reconocimiento, tratamiento, hospitalización o control cuando se aprecien indicios racionales que permitan suponer la existencia de peligro para la salud de la población debido a la situación sanitaria concreta de una persona o grupo de personas o por las condiciones sanitarias en que se desarrolle una actividad.

Artículo 3. Con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible.”

⁷⁴ *Vid. GARCÍA AMEZ, J., «La protección de los datos...», cit., págs. 53- 55.*

⁷⁵ Señala FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales...*, cit., pág. 279, que esta excepción no es aplicable a todos los supuestos en los cuales está presente una Administración Pública, ya que no será de aplicación en los casos en que la misma obtenga los datos de fuentes que son accesibles al público o si son fruto de una cesión por parte de otra Administración o de cualquier otro sujeto, público o privado.

⁷⁶ SALOM APARICIO, J., *Estudios...*, cit., págs. 82- 83, vierte una dura crítica a este precepto, pues si la regla básica de protección es el consentimiento, las excepciones al mismo deberán justificarse en aras al interés público, mereciendo un juicio de valoración caso por caso, no siendo muy correcto establecer una excepción genérica. También apunta una mala adecuación al contenido de la directiva 95/46/CE, concretamente a su artículo 7.3, en el sentido de que éste establece la excepción basándose en criterios objetivos. Es decir, en atención al fin perseguido y no subjetivos, como hace la legislación española.

persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento

La tercera excepción se aplica cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado⁷⁹.

Otros casos, ya específicos del campo sanitario, se contemplan en el artículo 9 LDO. En primer lugar, si existe un claro riesgo para la salud pública a causa de razones sanitarias, siempre que éstas aparezcan preestablecidas por medio de una Ley. En estos casos, y cuando el consentimiento no se hubiere recabado porque nos encontramos ante los supuestos que se prevén en la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en materia de Salud Pública⁸⁰, se deberá comunicar a la autoridad la adopción de tal medida en un plazo máximo de 24 horas si además se procede al internamiento obligatorio de personas⁸¹.

Segundo y último de los supuestos de este artículo 9 LDO, son aquellas situaciones en las que existe un riesgo inmediato grave para la integridad física o psíquica del enfermo, y no es posible conseguir su autorización. En todo caso, los datos se cederán consultando, cuando las circunstancias así lo permitan, a los familiares del paciente o a las personas que estuviesen vinculadas de hecho a él.

Más excepciones las encontramos en el artículo 11 LOPD, que contempla el caso en el cual se

⁷⁹ Sobre este tema ya hemos hablado páginas atrás, por lo que me remito a lo señalado en el punto 2, a la hora de hablar del principio de calidad.

⁸⁰ Es decir cuando se aprecien indicios racionales que permitan suponer la existencia de peligro para la salud de la población debido a la situación sanitaria concreta de una persona o grupo de personas o por las condiciones sanitarias en que se desarrolle una actividad.

⁸¹ Hay que señalar que lo previsto en este artículo viene a encajar perfectamente en el supuesto contemplado en el artículo 8 del Convenio de Oviedo, el cual viene a permitir la cesión de datos sanitarios sin consentimiento en aquellos casos en los cuales nos encontremos ante una situación de urgencia y no se pueda obtener el consentimiento adecuado, en cuyo caso se puede proceder inmediatamente a la realización de cualquier intervención que sea indispensable desde el punto de vista médico a favor de la salud de la persona afectada.

produce una cesión de datos autorizada por una ley o cuando su tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros -en cuyo caso la comunicación sólo se va a considerar como legítima, en tanto y cuanto se limite a la finalidad que la justifique-, o cuando la cesión sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Para concluir con el análisis del consentimiento se debe hacer referencia a la figura de las “instrucciones previas”, reguladas en el artículo 11 LDO, y que las define como:

“[...]documento por el cual, una persona mayor de edad, capaz y libre, manifiesta anticipadamente su voluntad, con objeto de que ésta se cumpla en el momento en que en que llegue a situaciones en cuyas circunstancias no sea capaz de expresarlos personalmente, sobre los cuidados y el tratamiento de su salud o, una vez llegado el fallecimiento, sobre el destino de su cuerpo o de los órganos del mismo[...].”

Este documento posibilita que una persona pueda emitir su consentimiento para que, sus datos, sean tratados en un futuro⁸². Para su validez, la LDO señala, en el artículo 11.3, que no se aplicarán aquellas que sean contrarias al ordenamiento jurídico, a la *lex artis*, ni las que no se correspondan con el supuesto de hecho que el interesado haya previsto en el momento de manifestarlas, quedando constancia razonada en la historia clínica del paciente, de todas aquellas anotaciones relacionadas con las previsiones que señalábamos anteriormente. Por otra parte, los puntos 2º y 5º del artículo 11 LDO, establecen la obligación de que, cada servicio de salud, regule el procedimiento que estime como adecuado para que, llegado el caso, se garantice el cumplimiento de las instrucciones previas de cada persona, que siempre han de costar por escrito, a la vez que, con el fin de asegurar la eficacia en todo el territorio nacional de las instrucciones previas manifestadas por los pacientes y

⁸²⁸² Sobre las instrucciones previas, *vid.* GALLEGO RIES-TRA, S., *El Derecho del Paciente a la Autonomía Personal, y las Instrucciones Previas: Una nueva Realidad Legal*, Thomson Reuters – Aranzadi, Cizur-Menor, 2009.

formalizadas de acuerdo con lo dispuesto en la legislación de las respectivas Comunidades Autónomas, se procede a crear en el seno del Ministerio de Sanidad y Consumo lo que se denomina como Registro Nacional de instrucciones previas, cuya regulación viene recogida en el Real Decreto 124/2007, de 2 de febrero, por el que se regula el Registro nacional de instrucciones previas y el correspondiente fichero automatizado de datos de carácter personal⁸³.

4.4. Principio de Seguridad.

El último de los principios recogidos en el título II LOPD es el principio de seguridad. Pensado para inspirar el almacenamiento y posterior custodia de los datos sanitarios, su formulación aparece en el artículo 9.2 LOPD en los siguientes términos:

“1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y evite su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.”

La importancia que la LOPD ha querido otorgar a la seguridad de los ficheros es tal, que GUICHOT apunta que la efectividad de los principios de la misma correrían el riesgo de desvanecerse si no se adoptasen medidas que garanticen que sólo el responsable del fichero, sus usuarios acreditados o el encargado del tratamiento, son quienes tienen acceso a los datos registrados⁸⁴. Con este objetivo, y dando un cumplimiento de la llamada reglamentaria que hacía la nor-

mativa de Protección Datos, se aprueba el RPD. Esta norma establece los requisitos de seguridad que deben cumplir todos los ficheros, sean públicos o privados, y que se materializan en lo que ella denomina *medidas de seguridad*, y que pueden ser definidas como procedimientos, reglas y estándares de carácter técnico y organizativo que tienen por objetivo garantizar la seguridad de los datos que aparecen registrados en un fichero.

El RPD establece lo que califica como niveles de seguridad, y que irán en función de la información tratada y la mayor o menor necesidad de garantizar la confidencialidad e integridad de la misma, diferenciando entre nivel básico, medio y alto. Según el artículo 81.3 RPD, los ficheros que contengan datos sanitarios han de contar con un nivel de protección alto, caracterizado por el hecho de que, junto con las medidas propias correspondientes a su nivel, incorpora además las relativas al nivel básico y medio⁸⁵.

Elemento fundamental de las medidas de seguridad es el documento de seguridad, de obligada tenencia según el artículo 81 RPD, y que contempla todas aquellas medidas que adopta el responsable del fichero en aras a cumplir con el RPD. Documento, que de conformidad con el artículo 81.3 RPD, deberá contener, como mínimo, los siguientes aspectos: ámbito de aplicación del documento con especificación detallada de los recursos protegidos, medidas,

⁸⁵ Las medidas que exige el RPD son las siguientes:

- a) Nivel básico: incluye la elaboración e implantación de la normativa de seguridad mediante un documento que deberá contener como mínimo las indicaciones del artículo 8 RDMS, la definición clara y documentada de las funciones que desempeñará y obligaciones que asumirá cada persona que tenga acceso a los datos y sistemas de información. Mantener una relación actualizada de usuarios con acceso autorizado y establecer sistemas de identificación y autenticación, la creación de un registro de incidencias, y la verificación por el responsable del fichero de la definición y correcta aplicación de los procedimientos de copias de seguridad.
- b) Nivel medio: se añaden a las anteriores algunos requisitos adicionales, como por ejemplo, más menciones en el documento de seguridad. Destaca la obligación de realizar una auditoria, interna o externa, que verifique el cumplimiento de las medidas, al menos cada 2 años, el cual quedará a disposición de la Agencia de Protección de Datos.
- c) Nivel alto: se añaden a los anteriores algunos requisitos en materia de distribución de soportes, registro de accesos, realización de copias de seguridad y transmisión a través de redes telemáticas.

⁸³ Sobre el mismo, *vid.* GALLEGO RIESTRA, S., *El Derecho del Paciente a la Autonomía Personal...*, *cit.*, págs. 197- 201.

⁸⁴ *Vid.* GUICHOT, E., *Datos personales...*, *cit.*, pág. 438.

normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el RPD, funciones y obligaciones del personal, estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan, procedimiento de notificación, gestión y respuesta ante las incidencias, los procedimientos de realización de copias de respaldo y de recuperación de los datos y la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

5. LOS DERECHOS DEL INTERESADO.

Hasta ahora hemos analizado los principios generales que rigen en nuestro ordenamiento jurídico la protección de los datos sanitarios, auténtica garantía del interesado frente a posibles vulneraciones del derecho a la intimidad o a la protección de datos, según la tesis a la que el lector se adhiera. Esta función, además de cumplirse con las obligaciones que hemos venido apuntando en páginas anteriores, se completa con el establecimiento de una serie de derechos que se derivan de los principios que anteriormente analizados, y que se otorgan frente a posibles abusos que se puedan cometer mediante el tratamiento de datos.

5.1. Derecho de Rectificación y de Cancelación de Datos.

El principio de calidad obliga a que los datos sean veraces y exactos. Para el caso de que no se cumplan los requisitos señalados en los puntos 4º y 5º del artículo 4 LOPD, se otorgan al interesado los derechos a la rectificación y cancelación de datos.

El primero, va a permitir al interesado solicitar, de aquella persona que es la responsable del fichero en el cual se encuentran almacenados los datos personales, que proceda a modificar su contenido, bien porque son inexactos o bien porque no son ciertos.

Por su parte, el derecho de cancelación persigue que los datos almacenados en el fichero, sean eliminados.

Aunque persiguen finalidades diferentes, ambos derechos están presididos por un mismo prin-

cipio, la veracidad, exactitud y actualidad de los datos. Además, según el artículo 16 LOPD, su ejercicio es igual, y aparece regulado en la Instrucción 1/1998, a pesar de que en el punto 2 de su norma primera los configure como derechos independientes aunque conectados entre sí.

A) Derecho de rectificación.

Enlaza directamente con la obligación que tiene el responsable del fichero de mantenerlo de tal manera, que refleje en condiciones exactas y actualizadas la salud de una persona, tal y como establece el artículo 4.3 LOPD⁸⁶.

Puede ser definido como aquella facultad que tiene el interesado de que, una vez que se ha constatado que un dato es incorrecto o inexacto, el responsable proceda a adecuarlo a la realidad⁸⁷, lo cual supone una diferencia con el derecho de cancelación, en el sentido de que, la persona que ejercita la rectificación, no persigue la destrucción de los datos, sino que sigan recogidos en un determinado fichero, aunque no en las mismas condiciones que estaban.

Según SERRANO PÉREZ comporta a su vez una serie de acciones, pues permite no sólo la rectificación de los datos, sino también que éstos sean aclarados, completados, o, simplemente, que se pongan al día para el caso de que las informaciones fueran inexactas completas, equívocas o atrasadas, algo que puede hacerse bien a instancia del interesado bien de oficio –en virtud del deber de actualización que señalábamos anteriormente⁸⁸.

En cuanto a la carga de la prueba de la falta del incumplimiento de este deber, recae en la persona que ejercita el derecho de rectificación, tal y como se deduce de la lectura de la norma tercera, en su punto 3, de la Instrucción 1/1998, que exige al interesado aportar la prueba documental de que

⁸⁶ Sobre el contenido de esta obligación puede consultarse SALOM APARICIO, J., *Estudios...*, cit., págs. 112 a 118 y artículo 31.1 RPD

⁸⁷ Se debe de recordar que la propia LOPD tipifica como una sanción grave, en su artículo 44.3 LOPD, la tenencia de datos inexactos, la cual está sancionada en el artículo 45.2 con una multa que va desde los 60.101,21 euros a los 300.506,05 euros, con la posibilidad, para el caso de que sea una Administración Pública quién cometa la infracción, de adoptarse las medidas establecidas en el artículo 46 LOPD.

⁸⁸ Vid. SERRANO PÉREZ, M. M., *El derecho fundamental...*, cit., págs. 359 y 360.

justifique la necesidad de una rectificación de los datos.

B) Derecho de cancelación.

La cancelación tiene como objetivo la eliminación de los datos del fichero en el cual se encuentran registrados⁸⁹. Si el anterior derecho lo enlazábamos con la obligación de actualización de la información, la cancelación viene vinculada con el principio del consentimiento, pues la persona, al ejercitar este derecho, ha decidido que sus datos no deben encontrarse registrados en un fichero, de modo que no se cuenta con el consentimiento del interesado, que recordemos es revocable en cualquier momento.

La finalidad perseguida consiste en evitar que los datos que se encuentran almacenados en un fichero, se perpetúen, convirtiéndose con ello en etiquetas definitivas para el individuo, con el peligro que esto supone para la identidad de los derechos de la persona⁹⁰.

La consecuencia es la supresión de los datos, o lo que es igual, su destrucción física. No obstante, la LOPD consciente de que una supresión inmediata de los datos supondría la pérdida de los elementos de prueba para posteriores demandas o procedimientos en los cuales se hace necesario acceder a estos datos, prevé una serie de excepciones en su artículo 18⁹¹.

La primera se da en los casos, en los que siendo precedente la cancelación de los datos, no es posible su extinción física, bien por razones técnicas bien por causa del procedimiento o soporte utilizado. Si se da este supuesto, el responsable del fichero procederá al bloqueo de los datos con el fin de impedir su ulterior proceso o utilización.

El segundo supuesto es si se demuestra que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.

Fuera de la LOPD nos encontramos que la Instrucción 1/1998, en el punto 5 de su norma tercera, establece otra excepción, no procederá el ejercicio

en aquellos casos, en los cuales se pudiese causar un perjuicio a intereses legítimos del afectado o de terceros, o cuando exista una obligación legal de conservar datos. Con relación a esta última precisión debe señalarse que el artículo 17 LDO establece la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial⁹².

C) Procedimiento de ejercicio de tales derechos.

El artículo 32 del RPD y la Instrucción 1/1998 desarrollan de manera mas extensa el procedimiento, que conforme al artículo 17.2 LOPD es gratui-

⁸⁹ Véase el artículo 31.2 RPD.
⁹⁰ SERRANO PÉREZ, M. M., *El derecho fundamental...*, cit., pág. 359, nota 597, pone un ejemplo claro de este riesgo, que sería el lastre que supondría para una persona arrastrar durante toda su vida datos reveladores de determinados tratamientos psíquicos.
⁹¹ Vid. GUICHOT, E., *Datos personales...*, cit., pág. 398.
⁹² Nótese que en este caso se emplea la expresión *como mínimo*, lo cual indica la posibilidad de que este periodo sea ampliado por parte de las Comunidades Autónomas en el ejercicio de sus competencias. No obstante, no todas han aprobado una Ley de Derechos del Paciente –véase el caso por ejemplo, la Comunidad Autónoma del Principado de Asturias–, mientras que otras mantienen el mismo plazo. Tal es el caso de la Comunidad Autónoma de Navarra (artículo 13.1, de la Ley Foral 11/2002, de 6 mayo, de derechos del paciente a las voluntades anticipadas, a la información y a la documentación clínica), Valencia (Ley 1/2003, de 28 de enero, de la Generalitat, de Derechos e Información al Paciente de la Comunidad Valenciana, la cual no regula el plazo de conservación de la historia, por lo que es de aplicación el establecido en la LDO), Galicia (artículo 20.3 de la Ley 3/2001, de 28 de mayo, reguladora del consentimiento informado y de la historia clínica de los pacientes), Castilla y León (el artículo 39 de la Ley 8/2003, de 8 de abril, de las Cortes de Castilla y León, sobre derechos y deberes de las personas en relación con la salud, establece una remisión a la LDO). Por su parte Extremadura, prevé un plazo de quince años (artículo 34.1 de la Ley 3/2001, de 28 de mayo, reguladora del consentimiento informado y de la historia clínica de los pacientes) Cataluña establece veinte años, contados desde la muerte del paciente (artículo 12 Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y a la documentación clínica). El resto de leyes no contemplan disposiciones específicas con respecto a la conservación de la historia clínica, luego habrá que entender como plazo el marcado en la LDO, si bien en este punto debe destacarse el Decreto 178/2005, de 26 julio, de la Consejera de Sanidad de la Comunidad Autónoma de Canarias, Aprueba el Reglamento que regula la historia clínica en los centros y establecimientos hospitalarios y establece el contenido, conservación y expurgo de sus documentos, que aunque establece que el plazo de conservación de la historia clínica es el marcado en la legislación estatal, regula con todo detalle el uso de la misma y los documentos que se han de destruir.

to, previéndose que, cuando el acceso a los ficheros revelare que los datos son inexactos o incompletos, inadecuados o excesivos, el interesado, podrá solicitar, del responsable del fichero, la rectificación, o en su caso cancelación de los mismos. Ahora bien, si se trata de datos que reflejen hechos constatados en un procedimiento administrativo, aquéllos, se considerarán exactos siempre que coincidan con éste.

Una vez solicitada la rectificación o cancelación de datos el responsable del tratamiento tendrá que hacer efectivo el derecho ejercitado por parte del interesado. Si los mismos hubiesen sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado. En el caso de que se mantenga el tratamiento por este último, también se deberá de proceder a la cancelación.

De acuerdo con lo dispuesto en el punto tercero de la norma tercera de la Instrucción 1/1998, la solicitud de rectificación deberá indicar el dato que es erróneo y la corrección que debe realizarse, debiendo ir acompañada de la documentación justificativa de la rectificación solicitada, salvo que la misma dependa exclusivamente del consentimiento del interesado.

El plazo para hacer efectiva la reclamación es de diez días, contados desde el momento de recepción de la solicitud; en el caso de que hubiere habido una cesión de datos, de conformidad con el punto segundo de la norma tercera de la Instrucción 1/1998, se deberá comunicar el ejercicio de tales derecho a las personas a quienes se ha cedido anteriormente los datos, según obliga el artículo 32.2 RDP.

Puede suceder que el responsable del fichero considere que no procede acceder a lo solicitado por el afectado, en tal caso se lo comunicará motivadamente, dentro del plazo de diez días que anteriormente señalábamos, a fin de que, por parte de éste, se pueda hacer uso de la reclamación prevista en el artículo 18.2 LOPD⁹³. Una vez transcurrido

⁹³ Artículo que establece la posibilidad de que, el interesado, al cual se le deniegue total o parcialmente el ejercicio de los derechos de acceso, rectificación o cancelación, pueda ponerlo en conocimiento de la APD, o en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos por la Agencia u organismo

el plazo previsto, y ante la ausencia de respuesta, la solicitud de rectificación o cancelación podrá entenderse desestimada a los efectos de la interposición de la reclamación que corresponda.

5.2. Derecho de Acceso y de Información.

Se recoge en el artículo 15.1 LOPD, desarrollado por la Instrucción 1/1998, en los siguientes términos:

“El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer con los mismos”

El acceso a los datos y la información sobre los mismos está estrechamente relacionado con el principio de transparencia o publicidad del tratamiento, configurándose de esta manera como el instrumento que permite al interesado hacer que el responsable del fichero cumpla con los postulados del mismo.

La LDO recoge también este derecho a la hora de hablar de la historia clínica en su artículo 18.1, cuando permite el acceso del paciente, en los límites que luego expondremos, a la documentación obrante en la historia clínica, e, incluso, obtener copia de todos aquellos que figuren en la misma, lo que enlaza a su vez con el artículo 10.2 del Convenio de Oviedo, que contempla el derecho de toda persona a conocer toda la información que se haya obtenido respecto a su salud⁹⁴.

En cuanto a la forma de ejercitarlo, puede ser por parte del interesado o de otra persona. En el artículo 9.3 LDO se detallan los supuestos en los cuales el consentimiento se ha obtenido por representación⁹⁵, mientras que el artículo 10.1 LDO

autonómico competente, será de seis meses. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

⁹⁴ No obstante, para el caso de datos sanitarios en poder de las Administraciones Públicas, también se debe de hacer referencia inexcusable al artículo 35 h) y 37.2 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en adelante LPC), en los cuales se establece el derecho del ciudadano al acceso de toda la documentación que sobre ella tengan las distintas Administraciones Públicas.

⁹⁵ Estos supuestos son los siguientes: cuando el paciente no sea capaz de tomar decisiones, a criterio del médico res-

detalla la información que se le ha de suministrar al paciente. Esta información, según se establece en el artículo 5.2 LDO, deberá ser suministrada de manera que la persona pueda entenderla de acuerdo con sus facultades, un deber que no cesa a pesar de que la persona hubiese sido declarada incapaz⁹⁶.

Este derecho de acceso y de información es de gran interés para el campo sanitario. Mediante el acceso al historial clínico la persona va a poder conocer mejor su estado de salud, para que, de este modo, pueda formar mejor su opinión sobre el consentimiento hacia un determinado acto médico, tal y como acertadamente indica EMALDI CIRRIÓN⁹⁷.

Al igual que sucede con cualquier derecho que se aprecie, los artículos 18.3 y 5.4 LDO señalan una serie de límites a su ejercicio. No se va a poder ejercitar en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente⁹⁸, ni en perjuicio del derecho de los profesio-

sionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas. Además, la LDO indica que, los centros sanitarios y los facultativos de ejercicio individual, sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso, el acceso de un tercero a la historia clínica motivado por un riesgo para su salud, se limitará a los datos pertinentes. Tampoco se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros.

El artículo 4.1 LDO establece la vertiente negativa de este derecho a la información, el derecho a no saber, también reconocido en el artículo 10.2 del Convenio de Oviedo, y que implica la decisión, que toma la persona, de que determinada información sobre su salud no se le facilite, algo que a tenor de lo dispuesto en la LDO debe ser respetado por los centros sanitarios⁹⁹.

Hasta ahora hemos estado analizando la facultad que tiene el interesado de acceder a todos aquellos datos respecto a su salud que obran en poder de una persona, pero en el campo sanitario se da una especialidad que difícilmente se dará en el ámbito de los personales. Cada persona cede sus datos para una determinada finalidad, aunque puede suceder que cuando esos datos están siendo tratados la persona que realiza el tratamiento se descubre información que el interesado no conoce o ignora su existencia. Es decir, lo que se conoce como hallazgos inesperados, algo frecuente en el campo sanitario. En tales supuestos, el facultativo deberá comunicárselo al interesado, pues el derecho de información en el campo sanitario supone una obligación de suministrar toda aquella información que se tiene sobre el interesado, el cual

pensable de la asistencia, o su estado físico o psíquico no le permita hacerse cargo de su situación. Si el paciente carece de representante legal, el consentimiento lo prestarán las personas vinculadas a él por razones familiares o de hecho; cuando el paciente esté incapacitado legalmente; cuando el paciente menor de edad no sea capaz intelectual ni emocionalmente de comprender el alcance de la intervención. En este caso, el consentimiento lo dará el representante legal del menor después de haber escuchado su opinión si tiene doce años cumplidos. Cuando se trate de menores no incapaces ni incapacitados, pero emancipados o con dieciséis años cumplidos, no cabe prestar el consentimiento por representación. Sin embargo, en caso de actuación de grave riesgo, según el criterio del facultativo, los padres serán informados y su opinión será tenida en cuenta para la toma de la decisión correspondiente.

⁹⁶ La información que se debe de suministrar al paciente, es la que se indica en el artículo 10 LDO.

⁹⁷ Vid. EMALDI CIRRIÓN, A., «Derechos de los sujetos sobre sus datos genéticos», AAVV., *IV Congreso Mundial de Bioética*, MARCELO PALACIOS (Ed.), Gijón, 2005, pág. 370, y *El consejo genético y sus implicaciones jurídicas*, Cátedra inter universitaria fundación BBVA- Diputación Foral de Vizcaya de Derecho y Genoma Humano, Comares, Bilbao-Granada 2001, págs. 265 a 269. A su vez, ALDAMA VAQUEDANO, C., «La protección de la intimidad y del derecho a la información», ROMEO CASABONA, C. (Ed.), *El convenio...*, cit., págs. 143, señala que el derecho de toda persona a obtener información sobre su salud, se configura como un presupuesto para poder ejercitar las cualidades que componen la esfera íntima del ser humano, sobre todo aquellas que afectan al conocimiento necesario para adoptar una postura vital, decidiendo en el ámbito terapéutico libre y voluntariamente.

⁹⁸ Así el artículo 5.4 LDO entiende por tal:

“[...]La facultad del médico para actuar profesionalmente sin informar antes al paciente, cuando por razones objetivas el conocimiento de su propia situación pueda perjudicar su salud de manera grave [...]”

De todos modos, en tales supuestos, el médico está obligado a dejar constancia razonada de las circunstancias que le han llegado a adoptar tal medida, en la historia clínica, debiendo comunicárselo a las personas vinculadas al paciente por razones familiares o de hecho.

⁹⁹ Sobre el contenido de este derecho, vid. EMALDI CIRRIÓN, A., *El consejo...*, cit., págs.274 a 276.

cede una serie de datos específicos cuyo contenido conoce, y por tanto, si se encuentran nuevas informaciones, ha de comunicárselo, al objeto de que el interesado tenga constancia de su existencia y decida si los cede o no para un tratamiento, pues si no se le notifica, y el responsable tiene en su poder tal información y la trata o almacena, estaría realizando sin el consentimiento del interesado, y se estaría contraviniendo con ello el principio del consentimiento que anteriormente señalábamos, que exige que éste sea específico y sobre una serie de datos¹⁰⁰. En este punto, el artículo 44.4.d) LOPD tipifica como infracción muy grave la tenencia o tratamiento sin consentimiento de este tipo de datos, y que según el artículo 45.3 LOPD, serán sancionadas con multa de 300.506,05 a 601.012,10 euros, con la posibilidad añadida de imponer las medidas establecidas en el artículo 46 cuando el sujeto responsable sea una Administración Pública, lógicamente la infracción no se impondrá cuando la tenencia o tratamiento de estos datos esté amparada por alguno de los supuestos, que anteriormente veíamos, y en los que no es necesario contar con el consentimiento del interesado.

De todos modos, de conformidad con el principio 8.4 la Recomendación (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa, sobre Protección de Datos Médicos, se impone la obligación a los centros médicos de informar a la persona que ha sido sometida a un análisis médico de todos aquellos hallazgos inesperados en los mismos, siempre y cuando se den una serie de condiciones: que la Ley nacional no prohíba el suministrar dicha información, la persona ha solicitado que se le notifique tales hallazgos y que el suministro de la información no cause un daño serio a la salud de la persona, a su familia sanguínea o uterina, a algún miembro de su familia social, o a alguna persona que presente un vínculo directo con su línea genético¹⁰¹.

El artículo 4.5 párrafo primero LIB ha establecido esta necesidad de comunicación de tales

¹⁰⁰ Igualmente establece este mismo derecho los artículos 4.5, párrafo segundo y 49 LIB.

¹⁰¹ También se muestra partidario de la opinión aquí sustentada, DE SOLA, C., «Privacidad y datos genéticos. Situaciones de conflicto (I)», *Revista de Derecho y Genoma Humano/Law and the Human Genome Review*, núm. 1, Julio-Diciembre 1994, pág. 184,

hallazgos, aunque no ya como una obligación del personal investigador, sino como un derecho cuya titularidad corresponde a la persona que ha cedido su información o muestras biológicas para la investigación.

5.3. Derecho de Oposición.

Este derecho no se reconoce de manera explícita en el título III LOPD, aunque no es algo que conlleve su inexistencia, pues la existencia del mismo se deduce en los artículos 6.4, 28, 30 y 31 LOPD¹⁰². No obstante, en este punto, el artículo 34 RPD ha recogido expresamente este derecho.

Se puede definir como aquella facultad, que tiene el interesado, consistente en oponerse a un determinado tratamiento de sus datos en aquellos supuestos en los cuales la normativa permite recogerlos sin su consentimiento. Para la AEPD, es necesario que se den dos condiciones, que una Ley no lo prohíba, y que exista un motivo fundado y legítimo para oponerse al tratamiento¹⁰³.

El propósito que persigue este derecho es, según ha señalado GARRIAGA DOMÍNGUEZ, compensar al interesado cuando no es necesario solicitar su consentimiento para tratar sus datos, de modo que es un instrumento garante de carácter netamente preventivo y cautelador del derecho a la intimidad del interesado¹⁰⁴.

Este derecho, no va poder ser ejercitado, cuando la justificación que ofrezca el interesado consiste en que los datos son erróneos o inexactos, dado que en tal caso lo que deberá de hacer es ejercitar el derecho de rectificación de datos.

El procedimiento, se regula en el artículo 35 RPD, y se ejercitará mediante solicitud dirigida al responsable del tratamiento, que resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se

¹⁰² Vid. GUICHOT, E., *Datos personales...*, cit., pág. 396. Por otra parte, el origen de este derecho se encuentra en el artículo 14 de la Directiva 95/46/CE, que expresamente reconoce este derecho.

¹⁰³ Vid. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Memoria del año 2000*, Madrid, 2001, pág. 139.

¹⁰⁴ Vid. GARRIAGA DOMÍNGUEZ, A., *Tratamiento de...*, cit., pág. 109. A su vez, GUICHOT, E., *Datos personales...*, cit., pág. 397. señala también que con este derecho se pretende preservar la identidad y la integridad del propio afectado.

responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 LOPD.

5.4. Derecho de Acceso al Registro General de Protección de Datos.

Se contiene en el artículo 14 LOPD. Faculta no sólo al interesado, sino a cualquier persona en general, a que pueda consultar a la AEPD los ficheros que están legalmente inscritos en el registro de esta entidad, aunque debe entenderse que también habilita para realizar tal actuación frente a los registros de las Agencias Autonómicas de Protección de Datos.

5.5. Derecho a la impugnación de valoraciones basadas exclusivamente en tratamientos automatizados.

Los artículos 13.1 LOPD y 36 RPD otorgan el derecho a todo ciudadano de no verse sometido a una decisión con efectos jurídicos que les afecte de manera directa, y que hubiese sido adoptada basándose únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. Así, puede impugnar los actos administrativos, o las decisiones privadas, que se adopten conforme a dichas valoraciones, teniendo en cuente, como apunta FERNÁNDEZ SALMERÓN, que este derecho únicamente es aplicable a los casos en los cuales existe un tratamiento automatizado de información¹⁰⁵. Para ello, la LOPD reconoce el derecho de la persona, que se ha visto afectada por dicha valoración, de poder obtener información del responsable del fichero respecto a los criterios de valoración y el programa que ha sido utilizado el tratamiento de datos en el cual se basó la decisión o el acto administrativo objeto de impugnación.

Para poder ejercitar este derecho es necesario que se de un único requisito, es necesario que la decisión o acto administrativo objeto de impugnación se base única y exclusivamente en el tratamiento de datos, de modo que si en la misma se apuntan otros fundamentos que no sean dicho tratamiento no se podrá ejercitar este derecho¹⁰⁶. Por

¹⁰⁵ Cfr. FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales...*, cit., pág. 383..

¹⁰⁶ Vid. GUICHOT, E., *Datos personales...*, cit., pág. 396. Por su parte SANTOS GARCÍA, D., *Nociones...*, cit., págs. 94-

su parte, el artículo 36.2 RPD contempla dos excepciones a este derecho: a) Si la decisión se ha adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato, y, b) la decisión está autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

5.6. Derecho a la Indemnización por daños. Especial atención a la responsabilidad patrimonial de la administración

El artículo 19 LOPD establece el derecho a recibir una indemnización para el caso de que se produzca un daño o lesión en sus bienes y derechos como consecuencia de un incumplimiento de lo dispuesto en la misma

Al abordar esta cuestión, lo primero que se ha de señalar es la coexistencia en este ámbito de dos regímenes diferentes de responsabilidad, que variarán en función del sujeto que cometa el daño: si se trata de daños cometidos por una Administración Pública o si se trata de un sujeto privado.

Cuando el daño es derivado de la actuación de un sujeto privado, éste se someterá al régimen establecido en la LOPD, y con ello a un régimen de responsabilidad objetiva¹⁰⁷. Brevemente, puede señalarse que, para poder dar lugar a indemnización, es necesario que exista un daño, daño que ha de traer su causa en un incumplimiento de alguna

95, exige que se den dos requisitos: que la decisión adoptada produzca efectos jurídicos -que sucederá cuando afecte a derechos fundamentales y libertades públicas de los interesados-, y afecte a los interesados de manera significativa. Opinión que no comparto, en el sentido que para ejercitar este derecho basta con que la decisión o acto administrativo se base única y exclusivamente en una valoración de datos personales, con independencia del grado en el que le afecte.

¹⁰⁷ Abordar la cuestión de la responsabilidad civil en esta materia excedería los límites de este trabajo, por todo ello, si se quiere profundizar en la cuestión, véase la obra de GRIMALT SERVERA, P., *La responsabilidad civil en el tratamiento automatizado de los datos*, Comares, Granada, 1999.

obligación impuesta por la LOPD, y que dicho incumplimiento pueda ser imputable al responsable de tratamiento de algún dato del interesado.

Si el daño es ocasionado por una Administración Pública, debe acudirse a la regulación específica de la responsabilidad patrimonial de las Administraciones Públicas, que viene de la mano de la LPC y el Real Decreto 429/1993, de 26 de marzo, por el cual se aprueban los procedimientos en materia de responsabilidad de las Administraciones Públicas.

Esta institución de la responsabilidad, configurada, tal y como acertadamente señala GARCÍA DE ENTERRÍA¹⁰⁸, como uno de los principales pilares sobre los cuales se asienta nuestro actual sistema de Derecho Administrativo, y que a su vez es una auténtica garantía del ciudadano, es acogida, aunque no era necesario hacerlo, en el artículo 19.2 LOPD. No han faltado autores, que como FERNÁNDEZ SALMERÓN, han criticado este artículo, pues la LOPD condiciona el nacimiento de este derecho a ser resarcido a la previa existencia de un incumpliendo de cualquiera de las obligaciones que la misma establece¹⁰⁹, de tal modo que en principio parece excluir aquellos daños que se deriven de actuaciones de las Administraciones Públicas que se ajusten a lo señalado en la misma. No obstante, esta contradicción es más aparente que real, ya que, el apartado segundo de este artículo, se remite en bloque a lo que disponga la legislación general sobre responsabilidad patrimonial de las Administraciones Públicas, la LPC, y que supone una remisión no sólo a los aspectos procedimentales, sino además a todo el régimen sustantivo, lo que incluye a su vez los supuestos que generan este derecho a obtener una indemnización¹¹⁰.

Así pues, la LOPD nos lleva a los artículos 139 a 144 LPC, de cuyo análisis se puede extraer que, con carácter general, el sistema articulado en esta norma, tal y como apunta LEGUINA VILLA¹¹¹, es

¹⁰⁸ Vid. GARCÍA DE ENTERRÍA, E. y FERNÁNDEZ- RODRÍGUEZ, T. R., *Curso de Derecho Administrativo II*, 9ª edición, Thomson- Civitas, Madrid, 2004, págs. 381 y 382.

¹⁰⁹ Cfr. FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales...*, cit., pág. 446.

¹¹⁰ Cfr. FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales...*, cit., págs. 446 y 447.

¹¹¹ Vid. LEGUINA VILLA, J., «La responsabilidad patrimonial de la Administración, de sus autoridades y del personal a

unitario¹¹², de un alcance general, y que se configura a su vez como una responsabilidad directa¹¹³, en la medida en que aquella persona que sufre el perjuicio puede reclamar directamente a la Administración su resarcimiento¹¹⁵. Por último, y como nota fundamental, presenta el carácter de objetiva, al operar al margen de toda idea de culpa¹¹⁶.

Sobre los requisitos que han de darse para poder declarar la responsabilidad patrimonial de la Administración, en primer lugar ha de existir una lesión resarcible. La responsabilidad se pone en

su servicio», LEGUINA VILLA, J. y MORÓN SÁNCHEZ, M. (Dirs.), *La nueva ley de régimen jurídico de las Administraciones Públicas y del Procedimiento Común*. Tecnos, Madrid, 1993, págs. 395 y 396.

¹¹² Ya que se aplica a todas las Administraciones Públicas, sin que ninguna de ellas sea excluida, derivándose no tanto de la LPC, sino de los artículos 106.2 y 149.1.18º CE.

¹¹³ Sin perjuicio de la posibilidad de que exista por medio un contrato de seguro de responsabilidad civil de la Administración. Sobre los problemas que en tal caso se suscitan, véase HUERGO LORA, A., *El seguro de responsabilidad civil de las Administraciones Públicas*, Marcial Pons, Madrid, 2002.

¹¹⁴ Vid. GARCÍA DE ENTERRÍA, E. y FERNÁNDEZ- RODRÍGUEZ, T. R., *Curso de Derecho Administrativo II*, 10ª edición, Thomson- Civitas, Madrid, 2006, pág. 379.

¹¹⁵ A juicio del destacado autor, la cláusula «el funcionamiento de los servicios públicos», comprende cualquier tipo de actuaciones extracontractuales de la Administración.

¹¹⁶ Sobre la objetividad existía un claro consenso doctrinal desde que el profesor GARCÍA DE ENTERRÍA, publicara, en 1956, el clásico libro *Los principios de la nueva ley de expropiación forzosa*, Instituto de Estudios Políticos, Madrid, 1956 (Existe una reedición del año 2006 por parte de la editorial Thomson- Civitas). No obstante, como consecuencia de la publicación del artículo de PANTALEÓN PRIETO, «Los anteojos del civilista: hacia una revisión del régimen de responsabilidad patrimonial de las Administraciones Públicas», *Documentación Administrativa*, núms. 237- 238, enero- junio, 1994, págs 238 a 252, se ha empezado a debatir sobre la conveniencia o no de realizar una reforma legal al respecto, MIR PUIGPELAT, O., *La responsabilidad patrimonial de la Administración. Hacia un nuevo sistema*, Civitas, Madrid, 2002 se muestra como uno de los mayores defensores de la tesis sustentada por PANTALEÓN PRIETO. En la jurisprudencia es ilustrativa la sentencia del Tribunal Supremo de 6 de noviembre de 1998 (Ar. 9020. Ponente, Sr. González Rivas), cuando afirmar que:

“no sólo no es menester demostrar para exigir aquella responsabilidad de los titulares o gestores de la actividad administrativa que ha generado un daño han actuado con dolo o culpa, sino que ni siquiera es necesario probar que el servicio público se ha desarrollado de manera anómala, pues los preceptos constitucionales y legales que componen el régimen jurídico aplicable extienden la obligación de indemnizar a los casos de funcionamiento normal de los servicios públicos” (La cursiva es nuestra)

marcha en el momento en el cual existe una lesión que sea resarcible. Es decir, aquel daño que sufre una persona en sus bienes y derechos, que presenta una nota característica, ser antijurídico, o lo que es igual, que la persona no tenga el deber jurídico de soportar, tal y como se dice en el artículo 141 LPC. Pero no es suficiente que exista un daño antijurídico, éste, según el artículo 139.2 LPC, ha de ser efectivo, evaluable económicamente, e individualizado con relación a una persona o grupo de personas. Además, es preciso que nos encontremos ante el funcionamiento de un servicio público que sea imputable a una Administración pública, y se pruebe la existencia de una relación de causalidad entre el hecho que se imputa a la Administración y el daño.

En cuanto a las causas de exclusión de la responsabilidad, la Administración no responde en los casos en los cuales existe un supuesto de fuerza mayor. Tampoco en el caso contemplado dentro del artículo 141.1 LPC, el cual establece que la Administración no va a responder de todos aquellos daños que no se hubiesen podido prever o evitar según el estado de los conocimientos de la ciencia o de la técnica existentes en el momento de producción de aquellos. Es decir, los llamados riesgos del desarrollo, y que fueron introducidos por medio de la reforma llevada a cabo por medio de la Ley 4/1999, de 13 de enero, que en este punto reformó el artículo 141.1 LPC al objeto de poner solución al conflicto que había suscitado las continuas demandas de responsabilidad patrimonial por contagio del VIH. No obstante, a pesar de tratarse de un supuesto de dudosa constitucionalidad, y en el cual la Administración no responde, se prevé la posibilidad de establecer medidas asistenciales o económicas para hacer frente a los daños que el particular ha sufrido, y que se concretarán, entre otras medidas, con la constitución de fondos de compensación.

Puede suceder que existan supuestos en los cuales concurren en la producción del daño varias Administraciones Públicas. La responsabilidad concurrente de las mismas se recoge en el artículo 140 LPC, según el cual, cuando de la gestión dimanante de fórmulas conjuntas de actuación entre varias Administraciones públicas se derive responsabilidad en los términos previstos en la LPC, las Administraciones intervinientes responderán de forma solidaria. En tales casos, el instrumento jurídico que regula la actuación conjunta podrá

determinar la distribución de la responsabilidad entre las diferentes Administraciones públicas. En otros supuestos de concurrencia de varias Administraciones en la producción del daño, la responsabilidad se fijará para cada Administración atendiendo a los criterios de competencia, interés público tutelado e intensidad de la intervención. Cuando no sea posible dicha determinación, la responsabilidad será solidaria¹¹⁷.

Finalmente, es independiente que la Administración Pública actúe sometida al derecho privado. En estos casos, según dispone el artículo 144 LPC¹¹⁸, responderán directamente de los daños y perjuicios causados por el personal que se encuentra a su servicio, considerándose la actuación del mismo como actos propios de la Administración bajo cuyo servicio se encuentre. La responsabilidad se exigirá de conformidad con lo previsto en los artículos 139 y siguientes de la LPC.

En los casos en los que la Administración ha sido declarada responsable, está obligada a ejercitar la acción de regreso frente al autoridad y demás personal a su servicio que ha causado el daño, tal y como impone el artículo 145.3 LPC, si bien, sólo posibilita el ejercicio de dicha acción, de manera errónea, a los supuestos en los cuales existe dolo, o culpa o negligencia graves por parte de la autoridad y demás personal al servicio de la Administración que ha sido condenada.

En cuanto al plazo del que dispone el interesado para hacer efectivo este derecho a ser indemnizado, es de un año, que empezará a contar desde el momento en el cual se ha producido el acto o el hecho que ha motivado la indemnización, o desde que se ha manifestado su efecto lesivo, no obstan-

¹¹⁷ Sobre la responsabilidad concurrente de las Administraciones Públicas véase MUÑOZ MACHADO, S., *La responsabilidad civil concurrente de las Administraciones Públicas*, 2ª edición, Civitas, Madrid, 1998, págs. 21- 229. Por otra parte, también puede suceder que el daño se provoque por un contratista de la Administración Pública o un concesionario de la misma, sobre este tipo de responsabilidad son de obligada referencia los trabajos de BOCANEGRA SIERRA, R., "Responsabilidad de contratistas y concesionarios de la Administración Pública por daños causados a terceros", *Revista Española de Derecho Administrativo*, núm. 18, 1978, págs. 397 a 406, "La responsabilidad civil de concesionarios y contratistas de la Administración por daños causados a terceros", *Documentación Administrativa*, núm. 237- 238, 1995 y "Concesionarios y contratistas", *Cuadernos de Derecho Judicial*, núm. 14, 1996, págs. 113- 122.

¹¹⁸ En la redacción dada por la Ley 4/1999, de 13 de enero.

te, si se pretende reclamar daños de carácter psíquico, el plazo empezará a contarse desde el momento en el cual se ha producido la curación o se ha determinado el concreto alcance de sus secuelas, tal y como se dice en el artículo 142.5 LPC.

6. PROTECCIÓN ORGÁNICA: LA AGENCIA ESTATAL DE PROTECCIÓN DE DATOS.

Los derechos que se recogen en la LOPD se verían desprotegidos si la LOPD no articulase órgano alguno que tuviera como fin principal velar por todo aquello que dispone sea cumplido en la práctica. Los artículos 35 y siguientes de la LOPD establecen la AEPD, objeto de desarrollo reglamentario por parte del Real Decreto 428/1993, de 26 de marzo, por el cual se aprueba el Estatuto de la Agencia de Protección de Datos. Así pues, España cuenta con la autoridad de control a la cual hace referencia el artículo 28 de la Directiva 95/46/CE, el cual obligaba a todos los Estados miembros a establecer una o más de estas autoridades que debía de actuar de manera independiente¹¹⁹. El artículo 35.1 LOPD recoge claramente esta nota de independencia de la AEPD, cuando dispone que la misma es un ente con personalidad jurídica propia y plena capacidad pública y privada que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones¹²⁰.

Las Comunidades Autónomas, que se encuentran avaladas en este punto por el artículo 41 LOPD y la sentencia del Tribunal Constitucional 290/2000¹²¹, anteriormente citada, pueden proceder a crear sus respectivas Agencias de protección de datos, cuya operatividad se ve limitada al territorio de la Comunidad Autónoma¹²².

¹¹⁹ En este punto el derecho español no sufrió la necesidad de crear tal órgano, puesto que la anterior normativa de protección de datos anterior a la LOPD, ya establecía tal autoridad de control.

¹²⁰ Vid. GUICHOT, E., *Datos personales...*, cit., pág. 453.

¹²¹ Sobre el reparto de competencias que se deriva de la citada sentencia, vid. TRONCOSO REIGADA, A., "La distribución competencial entre el Estado y las Comunidades Autónomas en protección de datos personales", *Nuevas Políticas Públicas*, núm. 1, 2005, págs. 116- 120.

¹²² Así se han creado en las Comunidades Autónomas de Madrid (Ley madrileña 8/2001, de 13 de julio de Protección de Datos de la Comunidad Autónoma de Madrid, y el Decreto madrileño 22/1998, de 12 de febrero, por el que se aprueba el

En cuanto a la composición de la AEPD, ésta consta de Director de la agencia española de protección de datos¹²³, un Consejo Consultivo, un registro general de protección de Datos, una Secretaría General y la subdirección General de Inspección de Datos.

Sus funciones varían según se trate de ciudadanos o de personas que manejen datos. Así, para los primeros, pasa por atender a sus peticiones y reclamaciones, proporcionar información de los derechos reconocidos en la LOPD y promover campañas de difusión a través de los medios del derecho a la protección de datos. Para los segundos, es la encargada de emitir autorizaciones previstas en la LOPD, requerir medidas de corrección, ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos, ejercer la potestad sancionadora, recabar ayuda e información que precise y autorizar las transferencias internacionales de datos.

7. CONCLUSIONES

Las nuevas tecnologías de la información han irrumpido en el campo sanitario, contribuyendo a que la asistencia sanitaria sea prestada con un mayor grado de eficacia, y por tanto que sus usuarios disfruten de un mayor grado de bienestar en lo que a su salud respecta. No obstante, éstos corren el riesgo de vulneración de su derecho a la intimidad. Frente a tales ataques el constituyente impuso la obligación para los poderes públicos de velar por este derecho frente a los avances de la informática. Siempre que se ha aprobado una norma reguladora de la Sanidad se ha reconocido el derecho a la intimidad, a pesar de quedarse en un mero reconocimiento del mismo, puesto que no detalla a fondo su protección. Esta tarea se deja a la LOPD y la LDO, que sí la cumplen.

Aunque la verdadera normativa rectora de la protección de datos sanitarios venga dada por estas

Estatuto de la Agencia de Protección de Datos de la Comunidad Autónoma de Madrid, Cataluña (Ley 5/2002, de 19 de abril, de creación de la Agencia Catalana de Protección de Datos, y el Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos), y el País Vasco (Ley del Parlamento Vasco 2/2004, de 25 de febrero).

¹²³ Nombrado por el Gobierno, a propuesta del Ministerio de Justicia, por un periodo de cuatro años.

dos leyes que hemos señalado, la existencia de otras que si bien no regulan su ejercicio, reconocen este derecho, puede provocar inseguridad jurídica en los profesionales sanitarios, y que supondrá generar el riesgo de violación por desconocimiento, siendo conveniente, cuando no necesaria, la aprobación de una normativa específica en materia de datos sanitarios, al igual que ya sucede con la información genética, actualmente regulada en la LIB.

La normativa comunitaria en este campo no ha sido transpuesta correctamente. En una cuestión tan crucial, como son los usos de los datos, el legislador español no ha incorporado la directiva 95/46/CE en los términos que ésta requiere, y está incumpliendo el derecho comunitario, aunque se debe elogiar la importante labor de la doctrina y la jurisprudencia en aras a corregir este defecto, así como el esfuerzo de la LIB en corregirlo para el sector de la investigación biomédica.

Respecto al contenido de la legislación se puede extraer la conclusión de que los datos, en virtud del principio de calidad, han de presentar una serie de características específicas, de modo que han de ser adecuados, pertinentes y no excesivos en relación con la finalidad para la cual se ha obtenido, que deberá ser determinada, explícita y legítima. A su vez, los datos obtenidos deberán ser veraces y exactos, otorgándose para el caso de no serlo, los derechos de rectificación y cancelación, que podrán ser ejercitados por parte del interesado, si bien, sus fines son diferentes, puesto que el primero persigue una sustitución o modificación de la información y el segundo su supresión.

Otro pilar fundamental en esta materia es la información que se tiene de proporcionar al interesado. Él mismo debe conocer una serie de cuestiones sobre sus datos que le van a permitir ejercer mejor sus derechos y poder emitir de mejor manera su consentimiento hacia el acto médico. También se ha de respetar su derecho a no saber, tal y como se desprende de la LDO y del Convenio de Oviedo.

Cuestión trascendental en este campo es el consentimiento del interesado. Junto con el principio de calidad de los datos, conforman los principales cimientos sobre los cuales se asienta toda la normativa. El consentimiento para ser válido deberá cumplir con una serie de características determinadas, pues ha de ser inequívoco, específico,

informado y revocable, si bien la LOPD y LDO establecen una serie de supuestos en los cuales no se exige el contar con el mismo.

En lo que al campo de los derechos del interesado respecta, éste cuenta con el derecho de rectificación y de cancelación de datos, acceso e información, oposición, acceso al registro general de protección de datos, a impugnar las valoraciones basadas exclusivamente en tratamientos automatizados, e indemnización por daños. Ambos derechos permiten defenderse frente a actuaciones que supongan una vulneración de toda la normativa analizada, aunque como todo derecho tiene una serie de límites que supone que su ejercicio no sea posible.

En España existe un marco normativo protector de la intimidad del usuario frente a las nuevas tecnologías de la información, si bien, no otorga un nivel adecuado de protección a este derecho fundamental recogido en el artículo 18.1 y completado con el 18.4 CE, por lo que sería conveniente realizar una revisión de la normativa en aras a salvaguardar de mejor manera el mismo, teniendo presente que también está en juego el derecho a la salud, que aunque goza de un nivel de protección menor que la intimidad debe de ser tenido en cuenta en este campo, sobre todo en un Estado al que se le exige una mayor intervención activa en la sanidad mediante el establecimiento de una serie de prestaciones sanitarias en aras a proporcionar un mayor bienestar a los usuarios de las mismas. De modo que la normativa debe intentar encontrar un punto de equilibrio entre estos el derecho a la asistencia sanitaria y a la intimidad de la persona, para lo que cumple una importante función en principio de proporcionalidad.