

La confidencialidad de la historia clínica

Antonio Troncoso Reigada
Profesor Titular de Derecho Constitucional

SUMARIO: I. LA HISTORIA CLÍNICA EN EL MARCO CONSTITUCIONAL: ENTRE EL DERECHO A LA VIDA Y A LA ASISTENCIA SANITARIA Y EL DERECHO A LA INTIMIDAD.— II. Principios y derechos de los ciudadanos en relación con la historia clínica. a) *La legislación reguladora de la historia clínica y de la protección de los datos de salud.* b) *El responsable de las historias clínicas. Diferencias principales entre los servicios sanitarios públicos y los servicios sanitarios privados.* c) *Finalidad y calidad de la historia clínica. La historia clínica como derecho del paciente. La centralización de las historias clínicas y su conservación.* d) *La información y el consentimiento para el tratamiento de datos de salud.* e) *La seguridad como garantía de la integridad y de la confidencialidad de la historia clínica. El deber de secreto.* f) *El derecho de acceso del paciente a la historia clínica y sus límites. La tutela de los derechos.*— III. EL ACCESO A LA HISTORIA CLÍNICA POR PERSONAS DISTINTAS AL INTERESADO. LA CESIÓN DE LA HISTORIA CLÍNICA. a) *El acceso a la historia clínica por parte de familiares y terceras personas.* b) *El acceso a la historia clínica por los profesionales sanitarios, por el personal de administración y gestión y por el personal de inspección.* c) *La cesión de la historia clínica para fines epidemiológicos, de salud pública y de investigación. La cesión de la historia clínica a la Administración sanitaria, a las compañías aseguradoras, a los órganos judiciales y a las Fuerzas y Cuerpos de Seguridad del Estado.*— IV. LA HISTORIA CLÍNICA DEL MENOR. a) *Derecho del menor a la intimidad y a la confidencialidad de sus datos sanitarios y el derecho de los padres a la información y al acceso a la historia clínica de sus hijos.* b) *Los casos difíciles: propuestas para la resolución del conflicto.*— V. LA CONFIDENCIALIDAD DE LAS HISTORIAS CLÍNICAS DENTRO DEL SISTEMA NACIONAL DE SALUD: LA LEY DE COHESIÓN Y CALIDAD DEL SISTEMA NACIONAL DE SALUD.— VI. LAS HISTORIAS CLÍNICAS NO INFORMATIZADAS.

I. LA HISTORIA CLÍNICA EN EL MARCO CONSTITUCIONAL: ENTRE EL DERECHO A LA VIDA Y A LA ASISTENCIA SANITARIA Y EL DERECHO A LA INTIMIDAD

Los datos de salud y la historia clínica tienen una enorme importancia porque son instrumentos necesarios para garantizar la asistencia sanitaria de las personas, y, por tanto, están íntimamente vinculados al derecho a la vida —art. 15 CE— y a la protección de la salud —art. 43 CE—¹. La acumulación de datos sani-

¹ Sobre esta cuestión me he referido anteriormente en A. TRONCOSO REIGADA, «La protección de los datos de salud y la historia clínica», *Actas del X Congreso Nacional de Derecho Sanitario*, Fundación Mapfre

tarios de los pacientes en las historias clínicas y su correcta conservación son elementos necesarios para poder llevar un seguimiento del estado de salud de las personas. De hecho, la supresión de datos relevantes de la historia clínica puede llegar a afectar gravemente a los tratamientos sanitarios, y, en última instancia, a la vida de las personas.

La gestión de la asistencia y de los servicios sanitarios en atención primaria, en atención especializada y en la urgencia exige necesariamente una acumulación masiva de información personal de los ciudadanos pues es a éstos a los que se les trata de garantizar su salud. Además de la asistencia sanitaria como derecho subjetivo, la salud pública es un bien jurídico colectivo. Existe un interés social que comprende los beneficios colectivos de la investigación médica y las políticas de prevención y de salud pública, actividades éstas que se materializan sobre información sanitaria de personas. La actividad sanitaria tiene como soporte recursos humanos y materiales limitados. Se hace imprescindible una actuación de planificación sanitaria que garantice la equidad en el acceso a las prestaciones. Los servicios sanitarios tratan de manera masiva información del personal destinado en el Sistema Nacional de Salud. También, más en general, la búsqueda de la calidad a través del control en el desempeño de la actividad sanitaria mediante protocolos, guías y pautas clínicas conlleva el manejo de datos personales. La mejora de la efectividad del trabajo exige en muchas ocasiones el tratamiento masivo de información de los pacientes y de los empleados. Así, la necesidad de buscar la eficiencia en el recurso a las prestaciones sanitarias exige adaptar y equilibrar los recursos para evitar dar a unos pacientes unos cuidados más costosos en detrimento de otros cuidados más básicos y necesarios².

Como ya hemos señalado en alguna otra ocasión, las tecnologías de la información y la comunicación son un instrumento muy positivo para la actividad sanitaria que redundan en la mejora de la calidad asistencial de los pacientes. Proyectos como la historia clínica electrónica y la tarjeta sanitaria, que requieren

Medicina, 2004 y en la «Presentación» a la *Guía de Protección de Datos en los Servicios Sanitarios Públicos*, Civitas, 2004, pp. 11-61. Cfr. también mi «Prólogo» al libro de J. SÁNCHEZ-CARO y F. ABELLÁN, *Datos de salud y datos genéticos. Su protección en la Unión Europea y en España*, Comares, Granada, 2004, pp. XV-XXX. También he tenido la oportunidad de abordar estas cuestiones en distintas conferencias organizadas en el marco del Congreso Anual de la Sociedad Española de Informática Sanitaria. Cfr. «La protección de los datos de salud», *Revista de la Sociedad Española de Informática Sanitaria*, núm. 48, 2004 y «La confidencialidad de la historia de salud», *Revista de la Sociedad Española de Informática Sanitaria*, núm. 58, 2006. El trabajo que ahora desarrollamos se circunscribe por razones de espacio a la historia clínica con finalidad asistencial. No abordamos en esta ocasión otras cuestiones interesantes como los ensayos clínicos, la investigación genética y biomédica, la farmacia o la receta electrónica. El tratamiento de datos de salud en el trabajo es especialmente importante —en la propia nómina, en la actividad de prevención de riesgos laborales, en la externalización de los servicios médicos de la empresa a través de mutuas, en la actividad de control del absentismo laboral—. Nos hemos ocupado de la cuestión en «Libertad sindical, libertad de empresa y autodeterminación informativa» en A. FARRIOLS, *La protección de datos de los trabajadores*, Fundación Largo Caballero, Madrid, 2006.

² Cfr. AA. VV., *Calidad en la asistencia sanitaria*, Instituto Europeo de Salud y Bienestar Social, Madrid, 1999, pp. 25-29 y 57-75; AA. VV., *La gestión del proceso asistencial: impacto de los sistemas de información médica*, MSC, Madrid, 2000, pp. 15-37; AA.VV., *Libro blanco para la mejora de los servicios públicos. Una nueva Administración al servicio de los ciudadanos*, MAP, Madrid, 2000, pp. 68-78; *Calidad.com. Ejemplos de prácticas de Calidad en la Comunidad de Madrid*, Madrid, 2000.

el establecimiento de repositorios de información sanitaria básica del ciudadano que permitan, por una parte, poner a disposición de cada ciudadano sus datos sanitarios, y, por otra, poner a disposición de los profesionales, con distintos niveles de acceso, información sanitaria sobre sus pacientes, contribuyen al progreso de la atención sanitaria de los ciudadanos. La historia clínica electrónica mejora la atención sanitaria a pacientes desplazados, al facilitar todos los datos sanitarios relevantes³. Lo mismo se puede decir de proyectos como el de facilitar información sanitaria personalizada a través de la red, que permite dar a grupos de enfermos –hemofílicos, enfermos de sida, celíacos, etc.– una información más concreta sobre su patología y sobre los avances científicos y farmacológicos; o la posibilidad de ofrecer servicios interactivos como la cita previa, la receta electrónica o los proyectos de telemedicina⁴. Además, los sistemas sanitarios públicos se encuentran con un aumento de las demandas de los ciudadanos, que requieren cada vez más prestaciones, lo que obliga a aumentar la eficiencia de los recursos a través del ahorro del gasto corriente. Las tecnologías de la información facilitan el almacenamiento de las pruebas diagnósticas, evitando su repetición y permiten reducir el tiempo que el personal facultativo dedica a la gestión –a la búsqueda de la información–, con la mejora consiguiente en el tiempo dedicado a la atención a los pacientes. El proyecto de receta electrónica, además de mejorar la atención farmacológica, está encaminado a la búsqueda de la eficiencia y al control del fraude. Igualmente, las tecnologías permiten el establecimiento de redes de investigación y de *benchmarking*, lo que mejora la gestión del conocimiento y el intercambio de experiencias entre los distintos servicios sanitarios.

³ La historia clínica electrónica es un proyecto complejo, debido fundamentalmente a que en el ámbito sanitario el *back office*, a pesar de encontrarse parcialmente informatizado con aplicativos en local, se encuentra muy desestructurado y hay una gran dificultad para establecer modelos de intercambios que sean válidos. En la Comunidad de Madrid hay que destacar el Proyecto AP-Madrid. Con este proyecto se establece una historia clínica centralizada –un centro de proceso de datos a nivel de Consejería– para toda la atención primaria. Progresivamente se pretende hacer lo mismo con la atención especializada– se comienza con los nuevos hospitales y se avanzará progresivamente con los más antiguos-. Entre atención primaria y especializada no habrá un modelo unificado sino una interoperabilidad ya que mucha información que hay en atención primaria no es necesaria para la atención especializada. El Servicio Vasco de Salud tiene desde hace varios años todo centralizado –tanto la atención primaria como la especializada–. En Galicia está centralizada la atención primaria. En Cataluña, dado que el modelo del *Servei Català de Salut* es un modelo público-privado –de sanidad privada concertada que forma parte de la red pública– no es posible centralizar la historia clínica en la Consejería. Por eso se pone en marcha un modelo de Historia Clínica Compartida. La Consejería centraliza únicamente unos índices y unos directorios de pacientes y cada centro sanitario comparte una información básica de cada paciente –no toda la historia clínica si no un resumen–. El profesional que atiende al paciente en cualquier centro se ve dirigido tecnológicamente a través de la Consejería con el centro donde está la información. El problema va a ser determinar qué información se va a compartir. Este modelo de Cataluña es muy interesante porque es el que mejor se puede extender al Sistema Nacional de Salud donde dada la descentralización de la gestión sanitaria en nuestro país no va a ser posible tener una historia clínica centralizada de ámbito nacional sino un proyecto de historia clínica compartida. Se debe establecer un centro de intercambio electrónico de información sanitaria, semejante a los centros de compensación de pagos bancarios. No se debe hablar de una historia clínica electrónica sino en una información sanitaria básica del ciudadano, más reducida, que se puede compartir –*infra* apdo. 5–.

⁴ Cfr. F. J. LÓPEZ CARMONA, «Salud en la red», en AA.VV., *Telemedicina, atención sanitaria y sus aspectos legales*, MSC-GGPJ, Madrid, 2002. Cfr. también del mismo autor «e-Salud, confidencialidad y seguridad de la información en el ámbito asistencial», *Revista datospersonales.org* núm. 10.

Por tanto, las tecnologías de la información se constituyen en un auténtico motor del cambio y del progreso en la calidad asistencial y en la equidad en el acceso a las prestaciones. Lo mismo se puede decir del impulso que las nuevas tecnologías han dado a la investigación genética que tiene que ser aprovechada para la mejora del derecho a la salud.

Sin embargo, al mismo tiempo que reconocemos que los servicios sanitarios trabajan con información personal —especialmente de pacientes— y que ésta sólo puede ser gestionada eficazmente con el apoyo de las tecnologías de la información y la comunicación, tenemos que señalar que los datos de salud de un paciente son algo que afecta de lleno a la esfera más personal e íntima de una persona, algo que habitualmente puede querer reservarse para uno mismo o para los más cercanos. Su conocimiento por terceras personas puede atentar gravemente a la intimidad personal y familiar. No hay que olvidar que en una historia clínica no sólo se encuentran datos de salud sino también de raza, de orientación sexual o de creencias. Existe un vínculo fuerte entre la confidencialidad de la información de salud y el libre desarrollo de la personalidad ya que muchas enfermedades —psiquiátricas, de transmisión sexual— generan un rechazo social. Las instituciones sanitarias no sólo almacenan datos de salud sino también muestras biológicas que permiten la investigación genética y que son capaces de revelar no sólo la salud presente sino la futura y no sólo referida al paciente sino también a la familia. Esta información genética puede convertirse en un importante elemento de discriminación en el ámbito laboral o asegurador⁵. Además, el acceso indebido a una información de salud puede dificultar el ejercicio de otros derechos fundamentales. Así, un alumno portador del virus del VIH puede tener dificultades para escolarizarse y para disfrutar del derecho a la educación —art. 27 CE—; un alcohólico rehabilitado que demanda un empleo puede encontrarse con problemas para ejercer su derecho al trabajo —art. 35 CE—⁶. La confidencialidad de la historia clínica —el acceso a la información sanitaria sólo las personas autorizadas y no terceras personas— es también un instrumento de garantía de la asistencia sanitaria ya que la atención sanitaria está basada en la confidencialidad de la relación médico-paciente, que es, sobre todo, una relación de confianza. Si el paciente piensa que la información que revela al facultativo va a ser conocida por terceras personas, se daña la confianza en la relación médico-enfermo, se limita la información que el paciente da al facultativo y, en definitiva, se perju-

⁵ El Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la biología y la medicina, firmado en Oviedo el 4 de abril de 1997, y ratificado por España en el año 1999, señala en el art. 12 que «[s]ólo podrán hacerse pruebas predictivas de enfermedades genéticas o que permitan identificar al sujeto como portador de un gen responsable de una enfermedad, o detectar una predisposición o una susceptibilidad genética a una enfermedad, con fines médicos o de investigación médica y con un asesoramiento genético apropiado».

⁶ Cfr. A. PUENTE ESCOBAR, «El tratamiento de los datos relativos a la salud. La ley 41/2002, de 15 de noviembre». *Revista Otrrosí*, núm. 50, 2003, pp. 76-82.

⁷ Especial importancia tiene la atención del propio profesional sanitario enfermo que muchas veces oculta su enfermedad por desconfianza acerca de la confidencialidad de esta información en los sistemas sanitarios lo que perjudica gravemente no sólo su salud sino también la de sus pacientes y compañeros.

dica la asistencia. Por tanto, junto al interés personal en el respeto al derecho a la intimidad, la confidencialidad de las historias clínicas es un bien constitucional colectivo⁷. En esta dirección, la acumulación de datos personales en los sistemas de información sanitarios es una potencial amenaza a los derechos de las personas. Como señala el documento *Principios Éticos de la Sanidad en la Sociedad de la Información*, elaborado por el Grupo Europeo de Ética de la Ciencia y de las Nuevas Tecnologías en su dictamen para la Comisión Europea, de 30 de julio de 1999, existen en este campo importantes valores en conflicto ya que la sociedad de la información y la comunicación afecta a la privacidad de las personas⁸. Así, los distintos proyectos en este ámbito –e-salud, hospital digital, receta electrónica, historia clínica electrónica, etc- deben hacerse compatibles con los derechos de esas personas a las que queremos ofrecer una mejor atención. El derecho a la vida que conlleva la atención sanitaria y que requiere datos de salud de las personas y el derecho a la intimidad que exige la confidencialidad de esta información personal son dos bienes constitucionales que frecuentemente entran en colisión y que deben ser adecuadamente compatibilizados. Es posible que el derecho a la vida y a la salud pueda primar en ocasiones sobre el derecho a la intimidad de las personas pero también la intimidad personal obliga a modificar muchos modelos de gestión sanitaria. No se trata de optar entre el derecho a la intimidad y una eficaz atención sanitaria sino buscar el respeto a todos ellos teniendo en cuenta el principio de proporcionalidad. Este será uno de los debates centrales de los próximos años donde la presión de las tecnologías de la información por sí mismas y por las demandas asistenciales, epidemiológicas y científicas van a obligarnos a recuperar la necesidad de un gran pacto, como señalaba Frosini, que tenga en cuenta todos los valores y derechos en presencia.

La Constitución Española contiene los principios y derechos que representan el marco constitucional de aplicación inicial a los tratamientos de datos personales en los servicios sanitarios. Por una parte, hay que recordar el derecho a la vida –art. 15 CE– y a la protección de la salud, por lo que compete a los poderes públicos organizar y tutelar la salud pública a través de medidas preventivas y de las prestaciones y servicios necesarios –art. 43 CE–⁹. El ciudadano se ha beneficiado de una progresiva universalización efectiva del derecho

⁸ *Ethical issues and healthcare in the information society. Opinion of the european group of ethics in science and new technologies to the European Commission*, 30 de julio de 1999.

⁹ El derecho a la vida y a la integridad física, reconocido en la Sección 1^o del Capítulo II del Título I de la Constitución, tiene una vertiente prestacional, objetiva, que hace referencia a la labor activa de los poderes públicos en garantía del mantenimiento de la vida y de la integridad física a través de una atención sanitaria. El derecho a la protección de la salud como principio rector de la política social y económica está recogido en el art. 43.1 y 2 CE. Este precepto no alberga derechos sino una directiva que debe orientar la legislación positiva, la práctica judicial y la actuación de los poderes públicos, pero que sólo puede ser alegado de acuerdo con lo que dispongan las leyes que lo desarrollen. Por tanto, el derecho subjetivo y principio rector del art. 43 no es un derecho fundamental –no tiene aplicación inmediata, no tiene una vertiente objetiva ex constitutione exigible a los poderes públicos–, y no tiene contenido esencial –en el enjuiciamiento de la legitimidad del desarrollo legislativo no se puede ir de lo abstracto a lo concreto–. Se está a expensas del desarrollo legislativo, en donde el legislador tiene un amplio margen de libertad. Cf: M. JIMÉNEZ DE PARGA, «El derecho constitucional a la protección de la salud» en *La salud como valor constitucional y sus garantías*, Universidad Rey Juan Carlos, Madrid, 2004, pp. 9-24.

a recibir una asistencia sanitaria, que le ha hecho titular de un conjunto de prestaciones por parte de los poderes públicos¹⁰ y que se ha extendido incluso a los extranjeros¹¹. Igualmente, el art. 18.1 garantiza «el derecho al honor, a la intimidad personal y familiar y a la propia imagen», al tiempo que el 18.4 señala que la ley «limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar y el pleno ejercicio de los derechos». El Tribunal Constitucional ha reconocido un derecho específico a la autodeterminación informativa en la Sentencia 292/2000, de 30 de noviembre, definiéndolo como el «[p]oder 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» –F. J. 7º–. Es importante señalar que este derecho fundamental a la protección de datos personales no tiene un carácter abstracto o genérico. Atribuye a su titular un haz de facultades que consiste en el poder jurídico de imponer a terceros la realización o la omisión de determinados comportamientos. Dentro del contenido de este derecho fundamental, se encontrarían los principios de calidad de los datos, información en la recogida de los mismos, consentimiento del afectado para su tratamiento y para la cesión, seguridad informática y deber de secreto. También los derechos de acceso, oposición, rectificación y cancelación sobre los datos de carácter personal sometidos a tratamiento¹². Se reconoce así el derecho de todos los pacientes a conocer qué datos sobre su salud se van a recoger y registrar, quién los va a utilizar, para qué finalidad y también su derecho de acceso a esta información y de rectificación cuando ésta sea errónea o inexacta. El Tribunal Constitucional ha definido el derecho fundamental a la protección de datos como un derecho autónomo nuevo y diferenciado del derecho a la intimidad que atribuye a la persona el control sobre sus datos personales, sean o no sean íntimos –los datos de conocimiento público también entran dentro del poder de disposición y control que da este derecho fundamental– y que protege a la persona –a la

¹⁰ La Ley 14/1986, de 25 de abril, General de Sanidad contenía la semilla de la universalización al establecer que el acceso a las prestaciones sanitarias se haga en condiciones de igualdad –art. 3–.

¹¹ La extensión a los extranjeros sin permiso de residencia pero empadronados en un municipio de los derechos de asistencia sanitaria y farmacéutica, y a los extranjeros no empadronados menores de edad se ha hecho efectivo a través de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social –art. 12–. Con anterioridad, el art. 10.3 LOPJM reconoció a los menores extranjeros el derecho a la asistencia sanitaria, aún cuando no residieran legalmente en España. *Cfr.* el estudio del Defensor del Menor en la Comunidad de Madrid sobre el derecho a la protección de la salud que se encuentra en *Menores inmigrantes en España*, Comunidad de Madrid, 2001, pp. 26-35.

¹² *Cfr.* P. LUCAS MURILLO, *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990; P. LUCAS MURILLO, *Informática y Protección de Datos Personales*, CEC, Madrid, 1993; J. M. ALVAREZ CIENFUEGOS, *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Aranzadi, Pamplona, 1999. *Cfr.* también A. TRONCOSO REIGADA, «La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional», *Cuadernos de Derecho Público*, núm. 19-20, 2003, pp. 231-334.

propia información personal— frente a las tecnologías de la información —también frente a los tratamientos manuales—, teniendo una dimensión esencialmente activa —ejercicio del derecho de acceso, adecuación del tratamiento a la finalidad, información de los tratamientos— que no encaja bien con la idea de injerencia o intromisión ilegítima ya que es el propio interesado el que en muchas ocasiones da sus datos personales. La protección de datos personales, a la vez que es un derecho autónomo, es un instrumento de garantía de otros derechos fundamentales ya que la informática puede ser utilizada para limitar el pleno ejercicio de los derechos. No obstante, a nuestro juicio, el derecho fundamental a la protección de datos personales no debe ser visto como un derecho absolutamente independiente sino vinculado con el derecho a la intimidad, aunque tutele otros derechos fundamentales como también hace el derecho a la intimidad¹³. De hecho, el único derecho mencionado expresamente en el art. 18.4 CE es el derecho a la intimidad. Muchos tratamientos de datos personales afectan principalmente al derecho a la intimidad. Esto ocurre especialmente en el ámbito sanitario ya que los datos de salud son por definición datos íntimos¹⁴. Por tanto, la protección de los datos de salud no sólo es consecuencia del derecho a controlar nuestros datos sino también del derecho a tener una vida privada y, en el fondo, de nuestra propia dignidad personal¹⁵.

Hay otros preceptos constitucionales que afectan indirectamente a la protección de datos sanitarios y a la historia clínica. Así, el art. 24 CE señala que todas las personas tienen derecho «a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos sin que, en ningún caso, pueda producirse indefensión», encomendando al legislador la regulación de «los casos en que, por razón de parentesco o de *secreto profesional*, no se estará obligado a declarar sobre hechos presuntamente delictivos». En el Título VIII relativo a la distribución territorial del poder se establece que el Estado tiene competencia exclusiva para regular «las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales» —art. 149.1.1º— y para regular las «bases y coordinación general de la sanidad» —art. 149.1.16º—; las CCAA tienen en razón del art. 148.1.21º —competencias sobre «sanidad e higiene»— y, sobre todo, sobre la gestión de la asistencia sanitaria. La reforma

¹³ Esta cuestión la hemos analizado en «La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional», *Cuadernos de Derecho Público*, núms. 19-20, 2003, esp. pp. 244-252.

¹⁴ Este es el motivo por el que De Miguel ha vinculado la protección de datos al derecho a la intimidad. Cfr. N. DE MIGUEL SÁNCHEZ, *Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público*, Tirant lo Blanch, Valencia, 2004, pp. 27-36 y *Secreto médico, confidencialidad e información sanitaria*, Marcial Pons, Madrid, 2002, pp. 262-270. Así, para esta autora, «se trata de una manifestación específica del derecho a la intimidad dotada de sus propias características, pero no de un derecho independiente, que responda a criterios que permitan sostener su autonomía» —*ibidem* p. 315—.

¹⁵ Esto es lo que hace que el número de denuncias de protección de datos en el ámbito de salud sean mucho más abundantes que en otros ámbitos: en este caso, el ciudadano lo denuncia porque se ve afectado en su más estricta intimidad.

de los Estatutos de Autonomía ha incluido también el reconocimiento de derechos y el establecimiento de principios rectores de las políticas públicas en el ámbito sanitario.

II. PRINCIPIOS Y DERECHOS DE LOS CIUDADANOS EN RELACIÓN CON LA HISTORIA CLÍNICA

a) *La legislación reguladora de la historia clínica y de la protección de los datos de salud*

El principal desarrollo legislativo producido hasta ahora sobre el derecho a la intimidad reconocido en el art. 18.1 de la Constitución ha sido la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen¹⁶. Esta Ley, básicamente, desarrolla el contenido de este derecho como límite a la libertad de expresión y al derecho a la información, en los términos previstos en el art. 20.4 CE. Por ello, la principal doctrina y jurisprudencia constitucional sobre el derecho a la intimidad ha tratado, sobre todo, de deslindar estos dos derechos enfrentados.

La legislación vigente hasta ahora sobre la historia clínica y sobre la protección de datos sanitarios, y, más en general, sobre derechos y obligaciones de los pacientes se caracterizaba por su escasez y por su antigüedad¹⁷. La Ley 14/1986, de 25 de abril, General de Sanidad tiene como objetivo el establecimiento y la ordenación del sistema sanitario, pero también alberga una voluntad humanizadora, en concreto en su Capítulo I «De los principios generales», dentro del Título Primero «Del Sistema de Salud», donde se recogían distintos derechos con respecto a las administraciones sanitarias, como el reconocimiento de la dignidad de la persona, de la libertad individual, del respeto de

¹⁶ Cfr. SSTTC 117/1994; 231/1998; 76/1990; M. MEDINA GUERRERO, *La protección constitucional de la intimidad frente a los medios de comunicación*, Tirant lo Blanch, Valencia, 2005, pp. 70-180; C. RUIZ MIGUEL, *La configuración constitucional del derecho a la intimidad*, Tecnos, Madrid, 1995; F. HERRERO-TEJEDOR, *Honor, intimidad y propia imagen*, Colex, Madrid, 1984; P. A. MUNAR, «Derecho a la intimidad», *Enciclopedia Jurídica Básica*, Cívitas, Madrid, 1995, III, pp. 3725-3728; J. VIDAL MARTINEZ, *El derecho a la intimidad en la Ley Orgánica de 5 de mayo de 1982*, Madrid, 1984; L. M. FARIÑAS MANTONÍ, *El derecho a la intimidad*, Madrid, 1983; D. ORTEGA, *Derecho a la información versus derecho al honor*, CEPC, Madrid, 1999.

¹⁷ La primera definición de derechos del enfermo hospitalario es realizada por el Reglamento de Régimen, Gobierno y Servicios de las Instituciones Sanitarias de la Seguridad Social, aprobado por Orden Ministerial de 7 de julio de 1972. Hay que destacar también el Real Decreto 2082/1978, de 25 de agosto, por el que se aprueban normas provisionales de Gobierno y Administración de los servicios hospitalarios y las garantías de los usuarios -Anexo II.Trece-apdos A al M- que desarrollaban algunas garantías de los usuarios de los servicios hospitalarios. También hay que citar la Carta de los Derechos y Deberes de los Pacientes y el Plan de Humanización de Hospitales ideado por el INSALUD en 1981. Posteriormente, el Reglamento General de Estructura, Organización y Funcionamiento de los Organismos de la Seguridad Social, de 1 de marzo de 1985, crea la Comisión de Humanización de Asistencia, encargada de velar por el bienestar y atención al paciente, analizar la información recabada por el Servicio de Atención al Paciente y ocuparse de los aspectos que pudieran mejorar la asistencia.

la intimidad personal y la garantía de la confidencialidad de la información personal —arts. 9, 10 y 61—. La Ley General de Sanidad reconocía el derecho de todas las personas 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 —art. 10.3—, lo que exige que la historia clínica esté a disposición de los enfermos y de los facultativos que directamente estén implicados en el diagnóstico del enfermo, así como a efectos de inspección médica o para fines científicos, «debiendo quedar plenamente garantizados el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica» —art. 61 LGS—¹⁸. No ha habido hasta ahora abundantes estudios constitucionales sobre la protección de datos sanitarios y sobre la historia clínica desde la perspectiva del derecho a la intimidad¹⁹. Así, la mayoría de los trabajos sobre este campo se han desarrollado desde el punto de vista del derecho administrativo sanitario o desde el campo de la ética médica²⁰. Tampoco la jurisprudencia constitucional ha tenido la oportunidad de madurar la cuestión, aunque sí la jurisprudencia del Tribunal Supremo²¹.

¹⁸ Las obligaciones y deberes de los pacientes con las instituciones y organismos del sistema sanitario están recogidos, entre otros, en el art. 11 de la Ley General de Sanidad y en la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en materia de Salud Pública, que establece distintas medidas que pueden ser adoptadas por las Administraciones Públicas con el objetivo de proteger la salud pública y que también implican obligaciones a los particulares.

¹⁹ Merece una atención específica N. DE MIGUEL SÁNCHEZ, *Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público*, cit. pp. 43-79 y *Secreto médico, confidencialidad e información sanitaria*, cit. pp. 260-306. Tiene un especial interés los trabajos de Javier Sánchez-Caro y Fernando Abellán. Cfr. J. SÁNCHEZ CARO y F. ABELLÁN, *La historia clínica*, Fundación Salud, Madrid, 2000; *id.*, *Telemedicina y protección de datos sanitarios*, Fundación Salud, Granada, 2002, pp. 52-136; *id.*, *Derechos y deberes de los pacientes*, Fundación Salud, Granada, 2003. Cfr. también AA.VV., *La Protección de Datos Personales en el Ámbito Sanitario*, Aranzadi, Cizur Menor (Navarra), 2002, pp. 145 y ss. En cambio, sí se están realizando estudios desde el derecho constitucional en relación con los datos genéticos. Cfr. J. RODRÍGUEZ-DRINCOURT, *Genoma Humano y Constitución*, Civitas, Madrid, 2002, pp. 37 y 122. Sobre esta cuestión, Cfr. también J. BLÁZQUEZ RUIZ, *Derechos Humanos y Proyecto Genoma*, Comares-MS, Granada, 1999, pp. 51-63 y 141-171; C. RUIZ MIGUEL, «La nueva frontera del derecho a la intimidad». *Revista Derecho y Genoma Humano* núm. 14, 2001, pp. 147-167; J. A. RODRÍGUEZ SEOANE, «De la intimidad genética al derecho a la protección de datos genéticos. La protección iusfundamental de los datos genéticos en el Derecho español (A propósito de las SSTC 290/2000 y 292/2000, de 30 de noviembre)». *Revista Derecho y Genoma Humano* núm. 17, 2002, pp. 152-154; J. SÁNCHEZ-CARO y F. ABELLÁN, *Datos de salud y datos genéticos. Su protección en la Unión Europea y en España*, Fundación Salud 2000, Madrid, 2004. A esta cuestión he tenido la oportunidad de referirme puntualmente en «Ficheros de perfiles de ADN y derecho fundamental a la protección de datos personales» en A. TRONCOSO REIGADA, *Estudios sobre Administraciones Públicas y Protección de Datos Personales*, Civitas-APDCM, Madrid, 2006, pp. 21-68.

²⁰ Cfr.; C. SÁNCHEZ CARAZO, *La intimidad y el secreto médico*, Díaz de Santos, Madrid, 2000, pp. 191-222; J. SÁNCHEZ-CARO y F. ABELLÁN, *El médico y la intimidad*, Díaz de Santos, Madrid, 2001; R. GARCÍA ONTOSO, M. SÁNCHEZ GONZÁLEZ, E. SÓLA y L. RODRÍGUEZ RAMOS, «Intimidad y confidencialidad en la práctica clínica», *VI Congreso Nacional de Derecho Sanitario*, Fundación Mapfre Medicina, 2000, pp. 63-108.

²¹ La jurisprudencia relativa al derecho a la intimidad en el ámbito sanitario de la Sala Contencioso-Administrativa del Tribunal Supremo y de la Audiencia Nacional, además de otras de interés en Audiencias Provinciales, es muy numerosa. Cfr. la sección de jurisprudencia de *diariomedico.com*, o en soporte papel, el trabajo de la Asociación Española de Derecho Sanitario, presentado por J. M. ÁLVAREZ CIENFUEGOS, sobre *La Historia Clínica*, Madrid, 1997.

En los últimos los ciudadanos se han hecho más conscientes de sus derechos en el ámbito sanitario, especialmente en lo que hace referencia al fortalecimiento del principio de autonomía personal en las relaciones médico-enfermo que supera una visión más paternalista²², el incremento de la preocupación social ante el dolor, especialmente en situaciones clínicas irreversibles, el acceso del paciente a su historia clínica y la intimidad y confidencialidad de sus datos sanitarios²³. Progresivamente se ha ido reconociendo un conjunto de derechos de los pacientes, entre los que destacarían entre otros la facultad de exigir una explicación comprensible sobre la naturaleza de su enfermedad y sobre los distintos tratamientos terapéuticos –derecho a la información²⁴– y su autonomía de decisión para aprobar su sometimiento a estos tratamientos, lo que se ha venido a denominar el «consentimiento informado»²⁵. El reconocimiento de los derechos de los pacientes se ha producido especialmente en el ámbito supranacional donde se han ido aprobando algunas normas y resoluciones de interés, entre las que merece destacarse especialmente el Convenio para la Protección de los Derechos Humanos y la Dignidad del ser humano con respecto a las aplicaciones de la biología y de la medicina, aprobado por el Comité de Ministros del Consejo de Europa y suscrito en Oviedo el 4 de abril de 1997, ratificado por España el 23 de julio de 1999²⁶, siendo el primer ins-

²² Ya la Ley General de Sanidad –art. 10.5– señalaba que todos tienen derecho a que se les dé «en términos comprensibles, a él y a sus familiares o allegados, información completa y continuada, verbal y escrita, sobre su proceso, incluyendo diagnóstico, pronóstico y alternativas de tratamiento», derecho a la información que es, lógicamente, el presupuesto del derecho a la libre elección entre opciones terapéuticas –art. 10.6 LGS– y a negarse a recibir el tratamiento –art. 10.9 LGS–. El Acuerdo del Pleno del Consejo Interterritorial del Sistema Nacional de Salud sobre Consentimiento Informado, adoptado el 6 de noviembre de 1995, reconocía que «todo paciente tiene derecho a que se le informe de su enfermedad y de las circunstancias relevantes que ésta implica».

²³ Cfr. M. IRABURU, *Con voz propia. Decisiones que podemos tomar ante la enfermedad*, Alianza Editorial, Madrid, 2005, esp. pp. 87-109; «Confidencialidad e intimidad», *Anales del Sistema Sanitario de Navarra*, vol. 29, núm. 3, 2006, pp. 49-59; «Estudio multicéntrico de investigación sobre la confidencialidad», *Med. Clin. Barc.* 2007, pp. 575-578.

²⁴ El Real Decreto 63/1995, de 20 de enero, sobre ordenación de las prestaciones sanitarias del Sistema Nacional de Salud incluía una genérica referencia a la información como derecho y como prestación efectiva dentro del catálogo de prestaciones. Cfr. anexo 1, apdo. 5.

²⁵ Cfr. A. PELAYO GONZÁLEZ-TORRE, *La intervención jurídica de la actividad médica: el consentimiento informado*, Cuadernos Bartolomé de las Casas, Dykinson, Madrid, 1997; J. C. GALÁN CORTÉS, *El consentimiento informado del usuario de los servicios sanitarios*, Colex, Madrid, 1997; P. SIMÓN LORDA, *El consentimiento informado*, Triacastela, Madrid, 2000; J. SÁNCHEZ-CARO y F. ABELLÁN, *Derechos y deberes de los pacientes*, Granada, 2003, esp. pp. 1-15. El consentimiento informado ha sido estudiado en los distintos Congresos Nacionales de Derecho Sanitario que celebra la Asociación Española de Derecho Sanitario y que publica la Fundación Mapfre Medicina. Cfr. en el IV Congreso Nacional –ed. 1998– J. M. ÁLVAREZ CIENFUEGOS, «La información clínica y el grupo de expertos del Ministerio de Sanidad y consumo: conclusiones», pp. 113-120.; en el V Congreso Nacional –ed. 1999– A. LIBANO, «El consentimiento informado 25 años después» pp. 299-302.

²⁶ Este Convenio materializaba su respaldo al consentimiento informado y al derecho a la intimidad del paciente. Cfr. los artículos de M. CARCABA, MARCELO PALACIOS, O. QUINTANA y C. DE SOLA sobre el Convenio de Oviedo en *Actas del VI Congreso Nacional de Derecho Sanitario*, Fundación Mapfre Medicina, pp. 189-227.

trumento internacional con carácter jurídico vinculante para los países que lo suscriben, como ha sido destacado por el Preámbulo de la Ley 41/2002, de 14 de noviembre, que más adelante analizaremos. Su especial valía, señala este Preámbulo, reside en el hecho de que establece un marco común para la protección de los derechos, estableciendo la necesidad de reconocer los derechos de los pacientes, entre los cuales está el consentimiento informado y la tutela de intimidad de la información relativa a la salud de las personas. Hay que mencionar también la Recomendación 1418/1999, de la Asamblea Parlamentaria del Consejo de Europa, sobre la protección de los derechos humanos y la dignidad de los enfermos terminales y moribundos. Igualmente debemos mencionar la Declaración sobre la promoción de los derechos de los pacientes en Europa, promovida el año 1994 por la Oficina Regional para Europa de la Organización Mundial de la Salud y la Recomendación, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre protección de datos médicos. Es obvio recordar aquí que la Constitución establece en el art. 10.2 que las normas y preceptos relativos a los derechos fundamentales y a las libertades «se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España».

El desarrollo legislativo de los derechos de los pacientes ha sido tradicionalmente deficiente. El catálogo de derechos descritos en la Ley General de Sanidad no hacía mención en unos casos y no agotaba en otros los concretos derechos fundamentales desarrollados en estos textos internacionales y reconocidos en sede jurisdiccional. Existía, además, una gran dispersión y una falta de sistematización de la normativa nacional e internacional relativa a derechos de los pacientes. Por tanto, era necesario llevar a cabo un desarrollo legislativo de los derechos de los pacientes, algunos de los cuales estaban implícitos en la Constitución o en la normativa sanitaria. Se hacía cada vez más imprescindible la necesidad de orientar mejor la actuación de los profesionales sanitarios, de forma que esta orientación no venga sólo de los Códigos deontológicos profesionales sino a través de las normas jurídicas, en virtud de la función pedagógica que tiene el derecho. Situaciones como las huelgas de hambre de los presos del Grapo o la negativa a las transfusiones de sangre por parte de testigos de Jehová, por poner sólo dos ejemplos, han revelado la conveniencia de que sea el legislador y no los Tribunales –los jueces de guardia o el Tribunal Constitucional– los que desarrollen los derechos fundamentales que la Constitución reconoce, dando preferencia a unos valores sobre otros cuando entren en colisión.

La necesidad de una normativa sobre derechos de los ciudadanos en el ámbito sanitario, también en lo que hace referencia al consentimiento informado y a la historia clínica, era especialmente importante en la Legislatura en la que se iba a acometer las transferencias del Instituto Nacional de la Salud a las once Comunidades Autónomas restantes. Era imprescindible que se garantizase la igualdad de derechos de los ciudadanos en el ámbito sanitario, cual-

quiera que sea en lugar de residencia –art. 137 y 149.1.1º CE–²⁷. Como señaló el Acuerdo de la Subcomisión Parlamentaria para la Consolidación y Modernización del Sistema Nacional de Salud, era necesario evitar que se produzcan discriminaciones por razones territoriales, asegurando el acceso equitativo a unos contenidos materiales. El sistema sanitario público «es un importante elemento de justicia redistributiva y de cohesión social que se ha de consolidar atendiendo a los principios básicos de equidad, solidaridad y aseguramiento público y único». Por eso, era imprescindible aprobar una Ley Básica sobre los derechos de los ciudadanos en el ámbito sanitario que regulase las condiciones que garantizan la igualdad de todos los ciudadanos en el ejercicio de sus derechos y en el cumplimiento de sus deberes constitucionales –art. 149.1.1º CE–. Era además una competencia exclusiva del Estado al hacer referencia a las bases y coordinación general de la sanidad –art. 149.1.16–²⁸. Hasta la aprobación de las reformas de los Estatutos de Autonomía, las Comunidades Autónomas se debían limitar a la divulgación de los derechos de los usuarios en los servicios sanitarios –a través de Cartas de derechos o servicios como ocurre en el Servicio Vasco y Catalán de Salud–, porque carecían de competencia para establecer clases nuevas de derechos o desarrollarlos. Por ese motivo, es discutible la competencia de los Parlamentos Autonómicos para aprobar normas relativas a la autonomía de los pacientes o al derecho a la intimidad, aunque sí para regular el ejercicio de los derechos que se aprueben por la legislación estatal. En especial hay que cuestionar la competencia del Parlamento de Cataluña para aprobar la –primera– Ley 21/2000, de 29 de diciembre, relativa al derecho a la información y a la consideración de las voluntades anticipa-

²⁷ Cfr. más ampliamente AA.VV., *Transferencias sanitarias: descentralizar y vertebrar*, Pricewaterhouse-Coopers, Madrid, 1999.

²⁸ El Ministerio de Sanidad elaboró durante el año 2000 un Anteproyecto de Ley de derechos fundamentales en el ámbito sanitario, más amplio y más ambicioso que el texto que finalmente aprobara el Congreso en la Ley 41/2002 y en el que tuve la oportunidad de intervenir como Director de Gabinete de la Subsecretaría del Ministerio de Sanidad y Consumo. Cfr. más ampliamente A. TRONCOSO REIGADA en las *Actas del X Congreso Nacional de Derecho Sanitario*, cit. Este texto fue empleado para presentar las 126 enmiendas a la Proposición de Ley 41/2002 y como borrador inicial de la Ley 16/2003, de 28 de mayo de Cohesión y Calidad del Sistema Nacional de Salud. Un elemento fundamental era la afirmación de la titularidad del derecho a la atención sanitaria a toda persona. Esto implicaría: por una parte, la desvinculación del derecho a recibir una prestación asistencial de la existencia, aunque sea de manera indirecta, de una relación laboral; por otra parte, la ampliación del titular de los derechos no sólo a los ciudadanos sino también a los extranjeros, en los términos que lo ha previsto la reciente Ley 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, que no ha sido modificado en este apartado por la Ley Orgánica 8/2000. Así, el Acuerdo de la Subcomisión Parlamentaria para la Consolidación y Modernización del Sistema Nacional de Salud, aprobado en el Pleno del Congreso de los Diputados el 18 de diciembre de 1997 señalaba también la necesidad de «llevar a cabo la universalización efectiva del derecho a la asistencia sanitaria, extendiéndolo a todos los grupos sociales y desvinculándolo de los regímenes de afiliación de la seguridad social». La primera recomendación del acuerdo es «consolidar el aseguramiento sanitario universal». En ella se afirma la necesidad de poner en marcha la reforma legal adecuada que permita «fijar los contenidos y el carácter del derecho a la asistencia sanitaria como derecho público subjetivo, personal y no contributivo, resaltando la importancia de la orientación de los servicios a los usuarios». También el Plan Estratégico del Insalud de 1999 iba dirigido a facilitar a los ciudadanos información sobre las prestaciones y su acceso a las mismas y la búsqueda de fórmulas que garanticen el ejercicio real de sus derechos.

das ya que el desarrollo de los derechos fundamentales es competencia del legislador estatal²⁹.

Esto no ha impedido que los Parlamentos de las Comunidades Autónomas hayan ido aprobando Leyes de Salud o Leyes Sanitarias que regulan algunos derechos como el consentimiento informado o el acceso a la historia clínica y que tienen contenidos idénticos o muy divergentes –no se sabe que es peor–. La legislación autonómica se ha caracterizado por regular el derecho a la protección de datos sanitarios y la confidencialidad de la historia clínica. Así, en esta dirección hay que señalar la Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid –LOSCAM– que establece como principios informadores de la organización y funcionamiento del Sistema Sanitario de la Comunidad de Madrid, la orientación al ciudadano como persona, su autonomía y la garantía de los derechos a la intimidad y a la protección de los datos de carácter personal –art. 26.1 LOSCAM–. Igualmente se afirma que «el ciudadano tiene derecho a mantener su privacidad y a que se garantice la confidencialidad de sus datos sanitarios, de acuerdo a lo establecido en la legislación vigente» –art. 27.3 LOSCAM–. Por último, se indica que la autoridad sanitaria garantizará «el derecho a recibir información sanitaria por medio del desarrollo de redes de información sanitaria integrada de calidad, cumpliendo con todas las medidas que estén vigentes en materia de protección de datos de carácter personal y de identificación mediante firma digital avanzada» –art. 29.2b) LOSCAM–.

Este es el escenario en el que es aprobada por las Cortes Generales 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. Posteriormente es aprobada la Ley 16/2003, de 28 de mayo de Cohesión y Calidad del Sistema Nacional de Salud que reconoce expresamente el derecho a una asistencia sanitaria pública, universal y gratuita³⁰. Son Leyes cercanas en el tiempo pero muy diferentes en su génesis. Si la Ley 16/2003, de 28 de mayo nace de un proyecto de Ley del Gobierno, la Ley 41/2002, de 14 de noviembre es consecuencia de una Proposición de Ley, planteada por el Grupo Catalán en el Senado, cuyo contenido ha sido fruto de distintos textos y trabajos preparatorios en el Gobierno, especialmente durante los años 1997-

²⁹ La Ley Catalana es reproducción de un borrador de anteproyecto del Ministerio, en el que participaron un grupo de expertos. Cfr. el texto D. MARTÍNEZ, «Información y documentación clínica: una propuesta de regulación básica», *Actualidad de Derecho Sanitario* núm. 63, 2000, pp. 505-525.

³⁰ La Ley de Cohesión y Calidad del Sistema Nacional de Salud ha establecido los principios vertebradores de la descentralización política de la sanidad, al tiempo que han definido la integración de los diferentes servicios de salud y políticas sanitarias dentro en un Sistema Nacional de Salud, con el objetivo de que la descentralización no afecte a la igualdad del derecho a recibir una asistencia sanitaria. La efectividad del derecho a recibir una asistencia sanitaria de calidad en todo el territorio nacional exige el establecimiento de un conjunto de principios que vertebrén el Sistema Nacional de Salud para que éste funcione como un auténtico Sistema donde el aseguramiento público universal e igual sea una realidad con independencia del lugar de residencia.

2001³¹. Esta Ley que desarrolla la autonomía del paciente y los derechos de información y documentación clínica en el Sistema Nacional de Salud tiene el carácter de Ley básica, al regular las condiciones que garantizan la igualdad de todos los ciudadanos en el ejercicio de sus derechos y en el cumplimiento de sus deberes constitucionales –art. 149.1.1 CE–³². La Ley 41/2002, de 14 de noviembre, como refleja su Preámbulo, es fruto de la voluntad del legislador de tratar de humanizar más los servicios sanitarios y atender mejor la dignidad de la persona, a través de un mayor respeto a la autonomía del paciente y a la confidencialidad de su historia clínica. En esta dirección, la Ley 41/2002, de 14 de noviembre, trata de tener su origen en lo previsto de manera muy inicial en la Ley General de Sanidad –arts. 9, 10 y 61– y en el Convenio de Oviedo, ya citado, para la Protección de los Derechos Humanos y la Dignidad del ser humano, con respecto a las aplicaciones de la biología y de la medicina, aprobado por el Comité de Ministros del Consejo de Europa en 1997.

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 representa la primera regulación específica de ámbito nacional sobre historia clínica, intimidad del paciente y protección de datos médicos. La historia clínica es, junto con el testamento vital y las voluntades anticipadas, uno de los temas que más ha centrado la atención de los médicos y de los juristas en los últimos diez años. La dudas sobre la titularidad de la historia clínica y los distintos niveles de acceso ha favorecido la aparición de frecuentes conflictos que han terminado en el ámbito jurisdiccional. Detrás de estos conflictos late la distinta percepción sobre de quién es la historia clínica, sobre sus fundamentos éticos y deontológico y sobre cómo resolver las incertidumbres y cuestiones que plantea su consulta diaria en la práctica clínica. La Ley 41/2002, de 14 de noviembre, trata de resolver los conflictos que surgen en el acceso y utilización de la historia clínica. Es una Ley que recoge muchas soluciones anticipadas por la jurisprudencia acerca del acceso a la historia clínica de los menores, de los fallecidos o de terceras personas por lo que es un texto legal que se caracteriza por resolver problemas, aportando respuestas concretas, no sólo principios generales.

No obstante, la principal regulación hasta ahora de la historia clínica era la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal –LOPD–³³, que si bien es una norma general y no una regu-

³¹ El Preámbulo cita expresamente el convenio de colaboración entre el Consejo General del Poder Judicial y el Ministerio de Sanidad y Consumo, en concreto el seminario conjunto sobre información y documentación clínica, que dio lugar a un Documento Final de un grupo de expertos en noviembre de 1997, publicado 1998, junto con las ponencias del Seminario y un análisis jurisprudencial 1990-1999. *Cfr.* AA.VV, *Información y documentación clínica*, vol. I y II, CGPJ-MS, Madrid, 1998 e *Información y documentación clínica. Su tratamiento jurisprudencial*, MSC, Madrid, 2000.

³² Sin embargo, el Parlamento de Cataluña recurrió esta Ley ante el Tribunal Constitucional por atribuirse toda ella el carácter de básico que, a su juicio, debía limitarse a algunos artículos de manea que se respete más la autonomía de la organización sanitaria de las Comunidades Autónomas. Se critica especialmente el art. 14.2 que establece que cada centro archivará las historias clínicas de sus pacientes.

³³ *Cfr.* J. APARICIO, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Navarra, 2002; M. VIZCAINO, *Comentarios a la Ley Orgánica de protección de datos de carácter personal*, Cívitas, Madrid, 2001.

lación sectorial para el ámbito sanitario, se aplica plenamente a los tratamientos de datos de salud. No podía ser de otra forma ya que esta Ley tiene como objeto «garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor, intimidad personal y familiar».

La Ley Orgánica 15/1999, de 13 de diciembre, es especialmente aplicable a la historia clínica ya que ésta es un tratamiento de datos personales, bien informatizado, bien manual estructurado, y esta Ley tiene como ámbito de aplicación «los datos personales registrados en soportes físicos, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos» –art. 2–. Además, las definiciones que se contienen en el art. 3 LOPD subrayan que fichero es «todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso», y tratamiento «toda operación y procedimiento técnico de carácter automatizado o no, que permita la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias». Estas definiciones encajan con las que el art. 3 de la Ley 41/2002, de 14 de noviembre, hace tanto de documentación clínica –«soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial» como de historia clínica– «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». De hecho, el Preámbulo de la Ley 41/2002, de 14 de noviembre, cita expresamente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y la Directiva Comunitaria 95/46, del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos.

De esta forma se entiende que para que sea de aplicación la Ley Orgánica 15/1999, de 13 de diciembre es necesario que exista un tratamiento de datos personales. Esto no presenta dudas en el tratamiento automatizado de datos personales pero sí cuando se trata de información en papel. Como señalaremos más adelante³⁴, no toda acumulación de documentación en papel supone un fichero. Para que pueda hablarse de fichero manual, es necesario que la información clínica se encuentre estructurada con arreglo a personas. Además, es necesario que el tratamiento que se haga sea de datos personales. El art. 3.a) LOPD define dato de carácter personal como cualquier información concerniente a persona física identificada o identificable. Por tanto, un dato de carácter personal no es sólo el relativo a personas identificadas sino también identificables. La Directiva 95/46/CE considera identificable una persona si su identidad puede determinarse, directa o indirectamente, como, por ejemplo, un número de identificación.

Señala el Considerando 26 de la Directiva que para determinar que una persona es identificable, hay que considerar el conjunto de medios que pueden ser

³⁴ Cfr. *infra* apdo. 6.

razonablemente utilizados por el responsable del tratamiento para identificar a una persona. Para que exista un dato de carácter personal, en contraposición al dato disociado «no es imprescindible una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados»³⁵. Para determinar que una persona es identificable, «hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona». Así, el número de tarjeta sanitaria es un dato de carácter personal. Por último, hace falta que la información sea de personas, entre las que deben incluirse las personas físicas –no las personas jurídicas también las fallecidas»³⁶.

Hasta la Ley 41/2002, de 14 de noviembre ha sido la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal –LOPD– la legislación más específica para regular el acceso a la historia clínica. Así, no se encuentran los ficheros sanitarios en el amplio ámbito de los ficheros que el art. 2 de la Ley 15/1999, de 13 de diciembre, excepciona –ficheros domésticos, ficheros de materias clasificadas, ficheros de terrorismo o de delincuencia organizada– o que se rigen principalmente por sus disposiciones específicas –ficheros de régimen electoral general, ficheros estadísticos, de calificación del personal de las Fuerzas Armadas, del Registro Civil y del Registro Central de Penados y rebeldes, y de imágenes y sonidos procedentes de videocámaras de las Fuerzas y Cuerpos de Seguridad-. De hecho, la propia Ley 15/1999, de 13 de diciembre, contempla específicamente los tratamientos de datos de salud –arts. 7, 8 y 11–³⁷.

No obstante, como ya hemos señalado en otra ocasión, la Ley Orgánica 15/1999, de 13 de diciembre, es confusa y representa un ejemplo de técnica legislativa deficiente, además de no ser fácilmente adaptable a las peculiaridades propias de la realidad asistencial³⁸. 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 representa la legislación específica de los tratamientos de datos sanitarios que se materializan a través de los distin-

³⁵ Sentencia de la Audiencia Nacional, de 8 de marzo de 2002.

³⁶ Esta cuestión la analizaremos infra apdo. 3.a). También se ha reconocido el derecho de acceso de un paciente al proceso asistencial de su propio nacimiento, que se podrá dar siempre que no afecte a la intimidad de la madre.

³⁷ Sin embargo, el Tribunal Superior de Justicia de Madrid, en la Sentencia de 12 de julio de 2000 Sección Octava–, considera que el fichero de historias clínicas para la actividad profesional del facultativo es un fichero de carácter personal. La Sentencia afirma que «el contenido del ordenador personal de un profesional de la medicina, en el que se incluyen las historias clínicas de sus pacientes, queda fuera del ámbito de aplicación de la LORTAD y consiguientemente, de la acción inspectora de la Agencia de Protección de datos, pues las eventuales violaciones del deber de confidencialidad del médico –extremo que en este caso concreto no consta que se haya producido en ningún momento– tienen sus posibles cauces jurídicos de reacción distintos y al margen de los establecidos en la LORTAD, por lo que los ficheros del facultativo, en cuanto se limitaban a recoger las historias clínicas de sus pacientes, permanecen al margen de dicha ley, y, en consecuencia, nunca podrá incurrir en las infracciones tipificadas». Esta Sentencia debe ser considerada como un caso fortuito.

³⁸ Cfr. A. TRONCOSO REIGADA, «La protección de datos personales», *cit.* pp. 261-267.

tos documentos de información y documentación clínica. La aprobación de esta norma viene a paliar parcialmente la posible insuficiencia de la Ley Orgánica 15/1999, de 13 de diciembre, para regular la problemática específica de los tratamientos de datos de salud³⁹. Por tanto, la problemática de la historia clínica y de la confidencialidad de los datos salud tiene que ser abordada desde dos perspectivas: por una parte, a partir de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Persona, que tiene el carácter de ley general; por otra, a partir 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, que sería la ley especial.

Si bien es cierto que la legislación de protección de datos personales no se adapta plenamente a la realidad sanitaria, también es verdad que la Ley 15/1999, de 13 de diciembre, admite la posibilidad de que los responsables de los ficheros y tratamientos puedan ampliar o especificar la regulación de protección de datos a las peculiaridades del sector en el que operan, mediante la aprobación de unos Códigos Tipo –art. 32–. Estos establecen unas condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como un conjunto de garantías que contribuyen al respeto a los principios y derechos de protección de datos⁴⁰. De esta manera, se facilita la integración de las disposiciones de la LOPD en el ámbito sanitario, implantando un régimen homogéneo de protección de datos de carácter personal entre los miembros de este sector. Lógicamente, la adhesión al Código Tipo en ningún caso modifica el régimen de obligaciones establecido por la LOPD y por el resto de normativa vigente en materia de protección de datos⁴¹. Como ejemplo de Códigos Tipo para el sector sanitario que figuran inscritos en la Agencia Española de Protección de Datos, hay que destacar los promovidos por el Colegio de Médicos de Madrid así como por agrupaciones empresariales de centros sanitarios catalanes, constituidas en 1977: el Código Tipo de la Agrupación Catalana de Establecimientos Sanitarios (ACES), y el Código Tipo de la Unión Catalana de Hospitales (UCH)⁴². También hay que destacar

³⁹ Distintos autores han afirmado la necesidad de una regulación específica que adapte la normativa general de protección de datos a la realidad sanitaria y que contemple también otras garantías frente al tratamiento de otros datos de salud derivados de la investigación genética, de los avances de la biotecnología y de la clonación terapéutica. Cfr. J. SÁNCHEZ-CARO, de J. SÁNCHEZ-CARO y F. ABELLÁN, *Datos de salud y datos genéticos*, op. cit. y J. M. ÁLVAREZ-CIENFUEGOS SUÁREZ. «La aplicación de la firma electrónica y la protección de datos relativos a la salud», *Revista Actualidad Informática Aranzadi*, abril, 2001, p. 4.

⁴⁰ Cfr. J. RUBÍ NAVARRETE, «Los códigos tipo: la alternativa de la autorregulación», *Actualidad Informática Aranzadi*, núm. 35, 2000.

⁴¹ Cfr. *Memoria de la Agencia Española de Protección de Datos 2002*. Muchas veces el código tipo sirve como una especie de sello de calidad o de acreditación de cumplimiento de la LOPD.

⁴² La Agrupación Catalana de Establecimientos Sanitarios (ACES) es una asociación privada sin ánimo de lucro, integrada por centros y establecimientos sanitarios privados de la Comunidad Autónoma de Cataluña; la Unión Catalana de Hospitales (UCH), es también una asociación empresarial voluntaria de entidades prestadoras de asistencia sanitaria, sociosanitaria y social y de otras entidades proveedoras de bienes y servicios a aquéllas, cuyo ámbito de actuación se limita igualmente a Cataluña.

el Código Tipo del Consejo General de Colegios de Médicos de España y el Código Tipo de Tratamiento de Datos de Carácter Personal para Odontólogos y Estomatólogos de España.

Vamos a analizar seguidamente las exigencias que establecen la Ley 41/2002, de 14 de noviembre y la LOPD a los tratamientos de datos en el ámbito sanitario y muy especialmente a la historia clínica para garantizar la protección de los datos de salud y la confidencialidad de las historias clínicas. Así, vamos a analizar quién es el responsable de las historias clínicas y cuáles son las principales diferencias entre los servicios sanitarios públicos y los servicios sanitarios privados en este ámbito; la finalidad y calidad de la historia clínica, la información y el consentimiento para el tratamiento de datos de salud; la seguridad y la obligación de secreto; y el derecho de acceso, rectificación y cancelación del paciente de los documentos que conforman la historia clínica, así como la tutela de estos derechos.

b) *El responsable de las historias clínicas en los servicios sanitarios públicos y en los servicios sanitarios privados: principales diferencias*

La determinación de quién es el responsable del fichero de historias clínicas o de datos sanitarios es de gran importancia porque será éste el obligado a declarar los ficheros, será ante él ante quien se ejerciten los derechos de acceso, rectificación y cancelación y es también éste quien va a responder ante la posible infracción que se cometa en este ámbito. La Ley 15/1999, de 13 de diciembre, señala que el Responsable del fichero será la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. La legislación propia de la Comunidad de Madrid –la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid– es algo más precisa a este respecto al establecer que cuando no sea posible la determinación del responsable del fichero, por estar atribuidas a diferentes órganos la competencia para decidir sobre la finalidad, contenido y uso del tratamiento, se entenderá por responsable del fichero el órgano titular de la función específica en que se concrete la competencia material a cuyo ejercicio sirva instrumentalmente el fichero –art. 7–. Por tanto, será el órgano titular de la competencia administrativa el que asume la responsabilidad del mismo y el que tienen que establecer los distintos niveles de acceso⁴³.

La Ley 41/2002, de 14 de noviembre, procura aportar luces acerca de quién es el responsable del fichero de historias clínicas. Con anterioridad a la aprobación de esta Ley ha existido una viva polémica sobre de quién era la historia clínica. Unos decían que era una información personal patrimonio del paciente; otros la vinculaban al profesional que era titular de los derechos de propiedad

⁴³ Este es un tema complejo porque verdaderamente quien decide que se traten datos de salud y cuál debe ser su finalidad es principalmente el legislador, no el órgano administrativo.

intelectual al verter en la historia clínica sus propios conocimientos; por último, se mantenía que era del centro que prestaba la asistencia sanitaria⁴⁴. Pues bien, el art. 17.4 de la Ley 41/2002, de 14 de noviembre establece que la gestión de la historia clínica por los centros con pacientes hospitalizados, o por los que atiendan a un número suficiente de pacientes bajo cualquier otra modalidad asistencial, según el criterio de los servicios de salud, se realizará a través de la unidad de admisión y documentación clínica, encargada de integrar en un solo archivo las historias clínicas. Por tanto, la gestión del fichero de historias clínicas le corresponde a las unidades de admisión y documentación clínica. Ahora bien, la custodia de dichas historias clínicas «estará bajo la responsabilidad de la dirección del centro sanitario». Por tanto, en los centros sanitarios corresponde la responsabilidad del fichero de historias clínicas a la dirección del centro⁴⁵. Los profesionales sanitarios que desarrollen su actividad de manera individual son «responsables de la gestión y de la custodia de la documentación asistencial que generen» –art. 17.5 de la Ley 41/2002, de 14 de noviembre–. El responsable del fichero de historia clínica de una consulta individual será del propio profesional sanitario –el dentista, el psiquiatra, el ginecólogo, etc.–⁴⁶. La responsabilidad del fichero de historias clínicas que corresponde a la

⁴⁴ Sirva como ejemplo de la polémica la conferencia que tuve la oportunidad de impartir en el Colegio de Médicos de Zaragoza en el año 2002 en un Seminario que llevaba por título «¿De quién es la historia clínica?». N. DE MIGUEL ha hecho un estudio doctrinal de las tres posturas –«Intimidad e historia clínica», *cit.* p. 28–. Ha defendido la propiedad del centro R. DE ÁNGEL YAGÜEZ, «Problemática de la historia clínica», *Información y Documentación clínica*, 1, *cit.*; la propiedad del médico la ha mantenido R. DE LORENZO, «¿De quién son propiedad las historias clínicas?», *Deontología, Derecho y Medicina*, Ilustre Colegio Oficial de Médicos de Madrid, Madrid, 1997; la propiedad del paciente la ha justificado T. GARCÍA HERNÁNDEZ y B. MARZO MARTÍNEZ, «La propiedad de la historia clínica», *La Ley*, vol. 5, 1996. Una posición integradora ha sido mantenida por C. M. 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*, vol. 1, núm. 1, 1993, pp. 14-15.

⁴⁵ Así, por ejemplo, corresponde a la gerencia de un hospital la responsabilidad de la infracción cuando aparecen historias clínicas abandonadas en la calle, sin perjuicio de eventuales responsabilidades de otros empleados por negligencia grave o mala fe en el desarrollo de sus funciones.

⁴⁶ Un supuesto complicado es el del profesional sanitario individual que alquila un quirófano en un hospital privado para operar, facilitándole también el hospital el anestesista y los cuidados de enfermería. Es razonable considerar que se trata de dos responsables distintos que tienen obligación de conservar información clínica. Tampoco parece descartable que se unifique la información clínica en el profesional sanitario que va a continuar la asistencia, en el marco de un contrato del art. 12 LOPD o con una cesión mediante consentimiento expreso del paciente. Otro supuesto difícil es el de los facultativos que ejercen en un centro sanitario privado. Está claro que si media una relación laboral o un arrendamiento de servicios –en virtud del cual existe una relación de dependencia entre el centro sanitario y el facultativo–, la responsabilidad de la historia clínica sería del centro sanitario, existiendo una relación asistencial entre el paciente y el centro. Un facultativo no puede dejar un centro médico –con el que mantiene una relación laboral y mercantil– y llevarse las historias clínicas a otro centro donde pretende continuar desarrollando la actividad asistencial. El centro médico es el responsable de las historias clínicas y tiene una obligación de custodia. Deben ser los pacientes –que lo deseen– los que soliciten una copia de la historia clínica para cambiar de centro médico y de facultativo. O puede ser el mismo médico el que traslade la solicitud con el consentimiento expreso del paciente. En el supuesto de que el centro sanitario se limita a alquilar las consultas a los facultativos, no existiría una relación de dependencia entre el centro sanitario y los facultativos que en el desarrollan su actividad profesional; se trataría, entonces, de un facultativo que ejerce la profesión de manera individual y que sería responsable de las historias clínicas de los pacientes, teniendo con estos directamente una relación asistencial. Por último, los profesionales sanitarios privados que atiendan a los asegurados de una compañía aseguradora sanitaria no mantienen con ésta una relación de dependencia y son los responsables de las historias clínicas de sus pacientes. Cualquier transmisión de información personal a estas compañías debe ser considerada una cesión de datos personales. *Cfr. infra* apdo. 3.c).

dirección del centro sanitario no tiene que hacer olvidar que la cumplimentación de la historia clínica, en los aspectos relacionados con la asistencia directa al paciente, será responsabilidad de los profesionales que intervengan en ella, que tienen el deber de custodiar adecuadamente las historias clínicas que manejen así como cooperar en la creación y mantenimiento de una documentación clínica ordenada y secuencial del proceso asistencial de los pacientes –arts. 15.3 y 17.3 de la Ley 41/2002, de 14 de noviembre–. En todo caso, cuando se pierden historias clínicas o aparecen abandonadas por la calle la responsabilidad corresponde a la dirección del centro sanitario –habitualmente al gerente–, aunque haya sido un empleado del hospital el que haya actuado indebidamente o haya incumplido una medida de seguridad. La responsabilidad en el procedimiento de infracción de protección de datos es objetiva⁴⁷, sin perjuicio de las actuaciones disciplinarias o del ejercicio de una acción penal o civil contra quién haya cometido la infracción. Por tanto, hay que dejar de debatir de quién es la historia clínica. Posiblemente la propiedad de la misma le corresponda al centro⁴⁸, el profesional sanitario mantiene sus derechos de propiedad intelectual en el ámbito de la relación laboral⁴⁹ y de intimidad en la notas subjetivas y el paciente tiene derecho de acceso a la documentación clínica y a obtener una copia de los datos que figuren en ella.

Determinado ya quién es el responsable del fichero de historias clínicas, es conveniente recordar que existen diferencias en la regulación jurídica de protección de datos entre ficheros públicos y ficheros privados, y, por tanto, entre los ficheros de los servicios sanitarios públicos y de los servicios sanitarios privados. Los ficheros públicos sanitarios se benefician de un conjunto de excepciones a los principios de protección de datos⁵⁰. Así, no es necesario el consentimiento para el tratamiento de datos para funciones administrativas –art. 6.2 LOPD–. Las Administraciones Públicas pueden llevar a cabo cesiones de datos personales para fines históricos, estadísticos o científicos –art. 11.2.e) LOPD–. Los centros públicos sanitarios tienen más posibilidades de compartir información personal en virtud del art. 21 LOPD que permite la comunicación de datos entre Administraciones Públicas para el ejercicio de competencias semejantes o de competencias que versen sobre las mismas materias, así como para la comunicación de datos de carácter personal que una

⁴⁷ Título VII «Infracciones y sanciones», arts. 43-49 LOPD. N. DE MIGUEL –*op. cit.* p. 314– ha señalado que la lesión que se produce a raíz del quebrantamiento del deber de secreto médico es imputable a la Administración cuando tiene lugar en un centro sanitario público, pues se produce en el marco de un servicio de estas características y, por tanto, se ha de responder en términos objetivos.

⁴⁸ La Ley 3/2001 de la Comunidad de Galicia, reguladora del consentimiento informado y de la historia clínica de los pacientes afirma: «Las historias clínicas son documentos confidenciales propiedad de la Administración sanitaria o entidad titular del centro sanitario, cuando el médico trabaje bajo la dependencia de una institución sanitaria. En caso contrario, la propiedad corresponderá al médico que realice la atención sanitaria».

⁴⁹ *Cfr.* A. VALDÉS ALONSO, *Propiedad intelectual y relación de trabajo*, Civitas, Madrid, 2001.

⁵⁰ *Cfr.* más ampliamente el *Manual de Protección de Datos para las Administraciones Públicas*, Civitas-APDCM, 2003, pp.

Administración Pública obtenga o elabore con destino a otra⁵¹. Esto permite, por ejemplo, las cesiones de datos sobre listas de espera entre los distintos hospitales y la propia Consejería de sanidad, etc. Los centros públicos estarán obligados a seguir la legislación más exigente en cuanto a la creación, modificación y supresión de ficheros, consecuencia lógica de las ventajas antes citadas de los tratamientos de datos realizados por las Administraciones Públicas. Mientras que los ficheros de centros sanitarios privados se crean a través de la notificación previa a la Agencia Española de Protección de Datos –art. 25 LOPD–, los ficheros de centros públicos sanitarios deben de crearse, modificarse o suprimirse a través de una disposición de carácter general y ser publicados en el Diario Oficial correspondiente –art. 20 LOPD–. Es una consecuencia de que la Administración Pública debe actuar siempre en virtud del principio de legalidad, vinculada positivamente –no solo negativamente– al derecho –positive bindung-. Además, si el régimen de infracciones es semejante –art. 43-44 LOPD–, no lo es el régimen sancionador. Así, las sanciones para los responsables de ficheros privados son económicas –desde 600 a 60.000 euros para infracciones leves, hasta 300.000 euros por infracciones graves, y hasta 600.000 euros por infracciones muy graves, como señala el art. 45 LOPD, sanciones que son acumulativas en el caso de que concurren varias infracciones distintas–; en cambio, la infracciones cometidas por responsables de ficheros públicos lleva aparejada, como señala el art. 46 LOPD, una resolución de infracción administrativa, el establecimiento de medidas para que cesen o se corrijan los efectos de la infracción, la notificación al responsable del fichero y a su superior jerárquico, la propuesta de iniciación de actuaciones disciplinarias y la comunicación al Defensor del Pueblo. Es decir, la Agencia de Protección de Datos no impone una sanción económica a un responsable de un fichero público, lo que sí hace con los responsables de los ficheros privados, ya que la sanción económica es costosa siempre para una entidad privada mientras que para la Administración Pública supone únicamente una redistribución de créditos o una modificación presupuestaria. Eso no obsta para que el ciudadano pueda ejercer el derecho a la indemnización cuando, como consecuencia de una infracción, sufra un daño o lesión en sus bienes o derechos –art. 19 LOPD–. La responsabilidad patrimonial del responsable de un fichero de titularidad pública se exigirá, de conformidad con el régimen de responsabilidad patrimonial de las Administraciones Públicas, ante la Jurisdicción Contencioso-Administrativa⁵². La declaración de una infracción a una Administración Pública supone un coste a veces mayor que el coste económico que es el político. Por último, la competencia para controlar los fiche-

⁵¹ La aplicación a los datos de salud de las excepciones al consentimiento para las cesiones –art. 11 LOPD– y para las comunicaciones de datos entre Administraciones Públicas –art. 22.1 LOPD– es una cuestión compleja que abordaremos posteriormente –*infra* 2.d) y 3.c)–.

⁵² Arts. 139-144. Cfr. J. GONZÁLEZ PÉREZ y F. GONZÁLEZ NAVARRO, *Comentarios a la Ley de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común*, I, 3.º ed, Cívitas, Madrid, 2004, pp. 3055 y ss.

ros de la Administración Pública sanitaria le corresponde a las Autoridades de Control de las Comunidades Autónomas, en el supuesto de que estén creadas. En cambio, los ficheros de los centros sanitarios privados son controlados como regla general a la Agencia Española de Protección de Datos –art. 41 LOPD–⁵³.

No siempre es fácil la delimitación entre Administración Pública y empresa privada para delimitar el régimen jurídico de los ficheros, dado el carácter público-privado en el que se desenvuelve la actividad sanitaria y el recurso cada vez más frecuente a la forma jurídica o al régimen jurídico privado para el desarrollo de la actividad de la Administración Pública, un hecho que ha sido calificado como de «huida al derecho privado»⁵⁴. El régimen jurídico de los ficheros públicos se aplica cuando se utilizan los siguientes conceptos: «funciones propias de las Administraciones Públicas en el ámbito de sus competencias» –art. 6 LOPD–, «las Administraciones Públicas» –art. 20 LOPD–, «Administraciones Públicas para el desempeño de sus atribuciones» y «para el ejercicio de competencias» –art. 21 LOPD– y a las Administraciones Públicas –art. 46 LOPD–. En la actualidad, la Administración sanitaria se caracteriza por el incremento de la gestión indirecta de los centros –especialmente hospitales–, a través de distintas técnicas contractuales –concesión, concierto– que atribuye la responsabilidad de su prestación a los particulares. En este supuesto nos encontramos con entidades privadas a las que hay que aplicar el régimen jurídico de los ficheros privados⁵⁵. La gestión directa centralizada de los centros sanitarios y hospitales da lugar, en cambio, a ficheros públicos. El problema estriba en la gestión directa descentralizada. En virtud de la Ley 8/2001, de 13 de junio, de Protección de Datos de Carácter Personal en la Comunidad, es la elección de la forma jurídica la que determina el régimen jurídico de los ficheros, esto es, la utilización de una forma jurídica privada –la de sociedad mercantil– para gestionar la sanidad daría lugar a ficheros privados mientras que la elección de una forma jurídica pública –la de Ente Público–, aunque recurra al Derecho privado, daría lugar a ficheros públicos⁵⁶.

⁵³ Esta es una cuestión bastante compleja. Me remito a lo expuesto en A. TRONCOSO REIGADA, *Las Comunidades Autónomas y la protección de datos personales*, Civitas, Madrid, 2006.

⁵⁴ Cfr. A. TRONCOSO REIGADA, *Privatización, Empresa Pública y Constitución*, Marcial Pons, Madrid, 1997.

⁵⁵ La reforma de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, mediante Ley 4/1999, ha resuelto el problema de la responsabilidad de los centros concertados, exigible en función de la Disposición Adicional duodécima en los mismos términos que para los centros públicos. Cfr. N. DE MIGUEL, *cit.* p. 314.

⁵⁶ El 2.1 de la Ley 8/2001, de 13 de julio de Protección de Datos de Carácter Personal en la Comunidad de Madrid atribuye a la Agencia Autonómica el control de los ficheros de todos los entes públicos, aunque recurran al Derecho privado, pero excluye el de las sociedades mercantiles: «1. La Agencia de Protección de Datos de la Comunidad de Madrid ejerce sus funciones de control sobre los ficheros de datos de carácter personal creados o gestionados por las Instituciones de la Comunidad de Madrid y por los Órganos, Organismos, Entidades de Derecho público y demás Entes públicos integrantes de su Administración Pública, exceptuándose las sociedades mercantiles a que se refiere el artículo 2.2.c).1 de la Ley 1/1984, de 19 de enero, reguladora de la Administración Institucional de la Comunidad de Madrid». Por tanto, las Entidades de Derecho público con personalidad jurídica propia que por la naturaleza de su actividad y en virtud de ley, hayan de ajustar sus actividades al ordenamiento jurídico privado son competencia de la

La utilización del derecho privado en la actividad no debe ser elemento constitutivo del carácter público o privado del responsable. Es claro que un Ente público no es un responsable privado de datos personales⁵⁷. La LOPD en los preceptos antes señalados en ningún momento exige el recurso al derecho administrativo o el ejercicio de potestades de derecho público para considerar un fichero como público. Sólo debe aplicarse el correctivo funcional del ejercicio de potestades de derecho público para considerar un fichero como público en el caso de los Colegios Profesionales, dado su carácter mixto o bifronte de Administración Corporativa que desarrolla funciones públicas y de asociación de particulares. Es frecuente que la Administración Pública y que las propias Autoridades de Control desarrollen parte de su actividad recurriendo al régimen jurídico privado sin que por ello sus ficheros sean privados. Especial complejidad presenta la figura de las fundaciones públicas sanitarias⁵⁸. Por tanto, la decisión que adopte la Administración Sanitaria en relación con la forma o el régimen jurídico de nuevos hospitales y centros sanitarios tiene consecuencias en relación con la aplicación de la normativa de protección de datos personales.

c) *Finalidad y calidad de la historia clínica. La historia clínica como derecho del paciente. La centralización de las historias clínicas y su conservación*

El primer principio es el principio de calidad de los datos, desarrollado en el art. 4 de la Ley 15/1999, de 13 de diciembre. Este principio exige –de manera resumida– que la información personal que se recoja sea adecuada, pertinente y no excesiva de acuerdo con una finalidad legítima; que la recogida de los datos no se produzca de manera fraudulenta o ilícita; que durante la vida del fichero, los datos se mantengan exactos, se almacenen de manera que se permita el ejercicio del derecho de acceso y sean tratados para la finalidad para la cual fueron recabados; por último, que los datos se cancelen cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que han

Agencia de Protección de Datos de la Comunidad de Madrid. Sólo tendrían la consideración de ficheros privados a tenor de la Ley 8/2001, de 13 de julio, y por tanto no serían competencia de la Agencia de Protección de Datos de la Comunidad de Madrid las empresas públicas que tengan la forma jurídica de sociedades anónimas en cuyo capital sea mayoritaria, directa o indirectamente, la participación de la Comunidad de Madrid. Las Fundaciones Sanitarias no tienen ese carácter de sociedades mercantiles.

⁵⁷ No obstante, hay que señalar que el Proyecto de Reglamento de desarrollo de la LOPD actualmente en tramitación sólo considera como ficheros públicos los entes públicos sometidos al derecho administrativo.

⁵⁸ El art. 111 de la Ley 50/1998, de 30 de diciembre, de Medidas Fiscales, Administrativas y de Orden Social define a las Fundaciones Públicas Sanitarias como «organismos públicos, adscritos al Instituto Nacional de Salud» –art. 2–. De hecho, el art. 3.2 del Decreto de 29 de enero de 2004 que establece la estructura orgánica de la Consejería de Sanidad establece que «La Administración Institucional adscrita a la Consejería de Sanidad y Consumo estará integrada por los siguientes Entes Públicos y Organismos Autónomos: Ente Público Fundación Hospital de Alcorcón». A nuestro parecer, la Fundación Hospital Alcorcón sería una persona jurídico-pública por lo que sus ficheros tendrían la consideración de ficheros públicos. Sin embargo, para la Agencia Española –Informe 66/2003 publicado en su web– estos ficheros son privados al no ejercer estas fundaciones potestades de derecho público, en virtud del arto 46.1.a) de la Ley 50/1992, de Fundaciones.

sido recabados. El principio de calidad también protege la confidencialidad de la información clínica, evitando que se traten datos excesivos en relación con una finalidad concreta⁵⁹.

La Ley 41/2002, de 14 de noviembre, lleva a cabo una interesante adaptación del principio de calidad en lo relativo al fichero de historias clínicas. Lo primero que hace esta Ley es definir la finalidad de la historia clínica pues es la finalidad lo que delimita la legitimidad del tratamiento. Pues bien, la historia clínica tiene «como fin principal facilitar la asistencia sanitaria» –art. 5–. Igualmente se señala que la historia clínica «es un instrumento destinado a garantizar una asistencia adecuada al paciente... –art. 16.1–. Queda claro que la historia clínica se redacta y se conserva para facilitar la asistencia sanitaria y no para otras finalidades. No obstante, el art. 4.2 LOPD señala que si bien los datos de carácter personal no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos, «no se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos». El art. 6 de la Ley General de Sanidad señala que las actuaciones de las Administraciones Públicas Sanitarias están orientadas a garantizar que cuantas acciones sanitarias se desarrollen estén dirigidas a la prevención de las enfermedades y no sólo a la curación de las mismas por lo que los datos personales que se recaben en el proceso asistencial, además de servir para la curación del paciente, tiene otros fines como los epidemiológicos, de investigación o dolencia⁶⁰. En esta dirección se considera uso legítimo de la historia clínica el acceso con fines epidemiológicos, de salud pública, de investigación o docencia, si bien se exige como regla general la separación de los datos personales de los de carácter clínico asistencial, de manera que quede asegurado el anonimato del paciente –art. 16.3 Ley 41/2002, de 14 de noviembre–. Por tanto, otras finalidades como la investigación científica o la epidemiología son compatibles y tienen un carácter complementario pero no son la principal finalidad de la historia clínica que es básicamente un instrumento para la asistencia sanitaria. El principio de calidad, como principio de adecuación y pertinencia, exige que el tratamiento de historias clínicas con finalidad epidemiológica, de investigación o de docencia se haga como regla general disociando previamente la información personal.

⁵⁹ Así, si la finalidad del tratamiento es la comunicación con el paciente, no sería necesario incluir en el remite de las cartas dirigidas a los pacientes referencias al Centro Sanitario concreto -Hospital Psiquiátrico- o a la especialidad –Servicio de Oncología–, ya que esto permite el conocimiento de la enfermedad por terceras personas –conserje, vecinos, empleado de correos–. Lo mejor en estos casos es incluir en el remite una referencia más general o una abreviatura. Así, por ejemplo, en relación con la citación de pacientes por SMS, y dado también el problema de seguridad de las comunicaciones, lo adecuado es que el mensaje le recuerde la fecha de consulta o de la práctica de la prueba, sin contener ninguna información relativa a la salud y con una abreviatura relativa al servicio sanitario. Igualmente, si los familiares que acompañan a un paciente ingresado piden justificantes por motivos laborales de la estancia en el centro es necesario el consentimiento del paciente y el justificante debe contener los datos mínimos. En el caso de que el paciente no pueda prestar su consentimiento, como veremos más adelante, se debe comprobar la existencia de una relación familiar o de hecho.

⁶⁰ Cfr. A. IGUALADA, «El uso de la documentación clínica en actividades distintas de la específica prestación asistencial», *Revista datospersonales.org* núm. 5, 2003.

No basta con cumplir la finalidad para respetar el principio de calidad. Hace falta, además, que se tratan únicamente aquellos datos adecuados y pertinentes para las finalidades explícitas y legítimas para las que se hayan obtenido, no pudiendo tratarse datos no adecuados o excesivos⁶¹. La Ley 41/2002, de 14 de noviembre delimita cuáles son los datos adecuados, pertinentes y no excesivos que deben constar en la historia clínica⁶². Esta Ley afirma que la historia clínica debe comprender el conjunto de los documentos relativos a los procesos asistenciales de cada paciente —art. 14.1—. Así, se señala que la historia clínica incorporará «todos aquellos datos que bajo criterio médico permitan el conocimiento veraz y actualizado del estado de salud del paciente»⁶³. El contenido mínimo de la historia clínica será el siguiente: documentación relativa a la hoja clínico-estadística, autorización de ingreso, informe de urgencia, anamnesis y exploración física, evolución, órdenes médicas, hojas de íter consulta, informes de exploraciones complementarias, consentimiento informado, informe de anestesia, informe de quirófano o de registro de parto, informe de anestesia patológica, evolución y planificación de cuidados de enfermería, aplicación terapéutica de enfermería, gráfico de constantes e informes clínicos de alta —art. 15.2—⁶⁴. La historia clínica no contiene únicamente información personal del paciente; también recoge la identificación de los médicos y de los demás profesionales que han intervenido en los procesos asistenciales —art. 14.1—⁶⁵. Este no tiene un derecho al anonimato, sin perjuicio del derecho de oposición cuando existan motivos fundados y legítimos —art. 6.4 LOPD—, por ejemplo, de seguridad, en cuyo caso se excluirá los datos relativos al facultati-

⁶¹ El principio de calidad en la toma de muestras biológicas exige que se haga de la manera menos intrusiva posible y con el mayor respeto a la intimidad de las personas. Esta cuestión la hemos analizado en «Ficheros de perfiles de ADN y derecho fundamental a la protección de datos personales», *cit.* Lo mismo aparece en la Ley Orgánica de Protección de la Salud y de la Lucha contra el Dopaje en el Deporte en relación con la toma de muestras de orina, sangre o cualquier fluido o muestra corporal.

⁶² La historia clínica ha sido también repetidamente estudiada en los distintos Congresos Nacionales de Derecho Sanitario que celebra la Asociación Española de Derecho Sanitario y que publica la Fundación Mapfre Medicina. *Cfr.* también las Actas del Congreso organizado por el Ministerio de Sanidad y Consumo y el Consejo General del Poder Judicial y celebrado el 22-23 de septiembre de 1997, en AA.VV., *Información y documentación clínica*, Madrid, 1997, Sobre la historia clínica y su acceso, *cf.* J. SÁNCHEZ-CARO y F. ABELLÁN, *La historia clínica*, Fundación Salud, 2000, pp. 37-59.

⁶³ *Cfr.* J. SÁNCHEZ-CARO y F. ABELLÁN, *La Historia Clínica*, *cit.* pp. 11-12.

⁶⁴ No obstante, muchas leyes autonómicas han aumentado este contenido mínimo. *Cfr.* la Ley 21/2000, de 29 de diciembre, de la Comunidad Autónoma de Cataluña, sobre los derechos de información relativos a la salud, la autonomía del paciente y la documentación clínica; la Ley 3/2001, de 28 de mayo, de la Comunidad Autónoma de Galicia, reguladora del consentimiento informado y de la historia clínica de los pacientes; la Ley 6/2002, de 15 de abril, de Salud de Aragón; la Ley Foral 11/2002, de 6 de mayo de Navarra, sobre los derechos del paciente a las voluntades anticipadas, a la información y a la documentación clínica; o la Ley 1/2003, de 28 de enero, de la Comunidad Autónoma de Valencia de derechos e información al paciente.

⁶⁵ Por tanto, debe saberse quién ha hecho cada anotación en la historia clínica. Además, la Ley 44/003, de 21 de noviembre, de ordenación de las profesiones sanitarios establece que los profesionales y los responsables de los centros sanitarios facilitarán a sus pacientes el ejercicio del derecho a conocer el nombre, la titulación y la especialidad de los profesionales sanitarios que les atienden —art. 5.e)—. En todo caso, en virtud del principio de calidad, no hace falta incluir en la historia clínica de un paciente datos que indiquen que se le ha tratado en un servicio de sanitario de ámbito penitenciario.

vo. Sin embargo, las notas subjetivas de los médicos no forman parte de la historia clínica, aunque no siempre sea fácil su delimitación, como más adelante señalaremos. La documentación administrativa como documentos contables, datos económicos, hojas de admisión u hojas de cita tampoco deben constar en la historia clínica no sólo porque no reflejan una información sobre el estado de salud del paciente, sino también porque facilita el acceso a la historia de personal ajeno a las profesiones sanitarias⁶⁶. El principio de calidad prohíbe la recogida de datos de manera desleal, fraudulenta o ilícita –art. 4.7 LOPD–. En esta dirección, el Grupo Europeo de Ética antes citado ha afirmado la prioridad de la obtención de los datos a través del propio interesado y no por medio de terceras personas⁶⁷.

Es importante resaltar que la Ley 41/2002, de 14 de noviembre, incluye además un deber nuevo de tratamiento de datos por parte del facultativo. Así, el art. 15 señala que «la historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. Todo paciente tiene derecho a que quede constancia, por escrito o en soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales realizados por el servicio de salud, tanto en el ámbito de la atención primaria como de atención especializada». De esta forma, todo profesional que intervenga en la actividad asistencial está obligado al cumplimiento de los deberes de información y documentación clínica –art. 2.6–. La cumplimentación de la historia clínica, en los aspectos relacionados con la asistencia directa al paciente, será responsabilidad de los profesionales que intervengan en ella –art. 15.3–. No hay opción, hay un deber de todo profesional sanitario de hacer historia clínica⁶⁸. Por tanto, hay que hacer historia clínica en todo el proceso asistencial, tanto en la urgencia, como en atención primaria y en atención especializada. Hay que hacer historia clínica sea cual sea la presión asistencial, desde el inicio al final del proceso, obligación que se extiende también a los servicios sanitarios privados⁶⁹. El hecho de que el principio de calidad de los datos implique en el ámbito sanitario el derecho de todo paciente a que en su historia clínica consten todos los datos que reflejen su estado de salud es una buena muestra de que la protección de datos

⁶⁶ El Código de Ética y Deontología Médica, de 10 de septiembre de 1999 señala que los sistemas de informatización utilizados en las instituciones sanitarias mantendrán una estricta separación entre la documentación clínica y la documentación administrativa.

⁶⁷ En esta dirección hay que señalar que la Ley 41/2002, de 14 de noviembre, establece el deber de pacientes y usuarios de facilitar los datos sobre su estado físico o su salud, de manera «leal» y verdadera, lo que facilita la calidad de la historia clínica.

⁶⁸ De igual forma, la Ley Orgánica de Protección de la Salud y de Lucha contra el Dopaje en el Deporte obliga a los equipos a llevar un libro en el que hacen constar los tratamientos médicos y sanitarios prescritos a los deportistas.

⁶⁹ El cumplimiento de este deber de información y documentación clínica suele cumplirse más en los servicios sanitarios públicos que en los servicios sanitarios privados. Téngase en cuenta que la ausencia de medios no suprime el derecho de los pacientes. Es verdad que en muchas ocasiones las historias clínicas pierden su dimensión asistencial y tienden a ser defensivas –como correlato de la medicina defensiva– para evitar posibles demandas posteriores.

personales tiene perfiles diferenciados del derecho a la intimidad del paciente ya que éste último implica una voluntad de poner límites a las intromisiones ilegítimas en la esfera privada. La obligación de hacer historia clínica y, por tanto, el principio de calidad de los datos, es, en este caso un instrumento de garantía de otro derecho fundamental como es el derecho a la vida y a recibir una adecuada asistencia sanitaria.

El principio de calidad exige también la plenitud y exactitud de la información clínica. La historia clínica de un paciente no cumple el principio de calidad si no es completa, es decir, si no contiene todos los documentos con los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial. Por ello, la Ley 41/2002, de 14 de noviembre señala que la historia clínica de cada paciente debe tener «la máxima integración posible de la documentación clínica de cada paciente, al menos en el ámbito de cada centro» –art. 14–⁷⁰. No basta con que toda la documentación clínica de un paciente se encuentre dentro de su historia clínica, hace falta también que se encuentre ordenada. Como hemos señalado antes, los profesionales deben cooperar en el mantenimiento de una documentación clínica secuencial y ordenada del proceso asistencial de los pacientes –art. 17.3–. La mejor forma de tener una historia clínica completa de cada paciente es que ésta se gestione en un solo archivo. La Ley 41/2002, de 14 de noviembre, señala que la historia clínica «se llevará con criterios de unidad e integración, en cada institución asistencial como mínimo, para facilitar el mejor y más oportuno conocimiento por los facultativos de los datos de un determinado paciente en cada proceso asistencial» –art. 15.4–. El legislador considera la centralización de las historias clínicas como un medio para la mejora de la asistencia⁷¹. Por ello, los centros hospitalarios o aquellos que atiendan a un número suficiente de pacientes bajo cualquier modalidad asistencial deben integrar las historias clínicas en un solo archivo, que como hemos señalado antes, debe ser gestionado por la unidad de admisión y documentación clínica –art. 17.4–. La centralización y la informatización de las historias clínicas es un proyecto que se está extendiendo en todos los servicios de salud ya que permite un mejor acceso de los profesionales sanitarios que deben prestar la asistencia a la información relevante del estado de salud del paciente, evitando la reiteración de pruebas diagnósticas. Por tanto, es necesario integrar toda la documentación clínica de un paciente en su historia clínica y todas las historias clínicas en un solo archivo. La integración de las historias clínicas en un solo archivo no es sólo la mejor forma de garantizar la plenitud y exactitud de las historias, es también una medida que favorece su seguridad –como señalaremos más adelante– y el ejercicio del derecho de acceso.

⁷⁰ El informe del Grupo de Expertos del SNS ya puso de relieve la necesidad de garantizar el principio de historia clínica única, que estaba ya recogido en el 61 LGS.

⁷¹ El art. 61 LGS señalaba que «en cada área de salud debe procurarse la máxima integración de la información relativa a cada paciente, por lo que el principio de historia clínica-sanitaria única por cada uno deberá mantenerse, al menos, dentro de los límites de cada institución asistencial».

No olvidemos que el principio de calidad exige que los datos sean almacenados de manera que se facilite el ejercicio del derecho de acceso –art. 4.6 LOPD–⁷².

Por último, la Ley 41/2002, de 14 de noviembre, define cuándo la documentación clínica ha dejado de ser necesaria o pertinente y es posible su cancelación⁷³. Si hasta ahora no existía certeza jurídica sobre cuándo la documentación clínica ha dejado de ser necesaria o cuándo puede ser cancelada, esta Ley establece un plazo *básico* de custodia de la documentación clínica –art. 17–. Los centros sanitarios están obligados a conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en su soporte original, «durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial». Es decir, el tiempo de conservación no son cinco años ya que éste sería el mínimo. De hecho, algunas Comunidades Autónomas han ampliado este plazo legal, regulando incluso la conservación de la historia clínica de fallecidos⁷⁴. Existe una obligación de conservar la documentación clínica durante el tiempo necesario en cada caso porque hay procesos asistenciales que justifican el mantenimiento de la documentación clínica –los oncológicos– y otros que no –una apendicitis–. Por tanto, el principio de calidad implica el expurgo y la destrucción de aquellos documentos e informaciones que forman parte de la historia clínica y que ya no son necesarios⁷⁵. No tiene sentido, por ejemplo, que en una historia clínica conste que a una mujer se le dispensó una píldora del día hace varios años⁷⁶. No obstante, en el ámbito sanitario la cancelación de los datos sanitarios no está exenta de algunos inconvenientes derivados de la necesidad de conservar información para poder realizar estudios genéticos, epidemiológicos y de salud pública. En este sentido, el art. 5.4 LOPD señala que «reglamentariamente se determinará el procedimiento por el que, por

⁷² No tendría sentido, por ejemplo, que el ejercicio del derecho de acceso por parte de un paciente obligue al personal del hospital a cuatro horas de «pantallazos» y a múltiples impresiones, y que esto al final resulte, además, incompleto.

⁷³ *Cfr. infra 2.1).*

⁷⁴ Así, la Ley 21/2000, de 29 de diciembre, de la Comunidad Autónoma de Cataluña, sobre los derechos de información relativos a la salud, la autonomía del paciente y la documentación clínica indica que la historia se ha de conservar un mínimo de 20 años desde la muerte del paciente. Sin embargo, se pueden seleccionar y destruir los documentos que no son relevantes para la asistencia transcurridos diez años desde la última atención al paciente. La Ley 3/2001, de 28 de mayo, de la Comunidad Autónoma de Galicia, reguladora del consentimiento informado y de la historia clínica de los pacientes establece la conservación por tiempo indefinido de determinada información –entre la que se encuentran informes de alta, hojas de consentimiento informado– y para el resto de un mínimo de cinco años tras la última asistencia prestada al paciente o desde su fallecimiento. La Ley 1/2003 de la Comunidad valenciana, determina que los documentos se conservarán como mínimo cinco años a partir de la fecha del último episodio asistencial en el que el paciente haya sido atendido o desde su fallecimiento; los documentos especialmente relevantes se conservarán indefinidamente o por el tiempo que fije la normativa vigente al respecto, mientras que las historias clínicas que sean prueba en un proceso judicial se conservarán hasta la finalización del mismo.

⁷⁵ Un buen criterio de expurgo se encuentra en el documento preparado por el Grupo de Expertos en Información y Documentación Clínica.

⁷⁶ De hecho, a nuestro juicio, esta información clínica debe ser cancelada mucho antes del plazo básico de cinco años, exactamente a partir de la fecha en que la administración de otra píldora no afecta a su salud.

excepción, atendidos valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos»⁷⁷. Los fines de la historia clínica distintos a los asistenciales como los epidemiológicos y de investigación requieren un mantenimiento más amplio de la documentación clínica, aunque, como hemos señalado antes, esto debe hacerse preferentemente a través de un procedimiento disociado, que evite la identificación de las personas afectadas. Una de las razones para la cancelación de la documentación clínica es la dificultad que supone su almacenamiento en condiciones que garanticen su seguridad. Por ello, la historia clínica electrónica va a favorecer la potencialidad científica y de salud pública de esta información personal. Hay información clínica cuya conservación al principio puede no parecer necesaria pero el tiempo ha demostrado su utilidad⁷⁸. La documentación clínica se conservara también a efectos judiciales.

d) *La información y el consentimiento para el tratamiento de datos de salud*

El principio de información en la recogida de datos personales obliga a informar a los interesados a los que se les solicita datos, de «manera expresa, precisa e inequívoca», de la existencia de un fichero, de la finalidad, de los destinatarios de la información, del carácter obligatorio o facultativo de la respuesta, de las consecuencias de la obtención de los datos y de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y de la identidad y dirección del responsable del tratamiento –art. 5 LOPD–. El derecho a la información en la recogida de los datos –como así lo denomina el art. 5 LOPD– trata de dar a la persona un conocimiento y, por tanto, un control sobre sus datos personales, de manera que pueda –en su caso– prestar el consentimiento para el tratamiento y ejercer sus derechos. Este es distinto del derecho a la información asistencial –art. 4 Ley 41/2002, de 13 de noviembre– que atribuye a los pacientes el derecho a conocer, con motivo de cualquier actuación en el ámbito de su salud, toda la información disponible sobre la misma y, como mínimo, la finalidad y naturaleza de cada intervención, sus riesgos y consecuencias. El debate durante los últimos años sobre el consentimiento informado y la preocupación por el respeto a la libre decisión de los pacientes han servido sin duda para garantizar una cierta información al paciente sobre su estado de salud⁷⁹. En todo caso, el

⁷⁷ La Ley 21/2000, de 29 de diciembre, de la Comunidad Autónoma de Cataluña autoriza la conservación de aquella información que, a juicio del facultativo, sea relevante a efectos preventivos, asistenciales o epidemiológicos.

⁷⁸ Cf. *infra* 3.c). Piénsese en pacientes que han fallecido antes de que se conociera la enfermedad –por ejemplo, de VIH, que hayan sido donantes, etc.–.

⁷⁹ Sin embargo, el consentimiento informado no sólo ha servido para garantizar un mayor conocimiento por parte del paciente de su situación; ha sido también en ocasiones un instrumento de los profesionales para exonerarse de responsabilidad ante eventuales reclamaciones judiciales, obteniendo la firma del paciente con anterioridad al proceso asistencial sin garantizar debidamente el derecho a recibir información asistencial. Cf. A. PELAYO GONZÁLEZ-TORRE, *La intervención jurídica de la actividad médica*, cit.

derecho a recibir una información sanitaria es algo más amplio que un instrumento para el consentimiento informado, que se desarrolla casi siempre de manera oral y que no incluye el acceso a su historia clínica. En lo que a nosotros atañe, hay que distinguir la información para el tratamiento de datos de salud de la información asistencial. La primera es una información que forma parte del contenido esencial del derecho fundamental a la protección de datos personales; la segunda es una información que facilita la autonomía del paciente en los distintos tratamientos médicos. La información en la recogida de datos se hace como regla general por escrito a través de una leyenda informativa en el mismo soporte en el que se recogen los datos ya que es la mejor forma de garantizar la información expresa, precisa e inequívoca y de asegurar la prueba. En cambio, la información asistencial como regla general, se proporciona verbalmente, dejando constancia en la historia clínica.

El cumplimiento del principio de información en la recogida de los datos es un buen ejemplo de la dificultad de adaptar las exigencias de la legislación de protección de datos personales a las peculiaridades propias de la realidad sanitaria. Así, este principio general de información expresa, precisa e inequívoca para el tratamiento de los datos personales debe ser armonizado con las exigencias del normal funcionamiento de la actividad sanitaria, de manera que no todos los actos asistenciales repetitivos o múltiples requieran la aplicación formal de este principio. De hecho, no será preciso informar acerca del carácter obligatorio o facultativo de la respuesta, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos y de la posibilidad del ejercicio de los derechos si se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban –art. 5.3 LOPD–. En muchas ocasiones, el cumplimiento de este principio de información podría llevarse a efecto por escrito en el momento de la entrada en el sistema sanitario bajo diferentes formas –por ejemplo, con el envío de la tarjeta sanitaria individual en los servicios públicos o privados–. También se puede facilitar esta información por escrito con el informe de alta de urgencia. La información del art. 5 LOPD puede venir incorporada a la petición del consentimiento informado, diferenciando la conformidad –después de recibir la adecuada información asistencial– para una actuación que afecta a la salud del principio de información de protección de datos personales. En otras ocasiones, habrá que acudir a carteles informativos en sala de espera. La información del tratamiento de imágenes en los hospitales por motivos de seguridad se hace a través de carteles. Corresponde al responsable del fichero la prueba del cumplimiento del principio de información –como señala el proyecto de Reglamento que desarrolla la LOPD–⁸⁰. En todo caso no es necesario informar en cada uno de las sucesivas recogidas de datos personales ya que esto podría burocratizar en

⁸⁰ Si la asistencia sanitaria se ha producido de manera telefónica, la información puede probarse mediante la grabación.

exceso del sistema sanitario y dificultar la gestión asistencial⁸¹. Lógicamente, si se van a utilizar los datos para una finalidad distinta hay que volver a informar. Por último, hay que recordar la posibilidad de exoneración del deber de información cuando los datos de carácter personal no hayan sido recabados del interesado y el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias –art. 5.5 LOPD–.

El consentimiento inequívoco del afectado tanto para el tratamiento de datos personales –art. 6 LOPD– como para la comunicación de datos a un tercero –art. 11 LOPD– es principio esencial de la protección de datos, que también es definido como un derecho a la autodeterminación informativa. Los datos de salud, como hemos señalado antes, son datos íntimos, vinculados a la dignidad de la persona, con un enorme potencial discriminador. Por eso, son considerados datos especialmente protegidos. La Directiva 95/46 y el Convenio 108 del Consejo de Europa utiliza la expresión más específica datos de salud y no la de datos sanitarios que englobarían también otros datos de carácter personal que puedan constar en otros ficheros de los centros sanitarios como los de recursos humanos o los de gestión económica y que no necesariamente sean datos de salud por lo que su nivel de protección puede ser menor⁸². Así, si los datos de ideología, religión o afiliación sindical merecen una especial protección al garantizar la libertad ideológica o religiosa –art. 16 CE–, los datos de salud son considerados datos especialmente protegidos y forman parte del derecho a la intimidad de la persona. Algo semejante puede decirse

⁸¹ Cfr. J. SÁNCHEZ-CARO y F. ABELLÁN, *Datos de salud y datos genéticos*, cit.

⁸² El Convenio 108 del Consejo de Europa aportó tempranamente algunos criterios delimitadores que contribuyen a perfilar el concepto de dato médico, al considerarse que la noción de datos de carácter personal relativos a la salud, 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 al consumo de drogas –Memoria explicativa del Convenio 108, apdo. 45, que aunque no fue ratificada por los Estados, tiene un valor interpretativo–. En esta dirección amplia, la Recomendación N° R. (97) 5, del Consejo de Europa, considera dato médico «a todos los datos de carácter personal relativos a la salud de la persona. Afecta igualmente a datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas». El apartado 38 de esta Recomendación considera que la expresión datos médicos debería incluir cualquier información que ofrezca una visión sobre la situación médica del individuo, incluyendo datos como los referidos al abuso de las drogas, abuso de alcohol y nicotina o consumo de drogas». La Sentencia del Tribunal de Justicia de las Comunidades en el caso Lidnquist –de 6 de noviembre de 2003– también ha apostado por un concepto amplio de datos de salud. Así, hay que considerar dato de salud la presencia de una minusvalía o el grado de minusvalía, así como el número de días de baja en un fichero de nóminas. Igualmente, el fichero de citas de médicos que permite deducir la patología que motiva la consulta es un dato de salud. En cambio, el dato de fumador o no fumador –ahora casi inexistente dada la extensión de la prohibición de fumar en lugares públicos– no sería, por sí mismo, un dato de salud si no viene unido con otros datos que indiquen el hábito, el nivel de consumo o la situación de abuso. Tampoco la condición de apto o no apto de un trabajador para un puesto de trabajo después de un reconocimiento médico. Cfr. J. RUBÍ, «El concepto de dato personal relativo a la salud en la ley orgánica de protección de datos personales», *Revista de Derecho y Genoma Humano*, núm. 25, 2006, pp. 185-195.

de los datos de raza que deben ser más protegidos como garantía de la prohibición de discriminación –art. 14 CE– o los datos de vida sexual vinculados al libre desarrollo de la personalidad –art. 10.1 CE–⁸³. La definición de estos datos como especialmente protegidos tiene consecuencias, especialmente en lo que hace referencia al consentimiento para el tratamiento o en la determinación de las medidas de seguridad aplicables⁸⁴. Así, los datos de ideología, afiliación sindical, religión o creencias sólo podrán ser tratados con el consentimiento expreso y por escrito del afectado. Además, se establece expresamente que en virtud de lo previsto en el art. 16.2 CE, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias por lo que cuando se proceda a recabar el consentimiento se advertirá al interesado de su derecho a no prestarlo. Los datos de carácter personal que hagan referencia al origen racial, a la salud o a la vida sexual «sólo podrán ser recabados, tratados y cedidos cuando así lo disponga una ley o el afectado consienta expresamente» –art. 7.3 LOPD⁸⁵–. Por tanto, se necesita el consentimiento expreso del afectado para tratar sus datos de salud⁸⁶ o la existencia de una habilitación legal. En este punto hay que señalar que la Ley 16/2003, de 29 de mayo, de cohesión y calidad del Sistema Nacional de Salud atribuye a la Administración sanitaria un conjunto de responsabilidades que implica el tratamiento de datos persona-

⁸³ El art. 8 de la Directiva 95/46 establece inicialmente el principio de prohibición de su tratamiento: «Los Estados prohibirán el tratamiento de datos personales que revelan el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o la sexualidad». Igualmente, el art. 6 del Convenio 108 del Consejo de Europa señalaba: «los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el Derecho interno prevea garantías suficientes. La misma regla regirá en el caso de datos de carácter personal relativos a condenas penales».

⁸⁴ Art. 4 del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal.

⁸⁵ Freixas ha criticado que el régimen de consentimiento sea distinto para los datos relativos a la libertad ideológica, religiosa y de culto y para los datos de origen racial, salud y vida sexual, y que en éste último caso el consentimiento sólo sea expreso, sin establecer una forma concreta para otorgarlo y que además el tratamiento pueda hacerse por Ley. Destaca que esto no se encuentra previsto ni en el Convenio 108 ni en la Directiva 95/46/CE. Para este autor, la intromisión en el honor y la intimidad de las personas puede producirse con la misma contundencia a través del conocimiento de ambas categorías de datos. Cfr. G. FREIXAS GUTIÉRREZ, *La protección de los datos de carácter personal en el derecho español*, Bosch, Barcelona, 2001, pp. 130-131. Sin embargo, no hay que olvidar que la protección de datos en este caso es un instituto de garantía tanto de la libertad ideológica como del derecho a la intimidad y sólo el primero alberga dentro de su contenido constitucional que nadie está obligado a revelar su ideología, religión o creencias. Para Rubí, si bien la Ley permite el consentimiento expreso pero no escrito para los datos de salud, la necesidad de probar en muchas ocasiones que se cuenta con este consentimiento aconseja que se materialice de manera escrita. Cfr. J. RUBÍ, «La confidencialidad de la información sanitaria, instrumentos de protección y garantía». En todo caso, no hay que olvidar –como ahora señalaremos– que la Ley exceptúa de este consentimiento el tratamiento de datos personales de los pacientes que acudan o vayan a ser tratados en centros sanitarios.

⁸⁶ Así, es necesario tener el consentimiento expreso del paciente para que su nombre y apellido figure en la puerta de su habitación ya que esto no parece imprescindible para la gestión de un servicio sanitario –art. 7.6 LOPD–. Igualmente, la creación de un fichero por parte una asociación privada con datos personales de afectados por una enfermedad requiere el consentimiento expreso de éstos.

les⁸⁷. El Tribunal Constitucional, en su Sentencia 202/1999, de 8 de noviembre, en relación con la denegación a un trabajador de la cancelación de sus datos médicos en un fichero informatizado de una entidad de crédito sobre bajas por incapacidad temporal señaló que el almacenamiento sin cobertura legal en soporte informático de los diagnósticos de un trabajador, sin mediar su consentimiento expreso, constituye una restricción desproporcionada del derecho fundamental a la protección de datos personales.

No obstante, la propia LOPD establece un conjunto de excepciones al principio de consentimiento⁸⁸. Así señala expresamente que no será preciso el consentimiento cuando «el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del art. 7, apartado 6, de la presente Ley⁸⁹ [...] siempre que no se vulneren los derechos y libertades fundamentales del interesado» –art. 6.2 LOPD–. Este artículo señala que podrán ser objeto de tratamiento los datos de ideología, religión o creencias, origen racial, salud o vida sexual «cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto» –art. 7.6 LOPD–. Este precepto está tomado del art. 8.3 de la Directiva 95/46/CE⁹⁰ y no se encontraba en la antigua LORTAD. Realmente

⁸⁷ Un ejemplo de tratamiento de datos de salud sin consentimiento del interesado por la existencia de una habilitación legal es el control que se hace a los deportistas en relación con el consumo de sustancias dopantes, que más que una actuación en el ámbito de la prevención o de la asistencia sanitaria –art. 7.6 LOPD– es una actividad administrativa en el deporte que se ejerce mediante la habilitación legal contenida en la Ley Orgánica de Protección de la Salud y de Lucha contra el Dopaje en el Deporte. Igualmente, la Administración de Tráfico puede tratar el dato de salud relativo a la pérdida de aptitud psicofísica para el carné de conducir porque existe una habilitación legal –Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial. En el caso del tratamiento de datos de salud de los trabajadores, la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales establece que esta vigilancia «solo podrá llevarse a cabo cuando el trabajador preste su consentimiento. El carácter voluntario del reconocimiento médico sólo se exceptúa, previo informe de los representantes de los trabajadores, en los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad. En todo caso, se deberá optar por la realización de aquellos reconocimientos o pruebas que causen las menores molestias al trabajador y que sean proporcionales al riesgo».

⁸⁸ La Directiva 95/46/CE recoge en su art. 8.2 distintas excepciones a la prohibición de tratamiento de datos especialmente protegidos, entre las que destaca que el tratamiento sea indispensable para el respecto de los derechos y obligaciones específicos del responsable del mismo en materia laboral, y aquellos supuestos en los que el tratamiento se refiera a datos que el interesado haya manifestado públicamente o sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

⁸⁹ Llama la atención en este caso que la Directiva 95/46/CE no reenvíe la excepción de la salvaguarda del interés vital –art. 8.2.c)– al 8.3, que tiene un contenido semejante al art. 7.6 LOPD.

⁹⁰ Una previsión semejante se encuentra en el Reglamento de la UE 45/2001/CE, de 18 de diciembre de 2000, del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

este párrafo, como toda la Ley, presenta dudas interpretativas y demuestra que la LOPD fue redactada con una técnica legislativa deficiente.

Por una parte, este precepto autoriza a tratar datos de ideología, religión y creencias en la historia clínica con la finalidad antes señalada. La información personal relativa al testamento vital —que son datos que revelan la ideología o las creencias de una persona— pueden ser tratadas en un fichero de instrucciones previas. No obstante, no parece tener mucho sentido tratar estos datos de ideología o religión con finalidad sanitaria⁹¹. Así, puede hacerse constar en la historia clínica el rechazo a recibir una transfusión de sangre sin necesidad de incluir que el paciente es testigo de Jehová. Este podía ser un dato excesivo para las finalidades previstas en el ámbito sanitario. Además, no tiene sentido que se sienta el principio de que sólo se pueden tratar datos de ideología o religión con el consentimiento expreso y por escrito del interesado y con la expresa advertencia de su derecho a no prestarlo para después decir que se puede tratar estos datos sin consentimiento del interesado con la mera habilitación legal del art. 7.6 LOPD. La única justificación residiría en que para el legislador el tratamiento del dato de ideología o religión en la historia clínica es una actividad de garantía del derecho a la vida, que tiene preferencia sobre la libertad ideológica o religiosa. El dato de raza o de vida sexual puede ser considerado adecuado para la finalidad sanitaria —aunque no en todos los supuestos—.

Por otra parte, este precepto representa una habilitación legal para el tratamiento de datos de salud, de raza o de vida sexual sin que el afectado consintiera expresamente cuando se cumplan dos condiciones. La primera es que el tratamiento de estos datos se haga para la prevención —actuaciones de salud pública—, para el diagnóstico médico, para la prestación de asistencia sanitaria o de tratamientos médicos o para la gestión de servicios sanitarios. La segunda es que quien lleve a cabo el tratamiento de datos sea un profesional sanitario sujeto al secreto profesional o por otra persona sujeta a un obligación equivalente de secreto. Por tanto, cuando se den estas dos condiciones es legítimo el tratamiento de datos sin consentimiento y sin otra habilitación legal mas que la que consta en este precepto⁹². El supuesto claro es el tratamiento de estos datos por personal sanitario facultativo o no facultativo con finalidad sanitaria⁹³.

⁹¹ Hay autores que han considerado que se trata de un error. Cfr. J. M. ÁLVAREZ-CIENFUEGOS SUÁREZ, «Notas a la nueva regulación de la protección de datos de carácter personal», *La Ley*, 3, 2000, p. 1712; M. VIZCIANO CALDERÓN, *Comentarios a la Ley Orgánica*, cit. p. 130. Este último autor afirma que «[n]o sería impensable que la mención del apartado 2, en el marco del epígrafe 6, respondiera a un simple error».

⁹² Como confirma el Eurobarómetro de la Comisión Europea sobre protección de datos personales publicado en marzo de 2004, los ciudadanos se sienten tradicionalmente más confiados en relación con el tratamiento de información personal que realizan las organizaciones sanitarias frente a otros ámbitos como empresas de comercio, emisores de tarjeta y compañías de seguro. Cfr. *Datos personales.org. Revista de la Agencia de Protección de Datos de la Comunidad de Madrid* núm 8, 2004.

⁹³ La Agencia Española también ha mostrado su disconformidad con aceptar que una finalidad asistencial justifica el tratamiento de datos de salud sin consentimiento en virtud de art. 7.6. Para la Agencia Española este art. 7.6 no puede interpretarse de manea genérica o extensiva (por ejemplo, en el sentido de que baste para el tratamiento de los datos la simple expresión de la opinión de un facultativo en tal sentido) sino que debe restringirse a los dos supuestos en que únicamente será de aplicación, esto es: que

El segundo párrafo del art. 7.6 LOPD añade más confusión cuando autoriza los tratamientos de los datos a los que se refiere el párrafo anterior cuando «el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento», lo puede sugerir que el segundo párrafo es una excepción del consentimiento, por lo que no lo sería el primer párrafo. En esta línea estaría también el sentido del art. 44.4.c) LOPD que señala como infracción grave «recabar y tratar los datos referidos en el apartado 3 del art. 7 cuando no lo disponga una Ley o el afectado no haya consentido expresamente». No obstante, nosotros mantenemos que el propio art. 7.6 LOPD prevé una excepción general del consentimiento para el tratamiento de estos datos especialmente protegidos con finalidad sanitaria⁹⁴. Esto estaría justificado en la vertiente objetiva –prestacional– del derecho a la vida, que anima toda la gestión asistencial y que se soporta sobre información personal que prevalecería sobre el derecho a la intimidad y a la protección de datos personales⁹⁵. De hecho, como ha señalado la jurisprudencia del Tribunal Constitucional, el derecho a la vida prima sobre la libertad ideológica y religiosa –art. 16 CE– y sobre la libertad personal –art. 17 CE– en los supuestos antes mencionados de negativa a las transfusiones de sangre por parte de testigos de Jehová o la alimentación forzosa a presos del Grapo en huelga de hambre⁷⁴ ya que sin vida no hay libertad ideológica, sin vida no hay libertad religiosa, y, por tanto, sin vida no hay derecho a la intimidad –STC 53/1985–⁹⁷.

una disposición normativa establezca y dispongan con carácter general dicho tratamiento de datos o bien que el mismo resulte efectivamente necesario e imprescindible para la salvaguarda de un interés vital y ello se justifique debidamente. Fuera de estos dos supuestos excepcionales, el régimen aplicable con carácter general es el del art. 7.3

⁹⁴ En esta dirección hay que señalar que la Ley 41/2002, de 14 de noviembre establece el deber de pacientes y usuarios de facilitar los datos sobre su estado físico o su salud, de manera «leal» y verdadera, así como el de colaborar en su obtención, especialmente cuando sean necesarios por razones de interés público o con motivo de la asistencia sanitaria –art. 2.5–. No olvidemos también, en este sentido, que hay enfermedades de declaración obligatoria.

⁹⁵ Sin embargo, hay que señalar que recientemente las Autoridades Europeas de Protección de Datos –Grupo de Trabajo del Artículo 29– han aprobado un Documento de Trabajo sobre Historia Clínica Electrónica. Este documento es muy restrictivo ya que parte de que la legislación comunitaria de protección de datos prohíbe el tratamiento de datos sensibles por lo que defiende una interpretación estricta de las excepciones que permiten el tratamiento de datos médicos.

⁹⁶ Cfr. SSTC 120/1990, de 27 de junio y 11/1991, de 17 de enero, sobre intervención en huelga de hambre. Cfr. más ampliamente AA.VV. *Intervenciones corporales y tratamientos sanitarios obligatorios. Internamientos voluntarios*, MSC-CGJPJ, 2000, pp. 117-157.

⁹⁷ De esta forma, es legítimo que un Ayuntamiento cree un fichero donde se registra las mujeres a las que se les dispensa la píldora del día después –aún sin su consentimiento– como garantía de que no se utiliza como método anticonceptivo habitual, dado los perjuicios que puede suponer para la mujer su recurso habitual. Este fichero puede crearse ya que los Ayuntamientos tienen competencias de salud pública y de asistencia sanitaria establecidas en la LBRL. No obstante, el Ayuntamiento debe con anterioridad declarar el fichero, no puede registrar nada más que los datos pertinentes y necesarios –la identificación de la mujer y fecha de dispensación–, debe cancelarlos cuando hayan dejado de ser necesarios –cuando haya transcurrido el tiempo suficiente–, debe informar de lo previsto en el art. 5 LOPD y debe adoptar las medidas de seguridad que garantizan la confidencialidad de la información. Cfr. STC 53/1985, de 11 de abril –sobre el aborto–. Cfr. mi reflexión en este sentido realizada en la *Guía de Protección de Datos Personales para Ayuntamientos*, Civitas-APDCM, 2004, p. 29.

Además, cualquiera que haya sido la voluntad del legislador en el art. 7, el art. 8 vuelve a autorizar expresamente que las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes «podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad»⁹⁸. Este art. 8 LOPD es especialmente relevante para la sanidad privada. Así, mientras que la sanidad pública es posible, como más adelante señalaremos, la comunicación de datos entre distintos centros sanitarios públicos, en el ámbito de la sanidad privada un profesional sólo podrá acceder a información sanitaria de un paciente si va a ser tratado en el mismo. En caso contrario, no podrá acceder ya que no es legítima la cesión de datos entre centros sanitarios privados si no existe consentimiento del interesado o el cumplimiento de una relación comercial que exija la conexión con ficheros de terceros –art. 11.2.c) LOPD–⁹⁹. No hay que olvidar tampoco que el art. 11.2.f) LOPD señala que no será preciso el consentimiento cuando «la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica».

El ejercicio del derecho a la oposición al tratamiento de datos personales no se encuentra expresamente regulado en la LOPD, salvo la mención indirecta del art. 6.5. No obstante, la oposición a los tratamientos de datos sanitarios no se produce en la práctica, dada la finalidad de la actividad sanitaria. En todo caso, como señala Martín Casallo, de producirse dicha oposición, podría evidentemente ser rechazada en aplicación de un criterio de primacía del derecho a la vida frente al derecho a la intimidad¹⁰⁰.

La Ley 41/2002, de 14 de noviembre, contiene una regulación distinta en materia de consentimiento. Dentro de los principios básicos, señala que toda actuación en el ámbito sanitario –no hay porqué circunscribir la expresión a la atención médica– «requiere, con carácter general, el previo consentimiento de los pacientes o usuarios». El consentimiento del paciente es la regla general que rige la asistencia sanitaria y éste debe obtenerse después de que el paciente reciba una información adecuada –art. 2.2–. En la misma dirección está el art. 8

⁹⁸ Para J. M. ÁLVAREZ-CIENFUEGOS SUÁREZ –«La aplicación de la firma electrónica y la protección de datos de la salud», *Actualidad Informática Avanzada*, núm. 39, 2001, p. 4–, una referencia tan genérica a la legislación sanitaria autonómica o estatal constituye una clara insuficiencia de la Ley para contemplar las complejas garantías que exige el tratamiento de los datos relativos a la salud de los ciudadanos mediante sistemas electrónicos. Este autor, al igual que otros como Javier Sánchez Caro o Carmen Sánchez Carazo, consideran necesaria la aprobación de una norma específica de protección de datos de salud que analice cuestiones como los avances de la biotecnología, la investigación genética, la historia clínica electrónica, etc.

⁹⁹ En el caso de las derivaciones de la sanidad pública a la sanidad privada para cumplir los compromisos de tiempos máximos de espera para intervenciones quirúrgicas, lo adecuado es informar al paciente, en el momento en el que se le solicita el consentimiento para la derivación, de que se va a producir una cesión de la historia clínica, para cumplir el art. 5 LOPD.

¹⁰⁰ Cfr. J. J. MARTÍN-CASALLO LÓPEZ «Derechos de acceso, rectificación y cancelación de los datos sanitarios en la LOPD», *Actas del VII Congreso Nacional de Derecho Sanitario*, Ed. Fund. Mapfre Medicina, 2001, p. 58.

de la Ley 41/2002, de 14 de noviembre, que señala que «[t]oda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado». El consentimiento será verbal por regla general, aunque se prescribirá por escrito en los casos de intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, aplicación de procedimientos que supongan riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente. En muchos supuestos hay que afirmar el consentimiento implícito que se deriva de la relación de los usuarios con los centros sanitarios y con sus profesionales. La extensión de esta regla general del consentimiento prevista para la asistencia sanitaria hacia el tratamiento de los datos sanitarios es incompatible con la excepción de este consentimiento establecido en la LOPD, que se refiere de manera específica a los tratamientos de datos de salud. No parece que tenga sentido exceptuar el consentimiento para el tratamiento de datos de salud –en virtud de la preferencia del derecho a la vida sobre la intimidad– para después exigir el consentimiento para cualquier actuación médica que afecte a la salud del paciente y que puede afectar a su vida. La respuesta estaría en que la autonomía del paciente en el ámbito sanitario no es plena. Es decir, la Ley 41/2002, de 14 de noviembre, reguladora de la autonomía del paciente no está desarrollando el derecho a la vida como bien renunciable por una simple razón formal. El desarrollo y límites de los derechos fundamentales se hacen por Ley Orgánica –art. 81 CE–, no por una Ley ordinaria y sin apenas debate público. Además, es lógico que cualquier decisión que adopte el paciente sobre una actuación médica quede reflejada en la historia clínica.

e) *La seguridad como garantía de la integridad y de la confidencialidad de la historia clínica. El deber de secreto*

Otro principio de protección de datos es el principio de seguridad de los datos –art. 9 LOPD–¹⁰¹. La seguridad de la información es una garantía de la integridad, de la disponibilidad y de la confidencialidad de la información de salud. La integridad de las historias clínicas es muy importante ya que una pérdida o destrucción de historias clínicas o una vulnerabilidad que afecte a su disponibilidad perjudica gravemente la atención sanitaria y, en definitiva, la vida de las personas¹⁰². Especialmente, la seguridad es una garantía de la confidencialidad de la historia clínica, es decir, de que sólo acceden a la información de salud las personas autorizadas y de que no se producen accesos por parte de terceras personas no autorizadas¹⁰³. Esto es especialmente importante

¹⁰¹ En relación con la seguridad de las historias clínicas en soporte papel, *cf. infra* apdo. 6.

¹⁰² Esto es lo que ocurrió cuando se quemaron 500.000 historias clínicas del Complejo Hospitalario Montecelo, de Pontevedra. Los propios facultativos tuvieron que reconstruir las historias clínicas preguntando incluso a los pacientes cuantos ciclos de quimioterapia llevaban.

¹⁰³ Así, el acceso a datos de historias clínicas del Hospital Severo Ochoa de Leganés por parte de personas no autorizadas –medios de comunicación, asociaciones privadas de pacientes– puede suponer un incumplimiento de las medidas de seguridad.

cuando estamos hablando de datos de salud, que se encuentran muy vinculados a nuestra intimidad personal y familiar, y, en última instancia, a la dignidad de la persona, a los derechos inviolables que le son inherentes y al libre desarrollo de la personalidad –art. 10.2 CE–. De hecho, una de las principales medidas para preservar nuestra intimidad y privacidad en el ámbito sanitario es limitar el número de personas que pueden acceder a la historia clínica, estableciendo las adecuadas medidas de seguridad que eviten los accesos no autorizados. Como ha señalado el Grupo de Ética de la Ciencia y de las Nuevas Tecnologías, la seguridad informática es un imperativo ético para garantizar el respeto a los derechos humanos y libertades del individuo y la confidencialidad de sus datos.

La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal ya fue consciente de la importancia de la seguridad. La Ley Orgánica 15/1999, de 13 de diciembre, continúa estableciendo en el art. 9 que el «responsable del fichero, o en su caso, el encargado del tratamiento, debe adoptar medidas tanto técnicas como organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural». Así se establece que no se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinen con respecto a su seguridad e integridad por la vía reglamentaria. Específicamente este precepto menciona la importancia de la seguridad de los datos especialmente protegidos al afirmar que reglamentariamente «se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley»¹⁰⁴. De hecho, es una infracción grave «mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen» –art. 44.3.b). Esta vía reglamentaria ha sido el Real Decreto 994/1999, de 11 de junio, que aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal y que ha establecido los requisitos y condiciones que deben reunir los ficheros automatizados y las personas que intervengan en su tratamiento¹⁰⁵. Este Real Decreto ha establecido para los datos de ideología, afiliación sindical, religión y creencias, raza, salud y vida sexual, así como los datos recabados para fines policiales la necesidad de implantar, además de las medidas de seguridad de nivel básico y de nivel medio, unas medidas de seguridad de nivel alto –art. 4.3– que pueden ser tanto organizativas o

¹⁰⁴ AA.VV, *La seguridad y confidencialidad de la información clínica. Informe SEIS*, Pamplona, 2000.

¹⁰⁵ La entrada en vigor de las medidas de seguridad de nivel alto, después de sucesivas prórrogas, se produjo el 26 de junio de 2002. Cfr. más ampliamente el análisis de las medidas de seguridad en el *Manual de Protección de Datos para las Administraciones Públicas*, Civitas-APDCM, Madrid, 2003, pp. 50-56.

funcionales como informáticas o de carácter técnico¹⁰⁶. Entre estas medidas de seguridad debemos destacar el establecimiento de un registro de accesos –que vela por la confidencialidad de las historias clínicas–, las copias de respaldo y seguridad –que vela por la integridad de las mismas–, la realización de auditorías de seguridad bianuales¹⁰⁷, el cifrado de las comunicaciones¹⁰⁸, seguridad en los traslados¹⁰⁹, etc. En la actualidad se encuentra en tramitación el proyecto de Real Decreto 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, que establece las medidas de seguridad en el tratamiento de datos de carácter personal –Título VIII–. Especialmente hay que destacar que este Proyecto incorpora un conjunto de medidas de seguridad para los ficheros o tratamientos no automatizados, entre los que se encuentran los ficheros de historias clínicas¹¹⁰.

¹⁰⁶ La Ley de confidencialidad de las historias clínicas de EEUU, además de prohibir la comulación de información a terceros, establece un conjunto de medidas organizativas: los pacientes no podrán ser interrogados sobre circunstancias concretas en las áreas de recepción, los tabloneros de anuncios en las salas de urgencias donde aparecen nombre y problemas médicos de los pacientes deben trasladarse a una ubicación alejada del público; el *software* debe permitir identificar al paciente por las iniciales; los centros deben dar la opción al paciente de decidir si quiere o no que sus datos estén en el listín telefónico. *Cfr. Diario Médico*, 16 de abril de 2003, p. 10.

¹⁰⁷ Las conclusiones de las auditorías de medidas de seguridad en los ficheros de salud indican que las medidas de seguridad que más se incumplen son las organizativas o funcionales, no las técnicas o informáticas. Entre las medidas informáticas que presentan un mejor nivel de cumplimiento hay que destacar la adecuada aplicación de los niveles de seguridad, las claves de identificación y autenticación y las copias de respaldo y de seguridad. Entre las que presentan un menor nivel de cumplimiento hay que incluir la actualización y adaptación del documento de seguridad, el registro de accesos, los registros de incidencias y los ficheros temporales.

¹⁰⁸ La transmisión de datos a través de redes públicas de telecomunicaciones se debe realizar cifrando los datos o bien utilizando cualquier otro mecanismo que garantice que la información no es inteligible ni manipulable por terceros –art. 23 del Real Decreto 994/1999–. No se puede transmitir información a los pacientes, por ejemplo, a través de una web de acceso libre. En todo caso, no siempre es fácil cifrar las comunicaciones, como ocurre con la telemedicina o con la atención sanitaria a través del teléfono que frecuentemente se grava en fichero. También es complicado el cifrado en la utilización de medios radiofónicos para la transmisión por los servicios de urgencia de datos de salud. El Reglamento de Medidas de Seguridad sólo es aplicable cuando los datos se obtengan o tengan como destino su incorporación a un fichero informatizado, lo que exigiría el cifrado de las comunicaciones o bien la utilización de cualquier otro mecanismo que garantice que la información no es inteligible ni manipulable por terceros –art. 26–. No lo es de aplicación el cifrado de las comunicaciones a la transmisión por fax ya que se trata en este caso de un fichero manual y no de un fichero informatizado, salvo que el fax sea entendido como un documento de entrada o de salida de un fichero informático. Sin embargo, aún en ese caso no parecen aplicables al fax muchas de esas medidas de seguridad. Le sería de aplicación la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones en relación con el secreto de las comunicaciones, la protección de los datos personales y los derechos y obligaciones relacionados con las redes y servicios de comunicaciones electrónicas. También le es de aplicación la Directiva relativa al sector de las telecomunicaciones que exige el cifrado de redes y servicios de telecomunicaciones como garantía para preservar el secreto de las mismas -Directiva 2002/58/CE, de 12 de junio, relativa al tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas. Es de aplicación aquí la Directiva 2002/21/CE, de 7 de marzo, relativa al marco regulador de las redes y los servicios de comunicaciones electrónicas.

¹⁰⁹ No hay más que comparar el envío de una nómina con el de la información que remiten los laboratorios para análisis clínicos.

¹¹⁰ *Cfr. infra* apdo. 7.

En todo caso, hay que señalar que el mantenimiento de las historias clínicas a través de un sistema informático garantiza mejor la conservación y la confidencialidad de la información –porque permite la implantación de medidas de seguridad– que el mantenimiento en papel de millones de documentos que conforman las historias clínicas. Los sistemas informáticos permiten la adopción de medidas como el control y restricción de acceso a los datos de los pacientes exclusivamente a los profesionales sanitarios que deben realizar el proceso asistencial y la implantación de otras medidas como el cifrado, la trazabilidad, la copia de respaldo y otras muchas medidas de seguridad que no pueden implantarse en la conservación en papel. De igual forma, los sistemas informáticos centralizados garantizan mejor la seguridad de la información que los sistemas informáticos no centralizados implantados en herramientas locales¹¹¹. Bajo estas premisas y con un claro respeto a los principios que establece la legislación vigente sobre protección de datos, los procesos de centralización informática de los ficheros de historias clínicas permiten garantizar una más adecuada atención a los pacientes, así como facilitar el cumplimiento de las obligaciones en materia de seguridad de los tratamientos que impone la normativa¹¹².

La Ley 41/2002, de 14 de noviembre, ha desarrollado una intensa regulación en relación a la seguridad de las historias clínicas, especialmente en lo que hace referencia a la integridad, disponibilidad y confidencialidad. Hay una clara preocupación en esta Ley tanto por conservar las historias clínicas como por garantizar su confidencialidad, estableciendo los oportunos niveles de acceso. Así, afirma –art. 14.2– que «cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información». Se resalta el principio de seguridad al indicar que las Administraciones sanitarias «establecerán los mecanismos que garanticen la autenticidad del contenido de la historia clínica y de los cambios operados en ella, así como la posibilidad de su reproducción futura –art. 14.3–. De alguna manera, esta Ley está pensando en la migración de la información clínica desde el soporte papel al informático al señalar que los centros sanitarios están obligados a conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, «aunque no necesariamente en su soporte original» –art. 17.1–. Las Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecua-

¹¹¹ Es especialmente grave el mantenimiento de información de salud de los pacientes en aplicaciones mono usuario en herramientas ofimáticas que no tienen las adecuadas medidas de seguridad. Lo mismo se puede decir de muchos sistemas informáticos regalados por las empresas farmacéuticas a los facultativos o a los servicios que se salen de los entornos del centro de salud o del hospital y sobre los que el gerente no puede responder.

¹¹² En todo caso, las Autoridades de Protección de Datos sólo deben valorar la idoneidad de estos tratamientos respecto a la efectiva tutela del derecho fundamental a la Protección de Datos que tienen los pacientes, no pudiendo analizar cualquier otro aspecto relativo a la gestión y a la oportunidad política.

das para archivar y proteger las historias clínicas y evitar su destrucción o pérdida accidental –art. 14.4–, lo que refleja una mención indirecta de las medidas de seguridad exigidas en el Real Decreto 994/1999, de 11 de junio, que aprueba el Reglamento de medidas de seguridad. De hecho, se afirma expresamente en el art. 17.6 que «son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal, y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal»¹¹³. Igualmente, las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso –art. 16.7–. Hay que destacar también que la centralización de la historia clínica en los centros sanitarios, establecida expresamente en la Ley 41/2002 y en la propia Ley General de Sanidad, que evita la duplicación de estas historias en los distintos servicios, facilita también la custodia de las historias clínicas y su confidencialidad. Más adelante analizaremos los distintos niveles de acceso a la historia clínica.

La Ley 41/2002, de 14 de noviembre, ha establecido una importante novedad al reconocer que la seguridad de la información no sólo es un principio que debe regir los servicios sanitarios sino también un derecho de los pacientes. Así, se establece en el art. 19 que el paciente «tiene *derecho* a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad». Por consiguiente, las historias clínicas deben estar protegidas por unas medidas de seguridad, pues éstas son la garantía de la intimidad y de la confidencialidad, de su integridad frente a pérdidas accidentales o sustracciones ante eventuales acciones judiciales por errores médicos, de la disponibilidad y eficiencia en la recuperación de la información, permitiendo progresivamente la movilidad de los pacientes y evitando la repetición de pruebas diagnósticas.

Hay un aspecto importante de la seguridad de las historias clínicas, que es el que hace referencia a la gestión de la historia clínica mientras que esté viva y su almacenamiento a partir de la fecha de alta de cada proceso asistencial. La Ley 41/2002, de 14 de noviembre, como hemos indicado antes, establece que los centros sanitarios están obligados a conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad para la debida asistencia al paciente «durante el tiempo adecuado a cada caso, y como

¹¹³ En todo caso, no queremos dejar de señalar que, en la medida en que la historia clínica esté en red, es de aplicación la Directiva 97/66 CE del Parlamento Europeo, que se ha modificado por la Directiva 2002/58 CE, que señala que el proveedor de un servicio público de telecomunicaciones deberá adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, de ser necesario en colaboración con el proveedor de la red pública de telecomunicación por lo que respecta a la seguridad de la red. Considerando las técnicas más avanzadas y el coste de su aplicación, dichas medidas deberán garantizar un nivel de seguridad adecuado para el riesgo existente.

mínimo cinco años desde la fecha del alta de cada proceso asistencial». Mientras que la historia clínica esté viva –se entiende que está viva cuando debe conservarse para la debida asistencia al paciente y como mínimo cinco años–, ésta debe mantenerse unida a los datos personales del paciente porque ésta es la mejor forma de evitar errores¹¹⁴. En cambio, cuando las historias clínicas se convierten en pasivas deben archivarse como regla general separando los datos identificativos de los documentos clínicos, como medida de seguridad, sin perjuicio de la investigación genética, científica, epidemiológica y docente¹¹⁵. Esta es una buena forma de poder conservar la documentación clínica, que puede ser enormemente valiosa a medio plazo, respetando a la vez el derecho fundamental a la protección de datos personales. La disociación de la información de salud para llevar a cabo estudios epidemiológicos y de investigación garantiza también la confidencialidad de la información de salud.

Otro principio fundamental es el deber de secreto, algo consustancial a la profesión sanitaria y que se remonta al Juramento Hipocrático, por el cual el médico se comprometía a mantener silencio sobre todo lo que viese u oyese en el curso del tratamiento o, incluso, fuera del mismo, referente a la vida de los hombres, que en ningún caso debería ser divulgado, considerando la discreción como un deber. El Código de Ética y Deontología Médica, adoptado por la Organización Médica Colegial el 10 de septiembre de 1999, señala que «[e]l secreto médico es inherente al ejercicio de la profesión y se establece como un derecho del paciente a salvaguardar su intimidad ante terceros»¹¹⁶. Nuestra Constitución se limita a señalar que la ley «regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos» –art. 24.2–. El Código Penal –la llamada Constitución negativa– señala que «[e]l profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años» –art. 199.2–. El secreto médico ha sido considerado tradicionalmente en su dimensión negativa, como un deber de reserva del profesional

¹¹⁴ Si la documentación clínica del paciente no incluye el nombre de éste, el profesional puede no tener la total seguridad que la documentación clínica corresponde a ese paciente en concreto, lo que provocaría errores involuntarios. Este es también el criterio que mantiene el Grupo de Expertos en Información y Documentación Clínica al afirmar que «la historia clínica deberá contener la información suficiente para identificar claramente al paciente». De hecho, uno de los problemas que se presentan en el ámbito asistencial es el de la identificación de la población extranjera, cuando se presta asistencia sanitaria a varios pacientes con una sola tarjeta. Esto se produce a partir del cambio legislativo por el que la policía tiene capacidad de acceder a los datos del padrón municipal de población extranjera, de manera que ésta se retrae de inscribirse en el padrón y obtener la tarjeta sanitaria individual.

¹¹⁵ Para ello la tabla que establezca la relación entre cada historia clínica y los datos personales del paciente debe conservarse en un archivo independiente *Cf.*: Recomendación 2/2004, de 30 de julio, sobre custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas.

¹¹⁶ Los Estatutos de la Organización Médica Colegial, aprobados por Real Decreto 1018/1980, de 19 de mayo, consideran falta grave «la infracción grave del secreto profesional, por culpa o negligencia, con perjuicio grave para tercero» y muy grave, la violación dolosa del mismo.

sanitario sin aceptar la vertiente positiva del mismo que atribuiría como contrapartida al paciente el derecho a exigir su cumplimiento¹¹⁷. Este deber de secreto individual se transforma en un secreto compartido cuando son un grupo de personas las que llevan a cabo la asistencia del paciente. Este deber no afecta únicamente al profesional sanitario sino también al profesional no sanitario, hablándose en este caso de la existencia de un secreto derivado, especialmente importante, como veremos más adelante, para el personal de administración y gestión que accede a información clínica para el ejercicio de sus funciones¹¹⁸. Lógicamente, el deber de secreto tiene unos límites como es la obligación de revelar información genética a familiares cuando exista un riesgo evidente para su salud o la obligación de comunicar ciertas enfermedades, como es el caso de la infección por VIH¹¹⁹. En principio se mantienen los criterios generales que rigen la confidencialidad y el secreto profesional, pero se presentan especialidades para mejorar la asistencia a estos enfermos y la protección de las personas con las que convivan. Así, por ejemplo, la decisión sobre informar o no en la escuela de la presencia de un niño o adolescente infectado por el VIH debe ser tomada en atención al interés del menor y después de una consulta entre la persona infectada, los padres, los profesores y el personal sanitario¹²⁰. El límite al deber de secreto y, por tanto, al derecho a la intimidad del enfermo de sida se hace más patente para proteger el derecho a la vida y a la salud de la persona con la que conviva. Normalmente el paciente no se niega a comunicar su enfermedad a la otra persona pero si se produce esta negativa, el médico debe tratar de persuadirle y si no lo consigue, informar él mismo a la pareja del enfermo¹²¹.

¹¹⁷ De Miguel critica que la Ley 41/2002, de 14 de diciembre, no haya aprovechado para afirmar de forma indubitada el derecho del paciente al secreto médico. *Cfr.* N. DE MIGUEL, «Intimidad e historia clínica», *cit.* pp. 11-12, 21 y 31. En todo caso, con independencia de que exista o no un derecho a exigir su cumplimiento, el incumplimiento del deber de secreto supone una indudable vulneración del derecho a la intimidad del paciente, que dispone de distintas garantías específicas o jurisdiccionales de protección de los derechos fundamentales.

¹¹⁸ Esta cuestión ha sido estudiada detenidamente por N. DE MIGUEL, *Secreto médico, confidencialidad e información sanitaria*, *cit.* pp. 51-143, esp. pp. 308-311.

¹¹⁹ *Cfr. infra* apdo. 3.c). Así, por ejemplo, la Ley 35/1988, sobre Técnicas de Reproducción Asistida reconoce el deber de secreto en relación con el anonimato del donante, pero permite conocer la identidad del donante en circunstancias excepcionales que comporten un peligro para la vida del hijo, o cuando proceda con arreglo a las leyes procesales penales –art. 5.5–. Esta cuestión ha sido analizada por el Tribunal Constitucional en la Sentencia 116/1997, de 17 de junio.

¹²⁰ El Consejo de Europa en la Recomendación 1116 (1989), de 29 de septiembre, de la Asamblea Parlamentaria, sobre sida y derechos humanos, insta al Comité de Ministros a que invite a los Estados miembros «a realizar todos los acuerdos necesarios para proteger la confidencialidad y/o el anonimato de las personas seropositivas y de las víctimas del SIDA».

¹²¹ *Cfr.* la Recomendación n.º R. (89) 14, de 24 de octubre, del Comité de Ministros, relativa a los aspectos éticos de la infección por VIH en el cuidado sanitario y en el marco social y la Recomendación n.º R. (97) 5, de 13 de febrero, ya citada relativa a la protección de datos médicos, que establece la recogida y tratamiento automatizado de estos datos. Sobre esta cuestión, *cf.* el interesante estudio de N. DE MIGUEL, *Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público*, *cit.* pp. 104-106, 110-114 y 216-217.

La legislación de protección de datos también recoge el deber de secreto profesional. El art. 10 LOPD señala que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsisten aún después de finalizar sus relaciones con el titular del fichero, o, en su caso, con el responsable del mismo. Lógicamente, estas obligaciones no son meramente teóricas sino que su omisión es una infracción muy grave. Así, el 44.3 LOPD señala que es una infracción muy grave «la vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del art. 7». No ha sido fácil la delimitación entre cesión de datos e incumplimiento del deber de secreto. Consideramos que la cesión de datos implica que haya un cedente –que es el responsable del fichero– y un cesionario –que lleve a cabo un posterior tratamiento de datos personales–. En cambio, el incumplimiento del deber de secreto se produce cuando cualquier empleado revelan datos personales que obran en un fichero a otras personas sin que la persona que reciba esta información vaya a realizar un tratamiento –no habría en este caso cedente ni cesionario–. Igualmente se estaría produciendo un incumplimiento del deber de secreto cuando el responsable del fichero de historias clínicas en papel no lo custodia de manera adecuada –aparecen abandonas historias clínicas en la calle– y no se encuentran aprobadas las medidas de seguridad para los ficheros manual-estructurados. En general, si se produce un acceso no autorizado a la historia clínica informatizada no estaríamos hablando de la omisión del deber de secreto sino del incumplimiento de una medida de seguridad. La obligación de secreto queda muy reforzada por la Ley 41/2002, de 14 de noviembre. En ella se establece que la persona «que elabore o tenga acceso a la información y documentación clínica está obligada a guardar la reserva debida» –art. 2.7–. Lo mismo se vuelve a repetir en el art. 16.6 cuando se señala que «el personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto». Se reitera de esta forma la previsión del 61 de la Ley General de Sanidad que señala «el deber de guardar secreto, por quien, en virtud de sus competencias, tenga acceso a la historia clínica». Queda claro que no sólo el facultativo puede vulnerar el deber de secreto sino cualquier persona que intervenga en el tratamiento de datos personales y que haya accedido a la historia clínica. Este deber de secreto se mantiene aunque haya finalizado la relación laboral con el responsable del fichero de historias clínicas. Muchas vulneraciones de estos derechos en los países mediterráneos, que tienen la característica de ser muy comunicativos, provienen de la omisión del deber de secreto entre los empleados¹²². La posibilidad de infringir este deber de secreto

¹²² En muchas ocasiones, antes de dar una información lo mejor es pedir su consentimiento. Así, en relación con la información presencial o telefónica acerca de si una persona se encuentra internada o no en un centro hospitalario, lo más indicado es preguntar al paciente en el momento del ingreso –especialmente en establecimientos psiquiátricos– si desea que se facilite esta información. Un ejemplo de incumplimiento del deber de secreto es que los familiares conozcan el fallecimiento del paciente a través de la empresa funeraria a la que ha comunicado la información alguien que trabaja en el centro sanitario.

se produce con más frecuencia con pacientes conocidos¹²³ o en localidades más pequeñas¹²⁴.

Por último, hay que señalar que la Ley 15/1999, de 13 de diciembre, permite el acceso a los datos por cuenta de terceros sin consentimiento del interesado «cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento» –art. 12–. En todo caso, hace falta un contrato por escrito o por cualquier otra forma que permita acreditar su celebración por el que el tercero, que se convierte en encargado del tratamiento, se comprometa a tratar los datos conforme a las instrucciones del responsable del fichero, a no destinar los datos para una finalidad distinta a las que figuren en el contrato, a no comunicar los datos a terceros ni siquiera para su conservación, a implantar las medidas de seguridad y, finalmente, a destruir o devolver los datos al responsable del fichero una vez cumplida la prestación contractual. La conservación de las historias clínicas en papel o la informatización de las historias clínicas se llevan a cabo frecuentemente con el apoyo de empresas externas, que son auténticas encargadas del tratamiento por cuenta del responsable del fichero¹²⁵. Así, la monitorización de un aplicativo de historia clínica electrónica no significa que existe un espía en la consulta. No es razonable quejarse del mal funcionamiento de la informática en la sanidad, al tiempo que se pone impedimentos a las mejoras tecnológicas en este ámbito apoyándose en empresas especializadas¹²⁶.

¹²³ Esto ocurre especialmente con personas que son noticia frecuentemente en la prensa del corazón.

¹²⁴ Las Sentencias del Tribunal Constitucional 37/1989, de 15 de febrero, y del Tribunal Supremo, de 4 de abril de 2001, analizaron el caso de una médica residente de un hospital dependiente de la Administración, que fue requerida para prestar sus servicios profesionales de asistencia neurológica a una persona a la que conocía, por proceder ambas de la misma localidad. Al examinar su historial clínico advirtió como antecedente quirúrgico la existencia de dos interrupciones legales del embarazo, circunstancia que fue manifestada a su madre, la que a la primera ocasión, en el pueblo, se lo comunicó a un familiar de la paciente. La condena fue de un año de prisión y dos de inhabilitación. Sobre esta cuestión, J. SÁNCHEZ CARO y F. ABELLÁN, *Datos de salud y datos genéticos*, cit. También se incumple el deber de secreto cuando se informa a los medios de comunicación de las enfermedades –o, simplemente, de la atención en un centro sanitario– de algunas personas conocidas.

¹²⁵ Existe un problema relativo a la conservación de las historias clínicas de los facultativos cuando éstos se jubilan o fallecen. El Colegio de Médicos de Madrid ha impulsado un proyecto de custodia de estas historias clínicas, convirtiéndose en encargado del tratamiento. Con este proyecto, además de facilitar el cumplimiento por parte del facultativo de su deber de custodia durante el tiempo necesario para la actividad asistencial y, al menos, cinco años, permite la creación de un banco de historias clínicas de la sanidad privada –sólo existe en la sanidad pública– que permita en el futuro estudios genéticos, epidemiológicos y de investigación. Cfr. *Memoria del III Premio a las Mejores Prácticas Europeas en materia de Protección de Datos para Administraciones Públicas*, cit. También puede llevar a cabo la custodia de la historia clínica otro profesional en el marco de un encargo de tratamiento. Este segundo profesional sólo sería responsable del fichero con el consentimiento expreso del paciente para la cesión o si va a continuar el tratamiento médico de este paciente en virtud del art. 8 LOPD.

¹²⁶ Recientemente se ha cuestionado la posible vulneración del derecho fundamental a la protección de datos personales por la Consejería de Sanidad de la Comunidad de Madrid por la adjudicación durante el año 2006 a la empresa Stacks del sistema informático que centralizará las historias clínicas de los centros de salud de la Comunidad de Madrid. A partir de las denuncias, la Autoridad de Protección de Datos Regional desarrolló unas actuaciones previas, exigiendo a la Consejería de Sanidad el contrato que regula su relación con la empresa Stacks. La Autoridad de Protección de Datos verificó materialmente la existencia de un contrato de confidencialidad que acredita su celebración y contenido, por el cual la empre-

Los centros médicos o los profesionales sanitarios no son meros encargados de tratamiento de las compañías aseguradoras sanitarias. La propia Ley 41/2002, de 14 de noviembre atribuye la responsabilidad del fichero a cada centro sanitario y al profesional individual, que deben conservar la historia clínica de sus pacientes. Esta obligación legal de conservar las historias clínicas de los pacientes impide que concluida la prestación contractual con la entidad aseguradora devuelvan o destruyan la historia clínica como exige el art. 12 LOPD al encargado del tratamiento. Además, estos centros llevan a cabo nuevos tratamientos de datos personales de salud distintos de los proporcionados por la entidad aseguradora y para finalidades distintas. Si los centros sanitarios o los profesionales no son encargados del tratamiento, tampoco lo son las entidades aseguradoras con las que se contrata un seguro de responsabilidad civil o patrimonial porque van a tratar los datos para una finalidad distinta. Estos son supuestos de cesiones de datos, como más adelante señalaremos. Tampoco la prestación de una asistencia pública a través de entidades privadas puede considerarse que se hace en el marco de un encargo de tratamiento. No parece que una entidad privada que preste un servicio público -en el marco de un contrato de gestión de servicios públicos -art. 156 LCAP- puede ser considerado un encargado del tratamiento. Se trata de cesiones de datos en las que el centro contratado tiene el carácter de responsable del fichero al llevar a cabo una propia actividad asistencial y conserva con esa finalidad la historia clínica. Otra cosa distinta es si lo que se externaliza es una actividad no asistencial -por ejemplo, el traslado en ambulancia-, donde sí se daría la figura del encargado del tratamiento. En este supuesto, el responsable del fichero ha de entregar al encargado de tratamiento la información mínima imprescindible para que pueda realizar el ser-

sa se convierte en encargado del tratamiento de la información, obligándose, durante todas las fases de validación de la migración, puesta en marcha de los centros, planes de prueba y validación de los programas entregados, a tratar los datos únicamente conforme a las instrucciones de la Consejería de Sanidad, a no utilizarlos con fines distintos, a no comunicarlos a terceras personas, a implantar las medidas de seguridad de nivel alto -cifrado y trazabilidad- y a devolver la información al responsable del fichero una vez finalizada la relación contractual que le une con la Consejería de Sanidad. Asimismo, en dicho contrato, Stacks asume la obligación de hacer cumplir el deber de secreto a todas las personas que van a participar en el proyecto así como a informarles de todas las obligaciones sobre protección de datos que asumen al participar en el mismo. Además, se advierte a Stacks de que en el caso de que destine los datos a otra finalidad o los comunique o los utilice incumpliendo las obligaciones que asume, será responsable de las infracciones cometidas y estará sujeta al régimen sancionador prescrito por la ley. Estas obligaciones se encuentran referidas también en los documentos públicos del Pliego de Cláusulas Administrativas particulares y el Pliego de Prescripciones Técnicas que han regido el procedimiento de adjudicación. Hay que señalar que la Consejería de Sanidad de la Comunidad de Madrid se encuentra en un mejor nivel de cumplimiento de la legislación de protección de datos que otras Comunidades Autónomas, teniendo en cuenta el nivel de regularización de los ficheros declarados. En este momento, existen inscritos en el Registro de Ficheros de Datos Personales de la Agencia de Protección de Datos de la Comunidad de Madrid 2.716 ficheros de titularidad de centros, órganos y unidades dependientes de la Consejería de Sanidad y Consumo de la Comunidad de Madrid, suponiendo una situación de claro liderazgo frente al resto de Comunidades Autónomas.

vicio contratado como exigencia del principio de calidad. Un supuesto especialmente complicado es el de laboratorios de análisis clínicos¹²⁷.

f) *El derecho de acceso del paciente a la historia clínica y sus límites. La tutela de los derechos*

La LOPD no contiene únicamente principios. También establece derechos que conforman el contenido del derecho fundamental de protección de datos. Además del derecho a la impugnación de las valoraciones basadas únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de la personalidad –art. 13–, que puede tener virtualidad frente a denegaciones o calificaciones de primas por parte de compañías de seguro¹²⁸, y del derecho de consulta al registro general de protección de datos –art. 14–, la Ley 15/1999, de 13 de diciembre establece otros derechos que son, como señala el Tribunal Constitucional en su Sentencia 292/2000, el contenido esencial del derecho fundamental a la protección de datos. Así, el interesado, como indica el art. 15 tiene derecho a «solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos». De hecho, cuando esta Ley regula las excepciones al derecho de acceso, no incluye los datos sanitarios –arts. 23 y 24 LOPD–. Este derecho de acceso sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto. Este límite temporal al derecho de acceso tenía un sentido cuando el ejercicio del derecho supone una carga de trabajo –y, por tanto, un coste– al responsable del fichero pero carece de sentido cuando este acceso a la propia información personal pueda hacerse por vía telemática en los servicios de Administración Electrónica¹²⁹. Este derecho es de aplicación en el ámbito de los ficheros de historias clínicas, ya que la LOPD cuando desarrolla los límites a estos derechos no menciona los ficheros de salud.

¹²⁷ Los laboratorios de análisis clínicos en muchas ocasiones tratan los datos por cuenta del centro médico y del profesional sanitario. Su actividad sanitaria es distinta a la de los anteriores y no parece tan clara su obligación de archivo de la historia clínica en virtud de la ley 41/2002, de 14 de noviembre. Parece que prestan un servicio al responsable del fichero, no deciden realmente sobre el tratamiento, no pueden destinar los datos a una finalidad distinta –no puede utilizar las muestras biológicas para analizar otros marcadores– y tienen que devolver o destruir la información una vez finalizada la actividad. Cualquier tratamiento que haga el laboratorio de análisis clínico distinto del indicado debe ser con el consentimiento del interesado. Sin embargo, también pueden ser considerados responsable del fichero. Son los propios pacientes los que acuden a los mismos y su actividad es de finalidad asistencial, aunque está más limitada que la del resto de los profesionales sanitarios, pudiendo cancelar la información en un plazo de tiempo más breve

¹²⁸ Sobre el uso de información sanitaria en la actividad aseguradora, *Cfr.* J. RUIZ FERRÁN y C. ZAMANILLO SARMIENTO, «Confidencialidad de datos clínicos y aseguramiento sanitario privado», *Actualidad Informática Aranzadi*, núm. 39, 2001, pp. 1 y ss.

¹²⁹ *Cfr.* en esta dirección el Proyecto de Ley de Acceso Electrónico a la Administración Pública, que ahora se encuentra en tramitación en el Senado.

Los derechos de acceso, rectificación y cancelación han tenido un desarrollo reglamentario, a través del Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal y a través de la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación. Estos textos normativos aportan una gran información sobre la forma de acceso a la historia clínica. Así, como señala el art. 11 del Real Decreto 1332/1994, los derechos de acceso, rectificación y cancelación son derechos personalísimos y pueden ser ejercidos por el afectado o por su representante legal, en casos de incapacidad o minoría de edad que imposibilite el ejercicio personal de los mismos¹³⁰. Parece también razonable que estos derechos puedan ejercitarse a través de cualquier persona con la autorización expresa y escrita del interesado. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, siempre de manera legible o inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. La información suministrada por el responsable del fichero al interesado deberá contener siempre los datos de base del afectado, el origen de esos datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que éstos se almacenaron.

La regulación del derecho de acceso a la historia clínica se encuentra muy desarrollada en la Ley 41/2002, de 14 de noviembre. Así, se reconoce el derecho de acceso a la historia clínica por parte del paciente y sus límites, al tiempo que se aborda también los posibles accesos por parte de terceras personas —como veremos más adelante—, estudiando igualmente y tratando de resolver las distintas situaciones conflictivas que habían sido analizadas ya por la jurisprudencia. Esta Ley afirma de manera taxativa el derecho de acceso a la historia clínica, del que es titular el paciente, tratando de poner fin a las denegaciones de este derecho. Así, el art. 18 señala expresamente que el paciente «tiene el derecho de acceso [...] a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella. Los centros sanitarios regularán el procedimiento que garantice la observancia de estos derechos». Este derecho de

¹³⁰ Estos derechos se ejercitan mediante una solicitud dirigida al responsable del fichero, que deberá contener: nombre, apellidos del interesado y fotocopia del DNI del interesado, en el caso de que alguien le represente, el DNI de la persona que lo represente así como el documento acreditativo de tal representación; petición en que se concreta la solicitud, es decir el fichero o ficheros sobre los que se quiere ejercitar la solicitud; domicilio a efectos de notificaciones, fecha y firma del solicitante; documentos acreditativos de la petición que formula. El responsable del fichero deberá contestar la solicitud que se le dirija con independencia de que figuren o no datos personales del afectado en sus ficheros. El responsable del fichero resolverá la petición de acceso en el plazo de un mes a contar desde la recepción de la solicitud. Transcurrido este plazo sin que de forma expresa se responda a la petición, ésta podrá entenderse desestimada y podrá plantearse una reclamación ante la Agencia Española de Protección de Datos o ante la Agencia Autonómica competente. Si la resolución fuera estimatoria, el acceso se hará efectivo en los diez días siguientes a la notificación.

acceso del paciente a la historia clínica se deduce del derecho a la información asistencial por el que todos los pacientes tienen derecho a conocer, con motivo de cualquier actuación en el ámbito de su salud, «toda la información disponible sobre la misma» –art. 4.1–¹³¹, así como del propio art. 5 que señala que el titular del derecho a la información asistencial es el paciente. Este derecho de acceso a la historia clínica está justificado tanto desde el respeto al derecho fundamental a la protección de datos personales y la libertad informática, que implica el acceso a la propia información personal, como desde el propio respeto del derecho a la libertad personal y a la vida, que justifica el conocimiento de todas aquellos datos e informaciones relevantes sobre el propio estado de salud que permite la autonomía del paciente –una conformidad consciente de toda actuación médica que afecte a su salud–¹³².

La obligación de hacer efectivo este derecho de acceso de los pacientes a la historia clínica se extiende tanto al centro sanitario público como al centro sanitario privado. La Ley 41/2002, de 14 de noviembre no establece únicamente obligaciones para la Administración o para los centros públicos¹³³, sino también para los centros sanitarios privados. Estamos hablando de derechos atribuibles a toda persona. Este sería, por tanto, un supuesto de vinculación de los particulares a los derechos fundamentales, por mediación legal, lo que no obsta para que, en algunos casos esta obligación viniera *ex constitutione*, por lo que podríamos hablar también aquí de *unmittelbare Drittwirkung*¹³⁴. Su incumplimiento es una lesión grave del derecho fundamental a la intimidad, a la protección de los datos y justifica no sólo una acción de tutela ante las Agencias de Protección de Datos personales, como después veremos, sino la apertura de un procedimiento contencioso administrativo o un procedimiento civil preferente y sumario de tutela de los derechos fundamentales. Es conveniente señalar las garantías a este derecho de acceso a la historia clínica porque tradicionalmente no ha sido respetado, especialmente en la sanidad privada¹³⁵. Por tanto, como hemos señalado antes, hay que dejar de debatir de quién

¹³¹ También se señala que la información clínica forma parte de todas las actuaciones asistenciales, será verdadera, se comunicará al paciente de forma comprensible y adecuada y está destinada a ayudarle a tomar las decisiones de acuerdo con su propia y libre voluntad. Lógicamente a la hora de facilitar el derecho de acceso del paciente debe tenerse en cuenta el derecho que tiene toda persona a que se respete su voluntad a no ser informada –art. 5 Ley 41/2002–.

¹³² Muchas veces, el derecho de acceso a la historia clínica y a obtener una copia de ésta se produce cuando el paciente, en virtud de su derecho de libre elección, quiere acudir a otro facultativo.

¹³³ El derecho de acceso a la historia clínica en la sanidad pública dispone también de la habilitación que le proporciona el derecho a la información de los ciudadanos y el acceso a los archivos y registros administrativos reconocido en el art. 105.b) CE y en los arts. 35.b) y 37.2 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. No obstante, el art. 37.6.b) de esta Ley remite a regulación específica el acceso a documentos y expedientes que contengan datos sanitarios personales de los pacientes.

¹³⁴ Sobre esta cuestión nos hemos referido en A. TRONCOSO REIGADA, *Privatización, Empresa Pública y Constitución*, Marcial Pons, Madrid, 2007, pp. 180-181.

¹³⁵ Es llamativa la desatención frecuente de este derecho teniendo en cuenta que el derecho de acceso a los ficheros sanitarios y, por tanto, a la historia clínica era ya reconocido también en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal –ya derogada–, y en la propia Ley General de Sanidad –art. 61– y en el Real Decreto de Ordenación de prestaciones sanitarias del Sistema Nacional de Salud.

es la historia clínica. Posiblemente la propiedad de la misma le corresponda al centro, el profesional sanitario mantiene sus derechos de propiedad intelectual, teniendo el paciente derecho de acceso a la documentación clínica y a obtener una copia de los datos que figuren en ella¹³⁶.

El derecho de acceso del paciente a la documentación de la historia clínica no es un derecho absoluto sino que tiene como límite el derecho a la intimidad y a la confidencialidad tanto de los profesionales sanitarios como de terceras personas que han incluido información en interés terapéutico del paciente —art. 18.3 Ley 41/2002, de 14 de noviembre—¹³⁷. Tanto las anotaciones personales del médico como los datos aportados por terceros no constituyen propiamente juicios clínicos, por lo que no formarían parte de la historia clínica y no serían objeto del derecho de acceso. Cuando hemos analizado anteriormente el contenido de la historia clínica no hemos incluido las anotaciones subjetivas ni información de terceras personas, aunque sí los profesionales que le han asistido. Así, por una parte, el derecho de acceso a la historia clínica no puede ir en perjuicio de los derechos de los profesionales sanitarios, los cuales pueden negarse a facilitar el acceso a las anotaciones subjetivas¹³⁸. El art. 18.3 de la Ley 41/2002, de 14 de noviembre señala que deben ser los profesionales los que pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas. Sin embargo, parece razonable que en ocasiones sea la propia unidad de admisión y documentación clínica la que limite el acceso a las anotaciones subjetivas, bien porque el profesional ya no trabaja en ese centro sanitario, bien por no retrasar el ejercicio del derecho de acceso por parte de los pacientes, bien porque esta unidad tiene los criterios técnicos homogéneos que aplicar en estos supuestos. Las anotaciones subjetivas es un concepto jurídico indeterminado que debe interpretarse de manera restrictiva, ya que éstas se constituyen en un límite al derecho de acceso de los pacientes a su historia clínica. Hay que verificar que no se produzca un abuso de la nota subjetiva que la convierta en algo excesivo —que vacíe el derecho de acceso a la propia historia clínica— o no pertinente. No siempre es fácil distinguir las anotaciones subjetivas de aquella información o juicio clínico que refleje el estado de salud del paciente y que necesariamente tiene que ser subjetivo —ya que el profesional sanitario es un sujeto, no un objeto—. Por ello, lo adecuado es que las anotaciones personales de los médicos que no sean profiamente juicios clínicos —sean notas subjetivas— no deben constar en la historia clínica¹³⁹. Esto es espe-

¹³⁶ Cfr. *supra* apdo. 2.b).

¹³⁷ La propia Constitución señala como límite al derecho de acceso a archivos y registros administrativos la intimidad de las personas —art. 105.b) CE—. Cfr. también en este sentido el art. 37.2 LRJAP y PAC.

¹³⁸ Cfr. P. HERNANDO; J. A. SEOANE y J. F. DE ASIS, «La reserva de las anotaciones subjetivas: ¿derecho o privilegio?», *Revista de Calidad Asistencial*, núm. 21, 2006, pp. 31-37 y J. A. SEINE, «Historia clínica y derechos fundamentales: una reflexión sobre las anotaciones subjetivas», *Revista datospersonales.org*, núm. 21, 2006.

¹³⁹ En la Comunidad de Madrid el proyecto AP-Madrid permite que se contenga la nota subjetiva en un apartado separado de la historia clínica al que no puede acceder el paciente. *Memoria del III Premio a las Mejores Prácticas Europeas en materia de Protección de Datos para Administraciones Públicas*, cit. Este proyecto permite un acceso *on line* a la propia información clínica. No obstante se ha optado por su implantación *ex nunc* y no *ex tunc*. La digitalización de las historias clínicas anteriores, además de ser costosa, presenta el problema de que su redacción por el facultativo se hizo pensando en que no iba a ser conocida por el paciente y hay mucha presencia de notas subjetivas.

cialmente recomendable en el caso de las historias clínicas en soporte papel ya que es enormemente difícil impedir materialmente el acceso de los pacientes a las anotaciones subjetivas de los médicos redactadas en la propia historia clínica. Por otra parte, el derecho de acceso del paciente a su historia clínica no alcanza aquellos datos que incluyan información sobre terceros que han facilitado determinados datos en interés terapéutico del paciente. Finalmente, aunque el paciente sea el titular del derecho a la información asistencial y del derecho de acceso a la historia clínica, estos derechos pueden limitarse por la existencia acreditada de un estado de necesidad terapéutica –art. 5.4–. Se entiende por estado de necesidad terapéutica la facultad del médico para actuar profesionalmente sin informar antes al paciente, cuando por razones objetivas el conocimiento de su propia situación pueda perjudicar su salud de manera grave. No se trata de una vuelta al paternalismo y una quiebra de la autonomía del paciente sino de una actuación que va encaminada a la protección de su salud. En este caso, el médico debe dejar constancia razonada de las circunstancias en la historia clínica y comunicará su decisión a las personas vinculadas al paciente por razones familiares o de hecho¹⁴⁰. Estos límites al acceso del paciente a la propia historia clínica establecidos en la Ley 41/2002, de 14 de noviembre, recoge los principios ya consolidados tanto en los textos internacionales como en la jurisprudencia del Tribunal Supremo¹⁴¹.

Analizado ya el derecho de acceso a la historia clínica, nos quedaría por analizar el derecho de rectificación y cancelación. La LOPD señala que cuando una persona tenga constancia de que los datos suyos que están en un fichero son inexactos, incompletos, inadecuados, excesivos o hayan dejado de ser necesarios, puede solicitar al responsable su rectificación o cancelación –art. 16–¹⁴². La Ley 41/2002, de 14 de noviembre, no es muy precisa en relación

¹⁴⁰ Tanto los límites a la información asistencial por el estado de necesidad terapéutica del paciente como la negativa a facilitar las anotaciones subjetivas de los médicos tienen una especial incidencia en los tratamientos psiquiátricos. Cfr: J. SÁNCHEZ-CARO y F. ABELLÁN, *El médico y la intimidad*, cit. pp. 181-198.

¹⁴¹ Esta excepción se encuentra recogida en distintos textos internacionales como la Declaración para la promoción de los derechos de los pacientes en Europa de 1994, la Recomendación, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre protección de datos médicos y el Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la biología y de la medicina, aprobado por el Comité de Ministros del Consejo de Europa y suscrito en Oviedo el 4 de abril de 1997. Cfr: también el análisis del caso Gaskin, juzgado por el Tribunal Europeo de Derechos Humanos, sentencia de 7 de julio de 1989 en J. SÁNCHEZ-CARO y F. ABELLÁN, *Datos de salud y datos genéticos*, cit.

¹⁴² El Real Decreto 1332/1994, de 20 de junio –art. 15– señala que en el caso de los derechos de rectificación, la solicitud deberá indicar el dato que es erróneo y la corrección que debe realizarse y deberá ir acompañada de la documentación justificativa de la rectificación solicitada, salvo que la misma dependa exclusivamente del consentimiento del interesado. En la solicitud de cancelación, el interesado deberá indicar si revoca el consentimiento otorgado, en los casos que la revocación proceda, o si, por el contrario, se trata de un dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa de la cancelación. En todo caso, la cancelación no procederá cuando pudiese perjudicar a intereses legítimos del afectado o de terceros, o cuando existiese una obligación de conservar los datos. El responsable del fichero deberá resolver la petición de rectificación y cancelación en el plazo de cinco días siguientes a la recepción de la solicitud. Si los datos rectificadas o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, a su vez, la lleve a cabo en su fichero. Transcurrido el plazo de cinco días

con el derecho de rectificación y cancelación de la documentación que obra en una historia clínica. Si bien la rectificación es posible en el ámbito sanitario cuando haya datos incorrectos o inexactos¹⁴³, no parece tan sencilla la cancelación de documentos de la historia clínica o de la propia historia clínica. Como hemos señalado anteriormente cuando hemos abordado la cancelación de oficio de documentos y de la propia historia clínica por parte del responsable del fichero¹⁴⁴, el ejercicio del derecho de cancelación podría estar en contradicción con la eficacia de la gestión sanitaria y la necesidad de mantener el contenido de la historia clínica, para facilitar la calidad asistencial y evitar la repetición de pruebas diagnósticas¹⁴⁵. Si bien la LOPD señala la cancelación cuando los datos hayan dejado de ser necesarios, el art. 17.1 de la Ley 41/2002, de 14 de noviembre, expresamente señala que los centros sanitarios están obligados a conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad para la debida asistencia al paciente «durante el tiempo adecuado a cada caso, y como mínimo cinco años desde la fecha del alta de cada proceso asistencial». Además de la conservación de la historia clínica para la debida asistencia al paciente, es necesario conservarla a los efectos judiciales oportunos o cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud, aunque en lo posible, se hará a través de un procedimiento disociado, que evite en lo posible la identificación de las personas afectadas –art. 17.2–. Es necesario, por tanto, que la conservación de la documentación clínica, cuando deje de obedecer a un proceso asistencial activo, se haga preferentemente de manera disociada.

Decía Giannini, que no hay derecho si no hay un Tribunal que lo aplique. Las actuaciones contrarias al derecho fundamental a la protección de datos personales, al derecho a la intimidad y a la confidencialidad de la historia clínica tienen una tutela tanto en el orden jurisdiccional civil, como en el penal así como a través del procedimiento de infracción y sanción y de tutela de derechos que se sustancia ante la Agencia de Protección de Datos.

sin que de forma expresa se responda a la solicitud de rectificación o cancelación, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación que corresponda ante la Agencia de Protección de Datos del Estado o Autonómica.

¹⁴³ En ocasiones es necesario corregir datos erróneos. Por ejemplo, si una historia clínica contiene que una persona es adicta al alcohol y esto no es cierto y se prueba, el paciente podrá exigir la rectificación en la historia clínica.

¹⁴⁴ *Cfr. supra 2.c).*

¹⁴⁵ Por ejemplo, no parece fácil cancelar datos relativos a un cáncer o una angina de pecho. El Real Decreto 1851/2005, de 16 de septiembre, establece la obligación de los centros de transfusión de contar con un registro de donantes con la identidad, historial y firma del donante, durante un plazo de tiempo al menos de 15 años en el caso de donaciones no utilizadas y de 30 años si la sangre ha sido transfundida –arts. 33 y 42–. No hará falta el consentimiento del interesado pero sí el cumplimiento del principio de información. La Recomendación 1/2004 ya mencionada señala que con periodicidad anual y siguiendo los criterios de la Comisión Central de Documentación Clínica u órgano equivalente, la Unidad de Admisión y Documentación Clínica o servicio equivalente hará una propuesta de expurgo y destrucción de los documentos de las historias clínicas correspondientes a episodios concluidos y que tengan una antigüedad superior al período establecido en la normativa vigente como mínimo y obligatorio de conservación de las mismas.

Así, muchas vulneraciones del derecho a la protección de los datos de salud tienen el carácter de intromisiones ilegítimas en el derecho a la intimidad de la persona, por lo que le es de aplicación la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen está plenamente vigente. Como hemos señalado, antes, la tutela de este derecho fundamental a la protección de datos personales se encontraría en el procedimiento preferente y sumario previsto para las vulneraciones de los derechos fundamentales de la Sección 1ª del Capítulo II del Título I. Si la lesión se produce en un centro sanitario público, la remisión debería ser al procedimiento de amparo contencioso previsto en la Ley 29/1998; si se produce en un centro privado, al procedimiento de amparo civil previsto en la Ley de Enjuiciamiento civil¹⁴⁶.

Es posible también acudir al procedimiento penal cuando se produzcan lesiones del derecho por los delitos del Título X del Código Penal «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», especialmente por los previstos en el Capítulo I «Del descubrimiento y revelación de secretos» —arts. 197-200—. Así, el que se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, cuando estos hechos afecten a datos de carácter personal que revelen ideología, religión, creencias, salud, origen racial o vida sexual o la víctima fuera un menor de edad o incapaz se le impondrá la pena de prisión de tres a cinco años —art. 197.5 del Código Penal—¹⁴⁷. Así, recientemente la Sala Penal del Tribunal Supremo ha considerado que la utilización de los datos personales de los pacientes de la sanidad pública con la finalidad de enviarles propaganda de las actividades desarrolladas en una clínica privada para obtener un beneficio económico incurre en un delito de uso indebido de información privilegiada¹⁴⁸.

Además, la Agencia de Protección de Datos es una autoridad control consecuencia de su competencia de velar por el cumplimiento de la legislación de protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación —art. 37.a) LOPD—. Así, la Agencia vela por el cumplimiento del principio de calidad, información, consentimiento, seguridad de los datos y deber de secreto. La vulneración de estos principios da lugar al ejercicio por la Agencia del procedimiento de infracción y de la potestad sancionadora. Igualmente, los interesados tienen también el derecho a ser indemnizados cuando sufran lesión

¹⁴⁶ Cfr. J. GARCÍA MORILLO, *La protección judicial de los derechos fundamentales*, Tirant lo Blanch, Valencia, 1994. M. CARRILLO, *La tutela de los derechos fundamentales por los Tribunales ordinarios*, CEC, Madrid, 1995.

¹⁴⁷ En Sentencia de 18 de febrero de 1999, la Sala de lo Penal del Tribunal Supremo condenó a un periodista, en virtud del art. 197 del Código Penal, por el delito de revelación de secretos, al apoderarse y utilizar en perjuicio de terceros datos reservados de carácter personal registrados en soportes informáticos, de los que se sirvió para publicar un artículo sobre dos internos en un centro penitenciario, enfermos de SIDA, que trabajaban en la cocina del mismo. Cfr. J. GÓMEZ NAVAJAS, *La protección de los datos personales. Un análisis desde la perspectiva del Derecho Penal*, Civitas, Madrid, 2005.

¹⁴⁸ STS, de 14 de enero de 2002.

por sus bienes o derechos como consecuencia del incumplimiento de la legislación –art. 19 LOPD–. Cuando se trate de ficheros de servicios sanitarios públicos, la responsabilidad se exigirá de conformidad con la legislación reguladora de la responsabilidad de las Administraciones Públicas; en el caso de que sean ficheros de servicios sanitarios privados, la acción se ejercitará ante los órganos de la jurisdicción ordinaria. Igualmente, las denegaciones de los derechos de acceso, rectificación y cancelación pueden ser objeto de reclamación ante la Agencia de Protección de Datos –art. 18 LOPD–. Así, el interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación podrá ponerlo en conocimiento de la Agencia de Protección de Datos, o en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación. El plazo máximo en que debe dictarse la resolución expresa de tutela es de seis meses. Contra las resoluciones de la Agencia de Protección de Datos existe la posibilidad de presentar un recurso contencioso-administrativo.

III. EL ACCESO A LA HISTORIA CLÍNICA POR PERSONAS DISTINTAS AL INTERESADO. LA CESIÓN DE LA HISTORIA CLÍNICA

a) *El acceso a la historia clínica por parte de familiares y terceras personas*

El acceso a los datos personales recogidos en un fichero solo puede realizarse por el titular de los datos –o por quien lo represente– en el ejercicio del derecho de acceso o por los empleados autorizados dentro de la persona jurídica del responsable del fichero –dentro del marco del propio principio de calidad–. Por tanto, sólo pueden acceder a la historia clínica el propio interesado y los profesionales que le atiendan en el centro sanitario. Ninguna otra persona puede acceder a esta información personal salvo que exista el consentimiento del interesado o una habilitación legal. Así, la Ley 41/2002, de 14 de noviembre indica que «toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley». Así, se obliga a los centros sanitarios a adoptar las medidas oportunas para garantizar este derecho, teniendo que elaborar las normas y los protocolos necesarios que garanticen el acceso legal a los datos de los pacientes –art. 7–. No es fácil calificar jurídicamente la solicitud de acceso a una historia clínica por una persona distinta al interesado –un familiar, la persona que conviva–. El art. 11 LOPD señala que los datos de carácter personal objeto de tratamiento «sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado». Si bien no parece razonable calificar como cesión el acceso de un familiar –ya que este no va a efectuar un posterior tratamiento de

esta información—, sí parece adecuado considerar que este acceso sólo es legítimo si existe el consentimiento del interesado o una previsión legal. Por ello, el acceso a la historia clínica por parte de terceras personas distintas al interesado tiene que partir del reconocimiento del derecho a la intimidad y a la protección de los datos de salud de los pacientes, lo que impide su conocimiento por los demás. El consentimiento del interesado para la cesión de datos es una garantía esencial de la intimidad y de la confidencialidad de esa información personal. La ley es la única forma de exceptuar este consentimiento porque sólo por ley se pueden limitar derechos fundamentales. Esto es especialmente aplicable a las historias clínicas.

Un caso específico es el acceso a la historia clínica por parte de personas allegadas. Así, en relación con la información asistencial, el art. 5 señala que también serán informadas las personas vinculadas a él, por razones familiares o de hecho, «en la medida que el paciente lo permita de manera expresa o tácita». 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 hecho¹⁴⁹. Es decir, para que estas personas vinculadas al paciente conozcan esta información asistencial es necesario que éste lo autorice, de manera expresa o tácita¹⁵⁰, o que carezca ya de capacidad. Lógicamente el conocimiento de esta información asistencial por parte de estas personas vinculadas al paciente supone el acceso a la historia clínica. En el resto de los supuestos, las personas vinculadas al paciente por razones familiares o de hecho no tienen acceso a la historia clínica¹⁵¹.

Un caso específico es el acceso a la historia clínica de los pacientes ya fallecidos. A nuestro juicio tienen derecho a la protección de datos personales tanto las personas vivas como los fallecidos. Sin embargo, el Proyecto de Real Decreto 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 señala que «[e]l Reglamento no será de aplicación a los datos referidos a personas fallecidas»¹⁵². La versión anterior era más amplia ya que hablaba «sin perjuicio de lo previsto en las Leyes y, en particular, de los derechos reconocidos

¹⁴⁹ El legislador debía haber establecido un orden en los familiares o en las personas vinculadas por razones de hecho en relación con la información y con el acceso a la historia clínica.

¹⁵⁰ Es contradictorio que se exija el consentimiento expreso o una habilitación legal para el tratamiento de datos de salud y se autorice la cesión de esta información a un familiar a través de un consentimiento tácito, que no es fácil de probar. En este caso, hay que entender que el art. 5 de la Ley 41/2002, de 14 de noviembre sería la habilitación legal que exige los arts. 7.3 y 11 LOPD.

¹⁵¹ En todo caso hay que señalar que, a diferencia de la Ley 15/1999, de 13 de diciembre y del art. 11 del Real Decreto 1332/1994, de 20 de junio, cuyo tenor literal insiste en el carácter personalísimo de este derecho y de que sólo puede actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o de minoría de edad que le imposibilite el ejercicio personal de los mismos, el art. 18.2 de la Ley 41/2002, de 14 de noviembre señala la posibilidad de que el derecho de acceso a la historia clínica sea ejercido por representación debidamente acreditada.

¹⁵² Establece como excepción que los familiares podrán dirigirse a los responsables de los ficheros para notificar el óbito y solicitar la cancelación. También prevé que los causahabientes puedan ejercer el derecho de acceso a los datos del causante, salvo que éste lo hubiera prohibido expresamente —art. 20.4—.

en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen». Como es sabido, la Ley Orgánica 1/1982, de 5 de mayo, sí reconoce a las personas fallecidas el ejercicio de los derechos al honor, a la intimidad o la imagen, que es ejercitado por sus familiares o por el Ministerio Fiscal. El derecho a la intimidad no se pierde con la muerte, ni tampoco la obligación del secreto médico. No parece razonable reconocer el derecho al honor y a la intimidad a las personas fallecidas y negarles el derecho fundamental a la protección de datos personales, que es también un derecho de la esfera personal y que se constituye muchas veces en una garantía del derecho a la intimidad. Mucho menos que esta limitación se haga a través de un Reglamento, ya que la titularidad de un derecho fundamental está sometido a reserva de Ley, en este caso, a reserva de Ley Orgánica. La Ley 41/2002, de 14 de noviembre reconoce a los familiares el derecho de acceso a la historia clínica del fallecido¹⁵³. Ni el derecho a la intimidad del paciente ni el secreto médico prescriben tras su muerte.

La Ley 41/2002, de 14 de noviembre regula expresamente el acceso de los familiares a la historia clínica del paciente fallecido. Así, señala que «[l]os centros sanitarios y los facultativos de ejercicio individual solo 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 hubiera 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. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros» –art. 18.4–.

El acceso de familiares o de terceras personas a la historia clínica de fallecido es una cuestión compleja. De la lectura de este precepto, se podrían extraer dos interpretaciones, más o menos restrictivas, en relación con el acceso de los familiares a la historia clínica del fallecido. La primera sería considerar terceras personas a las personas vinculadas al fallecido por razones familiares o de hecho por lo que éstas sólo podrán acceder a la historia clínica cuando exista un riesgo para su salud y sólo a aquellos pertinentes. Consideramos que esta interpretación es demasiado restrictiva, ya que una persona que el propio legislador califica como vinculada al paciente por razones familiares o de hecho no debe ser considerada un tercero. No tiene sentido que el legislador distinga entre familiares y terceras personas si el tratamiento va a ser semejante. Tampoco tiene sentido afirmar primero el acceso a la historia clínica de los familiares salvo que el fallecido lo haya prohibido expresamente para después limitarlo a los supuestos de un riesgo grave para la salud. Además, es contradictorio que las personas vinculadas al paciente por razones familiares o de hecho tengan un acceso pleno a información clínica mientras el paciente todavía vivo carezca de capacidad para entender –art. 5.3– y después no puedan

¹⁵³ De hecho, hasta ahora la Agencia Española ha dado tutela del derecho de los familiares al acceso a la historia clínica de los fallecidos.

acceder a la información cuando el paciente haya fallecido. Además, esta interpretación restrictiva limitaría mucho el ejercicio de acciones judiciales por errores médicos ya que el acceso a la historia clínica debería hacerse en el marco de un proceso civil ya iniciado sin haber valorado previamente los datos obrantes en la historia clínica y, por tanto, con el peligro de una condena en costas. La segunda posibilidad sería entender que las personas vinculadas al paciente por razones familiares o de hecho pueden acceder a la historia clínica salvo que el fallecido se hubiera opuesto y esto se acredite¹⁵⁴. En este último caso, sólo podrán acceder cuando exista un grave riesgo para su salud y sólo a los datos pertinentes ya que el derecho a la vida del familiar es más importante que el derecho a la intimidad del fallecido. De esta forma, la intimidad del paciente se encontraría suficientemente protegida dándole la oportunidad de oponerse expresamente a este acceso y, especialmente, prohibiendo en todo caso el acceso a información «que afecte a la intimidad del fallecido». La consideración de familiar debe alcanzar a la mujer, hijos, padres y hermanos –no al primo segundo– y la relación de hecho debe estar acreditada en el correspondiente registro o con la inscripción patronal. Los terceros son aquellas personas que no están vinculadas al paciente por razones familiares o de hecho. Estas sólo pueden acceder a la historia clínica cuando exista un grave riesgo para su salud y no a toda ella sino solo a los datos pertinentes¹⁵⁵. Lógicamente, el acceso de los familiares o de terceras personas a la historia clínica se encuentra sometido a los mismos límites que el acceso practicado por el propio paciente. No se facilitará, por tanto, información que afecte al derecho a la intimidad de terceras personas, lo que limita el acceso a aquellos datos aportados por terceros en interés terapéutico del paciente o a las anotaciones subjetivas de los médicos.

b) *El acceso a la historia clínica por los profesionales sanitarios, por el personal de administración y gestión y por el personal de inspección*

Los profesionales sanitarios deben también tener acceso a la historia clínica y así lo recoge expresamente la Ley 41/2002, de 14 de noviembre. Este no sería un supuesto de cesión de datos sino de acceso dentro del marco del responsable del fichero que debe estar previsto en el propio documento de seguri-

¹⁵⁴ N. de Miguel critica que la Ley se haya mostrado tan generosa con el acceso por parte de familiares a la información sanitaria, algo que resulta especialmente peligroso en el caso del paciente fallecido. Esta autora propone otros medios para cubrir la expectativa de los familiares como sería el acceso a la autopsia de practicarse ésta o la reclamación de la historia en el transcurso de un proceso judicial. Cfr. N. DE MIGUEL, «Intimidad e historia clínica», *cit.* pp. 20 y 30.

¹⁵⁵ J. Sánchez Caro y F. Abellán –que mantienen una posición restrictiva en este ámbito– han estudiado el acceso a la historia clínica por parte de parientes o familiares que hayan convivido con el paciente y tengan la posibilidad de ser contagiados de la enfermedad que padeciera el difunto. Se trata de analizar si el médico debe revelar las circunstancias de la enfermedad a las personas referidas. El mismo problema se presenta con las enfermedades hereditarias. Los autores señalan que la solución debe adoptarse a partir del principio de proporcionalidad y debe ponderar los bienes y valores en conflicto, incluido, desde luego, la gravedad de la enfermedad; 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. Cfr. J. SÁNCHEZ-CARO y F. ABELLÁN, *Datos de salud y datos genéticos*, *cit.*

dad. Como hemos señalado anteriormente, la historia clínica es un instrumento destinado fundamentalmente a garantizar una adecuada asistencia al paciente. Por este motivo, los profesionales sanitarios del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia –art. 16.1–. Esto significa que los profesionales sanitarios que no presten o que hayan dejado de prestar atención sanitaria a un paciente no deben acceder a su historia clínica¹⁵⁶. Cada centro «establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten» –art. 16.2–. Por ello, es fundamental que en los sistemas de historia clínica electrónica no se prevea un acceso general de todos los facultativos a todas las historias clínicas sino sólo a las de aquellos pacientes a los que se les presta asistencia¹⁵⁷. Así, los médicos de atención primaria deben poder acceder a los pacientes de su cupo pero no a todos los pacientes de esa área¹⁵⁸. Otro paso aún más importante es que el profesional sanitario no acceda a toda la información clínica del paciente sino sólo a aquella que le interese. Así, no es indispensable que un traumatólogo que atiende al paciente acceda a información de psiquiatría o de ginecología. Se habla así de la necesidad de unos sobres diferenciados dentro de la historia clínica electrónica como garantía de la confidencialidad. En todo caso, el establecimiento de niveles de acceso no debe perjudicar la asistencia y debe poder justificarse la excepción en casos concretos. No olvidemos que se ha superado la fase de una visión especializada para recuperar una visión más integral del paciente. Además, es conveniente establecer la posibilidad de que lo que un paciente revela a un concreto facultativo, si el paciente lo desea, no sea conocido por otros profesionales sanitarios: «Esta información te la digo solamente a ti y sólo la puedes ver tú». En todo caso, si el profesional considera que esta información es relevante para su salud y debe ser conocida por otros facultativos, debe tratar de convencer al paciente, dada la preferencia del derecho a la vida sobre la intimidad¹⁵⁹.

¹⁵⁶ El médico no puede acceder a la historia clínica de un paciente al que ya no presta asistencia sanitaria con la finalidad de defenderse en una demanda. El acceso legítimo es sólo para prestar una adecuada asistencia por lo que en este caso requeriría una autorización judicial. El problema reside en que en muchas demandas a médicos por responsabilidad civil es necesario contestar en un plazo perentorio –veinte días–. El respeto al principio de finalidad de la historia clínica no puede perjudicar el derecho a la tutela judicial efectiva del médico. Esta es una cuestión que debe aclararse en el ámbito del derecho procesal. En todo caso, es razonable considerar que dentro de la finalidad de la historia clínica está también la defensa de una determinada asistencia sanitaria lo que justificaría una autorización del órgano administrativo competente para permitir al médico el ejercicio del derecho de defensa. De igual forma, si la finalidad del acceso de un profesional a la historia clínica debe ser asistencial, éste no puede acceder a la historia clínica de un paciente para identificar a un familiar con el que ha tenido un altercado en el aparcamiento del hospital para poder presentar una denuncia.

¹⁵⁷ Lo mismo se puede decir del establecimiento de criterios restrictivos en el acceso al registro de últimas voluntades.

¹⁵⁸ En el modelo de AP-Madrid, no se establece una historia clínica centralizada entre atención primaria y especializada. No toda la información que está en primaria le interesa a la atención especializada. Lo que se pone en marcha es una interoperabilidad y un intercambio de información.

¹⁵⁹ El proyecto de informatización de la historia clínica de la Comunidad de Madrid presenta algunas ventajas en relación a la confidencialidad. *Cfr. Memoria del III Premio a las Mejores Prácticas Europeas en materia de Protección de Datos para Administraciones Públicas, cit.*

La finalidad de la historia clínica no es sólo el diagnóstico, la asistencia sanitaria o los tratamientos médicos sino también la gestión de los servicios sanitarios. Si los profesionales sanitarios pueden acceder a toda la historia clínica de sus pacientes, en cambio, el personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones –como por ejemplo, la cita previa, la admisión del paciente o las funciones contables y presupuestarias–, no estando legitimados para un acceso total a la historia clínica –art. 16.4 de la Ley 41/2002, de 14 de noviembre–. La historia clínica electrónica facilitará el establecimiento de distintos niveles de acceso a la historia clínica. En cambio, esto no parece de fácil aplicación a las historias clínicas en papel¹⁶⁰. Este planteamiento obliga a disponer en la unidad de admisión y documentación clínica o unidad equivalente de una relación –al menos por puestos, dado la movilidad del personal destinado en centros sanitarios– del personal autorizado a acceder a las historias clínicas, diferenciando entre el profesional sanitario y el personal de administración y gestión y diferenciando también qué documentos son accesibles por ambos. Como hemos señalado antes, es necesario que se archive de forma separada la documentación clínica que forma parte de la historia clínica *ex art.* 15 de la Ley 41/2002, de 14 de noviembre, de toda la documentación administrativa que la gestión de la historia puede generar como los documentos contables, las hojas de admisión o la hojas de cita previa que no forman parte de la historia clínica y a las que accede frecuentemente el personal de administración y gestión.

El problema estaría en el acceso de los trabajadores sociales a la historia clínica. Si bien el trabajo social no es una profesión sanitaria incluida como tal en la Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias, los trabajadores sociales tienen un deber de secreto idéntico al de los profesionales sanitarios. Sin embargo, la actividad de un trabajador social no es de prevención, de diagnóstico médico, de asistencia sanitaria o de gestión de servicios sanitarios sino que es una actividad de asistencia social. En todo caso, dado que la actividad sanitaria es cada vez más sociosanitaria y que en los equipos asistenciales puede haber médicos y trabajadores sociales, es razonable considerar a éstos, al menos, como un personal de administración y gestión de los centros sanitarios que sólo podrán acceder a los datos de la historia clínica relacionados con sus propias funciones –art. 16.4 Ley 41/2002, de 15 de noviembre–. El acceso a la historia clínica de los trabajadores sociales se limitará a una información mínima y para el ejercicio de las propias funciones. Son muchos los centros sociales que prestan también una actividad sanitaria. Esta última se desarrollará por profesionales sanitarios por lo que se deberá tener especial cuidado en dife-

¹⁶⁰ En la actualidad parece compleja la implantación de estos dos diferentes niveles de acceso –para profesionales sanitarios y para el personal de administración y gestión– a la historia clínica, dadas las peculiaridades de la realidad sanitaria –por ejemplo, el Hospital Universitario La Paz tiene 2 millones de historias clínicas con una media de 100 documentos cada una–. Esto no obsta para que, como principio y programa que debe guiar la actuación de la Administración Sanitaria, se encuentre el distinguir estos dos niveles de acceso a la historia clínica, de forma que el personal de administración y gestión de los centros e instituciones sanitarias acceda únicamente a aquellos datos de la historia clínica relacionados con sus propias funciones. *Cfr.* es esta dirección Recomendación 2/2004 ya citada. En algunos hospitales, por ejemplo, se sigue el criterio de no dar la historia clínica salvo al jefe de servicio. Si un médico residente pide la historia clínica, debe consultarla en la propia unidad de admisión y documentación clínica. Si lo pide el personal de administración y gestión, debe canalizar esta petición a través de la dirección médica del hospital.

renciar y separar el archivo y custodia de los datos de la historia social de aquellos que tienen como un fin específicamente asistencial sanitario y que se integran en la historia clínica del usuario¹⁶¹. La historia social sólo podrá recoger aquellos datos de salud que repercutan en la situación personal y social del usuario de la prestación social y siempre con el consentimiento expreso del afectado. Por tanto, el hecho de que este acceso del trabajador social a la historia clínica de un paciente no esté previsto legalmente no significa que esté prohibido. Significa simplemente que deberá requerirse al paciente o a su representante legal su consentimiento expreso¹⁶².

Por último, hay que analizar el acceso a las historias clínicas del personal de inspección, evaluación, acreditación y planificación. La Ley 41/2002, de 14 de noviembre establece que el personal sanitario que ejerza funciones de inspección, evaluación, acreditación y planificación tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia y de garantía del respeto a los derechos del paciente o a cualquier otra obligación del centro en relación con pacientes, usuarios, o la propia Administración sanitaria –art. 16.6–. Es razonable que la inspección sanitaria, que son profesionales sanitarios con la condición de funcionarios que llevan a cabo una labor de control, pueda acceder a historias clínicas e, incluso, retirarlas de un centro sanitario cuando se haya vulnerado el derecho a la intimidad y a la confidencialidad de los pacientes, haya riesgos para su adecuada custodia o conservación o con la pretensión de asegurar la remisión a los Tribunales en un procedimiento judicial abierto¹⁶³. El acceso de la inspección a la historia clínica sea un supuesto de acceso o de cesión dependerá de que la historia clínica se encuentre descentralizada por centros o por áreas o se encuentre centralizada. En el primer supuesto se tratará de una cesión de datos sin consentimiento del interesado habilitada por Ley; en el segundo supuesto se tratará de un acceso legítimo al fichero centralizado de historias clínicas dentro del marco del principio de calidad.

Existen otros posibles accesos o comunicaciones de datos de historias clínicas no previstos en la Ley 41/2002, de 14 de noviembre y que se plantean frecuentemente. Uno de estos supuestos es el acceso –o la comunicación de datos– de la historia clínica que tengan relevancia económica a la Intervención y a las unidades de control financiero, aunque éstas no tengan el carácter de

¹⁶¹ Cfr. la Recomendación 1/2005 de la Agencia de Protección de Datos de la Comunidad de Madrid sobre Archivo, Uso y Custodia de la Documentación que compone la Historia Social no informatizada. A esta cuestión me he referido en la «Introducción» a la *Guía de Protección de Datos en Servicios Sociales Públicos*, Civitas, Madrid, 2004.

¹⁶² Así, muchos trabajadores sociales deben conocer la medicación o las recetas dispensadas a los usuarios para realizar prestaciones domiciliarias o asistenciales a personas discapacitadas, mayores, e incluso para la propia seguridad en el trabajo en relación con pacientes con perturbaciones mentales o que puedan presentar episodios de violencia.

¹⁶³ Así, por ejemplo, en el caso del Hospital Severo Ochoa de Leganés la inspección retiró las historias clínicas del centro sanitario para garantizar la seguridad y confidencialidad de esa información. En virtud del art. 124.2 del Decreto 2065/1974, de 30 de mayo, que aprueba el Texto Refundido de la Ley General de Seguridad Social establece que los inspectores médicos y farmacéuticos del cuerpo de inspección sanitaria de la Administración de la Seguridad Social tendrán la consideración de autoridad pública.

personal sanitario. Sería acceso si esta unidad de intervención o de control financiero estuviera en el marco del responsable del fichero y sería cesión si está fuera de él. El principio de calidad permite el acceso a la documentación de la historia clínica a las personas autorizadas por el responsable del fichero en virtud de una finalidad compatible con la finalidad principal. En resumidas cuentas, se trata de que las personas adecuadas tengan la información adecuada para las finalidades adecuadas. El personal de intervención y las unidades de control financiero pueden ser consideradas personal de administración y gestión de manera que accedan solamente a aquella información necesaria para el cumplimiento de sus funciones. En el caso de que sea una cesión de datos –el control por parte de una intervención general–, hemos señalado anteriormente que el art. 11.2.a) LOPD permite la comunicación de datos sin consentimiento del interesado cuando exista previsión legal. Pues bien, tanto la legislación estatal como la autonómica establece que todos los actos, documentos y expedientes de la Administración de los que se deriven derechos y obligaciones de contenido económico, serán objeto de control por parte de la Intervención de la Administración. Lógicamente, la Intervención sólo puede acceder a datos que tengan repercusiones económicas como instrumento para controlar la legalidad del gasto¹⁶⁴. No olvidemos, por último, que el art. 11.2.d) LOPD expresamente autoriza la comunicación de datos al Tribunal de Cuentas o a los órganos autonómicos que cumplan funciones análogas.

c) *La cesión de la historia clínica para fines epidemiológicos, de salud pública y de investigación. La cesión de la historia clínica a la Administración sanitaria, a las compañías aseguradoras, a los órganos judiciales y a las Fuerzas y Cuerpos de Seguridad del Estado*

La propia Ley Orgánica 15/1999, de 13 de diciembre, establece que, con carácter general, el tratamiento de datos de salud requiere el consentimiento expreso del interesado o la existencia de una habilitación legal –art. 7.3 LOPD–. Este precepto excluye los supuestos de excepción del consentimiento previstos en el art. 6.2 LOPD ya que estos están destinados a tratamientos de datos que no sean especialmente protegidos. De hecho, las excepciones al supuesto más claro de tratamiento de datos de salud –consentimiento expreso y habilitación legal– se encuentran recogidas en el propio art. 7.6 LOPD –prevención, diagnóstico, asistencia y gestión de servicios sanitarios– y en el art. 8 LOPD –tratamiento de datos de salud de las personas que acudan o vayan a ser asistidas en un centro sanitario–.

Lógicamente, el criterio del consentimiento expreso y la habilitación legal para el tratamiento de datos de salud debe también aplicarse a las cesiones de datos de salud. El art. 11.1 LOPD señala que los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del

¹⁶⁴ Cfr. la Recomendación 2/2004 en la que se hace mención a esta cuestión.

cedente y del cesionario, con el consentimiento previo del interesado, consentimiento que para los datos de salud debe ser expreso. El art. 11.2 LOPD señala que, si bien la comunicación de datos a un tercero exige el previo consentimiento del interesado, no será preciso ese consentimiento en los siguientes supuestos: cuando la cesión se encuentre autorizada en una Ley; cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros; cuando la comunicación tenga por objeto los órganos judiciales o el Ministerio Fiscal, al Defensor del Pueblo, Tribunal de Cuentas en el ejercicio de las funciones que tengan atribuidas; cuando la cesión se produzca entre Administraciones Públicas y tenga por el objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos; o cuando la cesión de datos de carácter personal relativos a la salud «sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica» –art. 11.2–. Igualmente se señala que es legítima la comunicación de datos sin consentimiento del interesado cuando se produzca entre Administraciones Públicas que desarrollan idénticas competencias sobre las mismas materias –art. 21.1 LOPD–.

El problema es ahora determinar si estas excepciones al consentimiento para la cesión de datos a terceras personas se aplican también a los datos de salud. Inicialmente, si las excepciones del consentimiento para el tratamiento del art. 6.2 LOPD sólo se emplean para datos que no son especialmente protegidos, teniendo los datos de salud sus propias excepciones para el tratamiento, parece que tampoco le deben ser de aplicación las excepciones al consentimiento para la cesión que se aplicarían a todos los datos que no fueran especialmente protegidos. Desde esta perspectiva, la comunicación de datos de salud exigiría como regla general el consentimiento expreso o la existencia de una habilitación legal –art. 7.3 LOPD–. No obstante, parece que el legislador está pensando en los datos de salud cuando establece en el art. 11.2 LOPD como excepción del consentimiento «cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica». Además, no tiene mucho sentido impedir la comunicación de datos entre Administraciones Públicas que desarrollan idénticas competencias sobre las mismas materias, que en este caso equivale a la comunicación de datos entre centros públicos sanitarios con finalidad asistencial cuando el hecho de que sea una cesión o un acceso vinculado al principio de calidad depende únicamente de donde se sitúe la responsabilidad del fichero de historias clínicas –si en la Consejería o en el centro sanitario concreto–. Esta habilitación en el caso de los datos de salud también puede obtenerse ex arts. 7.6 y 8 LOPD ya que se trata de una cesión de datos para la prevención, el diagnóstico, la asistencia, los tratamientos médicos y la gestión de la asistencia sanitaria y son datos de personas que acuden a centros sanitarios o van a ser tratados en los mismos.

Además, algunos de los supuestos de cesión establecidos en el arto 11.2 LOPD han sido refrendados por la Ley 41/2002, de 14 de noviembre. La Ley 41/2002, de 14 de noviembre no prevé la cesión de datos de salud al Ministerio Fiscal ni al Defensor del Pueblo, pero parece que ésta es razonable ya que se trata también de órganos de tutela de los derechos fundamentales, si bien la comunicación debe limitarse a la información indispensable, como exigencia del propio principio de calidad. En cambio, no parece adecuado entender como excepción al consentimiento «cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros» ya que este supuesto contradice una exigencia de consentimiento expreso¹⁶⁵. En todo caso, si bien están vigentes algunos supuestos para la comunicación de datos de salud en virtud de los arts. 11 y 21 LOPD, esto no suprime el esfuerzo por alcanzar un consentimiento expreso o una habilitación legal clara para el tratamiento de datos de salud, especialmente cuando se trate de finalidades no asistenciales¹⁶⁶, como es el caso de las cesiones de datos a la Seguridad Social¹⁶⁷ y a la Administración Tributaria¹⁶⁸.

Hemos señalado antes que, si bien el fin principal de la historia clínica es la asistencia al paciente, hay otros fines compatibles como son los fines epide-

¹⁶⁵ Esta es la posición más general de la Agencia Española en los informes remitidos a las consultas de la Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA).

¹⁶⁶ Hay Leyes que expresamente prevén la cesión de datos, como el Decreto-Ley 9/1993, de 28 de mayo, que establece la cesión de información de ayudas sociales a afectados por VIH al Ministerio de Economía y Hacienda. La excepción del consentimiento de los afectados en virtud de la previsión legal no suprime la vigencia del principio de calidad, esto es, que la cesión se limite a los datos adecuados y pertinentes para el control de la subvención. Igualmente, la propia Ley Orgánica de Protección de la Salud y de Lucha contra el Dopaje en el Deporte prevé la comunicación de determinados datos de salud de los deportistas a organismos no sanitarios para el control del dopaje.

¹⁶⁷ La Disposición Adicional Cuadragésima de la Ley General de la Seguridad Social señala: «En los procedimientos de declaración de la incapacidad permanente, a efectos de las correspondientes prestaciones económicas de la Seguridad Social, así como en lo que respecta al reconocimiento o mantenimiento del percibo de las prestaciones de incapacidad temporal, orfandad o asignaciones familiares por hijo a cargo, se entenderá otorgado el consentimiento del interesado o de su representante legal, a efectos de la remisión, por parte de las instituciones sanitarias de los informes, documentación clínica y demás datos médicos estrictamente relacionados con las lesiones y dolencias padecidas por el interesado que resulten relevantes para la resolución del procedimiento, salvo que conste oposición expresa y por escrito de aquellos».

¹⁶⁸ Existe también una previsión amplia para la cesión de datos a la Administración Tributaria en virtud del art. 112.4 LOPD —a partir de la redacción de la LOPD— que exceptúa la exigencia de funciones semejantes sobre materias comunes del art. 21 LOPD. No parece claro si estamos ante un supuesto de excepción del consentimiento para la cesión que se incardina en el art. 11 LOPD —por lo que tendría más dificultad para aplicarse a los datos especialmente protegidos del art. 7 LOPD, lo que requeriría de otra habilitación legal que mencionara la cesión de datos de salud a la Administración Tributaria— o ante una habilitación general para la cesión de datos a la Administración Tributaria. No obstante, el arto 111 de la Ley General Tributaria señala que «toda persona natural o jurídica, pública o privada, estará obligada a proporcionar a la Administración Tributaria toda clase de datos, informes o antecedentes con trascendencia tributaria, deducidos de sus relaciones económicas, profesionales o financieras con otras personas». La referencia a toda clase de datos del legislador incluye, a nuestro juicio, los datos de salud. En todo caso, es aplicable también en este caso el principio de calidad por lo que la cesión de datos debe limitarse a los mínimos imprescindibles para cumplir la finalidad. Así, se ha planteado la necesidad de ceder desde los centros médicos la relación de pacientes atendidos, régimen económico y médico correspondiente, para proceder a una comprobación de los ingresos de los profesionales médicos. Esta comunicación debe contener la menor información posible referida a los pacientes como exigencia del principio de calidad.

miológicos, de salud pública o de investigación y de docencia. La LOPD no considera fines incompatibles los estadísticos o científicos –art. 4.2–¹⁶⁹. Estamos hablando de un tratamiento de la historia clínica –que sería acceso si se produce en el marco del responsable del fichero o cesión si se produce fuera de él– para fines epidemiológicos, de salud pública, de investigación o docencia sin consentimiento del interesado. En este caso, el conflicto se produce entre el derecho a la intimidad del paciente, y el derecho a la salud entendido en su acepción comunitaria de bien colectivo¹⁷⁰. En la regulación de los usos de la historia clínica el legislador no sólo debe tener presente la tutela del derecho individual a la intimidad o la vida sino también otros bienes colectivos como la salud pública o la investigación, que tienen una especial relevancia para todo¹⁷¹. El propio art. 6 de la Ley 41/2002 reconoce el derecho a una información epidemiológica, señalando que «[l]os ciudadanos tienen derecho a conocer los problemas sanitarios de la colectividad cuando impliquen un riesgo para la salud pública o para la salud individual, y el derecho a que esta información se difunda en términos verdaderos, comprensibles y adecuados para la protección de la salud, de acuerdo con lo establecido por la Ley»¹⁷². Ya hemos señalado que la LOPD establece en el art. 11.2.c) que la cesión de datos de carácter personal relativa a la salud no exige el consentimiento del interesado cuando «sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica». Por ello, la Ley 41/2002, de 14 de noviembre señala que «el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter personal y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación a cada caso» –art. 16.3–¹⁷³. El acceso a la historia clínica con esos fines queda claro en la regulación de la conserva-

¹⁶⁹ Cfr. *supra* apdo. 2.c). Osakidetza-Servicio Vasco de Salud ha aprobado un procedimiento de acceso a la documentación clínica de atención primaria para uso no asistencia. Cfr. *Memoria del II Premio a las Mejores Prácticas Europeas en materia de Protección de Datos*, Civitas, Madrid, 2006, pp. 391-412.

¹⁷⁰ Exposición de Motivos de la Ley 41/2002, de 14 de noviembre.

¹⁷¹ La Directiva Comunitaria 95/46, de 24 de octubre, apunta la presencia de otros intereses generales como los estudios epidemiológicos, las situaciones de riesgo grave para la salud de la colectividad, la investigación y los ensayos clínicos, que, cuando están incluidas en normas de rango de Ley, pueden justificar una excepción motivada a los derechos del paciente. En esta línea, la Recomendación de 13 de febrero de 1997, del Consejo de Europa, relativa a la protección de los datos médicos, después de afirmar el principio del consentimiento del interesado, indica que este principio puede restringirse si así lo dispone una ley y constituye una medida necesaria para el interés general. Cfr. J. SÁNCHEZ CARO y F. ABELLÁN, *Derechos y Deberes de los Pacientes. La Ley 41/2002, de 14 de noviembre: consentimiento informado, historia clínica, intimidad e instrucciones previas*, Ed. Derecho Sanitario Asesores, Madrid, 2003.

¹⁷² La Ley General de Sanidad consideraba ya como actividad fundamental del sistema sanitario la realización de estudios epidemiológicos necesarios para orientar con mayor eficacia la prevención de riesgos para la salud, así como la planificación y evaluación sanitaria, debiendo tener como base un sistema organizado de información sanitaria, vigilancia y acción epidemiológica –art. 8–. Cfr. también los arts. 21.1.f), 23, 40.12 y 13 y la disposición adicional segunda.

¹⁷³ Cfr. art. 10.3 y 5 LGS. El art. 61 LGS señalaba que la historia clínica personalizada estará a disposición para fines científicos, sin perjuicio del respeto al derecho a la intimidad del paciente.

ción de la documentación clínica, al prever el mantenimiento de ésta «cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud» –art. 17.2–.

No obstante, la excepción del consentimiento para los datos especialmente protegidos se produce para «la prevención o el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios» –art. 7.6 LOPD–, no para estudios científicos o de investigación¹⁷⁴. La Ley 41/2002, de 14 de noviembre, si bien señala que los fines epidemiológicos, de salud pública, de investigación o de docencia son usos legítimos de la historia clínica¹⁷⁵, establece que el acceso a la historia clínica con estos fines «obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente dé su consentimiento para no separarlos» –art. 16.3–¹⁷⁶. Igualmente, cuando se prevé la conservación de la historia clínica con fines epidemiológicos o de investigación «se hará de forma que se evite en lo posible la identificación de las personas afectadas» –art. 17.2–¹⁷⁷. La Ley 15/1999, de 13 de diciembre, define –art. 3.f)– como disociación –«todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable»–¹⁷⁸. La disociación en el ámbito de la investigación epidemiológica, de salud pública, de investigación o de docencia excluiría la vigencia de la legislación de protección de datos personales, al no tener como objeto información

¹⁷⁴ Cfr. A. IGUALADA, «El uso de la documentación clínica en actividades distintas de la específica prestación asistencial», *cit.* Pero también es verdad que estas finalidades son consideradas compatibles en relación con el art. 4 LOPD, que no exige la disociación de esta información.

¹⁷⁵ De hecho, el tratamiento de información con fines epidemiológicos y de investigación es una obligación de los profesionales. Así, la Ley 41/2002, de 14 de noviembre establece que los profesionales tienen el deber de cumplimentar los protocolos, registros, informes, estadísticas y documentación asistencial y administrativa en relación con los procesos clínicos en los que intervienen, al igual que «los que requieran los centros o servicios de salud competentes y las autoridades sanitarias, comprendidos los relacionados con la investigación médica y la información epidemiológica» –art. 23–.

¹⁷⁶ La Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid, atribuye como función de la Autoridad en Salud Pública la promoción de la vigilancia epidemiológica tanto de las enfermedades transmisibles como no de las no transmisibles, y de todos los determinantes del proceso salud-enfermedad relacionados con la interacción del individuo con el medio. Para cumplir estos fines, el art. 55.5 de la LOSCAM establece los datos relativos a la salud serán cedidos a la Administración Sanitaria de la Comunidad de Madrid por parte de los responsables de los ficheros, cualquiera que sea su titularidad, cuando resulten necesarios para prevención de la enfermedad, o la realización de estudios epidemiológicos. Esto debe hacerse «con sujeción a lo establecido en la norma estatal y autonómica aplicable».

¹⁷⁷ Esto se aplica claramente a los estudios estadísticos. Así, la cesión de datos de salud a la Administración de tráfico con la finalidad de elaborar estadísticas sobre la evolución clínica de pacientes heridos en accidentes de tráfico –si han fallecido o si continúan hospitalizados pasados treinta días del accidente– debe darse disociada tanto por falta de adecuada previsión legal así como por exigencia del principio de calidad.

¹⁷⁸ En este sentido, el Proyecto de LOPD propuso un sistema de disociación limitada, en el que los datos identificativos del paciente se sustituirían por un código del que nunca pudiera extraerse su identidad pero que, al ser único, permitía una acumulación de toda la información clínica de un paciente. Quisiera destacar como ejemplo de disociación el proyecto de «Registro alemán para terapia de trasplante de riñón» de QuaSi-Niere Berlín (Alemania). Cfr. el *III Premio a las Mejores Prácticas Europeas en materia de Protección de Datos para Administraciones Públicas*, en prensa, Civitas, Madrid, 2007.

sobre personas físicas identificadas o identificables –art. 3.a)–¹⁷⁹. No obstante, la Ley 41/2002, de 14 de noviembre, establece esta disociación como «regla general», lo que no impide su custodia disociada pero la posibilidad de su asociación, de modo que esta disociación se convierte, en el fondo, en una medida de seguridad¹⁸⁰. No es fácil llevar a cabo la disociación cuando la información clínica se encuentre en soporte papel. En ocasiones, es necesario limitar la intimidad de la personas para permitir una actividad investigadora en beneficio de la comunidad¹⁸¹. Esta precisión tiene especial importancia para la investigación epidemiológica con datos de carácter personal donde es casi imposible obtener el consentimiento para el tratamiento de cada una de las personas y donde una obligación absoluta de disociación genera quejas en la comunidad científica al afectar a las investigaciones¹⁸². En este punto es especialmente importante el principio de calidad y proporcionalidad en el tratamiento de datos personales. Esto quiere decir que sólo debe tratarse una historia clínica con datos personales para fines epidemiológicos o de investigación si sólo de esta forma se puede desarrollar esta actividad¹⁸³. Teniendo claro que el tratamiento es adecuado –juicio de adecuación– y que el fin a alcanzar –la actividad epidemiológica o de investigación– es proporcional con el medio –el tratamiento de datos de salud–, por lo que se respeta también el juicio de proporcionalidad en sentido estricto, es necesario plantearse el juicio de necesi-

¹⁷⁹ Para que haya una auténtica disociación es necesario que resulte imposible asociar un determinado dato con una persona concreta. Lógicamente, el número de historia clínica es un dato de carácter personal. Como hemos señalado antes, la normativa comunitaria entiende que el afectado no será determinable cuando su identificación exija un esfuerzo desproporcionado que sea suficiente para disuadir a quien accede al dato de la identificación de la persona a la que el mismo se refiere. Sin embargo, la Agencia Española ha entendido tradicionalmente que la mera posibilidad, incluso remota, de asociar la información a través de cualquier medio nos llevaría a un tratamiento de datos personales. Así, un identificador personal constituido mediante un algoritmo de encriptación de sentido único, generado a partir de datos relativos al primer apellido, segundo apellido, fecha de nacimiento y sexo será un dato de carácter personal. En todo caso, una disociación parcial es recomendable en la actividad investigadora como medida de seguridad.

¹⁸⁰ A veces es necesaria una información personalizada, por ejemplo, para llevar a cabo un programa de vacunación de población extranjera. También se producen cesiones de datos personales de origen racial por parte de centros educativos para este fin.

¹⁸¹ La legislación de la Comunidad de Madrid es más flexible. Así, la Ley 12/2002, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid establece como una función de la Autoridad Sanitaria Pública la promoción de la vigilancia epidemiológica: «A tal fin, y con sujeción a lo establecido en la norma estatal y autonómica aplicable a la materia de protección de datos de carácter personal, los datos relativos a la salud serán cedidos a la Administración Sanitaria de la Comunidad de Madrid por parte de los responsables de los ficheros, cualquier que sea su titularidad, cuando resulten necesarios para la prevención de la enfermedad o la realización de estudios epidemiológicos». Es una habilitación a favor de la Administración Sanitaria Pública por lo que para el resto de los supuestos hay que pedir el consentimiento expreso o proceder a disociar esta información.

¹⁸² Martín Moreno ha reclamado «el reconocimiento del papel de la investigación y el derecho a que no haya más obstáculos que los que razonablemente imponen los principios éticos exigibles y el trabajo bien hecho». Cfr. J. M. MARTÍN MORENO, «Epidemiología y respeto a la confidencialidad sobre los datos personales: a propósito de una propuesta de Directiva europea». *Gaceta Sanitaria*, núm. 45, 1994, p. 320. Cfr. también en esa misma dirección J. APARICIO SALOM, *Estudio sobre la Ley Orgánica*, cit. p. 175.

¹⁸³ La infracción declarada por la APDCM al Hospital Gregorio Marañón por el abandono en un contenedor de reciclaje de papel de historias clínicas, motivado porque un médico en formación –Mir– las retiró para llevar a cabo un estudio científico y, por error, éstas fueron tiradas no se hubiera producido de haberse disociado esta información.

dad, esto es, que el mismo fin —este estudio epidemiológico o de investigación— no pueda ser desarrollado sin datos de carácter personal¹⁸⁴. Además, existe, en ocasiones una habilitación legal específica para la comunicación de datos personales con fines epidemiológicos. Este es el caso de la notificación obligatoria a las autoridades sanitarias de los casos de enfermedad y fallecimiento de las víctimas de determinadas enfermedades infecciosas¹⁸⁵. En cualquier caso, el acceso a la historia clínica con fines epidemiológicos, de salud pública, de investigación o de docencia no debe ser indiscriminado sino que también «queda limitado estrictamente a los fines específicos de cada caso» —art. 16.3 *in fine*—.

Recientemente se ha planteado en Cataluña el problema de la utilización de historias clínicas con fines de política lingüística. Ya hemos señalado que la finalidad principal de la historia clínica es la asistencia al paciente y que otros fines sanitarios como los epidemiológicos, de salud pública o de investigación y de docencia son fines compatibles, aunque no sean el fin principal. Además, es necesario como regla general la disociación de la historia clínica. La política lingüística no es un fin sanitario que justifique el acceso a la historia clínica —contravendría el principio de finalidad—, salvo que se entienda dentro de un proyecto de calidad asistencial que trate de analizar la lengua como vehículo para la asistencia sanitaria. En todo caso es necesario separar previamente la información personal de la clínico— asistencial ya que para llevar a cabo el estudio lingüístico no es necesario —es excesivo— conocer el titular de cada historia clínica. Esta evaluación sólo podía haber sido efectuada por una empresa externa si existe un contrato por el que esta empresa se convierte en encargada del tratamiento de los datos por cuenta del responsable —art. 12 LOPD—. En todo caso, lo razonable es que sea la propia la inspección sanitaria —que tiene la competencia de velar por la calidad asistencial, dentro del cual sí podría estar el análisis de la lengua vehicular de la asistencia como garantía del derecho a una información comprensible— la que lleve a cabo el estudio lingüístico de las historias clínicas previa diso-

¹⁸⁴ En todo caso, lo más indicado es tratar de pedir el consentimiento del interesado en la medida en que sea posible.

¹⁸⁵ Así, el Real Decreto 2210/1995, de 28 de diciembre, crea la Red Nacional de Vigilancia Epidemiológica, cuya finalidad es la recogida y análisis de la información epidemiológica que contribuya a la aplicación de medidas de control individual y colectivo. Contiene un Anexo I con una lista de enfermedades de declaración obligatoria. Este Real Decreto garantiza la implantación de medidas de seguridad de los datos y establece el deber de confidencialidad. Este Registro fue inspeccionado en 1998 por la Agencia Española de Protección de Datos. La Agencia ha afirmado en ese ámbito claramente el derecho a la protección de datos personales. Esto supone que el Centro sólo puede recabar y tratar los datos de afectados de sida que acudan directamente al mismo o cuando el tratamiento sea necesario de conformidad con lo previsto en el artículo 7.6 LOPD. Fuera de estos supuestos, será necesario el consentimiento previo del afectado. El Centro Nacional de Epidemiología podrá comunicar o ceder a las Comunidades Autónomas y a las Administraciones Sanitarias los datos de salud por él recabados en los términos contemplados por el artículo 11 apartados 1 y 2.f) de la LOPD y por la Ley Orgánica 3/1986, de Medidas especiales en materia de salud pública. Sobre esta cuestión *cf.* también la Orden Ministerial de 21 de febrero de 2001 por la que se regula la Red Nacional de Vigilancia Epidemiológica, en relación con las encefalopatías espongiiformes transmisibles humanas. En todo caso, estamos hablando de cesión de datos —no del límite al deber de secreto ya analizado *supra* 2.e)— ya que la comunicación de esta información se produce para un posterior tratamiento de datos. *Cfr.* más ampliamente N. DE MIGUEL, *Tratamiento de datos personales en el ámbito sanitario*, cit. pp. 110-115.

ciación de la información personal. El acceso a la historia clínica personalizada, si no es con una finalidad claramente asistencial, sólo puede hacerse con consentimiento expreso del afectado o con una habilitación legal.

Otro supuesto interesante es la comunicación de datos de centros sanitarios privados y públicos a la Administración Sanitaria sin consentimiento del interesado. La comunicación de datos de historias clínicas desde los centros sanitarios privados a las Administraciones Públicas puede hacerse cuando exista una habilitación legal que así lo establezca —art. 11.2.a) LOPD—. La comunicación de datos entre centros sanitarios públicos de atención primaria y especializada se encuentra habilitada por el mismo art. 8 LOPD que permite acceder a la historia clínica de un paciente al que se le vaya a prestar asistencia sanitaria. En todo caso, el paso de un modelo de historia clínica descentralizada en cada uno de los centros a un modelo de historia clínica centralizada e informatizada a nivel de cada una de las Comunidades Autónomas transforma estas cesiones de historias clínicas en accesos dentro del marco del mismo responsable del fichero y vinculados al propio principio de calidad. Cuestión específica es la comunicación de datos desde centros sanitarios públicos a la Administración Pública. El régimen de comunicación de datos entre Administraciones Públicas se ha endurecido en virtud de la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre¹⁸⁶. Sólo es legítima la comunicación de datos sin consentimiento del interesado cuando se produzca entre Administraciones Públicas que desarrollan idénticas competencias sobre las mismas materias —art. 21.1 LOPD—. Por tanto, es legítima la comunicación de datos de historias clínicas desde los centros sanitarios públicos a la Consejería de Sanidad y al Ministerio de Sanidad, por ejemplo, para el mantenimiento de un fichero centralizado de listas de espera máxima o de garantía de respuesta asistencial¹⁸⁷. En relación con la comunicación de datos entre centros sanitarios privados, no parece claro legitimarla en razón de que la cesión 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 —art. 11.2.c) LOPD—. La cesión de información clínica de un paciente desde un centro sanitario privado a otro centro donde va a ser atendido puede justificarse en virtud del art. 8 LOPD que permite que las instituciones y los centros sanitarios públicos y privados proce-

¹⁸⁶ *Cfr.* una crítica a esta cuestión en A. TRONCOSO REIGADA, «La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional», *cit.*

¹⁸⁷ Es lógico que se cree un registro unificado de pacientes en una Consejería a partir de la cesión de información de los hospitales, con la finalidad de reducir la lista de espera quirúrgica. La comunicación de datos de pacientes que superan la espera máxima a ficheros centralizados de listas de espera o a centros de respuesta sanitaria, es una comunicación de datos en virtud del art. 21 LOPD o un acceso en virtud del art. 4 LOPD. También podrá cederse la historia clínica de un paciente a un centro privado concertado en el que vaya a practicarse la intervención —art. 8 LOPD—. No se trata de un encargo del tratamiento ya que el fichero de lista de espera trata los datos para una finalidad distinta. Igualmente, el centro sanitario al que el paciente es derivado tiene la obligación de conservar la historia clínica con la finalidad asistencial y tiene el carácter de responsable del fichero. En todo caso, es necesario informar al paciente de que se encuentra registrado en el fichero unificado de pacientes y de las cesiones a centros sanitarios privados en cumplimiento del art. 5 LOPD. Lo mismo es de aplicación en relación con la segunda opinión médica en la sanidad pública.

dan al tratamiento de los datos de carácter personal de las personas que a ellos acudan o hayan de ser tratados en los mismos.

Un problema específico es la comunicación de datos de salud de los centros médicos a las compañías aseguradoras para la cobertura de los actos médicos¹⁸⁸. Nos referimos tanto a las compañías aseguradoras con las que se contrata la asistencia sanitaria —que van a abonar esta asistencia— como a las entidades aseguradoras con las que se contrata un seguro de responsabilidad civil y patrimonial y que necesitan valorar los daños. El art. 18 de la Ley 50/1980, de 8 de octubre, de contrato de seguro señala que el asegurador «está obligado a satisfacer la indemnización al término de las investigaciones y peritaciones necesarias para establecer la existencia del siniestro y, en su caso, el importe de los daños que resulten del mismo. En cualquier supuesto, el asegurador deberá efectuar, dentro de los cuarenta días, a partir de la recepción de la declaración del siniestro, el pago del importe mínimo de lo que el asegurador pueda deber, según las circunstancias por él conocidas». Por tanto, como señala la Agencia Española, «de dicho precepto se desprende que el asegurador tiene la obligación legal de realizar las investigaciones y peritaciones precisas tanto respecto de la existencia del siniestro como sobre el importe de los daños si estos se hubieran producido»¹⁸⁹. El art. 105 de la Ley 50/1980, de 8 de octubre señala que «cuando el riesgo asegurado sea la enfermedad, el asegurador podrá obligarse, dentro de los límites de la póliza, en caso de siniestro, al pago de ciertas sumas y de los gastos de asistencia médica y farmacéutica». Igualmente, el art. 103 señala que «los gastos de asistencia sanitaria serán por cuenta del asegurador, siempre que se haya establecido su cobertura expresamente en la póliza y que tal asistencia se haya efectuado en las condiciones previas en el contrato». Igualmente, el art. 106 indica que «los seguros de enfermedad y de asistencia sanitaria quedarán sometidos a las normas contenidas en la sección anterior en cuanto sean compatibles con este tipo de seguros». Como señala la Agencia Española de Protección de Datos, «la Ley impone a la entidad aseguradora la obligación de satisfacer el gasto de asistencia sanitaria efectuado como consecuencia de la enfermedad del asegurado, lo que exigirá conocer cuál será éste, dado que la asistencia se realizará generalmente por terceros ajenos a la propia entidad aseguradora, y en consecuencia esta obligación parecería incluir un indicio de la necesidad de comunicación a la aseguradora de los datos necesarios para conocer la actividad asistencial realizada». Esta habilitación legal cubre la comunicación de datos de un tercero —que no ha contratado la póliza— y al que habrá que indemnizarle por los daños y perjuicios causados por un hecho previsto en el contrato de seguro. Además de esta habilitación legal, lo normal es que se pida el consentimiento expreso para comunicar la

¹⁸⁸ Esta cuestión ha sido analizada en el Informe de la Agencia Española de Protección de Datos, de 21 de julio de 2004. Nuestra posición es parcialmente distinta.

¹⁸⁹ Igualmente, el art. 6 de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor, a partir de la redacción que la Ley 30/1995, de 8 de noviembre, señala que «el asegurador, dentro del ámbito del aseguramiento obligatorio y con cargo al seguro de suscripción obligatoria, habrá de satisfacer al perjudicado el importe de los daños sufridos en su persona y en sus bienes, el cual, o sus herederos, tendrá la acción directa para exigirlo».

información cuando se suscribe esta póliza. En todo caso, la comunicación remitida a la compañía de seguros debe respetar el principio de calidad, esto es, debe limitarse a los datos adecuados y pertinentes para la prueba y facturación del gasto sanitario.

En todo caso, a nuestro juicio también puede considerarse que existe un consentimiento expreso. Cuando alguien contrata un seguro de salud está asumiendo que la asistencia sanitaria realizada en virtud de ese contrato se comunicue a la compañía con la que está contratando. Cuando un paciente acude a un centro sanitario y entrega la tarjeta del seguro de asistencia sanitaria, está consintiendo expresamente con la cesión a la entidad de la que se muestra la tarjeta. Esta sería un manifestación de voluntad libre, inequívoca, específica e informada, y expresa mediante la cual el interesado consiente el tratamiento de datos personales que le conciernen –art. 3.b)–. En todo caso, es aconsejable reforzar el consentimiento expreso para la cesión de datos en el momento de contratar la póliza o en el momento del acto médico, así como el cumplimiento del principio de información del art. 5 LOPD. Igualmente, la declaración de fichero debe prever estas cesiones de datos de carácter personal. La cesión de datos debe respetar el principio de calidad lo que obliga a comunicar la realización de actos médicos pero no de los resultados salvo que de esos se derive otras posibles actuaciones sanitarias o que puedan incidir en la responsabilidad patrimonial.

Un supuesto semejante es la responsabilidad patrimonial de las Administraciones Públicas por negligencias o errores médicos y que requiere para la contestación de la reclamación del interesado el conocimiento de la historia clínica. En ocasiones, la información clínica no la facilita el demandante o si la facilita, esta se encuentra incompleta. No hay una autorización del interesado y no existe todavía un procedimiento judicial por lo que no se puede obtener la historia clínica mediante autorización judicial. La tramitación de la responsabilidad patrimonial de las Administraciones Públicas se encuentra regulada en el art. 139 y ss de la LRJAP y PAC y en el Real Decreto 429/1993, de 26 de marzo, por el que se aprueba el Reglamento de los procedimientos de las Administraciones Públicas en materia de responsabilidad patrimonial. Este último señala que corresponde al órgano que tramite el procedimiento los actos de instrucción que sean necesarios para la determinación, conocimiento y comprobación de los datos en virtud de los cuales deba pronunciarse –art. 7–. La Administración Pública puede tratar los datos sin consentimiento del interesado en virtud de una competencia administrativa –art. 6.2 LOPD– pero el problema estriba en que esto no se aplica a los datos especialmente protegidos. A nuestro juicio hay que considerar que dentro del principio de finalidad de la historia clínica no sólo está prestar una adecuada asistencia sino también responder a las reclamaciones patrimoniales por esa actividad asistencial siempre que quien acceda tenga competencia para ello.

Otra cuestión importante son las cesiones de datos de historias clínicas destinadas a centros sanitarios de otros países. Este último supuesto es cada vez más frecuente en el ámbito de la Unión Europea dentro del principio de libre circulación de pacientes pero cada vez más se extiende a otros países fuera del

ámbito de la Directiva 95/46/CE. En este caso, hay que estar a la normativa relativa a transferencias internacionales de datos, que prohíbe las transferencias con destino a países que no tengan un nivel de protección equiparable, salvo que, además de respetar lo previsto en la LOPD, se obtenga una autorización previa del Director de la Agencia Española de Protección de Datos. La Agencia Española de Protección de Datos evalúa el carácter adecuado del nivel de protección que ofrece un país atendiendo a un conjunto de circunstancias¹⁹⁰. No obstante, la LOPD trata de favorecer las transferencias internacionales de datos de salud a otros países con finalidad de asistencia sanitaria, en otra muestra de la preferencia del derecho a la vida sobre el derecho fundamental a la protección de datos. Así, se prevé expresamente la transferencia cuando sea necesaria «para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o la gestión de servicios sanitarios» –art. 34.c) LOPD–¹⁹¹.

La cesión de la historia clínica a los órganos judiciales está vinculado a otro derecho, el de tutela judicial efectiva –art. 24.1 CE–, que es también un derecho fundamental de la Sección 1.^a del Capítulo II del Título I de la Constitución y que está al mismo nivel que el derecho a la intimidad y el derecho a la protección de datos personales¹⁹². De hecho, el propio conocimiento de los Tribunales es la garantía de todos los derechos e intereses legítimos. La cesión de la historia clínica por parte de los órganos judiciales no plantea ningún inconveniente cuando se cuenta con la autorización del paciente. En el caso de que éste no la dé, el médico ha invocado en ocasiones el secreto profesional –art. 24.2 CE–. El problema es que este secreto profesional está en contradicción no con la voluntad del órgano judicial sino con el derecho a la tutela judicial efectiva de otro ciudadano. Es decir, no se trata de un conflicto entre el derecho a la intimidad y a la protección de los datos de carácter personal, y la competencia de los Tribunales sino entre esos derechos y el derecho que tienen todas las personas «a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión». Este conflicto de derechos debe ser resuelto por el juez, no por el médico. Es decir, no le corresponde al médico valorar la solicitud judicial y la intimidad del paciente y decidir en consecuencia; la tutela de los derechos y la resolución de los conflictos está en nuestro sistema político en manos de los jueces, única instancia independiente, inamovible, responsable y sometida únicamente al imperio de la Ley –art. 117 CE–. No olvidemos que el art. 118 CE señala que es obligado «cumplir las sentencias y demás resoluciones firmes de los Jueces y Tribunales, así como prestar la colaboración requerida por éstos en el curso del proceso en al ejecución de lo resuelto».

¹⁹⁰ Cfr. arts. 33-34 LOPD relativo al movimiento internacional de datos. Cfr. más ampliamente D. SANCHO VILLA, *Transferencia internacional de datos personales*, APD, 2003, pp. 25-29.

¹⁹¹ Existen también habilitaciones legales para la transferencia internacional de datos de salud a centros no sanitarios como ocurre con la cooperación internacional contra el dopaje.

¹⁹² Cfr. J. SEOANE PRADO, «La historia clínica ante los Tribunales», en M. T. CRIADO DEL RÍO, *Aspectos médico-legales de la historia clínica*, Colex, Madrid, 1999, pp. 291 y ss.

La propia Ley 41/2002, de 14 de noviembre, es consciente de la legitimidad de la cesión de historias clínicas a los órganos judiciales. De hecho, uno de los supuestos de conservación de la documentación clínica es a efectos judiciales –art. 17.2–. Así, después de afirmar que el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública o de investigación o docencia debe hacerse preservando los datos identificativos separados de los clínico-asistenciales, para asegurar como regla general el anonimato del paciente, se exceptúa de este principio «los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuáles se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente» –art. 16.3–. Por tanto, si la cesión de historias clínicas con finalidad epidemiológica o de investigación debe hacerse de manera disociada –no habría en puridad cesión de datos personales–, la cesión de la historia clínica a los órganos judiciales debe ir personalizada. Eso no obsta para que el acceso a los datos y documentos de la historia clínica queda limitado «estrictamente a los fines específicos de cada caso» –art. 16.3 *in fine*–. Por ello, los jueces deben limitar su petición de acceso a la historia clínica a los datos imprescindibles y los médicos, vista a veces la ambigüedad de algunas peticiones judiciales, tienen que aplicar el principio de proporcionalidad, dando la información que consideren necesaria en cada caso, y pidiendo aclaraciones, si resulta necesario, a los propios órganos judiciales¹⁹³. A la hora de la cesión de datos a los órganos judiciales, es conveniente diferenciar también las distintas jurisdicciones en virtud de los bienes jurídicos tutelables. Así, tiene una primacía clara el orden penal sobre el orden civil. El juez debe ser muy cuidadoso a la hora de pedir información de la historia clínica. Es razonable que en una demanda contra una compañía de seguros por un accidente de tráfico se pidan los antecedentes en la especialidad de traumatología –por si había lesiones previas al accidente– pero no la asistencia sanitaria en otras especialidades. Esto es especialmente importante en los procesos de separación y divorcio. La asistencia sanitaria está basada en la confianza del paciente en la confidencialidad de su información clínica. Si se rompe la confianza, se perjudica gravemente la asistencia sanitaria que, no lo olvidemos, es el fin principal de la historia clínica. Si el paciente piensa que todo lo que cuenta al médico se va a dar después al juez, puede retraerle a la hora de confiar en su médico.

Igualmente, aunque no está previsto expresamente en la Ley 41/2002, de 14 de noviembre, es posible la cesión de datos de historias clínicas a las fuerzas y cuerpos de seguridad del Estado. Así, el art. 22.2 de la LOPD regula la «recogida y tratamiento *para fines policiales* de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas». Ahora bien, limita esta posibilidad «a aquellos supuestos y categorías

¹⁹³ Muchas de las providencias de los órganos judiciales son genéricas, debido a la acumulación del trabajo de muchos jueces. Por ello, los médicos tienen que actuar de buena fe, interpretando qué información es útil al órgano judicial, y no enviando aquella información que a todas luces puede parecer excesiva.

de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales». Pues bien, en relación con el tratamiento de datos de salud con fines policiales, hay que señalar que el art. 22.3 LOPD permite la recogida y tratamiento de los datos de salud y del resto de los datos especialmente protegidos mencionados en el art. 7.2 y 7.3 LOPD que podrá realizarse «exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de la legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales». Así, si como regla general los ficheros de las Administraciones Públicas no pueden tratar datos especialmente protegidos si no es con el consentimiento expreso –y por escrito, para datos de ideología, afiliación sindical o creencias–, las Fuerzas y Cuerpos de Seguridad pueden tratar datos especialmente protegidos para fines policiales sin el consentimiento del interesado. Los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado para fines policiales –no para fines administrativos– se benefician de un conjunto de prerrogativas para el tratamiento de datos que no disponen el resto de las Administraciones Públicas. Así, los Fuerzas y Cuerpos de Seguridad del Estado pueden denegar en los ficheros con fines policiales los derechos de acceso, rectificación y cancelación «en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se están realizando»; también pueden excepcionar el principio de información en la recogida de datos cuando afecte «a la seguridad pública o a la persecución de infracciones penales o administrativas» –*ex* art. 23.1y 24.1 LOPD-. Esto no le ocurre al resto de los ficheros de fuerzas y cuerpos de seguridad que han sido recogidos con fines administrativos y que están sujetos al régimen general de la LOPD –art. 22.1 LOPD-. Es decir, los ficheros con fines administrativos de las Fuerzas y Cuerpos de Seguridad no pueden tratar datos especialmente protegidos sin el consentimiento de la persona, que deberá ser informada del tratamiento de sus datos y que podrá ejercer los derechos de acceso, rectificación y cancelación.

El art. 22 LOPD no es un artículo claro ya que no habla de cesión de datos de salud a la policía sino de recogida y tratamiento, dentro del cuál se interpreta una habilitación legal para la cesión de todos los datos que obren en ficheros públicos o privados a las fuerzas y cuerpos de seguridad del Estado. Llama la atención que este precepto no prevea una autorización judicial en el caso de los datos especialmente protegidos –como es el caso de los datos de salud– pues ésta es la regla general en las limitaciones efectuadas por la policía de los derechos a la privacidad personal establecidos en el art. 18 de la Constitución Española. Así, si este precepto constitucional reconoce el derecho a la inviolabilidad del domicilio, por lo que no es posible la entrada o registro de la policía sin consentimiento del interesado o resolución judicial

salvo en caso de flagrante delito¹⁹⁴, o el derecho al secreto de las comunicaciones salvo resolución judicial¹⁹⁵, teóricamente podría reconocer también el derecho fundamental a la protección de datos personales y, especialmente, la confidencialidad de los datos de salud frente a la policía, salvo que exista autorización judicial. Sin embargo, como ya hemos señalado, el derecho fundamental a la protección de datos se encuentra más limitado, habiendo permitido el legislador el tratamiento de datos personales –que no sean especialmente protegidos– sin consentimiento de la persona para funciones administrativas –art. 6.2 LOPD–, incluso de los datos especialmente protegidos como los datos de salud por las Fuerzas y Cuerpos de Seguridad para fines policiales –art. 22.3 LOPD–. Eso no obsta para que la policía preferentemente y, salvo supuestos de urgencia e inmediatez, utilice el mismo procedimiento para el acceso a datos de salud que para la entrada en domicilio o la interceptación de las comunicaciones: solicitar la autorización judicial como regla general, que se suele dar con una gran rapidez, y que es un instrumento adecuado para salvaguardar las exigencias del art. 22.3 LOPD referidas al control de legalidad de la actuación administrativa¹⁹⁶. El auténtico límite a la cesión de datos de salud a las Fuerzas y Cuerpos de Seguridad es el principio de calidad y la finalidad del tratamiento: no está justificado para los ficheros con fines administrativos de las Fuerzas y Cuerpos de Seguridad del Estado sino para los ficheros policiales, esto es, aquellos destinados para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales; además, sólo deben tratarse aquellos «datos que resulten necesarios» y solo podrá «realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta». Quiero resaltar esto especialmente porque si bien el art. 22.3 LOPD incluye todos los datos especialmente protegidos, hay que resaltar que en la relación clínica médico-paciente, que está basada en la confianza, se revela al médico una información que no se diría si se sabe que esto va a ser conocido por la policía o por los Tribunales. Una cesión indiscriminada de toda la historia clínica a la policía o a los jueces puede afectar al derecho a no declarar contra sí mismo y a no confesarse culpable –arts. 17 y 24 CE–. Por último, hay que señalar que los ficheros con fines policiales de las Fuerzas y Cuerpos de Seguridad deben implantar las medidas de seguridad de nivel alto¹⁹⁷.

¹⁹⁴ STC 341/1993, de 18 de noviembre, que definía el concepto de flagrancia. Arts. 202-204 y 534 del Código Penal; arts. 545-578 de la Ley de Enjuiciamiento Criminal.

¹⁹⁵ SSTC 114/1984, de 29 de noviembre, sobre secreto de las comunicaciones o 82/2002, de 22 de abril, –intervención proporcionada, motivada y controlada–. Arts. 197, 198 y 535-536 del Código Penal y 579-588 de la Ley de Enjuiciamiento Criminal.

¹⁹⁶ Este es el criterio mantenido en la Recomendación 2/2004. En todo caso, en supuestos de urgencia e inmediatez, el solicitante debe acreditar la pertenencia a las fuerzas y cuerpos de seguridad y la capacidad suficiente para solicitar la información, debe justificar la petición en el marco de unas diligencias policiales y debe indicar a qué documentos de la historia clínica desea acceder, debiendo quedar constancia de la petición policial.

¹⁹⁷ Art. 4 del Real Decreto 994/1999, de 11 de junio.

IV. LA HISTORIA CLÍNICA DEL MENOR

Los menores son titulares de derechos fundamentales que también ejercen en el ámbito sanitario¹⁹⁸. La Carta Europea de los Niños Hospitalizados, aprobada por Resolución del Parlamento Europeo, de 13 de mayo de 1986, ha reconocido también un conjunto de derechos específicos de los menores en el ámbito sanitario¹⁹⁹. Entre estos derechos, el menor tiene también un derecho a la intimidad y a la protección de sus datos personales, que se extiende no sólo al derecho de acceso a la historia clínica sino también a la garantía de su confidencialidad frente a accesos indebidos de ésta. No obstante, la capacidad de decisión y de ejercicio de derechos del menor en el ámbito sanitario se encuentra modificada al ser éste un ámbito donde el bien jurídico en presencia es la propia vida y la integridad de la persona. Realmente, el derecho a la intimidad del menor en el sector sanitario es deudor en parte de la mayor o menor facultad para tomar decisiones sanitarias sobre su propia vida. En todo caso, el derecho a la información del menor siempre irá más lejos que su facultad para autorizar tratamientos médicos o para negarse a ellos.

a) *Derecho del menor a la intimidad y a la confidencialidad de sus datos sanitarios y el derecho de los padres a la información y al acceso a la historia clínica de sus hijos*

Históricamente se ha mantenido que el menor de edad civil carecía de capacidad para adoptar decisiones en el ámbito sanitario que implicasen aceptación o rechazo de tratamientos sanitarios. Esto era lo propio de una época en la que se valoraban de manera relativa tanto los derechos de los pacientes como la propia autonomía de los menores. Cuando se trataba de menores, era el médico quién decidía lo mejor para el menor contando con los padres. Al igual que ha ocurrido con los pacientes en general, de manera progresiva ha avanzado la posición que pretende otorgar al menor una cierta autonomía y participación en la toma de decisiones sanitarias. Doctrinalmente han ido aparecido

¹⁹⁸ Sobre los derechos fundamentales del menor, Cfr. I. LÁZARO GONZÁLEZ, *Los menores en el Derecho español*, Universidad Pontificia de Comillas, Tecnos, Madrid, 2002, pp. 538 y ss. Cfr. también I. E. LÁZARO GÓNZALEZ y I. V. MAYORAL NARROS *Jornadas sobre Derecho de los Menores*, Universidad Pontificia de Comillas, Madrid, 2003. Hemos tenido la oportunidad de analizar esta cuestión en las II Jornadas sobre Derecho de los Menores. Cfr. A. TRONCOSO REIGADA, «La protección de los datos sanitarios del menor», *Nuevos retos que plantean los menores al Derecho*, Universidad Pontificia de Comillas, Madrid, 2004, pp. 213-241.

¹⁹⁹ En esa Carta se establecen, entre otros, los siguientes derechos: derecho del niño a que no se le hospitalice sino en el caso de que no pueda recibir los cuidados necesarios en su casa o en un ambulatorio; derecho del niño a la hospitalización diurna, sin que ello suponga carga adicional para los padres; derecho a estar acompañado de sus padres o de la persona que los sustituya el máximo tiempo posible durante su permanencia en el hospital; derecho a negarse como sujeto de investigación; derecho a estar con otros niños siempre que sea posible; derecho a disponer de espacios adecuados de educación y juego; derecho a continuar la formación escolar en los propios hospitales que deberán tener personal docente o a recibir una atención educativa domiciliaria. Posteriormente, la Comisión Hospitalaria de la Comunidad Europea hizo públicas unas Recomendaciones sobre Hospitalización Infantil. Cfr. el Informe del Defensor del menor, *Derechos de los niños hospitalizados*, Comunidad de Madrid, 2201.

conceptos como «el menor no tan menor», «el menor maduro», que tratan de hacer referencia al menor de edad como sujeto que es capaz de comprender y autorizar tratamientos médicos²⁰⁰. Así, el Convenio de Oviedo de 1997, que entró en vigor el 1 de enero de 2000, señala que la opinión del menor debe ser tomada en consideración como un factor que será tanto más determinante en función de su edad y su grado de madurez –art. 6.2–. Esta posición se recoge también en el art. 8.2 y 10.6 del Código de Ética y Deontología de la Organización Médica Colegial²⁰¹. La propia Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor señala –art. 9.1– que el menor tiene derecho a ser oído, tanto en el ámbito familiar como en cualquier procedimiento administrativo o judicial en que esté directamente implicado y que conduzca a una decisión que afecte a su esfera personal, familiar y social. En general, distintos estudios sobre el desarrollo de la capacidad psicológica y moral de los menores consideran que a partir de los doce años éste se ha desarrollado de modo suficiente como para poder participar progresivamente en las decisiones que afecten a su salud. La normativa sanitaria de los últimos años se apoya en esta posición científica.

No nos corresponde ahora analizar en profundidad la titularidad por parte de los menores del derecho fundamental a la protección de datos personales²⁰². En general el ordenamiento jurídico ha atribuido progresivamente a los menores una mayor capacidad de obrar tanto en el orden civil como ante las Administraciones Públicas como forma de promover su autonomía como sujetos²⁰³. El derecho a la protección de datos personales es, como hemos señalado antes, un derecho personalísimo por lo que por regla general debe poder ser ejercido por los menores. Así, el ejercicio del derecho de acceso, rectificación y cancelación le corresponde al titular de los datos. Podrá actuar «el representante legal cuando la persona se encuentre en situación de incapacidad o de minoría de edad *que le imposibilite el ejercicio personal de los mismos*»²⁰⁴. En el ámbito de la protección de datos personales se ha considerado que los mayores de catorce años disponen de condiciones de madurez para dar su consentimiento para el tratamiento de sus datos personales y para ejercitar los derechos. Para los

²⁰⁰ Cfr. muy especialmente sobre la cuestión F. MONTALVO JÄÄSKELÄINEN y otros, «El derecho del niño a la asistencia sanitaria como manifestación de su supervivencia», en I. LÁZARO GONZÁLEZ, *Los menores en el Derecho español*, cit. pp. 560-599.

²⁰¹ Cfr. G. HERRANZ, *Comentarios al Código de Ética y Deontología Médica*, Eunsa, Pamplona, 1993 –a la versión anterior a la actual, que es de 1999–.

²⁰² Remito la exposición general sobre la titularidad de los menores del derecho fundamental a la protección de datos personales a A. TRONCOSO REIGADA, «La protección de los datos sanitarios del menor», *Nuevos retos que plantean los menores al Derecho*, cit. pp. 213-222.

²⁰³ En la doctrina americana, Tribe ha defendido un control estricto de constitucionalidad sobre las leyes que restrinjan el ejercicio de derechos por parte de los menores, considerando a éstos a *discrete and insular minorities* –*Carolene Prods. v. United States*–, y la minoría de edad como una categoría sospechosa de ser utilizada para la discriminación. Cfr. L. TRIBE, *American Constitutional Law*, 2.º ed. The Foundation Press Inc. 1988, pp. 1588-1599.

²⁰⁴ Cfr. art. 11 del Real Decreto 1332/1994, de 20 de junio y Norma Primera de la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

menores de catorce años hay que estar a sus condiciones de madurez ya que como regla general el representante legal actuará en su nombre.

No obstante, no parecen trasladables directamente al ámbito sanitario estos criterios sobre la capacidad del menor de edad de ejercer sus derechos en general, y de ejercitar su derecho de acceso a sus datos personales en particular. Si bien la salud es, como el derecho a la autodeterminación informativa, un derecho personalísimo, su protección no puede estar en manos del paciente si no consta realmente su capacidad de juicio y de discernimiento. No puede afirmarse una presunción general de capacidad de los menores de edad, en materia que afecte a su vida o a su integridad física. Esta presunción existe sólo para los mayores de edad. Una cosa es predicar para los menores una mayor capacidad de decisión en algunas esferas, y otra bien distinta es presumir que el menor puede, en principio, decidir en el ámbito sanitario²⁰⁵. Una cosa es darle al menor una mayor participación en las decisiones sobre su asistencia sanitaria y una mayor información, y otra atribuirle la capacidad completa de decisión y la facultad exclusiva para exigir información, excluyendo a los padres. Es imprescindible distinguir situaciones. No es lo mismo ser informado, que ser escuchado y participar en la toma de la decisión, o que autorizar y dar el consentimiento para el tratamiento médico. Esto ocurre igualmente en relación a las distintas edades del menor. No se puede plantear una capacidad absoluta *in genere* de los menores. Hay que estar a cada caso, especialmente, a los distintos tramos de edad.

La Ley 41/2002, de 14 de noviembre reconoce al menor, el derecho a la intimidad y a la confidencialidad de sus datos personales, porque si la ley lo hubiera querido excluir, lo habría hecho expresamente. En general, al regular el derecho a la información asistencial, se dice que «[e]l titular del derecho a la información asistencial es el paciente» —art. 5.1—²⁰⁶. En todo caso, como hemos señalado anteriormente, seguidamente se prevé que «también serán informadas las personas vinculadas a él por razones familiares o de hecho, en la medida que el paciente lo permita de manera expresa o tácita». Por tanto, la regla general es que sólo debe darse información asistencial al paciente o a la persona que éste autorice. La Ley 41/2002 ha abordado de manera específica la problemática que se presenta cuando las personas tienen sus capacidades disminuidas o aún no desarrolladas, como es el caso de los menores. Así, aún en el supuesto de incapacidad, el paciente será informado «de modo adecuado a sus posibilidades de comprensión, cumpliendo con el deber de informar también a su representante legal» —art. 5.2—. Este supuesto se diferencia de aquél en el cual el paciente carece, a juicio del médico, de capacidad para entender la información a causa de su estado físico o psíquico, y donde está justificado

²⁰⁵ Cfr. F. MONTALVO JÄÄSKELÄINEN y otros, «El derecho del niño a la asistencia sanitaria como manifestación de su supervivencia», *loc. cit.* p. 570. En esta posición D. PÉREZ-CARCELES, E. OSUNA y A. LUNA, «El consentimiento del menor de edad», *XIII Congreso Mundial sobre Derecho Médico —apud F. MONTALVO—*. Una posición contraria en P. SIMÓN LORDA, *El consentimiento informado*, Triacastela, Madrid, 2000 p. 279.

²⁰⁶ La misma expresión se encuentra en el Acuerdo del Pleno del Consejo Interterritorial del Sistema Nacional de Salud sobre Consentimiento Informado, adoptado el 6 de noviembre de 1995, ya citado.

que la información se ponga en conocimiento de las personas vinculadas a él por razones familiares o de hecho –art. 5.3–. Por tanto, el paciente menor de edad tiene derecho inicialmente a ser informado de modo adecuado a su capacidad de comprensión y a acceder a sus datos sanitarios en esa misma proporción. La Carta Europea de los Niños Hospitalizados reconoce su derecho a recibir una información adaptada a su edad, su desarrollo mental, su estado afectivo y psicológico, con respecto al conjunto del tratamiento médico al que se le somete y a las perspectivas positivas que dicho tratamiento ofrece.

El problema que se plantea es, como veremos más adelante, la compatibilidad entre el derecho a la intimidad, a la confidencialidad y a la protección de datos personales del menor y el derecho a la información de los padres que, al ejercer la patria potestad, quieren acceder y conocer la historia clínica de sus hijos. Como criterio general, es el propio paciente él que tiene el derecho de acceso a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella. Este derecho puede ejercerse también por representación debidamente acreditada –art. 18 Ley 41/2002–. No obstante, el derecho de acceso a la historia clínica y a datos sanitarios por parte del menor de edad depende de su mayor o menor autonomía como paciente a la hora de dar su consentimiento para determinados tratamientos médicos. Es decir, el derecho a la información sanitaria y al acceso a datos sanitarios de los menores tiene que ser proporcional a su facultad para prestar el consentimiento o para ser escuchado. Si el menor no tiene información, con qué criterios va a poder opinar o va a prestar su consentimiento. Esto no quiere decir que la edad para el acceso a los datos sanitarios deba ser la misma que para prestar el consentimiento, porque la madurez para conocer no puede ser la misma que para poner en peligro la vida. Igualmente, el derecho de acceso de los padres a la historia clínica de los hijos va aparejado a su capacidad para dar su consentimiento necesario como representantes legales para determinados tratamientos médicos. No tiene sentido mantener la confidencialidad de los datos sanitarios de los menores frente a los padres si estos últimos son los que tienen que decidir. La capacidad de exigir la confidencialidad no puede ser independiente de la posibilidad de prestar el consentimiento para el tratamiento. La Ley 41/2002, de 14 de noviembre, ha abordado la capacidad de los menores en el ámbito sanitario, especialmente su facultad para prestar su consentimiento para los tratamientos médicos, lo que ayuda también para determinar el acceso a la historia clínica, tanto del menor como de sus padres. No obstante, si bien esta Ley trata de manera adecuada el consentimiento de los menores, fijando edades precisas, no hace lo mismo con el derecho a la intimidad y al acceso a la historia clínica, tanto de los menores como de sus padres. La Ley 41/2002 tiene un vacío en materia de confidencialidad, no existiendo una equiparación legal a las edades para prestar el consentimiento, por lo que siempre nos encontraremos con dificultades interpretativas.

Como hemos señalado antes, como regla general, toda actuación en el ámbito de la salud de un paciente necesita «el consentimiento libre y voluntario del afectado, una vez que, recibida la información prevista [...], haya valorado las opciones propias del caso» –art. 8.1 Ley 41/2002–. La propia Ley prevé unos supuestos donde existen límites a este consentimiento informado y

donde se da el consentimiento por representación. Así, la Ley 41/2002 permite este consentimiento por representación cuando el paciente «no sea capaz de tomar decisiones, a criterio del médico responsable de la asistencia, o su estado físico o psíquico no le permita hacerse cargo de su situación. Si el paciente carece de representante legal, el consentimiento lo prestarán las personas vinculadas a él por razones familiares o de hecho» –art. 9.3.a)–. La Ley 41/2002 regula específicamente el consentimiento por representación para los pacientes menores de edad estableciendo esta posibilidad «[c]uando el paciente menor de edad no sea capaz intelectual ni emocionalmente de comprender el alcance de la intervención» –art. 9.3.c)–, distinguiendo algunos supuestos:

El primero sería el de pacientes con dieciséis años cumplidos o emancipados, donde no cabe prestar el consentimiento por representación. Se entiende que este menor de edad tiene derecho a la información y al acceso a la historia clínica. Los padres serán informados y su opinión será tenida en cuenta para la adopción de decisiones en caso de actuación de grave riesgo, por lo que se entiende que en el supuesto de una enfermedad grave tienen derecho de acceso a la historia clínica, aún sin autorización del menor. El Código Penal señala –art. 155– que en «los delitos de lesiones, si ha mediado el consentimiento válida, libre, espontánea y expresamente emitido del ofendido, se impondrá la pena inferior en uno o dos grados. No será válido el consentimiento otorgado por un menor de edad o un incapaz». Este precepto dificulta los tratamientos médicos graves de mayores de dieciséis años que cuenten con el consentimiento informado de éstos pero no de sus representantes legales ya que puede ser constitutivo de un delito de lesiones. Este criterio de reconocer al mayor de dieciséis años la facultad para dar su consentimiento no se aplica a todos los supuestos. Así, sólo una persona mayor de edad, capaz y libre puede otorgar un testamento vital o un documento de instrucciones previas –art. 11 de la Ley 41/2002–. Algunos supuestos como el de interrupción voluntaria del embarazo o los tratamientos con técnicas de reproducción humana asistida se rigen por su legislación específica –art. 9.4 de la Ley 41/2002– que exige tener dieciocho años cumplidos, al estar presentes en estos supuestos derechos de terceras personas merecedores de protección²⁰⁷. En todo caso hay que señalar que los padres deben poder acceder a la historia clínica de los menores cuando se trate de temas de salud importantes, sin perjuicio de que su opinión sólo sea tenida en cuenta en caso de actuación de grave riesgo. La capacidad de acceso de los padres a la historia clínica, mientras que mantengan la patria potestad, tiene que ser mayor que su capacidad de tomar la decisión y no debe limitarse a las actuaciones de grave riesgo.

²⁰⁷ El art. 5.6 de la Ley 35/1998, de 22 de noviembre, sobre Técnicas de Reproducción Humana Asistida establece que los donantes de gametos y preembriones deberán tener más de dieciocho años y plena capacidad de obrar; el art. 6.1 señala la mujer deberá tener dieciocho años al menos y plena capacidad de obrar para ser receptora o usuaria de las técnicas reguladas en la ley. Cfr. más ampliamente Y. GÓMEZ, *El Derecho a la Reproducción Humana Asistida*, Madrid, 1994; J. VIDAL (coord.), *Derechos Reproductivos y técnicas de reproducción asistida*, Comares, Granada 1998, pp. 78-83; AA. VV., *Bioética y Justicia*. Actas del Seminario sobre Bioética y Justicia celebrado en Madrid del 6 al 8 de octubre de 1999, MSC-CGPJ, Madrid, 2000, pp. 383-468.

El segundo supuesto sería el de pacientes con doce años cumplidos. El consentimiento para el tratamiento médico lo da el representante legal del menor después de haber escuchado su opinión. Esto significa que el derecho a la información y al acceso a la historia clínica en cualquier tema de salud –también leve– lo tienen sobre todo los representantes legales, teniendo el menor un acceso a su información sanitaria adecuado a la facultad legal de dar su opinión. El legislador no ha optado por requerir el consentimiento a los mayores de doce años, además de a sus padres o representantes legales, como forma de completar ese consentimiento; se limita a afirmar que deben ser escuchados. De esta forma, se evita el conflicto en aquellos casos en los que la voluntad del menor no sea coincidente con la de sus padres o representantes legales. En todo caso, el menor es titular del derecho a ser informado sobre el tratamiento. Además, existe normativa específica que atribuye a los mayores de doce años una mayor capacidad de decisión. Así, el Real Decreto 561/1993, de 19 de abril, por el que se regula los requisitos para la realización de ensayos clínicos establece que los mayores de doce años deben dar su consentimiento para participar en ese ensayo, no bastando el del representante legal –art. 12.5–, lo que además ha de ser puesto en conocimiento del Ministerio Fiscal –art. 11.5–. El problema será cuando exista una contradicción entre voluntades, que puede tener que ser resuelta por los órganos judiciales.

El tercer supuesto sería el de pacientes que no han cumplido todavía los doce años. Estos menores tienen dificultades cognitivas –de discernir– y valorativas –libre albedrío para la toma de decisiones–. Se da aquí plenamente la previsión de que el paciente menor de edad no es capaz intelectualmente ni emocionalmente de comprender el alcance de la intervención, por lo que todos sus derechos se ejercitan a través de su representante legal. El consentimiento para el tratamiento médico lo prestan sus representantes legales teniendo éstos el derecho de acceso a la historia clínica y a los datos sanitarios, no teniendo ningún derecho en este ámbito el menor de edad.

La delimitación de la capacidad de decisión y, por tanto, de acceso a información clínica en virtud de un criterio de tramos de edades, que es el recogido en la Ley 41/2002, es el más habitual en los países de nuestro entorno²⁰⁸.

²⁰⁸ No obstante, algunos de estos países tienen posiciones más amplias. En el Reino Unido, la *Children Act* de 1989 situó al menor maduro en los dieciséis años, atribuyéndole capacidad para consentir tratamientos médicos sin intervención de los padres, teniendo éstos la facultad de ser informados en los casos de intervenciones quirúrgicas de alto riesgo, salvo que el menor no lo autorice. Para los menores de dieciséis años, el derecho inglés atribuye al menor la capacidad de consentir el tratamiento cuando pueda comprender su finalidad, naturaleza y riesgos. Rivero pone el ejemplo de la Sentencia *Gillieck versus West Norfolk and Wisbeck Area Health Authority* (1986) donde el Tribunal admitió el consentimiento de un menor de dieciséis años para un tratamiento anticonceptivo sin informar a los padres ya que el menor comprendía la naturaleza del mismo. El límite está puesto en la incapacidad del menor para negarse a tratamientos cuando esta negativa pueda poner en peligro su vida. Esta misma posición amplia respecto a las facultades del menor de edad, especialmente en lo relativo a la interrupción voluntaria del embarazo se ha dado en EEUU, acudiendo al principio del *best interest*. En distintas sentencias, el Tribunal Supremo de EEUU anuló la reglamentación estatal que exigía la notificación a los padres de los abortos realizados a menores de edad –*Planned Parenthood of Central Missouri v. Danforth* (1976) y *Bellotti v*

Su carácter básico facilita la homogeneidad, en una legislación autonómica que empezaba ya a ser contradictoria²⁰⁹. El establecimiento de tramos de edades tiene la ventaja de dar una mayor seguridad jurídica al médico a la hora de considerar cuando nos encontramos con un menor maduro capaz de dar su consentimiento para los tratamientos médicos. La referencia a edades también se encuentra en el Código Civil para el ejercicio de derechos y en el Código Penal como eximente de la responsabilidad penal –art. 19–²¹⁰. Otro criterio para deslindar sería según la gravedad del acto médico, pero esto hubiera introducido una gran complejidad. En cualquier caso, la Ley 41/2002 ha querido establecer un principio que incide específicamente en la prestación del consentimiento por representación, afirmando que «será adecuada a las circunstancias y proporcionada a las necesidades que haya que atender, siempre en favor del paciente y con respeto a su dignidad personal. El paciente participará en la medida de lo posible en la toma de decisiones a lo largo del proceso sanitario» –art. 9.5–. Este principio permite modular el automatismo de una decisión sólo basada en tramos de edad, de forma que se tenga también en cuenta el grado de madurez del menor, de manera que no haya situaciones o cambios jurídicos radicales en materias que puedan afectar a la propia vida un día antes o después de cumplir dieciséis o dieciocho años²¹¹.

Baird (1979)–. En todo caso, la situación legal en EEUU varía de un Estado a otro. Cfr. F. RIVERO HERNÁNDEZ, «Intervenciones corporales obligatorias y tratamientos sanitarios obligatorios», en AA.VV, *Internamientos involuntarios. Intervenciones corporales y tratamientos sanitarios obligatorios*, Actas de la Jornada Conjunta Ministerio de Sanidad y Consumo y Consejo General del Poder Judicial celebrada en Madrid el 24-6-1999, Madrid, 2000, pp. 207-229, esp. pp. 213-216. Cfr. L. TRIBE, *American Constitutional Law*, cit. pp. 1588-1593.

²⁰⁹ La Ley 21/2000, de 29 de diciembre, del Parlamento de Cataluña sobre los derechos de información concierne a la salud y la autonomía del paciente y a la documentación clínica –que fue el primer texto legislativo, y que se había basado en un Anteproyecto de Ley anterior preparado por el Ministerio de Sanidad y Consumo– permitía –art. 7– a los mayores de dieciséis años la posibilidad de dar su consentimiento, sin necesidad de informar a los padres. En iguales términos se expresa La Ley Foral Navarra, de 25 de abril de 2002, sobre los derechos del paciente a las voluntades anticipadas, a la información y a la documentación clínica –art. 7.2.b)–. La Ley 1/2003, de 28 de enero, de derechos e información al paciente de la Comunidad Valenciana sólo prevé que el menor emancipado dé personalmente su consentimiento –art. 9–. En cambio, la Ley 3/2001, de 28 de mayo, del Parlamento de Galicia reguladora del consentimiento informado y de la historia clínica de los pacientes no establecía ninguna capacidad al mayor de dieciséis años, limitándose a afirmar que el consentimiento le corresponde a sus padres o representantes legales, debiendo ser tomada en consideración la opinión del menor en función de su edad y su grado de madurez –art. 6–.

²¹⁰ La redacción original del Código Civil asociaba la posesión de la aptitud para realizar determinados actos y negocios al dato objetivo de la edad. Sin embargo, las modernas leyes reformadoras del Código Civil conceden la capacidad de obrar en función de la aptitud de cada persona, prescindiendo del dato objetivo de la edad. Esta orientación, a juicio de Díez-Picazo y Gullón, es arbitraria e insegura, pues deja la apreciación de la capacidad a un juicio subjetivo, aunque atiende a un objetivo justo, cual es la ampliación de la capacidad de obrar del menor en lo que no perjudique el desarrollo de su personalidad. Cfr. L. DIEZ-PICAZO Y A. GULLÓN, *Sistema de Derecho Civil*, Tecnos, 10.º ed, 2001, p. 226.

²¹¹ Se ha producido un debate, con anterioridad a la Ley 41/2002, sobre la conveniencia de fijar unos tramos de edad. Cfr. S. ROMEO MALANDA, «El valor jurídico del consentimiento prestado por los menores de edad en el ámbito sanitario», *La Ley* núm. 5185-5186, noviembre 2000; I. M. MARTÍNEZ-PEREDA RODRÍGUEZ, «La minoría madura», en Asociación Española de Derecho Sanitario, *Actas del IV Congreso de Derecho Sanitario*, Fundación Mapfre Medicina, 1988, pp. 71-91.

De todo ello se deduce que la Ley 41/2002 es más exigente que la normativa general en cuanto a la atribución a los menores de edad de capacidad para ejercitar derechos en el ámbito sanitario. Si la regla general es reconocer una importante capacidad de obrar en derecho a partir de los catorce años, la Ley 41/2002 ha elevado esta edad a los dieciséis años exista o no emancipación. Entre los doce y los dieciséis años es necesario escuchar la opinión del menor, pero el consentimiento le corresponde a sus padres. En todo caso, la Ley introduce la apreciación sobre la capacidad intelectual y emocional del menor para comprender el alcance de una intervención, como criterio importante para la solicitud del consentimiento por representación y, por tanto, para el ejercicio de los derechos de acceso a la historia clínica y a los datos sanitarios.

b) *Los casos difíciles: propuestas para la resolución del conflicto*

Después de analizar las previsiones legales y sus silencios, tenemos que incidir que en este ámbito del acceso de los padres y de los hijos a los datos sanitarios de éstos nos encontramos con distintos derechos en conflicto. Por una parte, el derecho a la intimidad y a la confidencialidad de los menores –art. 18 CE–, unido al secreto médico al que está obligado el profesional sanitario y que le exige respetar la confidencialidad de lo revelado por el menor y velar principalmente por su salud. Por otra parte, el derecho de los padres, que ejercen la patria potestad, a acceder a la información sanitaria del menor en beneficio de éste.

Estos derechos en conflicto tienen que valorarse a la hora de resolver los casos concretos. El principal problema que plantea la Ley 41/2002 es su contraste con la realidad, especialmente en lo relativo a los pacientes entre doce y dieciséis años. No parece que haya inconveniente en atender a pacientes entre doce y dieciséis años que acuden solos a la consulta. En la mayoría de los casos se trata de diagnosticar y tratar dolencias banales. Estos pacientes menores tienen derecho de acceso a su historia clínica y a sus datos sanitarios. El problema es si el menor de dieciséis años acude al médico sin consentimiento y sin conocimiento de los padres para donaciones de sangre, tratamiento de enfermedades venéreas; especialmente si acude por enfermedades de transmisión sexual, enfermedades psiquiátricas o tratamiento de enfermedades incurables. Un problema semejante se da incluso si acude un mayor de dieciséis años, al ser algunos de estos supuestos problemas graves de salud. A pesar de que el menor haya acudido sólo a la consulta, hay que valorar la obligación de los médicos de informar a los padres y de darles acceso a las historias clínicas de sus hijos. Como criterio general, parece que inicialmente se impone la obligación del profesional sanitario de informar a los padres de los menores de dieciséis años, pudiendo tener este supuesto más excepciones en el caso de mayores de dieciséis años.

Los temas sexuales obligan a mantener posiciones más matizadas. Un supuesto que se plantea frecuentemente es el caso de los menores que solicitan la prescripción de métodos anticonceptivos o el uso de la píldora del día des-

pués. En el caso de mayores de dieciséis años que solicitan estos tratamientos, no es necesario informar a los padres, aunque se trate de una medicación que pueda tener algunas complicaciones. Estos no son temas importantes de salud, aunque en medicina no haya realmente procesos menores ya que todo se puede complicar²¹². Como regla general, los padres no deben tener acceso a la historia clínica de sus hijos mayores de dieciséis años, si éstos se oponen, cuando no estemos ante un tema importante para su salud. Más dificultades plantea la solicitud de anticonceptivos por parte de menores de dieciséis años, sin consentimiento y sin conocimiento de los padres. La reforma del Código Penal de 1999 atribuye a los menores cierta capacidad de decisión para tener relaciones sexuales a partir de trece años. Por una parte, el menor no quiere hacer partícipes a sus padres en un tema que afecta al desarrollo de su personalidad. Por otra parte, les corresponde a los padres ejercer la patria potestad en beneficio de los hijos y de acuerdo con su personalidad –art. 154 del Código Civil–. En estos casos, el médico puede no estar obligado a informar a los padres siempre que nos encontremos con un menor de dieciséis años maduro y siempre que su conducta no suponga ningún riesgo leve para su salud. En el conflicto entre el derecho a la intimidad del menor y su libre desarrollo de la personalidad, y la patria potestad de los padres, parece que prima el primero, aunque sea un menor de dieciséis años²¹³. No tiene sentido que tengan los padres derechos a acceder a una historia clínica donde se contienen datos de información sexual, para limitar una facultad que a los menores les atribuyen las leyes. Si en beneficio del menor los padres no deben conocer algún dato, el médico no debe darlo. En cambio, cuando la conducta del menor pueda suponer un riesgo –no hace falta que sea grave, basta con que sea leve– para la salud del menor, debe informarse a los padres. La patria potestad se debe ejercer en beneficio del menor y a favor del desarrollo de su personalidad. El criterio de interpretación debe ser siempre el interés del menor²¹⁴.

La confidencialidad del adolescente mayor de dieciséis años se debilita, por tanto, si hay una amenaza grave para su salud o para su vida. Este es el caso

²¹² Un claro ejemplo es el *piercing*, que puede causar hepatitis u otras enfermedades infecciosas.

²¹³ En Francia ésta cuestión está resuelta legalmente. El art. 50 de la Ley 90/86, de 23 de enero de 1990, extiende las disposiciones sobre los derechos de los menores a la contracepción, al test de detección del sida y al tratamiento de ciertas enfermedades sexuales transmisibles, reconociendo que el menor tiene un derecho a la personalidad que le permite actuar de manera autónoma en una serie de materias conflictivas como anticoncepción, sexualidad y enfermedades infecciosas. Cfr. J. SÁNCHEZ-CARO y F. ABELLÁN, *El médico y la intimidad*, cit. p. 208.

²¹⁴ Esta cuestión fue planteada ante la Sala Contencioso-Administrativa del Tribunal Superior de Justicia de Aragón –Sección 1ª–. Una asociación de padres impugnó una Circular del INSALUD y de la Diputación de Aragón, que facilitaba que adolescentes entre quince y diecisiete años pudieran asistir a centros públicos de orientación sexual para recibir en ellos información sobre anticoncepción y sexualidad, sin necesidad de estar acompañados de sus padres. La Sentencia, de 26 de octubre de 1992, inadmitió el recurso por defectos de forma, pero la cuestión de fondo fue analizada en dos votos particulares contradictorios: uno hacía prevalecer la capacidad de decisión del menor y el respeto a su intimidad que permitía ocultar información a los padres en beneficio del menor; otra hacía primar la responsabilidad y el necesario conocimiento de los padres.

de la adicción a las drogas o al alcohol –frecuentes intoxicaciones etílicas– o de los problema psiquiátricos. Así, en supuestos como los trastornos alimentarios –la anorexia nerviosa–, la labor de los padres es fundamental para evitar los procesos de desnutrición agudos. Igualmente es imprescindible la colaboración de los padres para la detección precoz de las conductas suicidas. En estos casos, el *balancing* constitucional ya no es entre el derecho a la intimidad del menor y la patria potestad de los padres sino entre la confidencialidad del menor y el derecho a la vida, que obliga a informar a los padres como forma para garantizar el tratamiento. Como ha señalado reiteradamente el Tribunal Constitucional en distintas Sentencias²¹⁵, la vida es un bien indisponible e irrenunciable; es el fundamento de los demás derechos constitucionales, porque sin vida no hay libertad ideológica, sin vida no hay libertad personal, sin vida no hay derecho a la intimidad. En este caso, es el propio principio del interés superior del menor el que obligaría a informar a los padres. El tratamiento psiquiátrico del adolescente implica límites en relación con la confidencialidad de los datos del menor, ya que la inmadurez psicológica puede llegar a comprometer su capacidad para conocer y tomar la decisión más adecuada²¹⁶.

En todo caso, también es posible optar por no informar a los padres, especialmente en el caso de que los menores sean portadores del VIH o de que tengan una adicción a sustancias tóxicas²¹⁷. El médico puede tener miedo a perder la confianza del menor y llega a pensar que si los padres van a conocer su enfermedad, éste va a ocultar información o va a dificultar el tratamiento. Es posible en estos casos llevar a cabo determinados pactos con los menores, también llamados alianzas terapéuticas, que son más característicos de otros ámbitos como el de las incapacidades temporales para el trabajo, y que sigue la siguiente fórmula²¹⁸: «si tu sigues viniendo a la consulta semanalmente y compruebo que has dejado de tomar esas sustancias, no se lo digo a tus padres. Pero si no cumples el pacto, se lo digo a tus padres». En el fondo, se trata de no perder al paciente, ya que a éste se le puede perder si se le violenta su intimidad de una manera agresiva: «el paciente es como el honor, que una vez perdido ya no se recupera más»²¹⁹. Esta actitud del médico exige, sobre todo, ganarse la confianza del menor, al que el médico no conoce, lo que requiere tiempo, dedica-

²¹⁵ Cfr. SSTC 53/1985, de 11 de abril, sobre el aborto; 120/1990, de 27 de junio y 11/1991, de 17 de enero, sobre huelgas de hambre.

²¹⁶ Una excepción clara de la confidencialidad es la que presenta el adolescente esquizofrénico que no desea que se informe a sus padres, ya que en este caso el deber ético de proporcionarle el tratamiento más adecuado prevalece sobre la confidencialidad. En otras ocasiones, la confidencialidad del adolescente es necesaria durante el tratamiento por lo que no informar a los padres es una condición a menudo necesaria para su tratamiento. Cfr. J. SÁNCHEZ-CARO y J. SÁNCHEZ CARO, *El médico y la intimidad*, cit. pp. 205-207.

²¹⁷ En la práctica se avisa poco a los padres ya que no siempre hay tiempo ni posibilidad de identificarlos.

²¹⁸ Cfr. F. MONTALVO, «El menor en el ámbito sanitario», *II Jornadas sobre Derecho de los Menores, in voce*.

²¹⁹ Cfr. M. R. PADILLA, «El menor en el ámbito sanitario», *II Jornadas sobre Derecho de los Menores, in voce*.

²²⁰ Problemas añadidos son el escaso tiempo que se puede dedicar a cada paciente en atención primaria y la dificultad de dialogar con los menores inmigrantes que no dominan aún el castellano. Cfr. el estudio del Defensor del Menor en la Comunidad, *Menores inmigrantes en España*, cit. p. 35 –apdo. «Posibles iniciativas en materia de salud»–.

ción y, sobre todo, diálogo, para quitar muchas veces la angustia²²⁰. La mayoría de las veces el médico se ve obligado a tomar las decisiones sobre la marcha, por lo que es conveniente la elaboración en estos casos de protocolos de actuación y que cualquier decisión que se tome y los motivos que la justifiquen se hagan constar en la historia clínica. El médico no debe estar sólo. Es recomendable que las decisiones se adopten de manera colegiada en equipos o unidades de tipo social, donde estén presentes psicólogos, trabajadores sociales y personal facultativo, y que permiten compartir la responsabilidad ante posibles reclamaciones posteriores de los padres. Otras veces se opta por avisar a los padres de manera que se evite la inseguridad de los médicos frente a posibles reclamaciones de los padres que acusan al facultativo de tomar decisiones que les corresponden a éstos. Hay médicos que piensan que no pueden ser protagonistas de todo y que no pueden asumir solos la responsabilidad. En muchos casos, los pacientes adolescentes deben ser animados a informar ellos mismos a sus padres de los asuntos que éstos deban conocer²²¹.

En la mayoría de los casos, los representantes del menor serán sus padres o sus tutores legales, dentro de una situación de normalidad. En caso de padres separados, ambos mantienen la patria potestad sobre el menor y tienen derecho al acceso a la historia clínica, salvo que alguno de ellos tenga privada la patria potestad por decisión judicial. En el supuesto de padres no sólo separados sino enfrentados respecto a los intereses del niño, o de padres con problemas personales y sociales tan complejos que hacen dudar de su gestión en beneficio del hijo, se debe consultar a las instituciones específicas²²². Cuando el menor va sólo a la consulta, o es un tema sexual que le da vergüenza, o una cuestión social o familiar que puede ser grave. En ocasiones, el profesional sanitario se enfrenta a circunstancias como malos tratos sobre los niños o a posibles abusos sexuales por parte de los padres que obliga al médico a denunciar y a no dar a los padres el acceso a la historia clínica.

El médico que atiende al menor tiene el deber de velar, a la hora de facilitar la información a los padres o de mantenerla reservada, para que cualquier decisión suya vaya encaminada a beneficiar al paciente y no a perjudicarlo. Siempre debe regirse por el principio del interés superior del menor a la hora de facilitar el ejercicio de los derechos de acceso de padres e hijos a la historia clínica de los menores. En situaciones de duda o ante problemas graves –por ejemplo, si la decisión de los padres o del hijo puede perjudicar gravemente al

²²¹ Sobre esta cuestión, véase el apartado relativo a jóvenes y adolescentes del documento elaborado por el INSALUD «Principios y Prácticas de asesoramiento sobre el VIH 25». En principio, hay que dar a los padres toda la información para que adopten las decisiones oportunas sobre sus hijos. En otras ocasiones, es mejor para el tratamiento médico ocultar parte de la información a los padres. Siempre es conveniente fomentar el diálogo con el menor y comentar qué información se va a suministrar a los padres, teniendo siempre presente el interés superior del menor y la necesidad de no perder al paciente por revelar la información sanitaria a sus progenitores.

²²² El art. 299 del Código Civil prevé el nombramiento, en su caso, de un Defensor Judicial si existe conflictos de intereses.

menor o si existe desacuerdo entre los padres–, puede acudir al Ministerio Fiscal o a los órganos judiciales²²³. El art. 158.3 del Código Civil establece que el Juez, de oficio, a instancia del propio hijo, de cualquier pariente o del Ministerio Fiscal dictará las disposiciones que considere oportunas a fin de apartar al menor de un peligro o de evitarle perjuicios. El médico acude habitualmente al juez huyendo de la responsabilidad que frecuentemente aparece por una judicialización de las consecuencias de los procesos sanitarios. Los hospitales disponen también de Comités de Ética, que permiten analizar y proponer, si procede, alternativas o soluciones –no de carácter vinculante– a los conflictos éticos, evitando derivarlo todo a los órganos judiciales, ya que normalmente la resolución judicial no va a discutir con el profesional sanitario la idoneidad de los tratamientos sanitarios y va a autorizar la intervención, pudiendo ser este requerimiento al juez una suerte de medicina defensiva²²⁴. El médico también puede acudir a instituciones como el Defensor del Pueblo o instituciones autonómicas con funciones análogas. Estas instituciones facilitan la identificación de los intereses y valores enfrentados y la determinación de cuál debe prevalecer²²⁵. La Ley 41/2002 trata de delimitar jurídicamente los distintos supuestos en conflicto, pero mantiene un ámbito para la deliberación del profesional sanitario, ya que las leyes nunca podrán dar recetas rápidas para resolver problemas humanos complejos que se producen en la práctica cotidiana y que deben ser resueltos por estos profesionales de acuerdo con su buen hacer y su experiencia²²⁶.

²²³ No siempre la decisión de los padres o del menor protege a éste. Este es el caso del rechazo a determinados tratamientos médicos por parte de los padres o del hijo mayor de dieciséis años por no ser adecuado a sus convicciones religiosas. Esto es especialmente grave cuando se pone en peligro el derecho a la vida y a la integridad física –art. 15 CE–, que es un bien constitucional indisponible e irrenunciable –STC 53/1985–. Cfr. J. GONZÁLEZ PÉREZ, «La protección de la juventud y de la infancia», *Manual Fraga. Homenaje Académico*, Fundación Canovas del Castillo, Madrid, 1997, p. 718. Cfr. los distintos supuestos en F. RIVERO HERNÁNDEZ, «Intervenciones corporales obligatorias y tratamientos sanitarios obligatorios», *loc. cit.* pp. 207-229.

²²⁴ Sobre la cuestión véase el Decreto 61/2003, de 8 de mayo, del Consejo de Gobierno de la Comunidad de Madrid que regula el régimen jurídico de funcionamiento y la acreditación de los Comités de Ética para la Asistencia Sanitaria y crea y regula la Unidad de Bioética y Orientación Sanitaria y el Comité Asesor de Bioética de la Comunidad de Madrid –esp. art.3–. Existen también para este menester las Comisiones Deontológicas de los Colegios Profesionales.

²²⁵ La Comunidad de Madrid dispone de dos instituciones específicas para la protección de los menores en el ámbito sanitario: el Defensor del Menor y el Defensor del Paciente. La Institución del Defensor del Menor se crea por la Ley 6/1995, de 28 de marzo, de Garantías de los Derechos de la Infancia y Adolescencia en la Comunidad de Madrid, y queda definida como «Alto Comisionado de la Asamblea de Madrid para salvaguardar los derechos de los menores en la Comunidad de Madrid». Posteriormente, la Ley 5/1996, de 8 de julio, del Defensor del Menor en la Comunidad de Madrid concreta el ámbito competencial de esta Institución. Cfr. más ampliamente «La figura del Defensor del Menor: marco normativo» y «La institución del Defensor del Menor como organización relacional: la cuestión de legitimidad», en *Defensor del Menor en la Comunidad de Madrid. Estudios e Investigaciones 2001*, Asamblea de Madrid, 2003. El Defensor del Paciente se crea por la Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid y es definido como un órgano de la Administración Sanitaria encargado de gestionar las quejas, reclamaciones y sugerencias en relación con los derechos de los pacientes, teniendo como principal objetivo «intermediar en los conflictos que planteen los ciudadanos como usuarios del Sistema Sanitario de la Comunidad de Madrid» –art. 36–.

²²⁶ Cfr. N. MARTÍN ESPILDORA, Tribuna, *Diario Médico* 7-3-2003 p.10.

V. LA CONFIDENCIALIDAD DE LAS HISTORIAS CLÍNICAS DENTRO DEL SISTEMA NACIONAL DE SALUD: LA LEY DE COHESIÓN Y CALIDAD DEL SISTEMA NACIONAL DE SALUD

Hasta ahora hemos analizado principalmente la confidencialidad de la historia clínica en el ámbito del propio centro sanitario público y privado y del propio servicio de salud autonómico. Nos corresponde analizar ahora brevemente la protección de los datos de salud desde la perspectiva de un Sistema Nacional de Salud. La Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud ha reconocido expresamente el derecho a una asistencia sanitaria pública, universal y gratuita. Al mismo tiempo, nuestra Constitución en su Título VIII, los Estatutos de Autonomía así como la legislación sanitaria, en especial, la Ley 14/1986, de 25 de abril, General de Sanidad ya habían establecido un modelo de prestación sanitaria fuertemente descentralizado que permitía la asunción por las Comunidades Autónomas de competencias en materia de gestión de la sanidad, quedando reservado al Estado la regulación de las bases y la coordinación general de la sanidad.

La General de Sanidad, y más recientemente, la Ley de Cohesión y Calidad del Sistema Nacional de Salud han establecido los principios vertebradores de la descentralización política de la sanidad, al tiempo que han definido la integración de los diferentes servicios de salud y políticas sanitarias dentro en un Sistema Nacional de Salud, con el objetivo de que la descentralización no afecte a la igualdad del derecho a recibir una asistencia sanitaria. La efectividad del derecho a recibir una asistencia sanitaria de calidad en todo el territorio nacional exige el establecimiento de un conjunto de principios que vertebran el Sistema Nacional de Salud para que éste funcione como un auténtico Sistema donde el aseguramiento público universal e igual sea una realidad con independencia del lugar de residencia.

Este objetivo sólo puede ser alcanzado a través de la coordinación y la cooperación de todas las Administraciones públicas sanitarias que permita una atención integral de la salud, tanto en el aspecto preventivo como en el puramente asistencial y de rehabilitación. La Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud ha desarrollado así un conjunto de mecanismos de coordinación y cooperación en algunos ámbitos donde es especialmente precisa esta colaboración, entre los que destaca el establecimiento de sistemas de información que permita que esta información fluya dentro del Sistema Nacional de Salud, creándose órganos específicos como el Observatorio del Sistema Nacional de Salud –art. 1– o el Instituto de Información Sanitaria.

El funcionamiento cohesionado del Sistema Nacional de Salud que permita la existencia de un servicio público sanitario de calidad y en condiciones de igualdad se basa en un sistema de información sanitaria que garantice la disponibilidad de la información y la comunicación recíprocas entre la Administración Sanitaria General del Estado y la de las Comunidades

Autónomas²²⁷. Este sistema debe contener información sobre los pacientes –usuarios del Sistema– y sobre los profesionales al servicio del Sistema Nacional de Salud –los recursos humanos a disposición de las distintas Administraciones Públicas–. La existencia de una tarjeta sanitaria individual que facilite el acceso de los ciudadanos a las prestaciones del Sistema Nacional de Salud –a la que nos referimos específicamente– requiere de un sistema de información que incluya los datos básicos de identificación del titular, su derecho a las prestaciones y la entidad responsable de la asistencia sanitaria, con un modelo que permita la lectura y comprobación de datos en todo el territorio nacional²²⁸. Igualmente, la planificación de las necesidades de recursos humanos dentro del Sistema Nacional de Salud exige un sistema de información con datos de los profesionales sanitarios actualmente existentes en cada una de las especialidades que permita un trabajo planificado –art. 35–. El establecimiento de un sistema de información es también necesario para la mejora de la calidad del sistema sanitario, que exige que cualquier actuación se establezca sobre la base de indicadores estadísticos –art. 59–. También las políticas de salud pública requieren una coordinación de los sistemas de información epidemiológica –art. 65–²²⁹.

Por ese motivo la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud pone en marcha un sistema de información sanitaria en el Sistema Nacional de Salud que garantice la disponibilidad de la información y la comunicación recíprocas entre las Administraciones sanitarias en el marco de los objetivos establecidos por el Consejo Interterritorial del Sistema Nacional de Salud –art. 53–. Se establece así un sistema de información de salud y el intercambio de información entre servicios, creándose una auténtica red –art. 54–. Le corresponde al Consejo Interterritorial del Sistema Nacional de Salud establecer la definición y normalización de datos y flujos, la

²²⁷ La Disposición Adicional Tercera de la Ley 41/2002, de 14 de noviembre ya anticipaba la implantación de un sistema de compatibilidad y coordinación de las historias clínicas, que, teniendo en cuenta la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, para evitar que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición.

²²⁸ Como hemos señalado anteriormente *supra* –apdo. 1–, la atribución a las Comunidades Autónomas de las competencias de gestión sobre los diferentes servicios de salud hace imposible, a nuestro juicio, un modelo de historia clínica centralizada para todo el Sistema Nacional de Salud. Lo más razonable es un proyecto de historia clínica compartida, semejante al impulsado por el Servei Català de Salut de forma que la historia clínica se encuentre en centros de procesos de datos de cada Comunidad Autónoma pero haya la posibilidad de intercambiar electrónicamente información sanitaria. Para ello, es necesario determinar qué, información sanitaria básica del ciudadano –más reducida que la totalidad de la historia clínica– se va a compartir entre las diferentes Comunidades Autónomas, además de ponerse de acuerdo en la terminología y en el lenguaje. Así, el Real Decreto 183/2004, de 30 de enero, señala que la finalidad del código de identificación es facilitar la búsqueda de la información sanitaria de un paciente que puede encontrarse dispersa en el Sistema Nacional de Salud, con el fin de que pueda ser localizada y consultada por los profesionales sanitarios –art. 4.3–.

²²⁹ En relación con las redes de datos sanitarios, la tarjeta sanitaria informatizada y los sistemas de ayuda en la toma de decisiones médicas, *cfr.* la Opinión del Grupo Europeo de Ética de las Ciencias y de las Nuevas Tecnologías sobre los *Aspectos éticos de la utilización de datos personales sanitarios en la sociedad de la información*, *cit.*

selección de indicadores y los requerimientos técnicos necesarios para la integración de la información. Todas las Administraciones implicadas –Comunidades Autónomas, Administración General del Estado, Entidades Gestoras de la Seguridad Social– aportarán a este sistema de información sanitaria los datos necesarios para su mantenimiento y desarrollo. Todas las Administraciones, tanto autonómicas como estatal, tienen derecho de acceder y disponer de los datos que formen parte del sistema de información que precisen para el ejercicio de sus competencias.

En relación con el modelo de intercambio de información sanitaria para la atención a los pacientes en el Sistema Nacional de Salud, hay que destacar la regulación que la Ley 16/2003, de 28 de mayo, hace acerca de la tarjeta sanitaria individual –art. 57–, que ha sido desarrollado por el Real Decreto 183/2004, de 30 de enero. El modelo propuesto se fundamenta en la identificación unívoca de los usuarios –a través de esta tarjeta– y en la interoperabilidad de los sistemas de información de todas las Administraciones participantes, que son los que conservan la historia clínica del paciente²³⁰. De hecho, el acceso de los ciudadanos a las prestaciones de la atención sanitaria que proporciona el Sistema Nacional de Salud se facilita a través de la tarjeta sanitaria individual, como documento administrativo que acredita determinados datos de su titular, el derecho que le asiste en relación con la prestación farmacéutica y el servicio de salud o entidad responsable de la asistencia sanitaria. Los dispositivos que las tarjetas incorporen para almacenar la información básica y las aplicaciones que la traten deben permitir que la lectura y comprobación de los datos sea técnicamente posible en todo el territorio del Estado y para todas las Administraciones Públicas. El Real Decreto 183/2004, de 30 de enero, señala que la tarjeta sanitaria individual incorpora un código de identificación personal que tiene como finalidad facilitar el rastreo de información sanitaria de un paciente existente en diferentes puntos del Sistema Nacional de Salud, con el fin de que pueda ser localizada y consultada siempre y cuando ello redunde en la mejora de la atención sanitaria y bajo las condiciones que legalmente se estipulen²³¹. El establecimiento de un código de identificación personal único exige una base de datos que recoja la información básica de asegurados del Sistema Nacional de Salud, de forma que todos los servicios de salud puedan disponer de un servicio de intercambio de información sobre la población pro-

²³⁰ Sobre los distintos modelos de intercambio de información de pacientes, *cf.*: F. LÓPEZ CARMONA, «salud: confidencialidad y seguridad de la información en el ámbito asistencial», *cit.* En el modelo centrado en la red, basta con que el paciente se identifique –mediante un simple código individual hasta por tarjetas inteligentes, certificados electrónicos, parámetros biométricos– para que se desencadene un conjunto de procesos electrónicos de intercambio de información que acreditan el derecho de acceder a una prestación y el intercambio de información clínica. En cambio, el modelo centrado en el paciente está basado en que éste lleve su propia información clínica a través de tarjetas inteligentes –con chip integrado–.

²³¹ En todo caso, hay que señalar que la CNIL se ha mostrado favorable a la existencia de un número de identificación personal para acceder a las historias clínicas distinto del DNI ya que este último facilita la comunicación de la información de salud con otros fines. Sin embargo, el Gobierno francés se ha opuesto a este planteamiento. *Cf.*: *Le Monde*, 25 de junio de 2007.

regida. El núcleo del sistema mantiene únicamente una base de datos de población protegida con una información básica de los usuarios del Sistema Nacional de Salud, así como un fichero histórico de las distintas situaciones de aseguramiento. Esta base de datos de población protegida del Sistema Nacional de Salud permite el intercambio de información entre Administraciones sanitarias, dando coherencia a los datos de aseguramiento, evitando la adscripción simultánea a distintos servicios de salud y permitiendo una mayor rentabilidad en los cruces de datos. El modelo trata de facilitar la interoperabilidad entre todos los agentes del Sistema Nacional de Salud, manteniendo sus peculiaridades tanto tecnológicas como funcionales. Así, el núcleo del Sistema Nacional de Salud no dispone de los usuarios físicos sino que se produce un intercambio de información entre los servidores de los servicios de salud y del servidor central²³².

La Ley 16/2003, de 28 de mayo, no sólo ha establecido un sistema de información con datos personales sino que ha recordado las exigencias a este respecto de la legislación de protección de datos personales. Así, se prevé expresamente que «[l]a cesión de los datos, incluidos aquellos de carácter personal necesarios para el sistema de información sanitaria, estará sujeta a la legislación en materia de protección de datos de carácter personal y a las condiciones acordadas en el Consejo Interterritorial del Sistema Nacional de Salud» –art. 53-. Además, este intercambio telemático de información «se realizará de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en la Ley 41/2002, de 14 de noviembre». Por tanto, el intercambio de información desde los distintos Servicios Sanitarios tiene que ajustarse a los principios y a los derechos de protección de datos antes analizados.

De esta forma, este sistema de información debe respetar el principio de calidad –art. 4 LOPD–, lo que supone, por ejemplo, no tratar más datos de los necesarios, tener unos criterios de acceso restrictivos y cancelar la información clínica pasados los plazos establecidos legalmente²³³. El art. 57 de la Ley 56/2003 establece los aspectos esenciales de la Tarjeta Sanitaria Individual, la asignación del Código de Identificación Personal del Sistema Nacional de Salud y la Base de Datos de población protegida. Así, la tarjeta sanitaria sólo debe contener los datos básicos de identificación del titular de la tarjeta, el derecho que le asisten en relación con la prestación farmacéutica y el servicio de salud responsable de la asistencia²³⁴. Si bien en la tarjeta sanitaria no se con-

²³² Esta cuestión ha sido analizada por J. FERNANDO MUÑOZ MONTALVO, «La protección de datos personales en el Sistema Nacional de Salud», *Datospersonales.org*.

²³³ Por ejemplo, se establece que la base de datos de pacientes del sistema de información sanitaria debe de tener un procedimiento de actualización de los usuarios del Sistema Nacional de Salud, lo que implica un servicio de intercambio que permita la depuración de titulares de tarjetas sanitarias –art. 56–.

²³⁴ El art. 2 del Real Decreto 183/2004, de 30 de enero señala que todas las tarjetas sanitarias incorporarán una serie de datos básicos comunes y estarán vinculadas a un código de identificación personal único de cada ciudadano en el Sistema Nacional de Salud. En concreto incorporará la Administración Sanitaria emisora de la tarjeta, apellidos y nombre del titular de la tarjeta, código de identificación personal asignado por la Administración sanitaria que emite la tarjeta, modalidad de la prestación farmacéutica y una leyenda que informa de su validez en todo el Sistema Nacional de Salud –art. 3–.

tienen datos especialmente protegidos –por lo que la inclusión de datos en el sistema de información, sin perjuicio de que exista una habilitación legal, puede ser desarrollado sin consentimiento del interesado porque es para el desarrollo de una actividad administrativa–, la finalidad del modelo es la comunicación de datos de salud para que los ciudadanos reciban la mejor asistencia posible. Así, la Ley 16/2003 establece que «con el fin de que los ciudadanos reciban la mejor atención sanitaria posible en cualquier centro o servicio del Sistema Nacional de Salud, el Ministerio de Sanidad y Consumo coordinará los mecanismos de intercambio electrónico de información clínica y de salud individual previamente acordados con las Comunidades Autónomas, para permitir tanto al interesado como a los profesionales que participan en la asistencia sanitaria el acceso a la historia clínica en los términos estrictamente necesarios para garantizar la calidad de dicha asistencia y la confidencialidad e integridad de la información, cualquiera que fuese la Administración que la proporcione» –art. 56–. Se va a producir, por tanto, una comunicación de datos de salud entre Administraciones sanitarias con habilitación legal. La Ley 16/2003 establece una fuerte habilitación legal para la comunicación de datos entre servicios de salud públicos, de manera que se pueda obviar la previsión del arto 21.1 LOPD que permite la comunicación de datos entre Administraciones Públicas para competencias semejantes para las mismas materias y que es discutible en el ámbito de los datos especialmente protegidos. En cambio, la comunicación de datos de salud entre servicios de salud privados –sociedades médicas, centros sanitarios privados, etc. sólo se puede producir si el paciente acude o va a ser tratado en el mismo, en virtud del arto 8 LOPD–. En todo caso, no hay que olvidar que la propia LOPD permitía la cesión de datos por motivos de urgencia sanitaria –art. 11–. Siempre hay que respetar el principio de información a los pacientes sobre la existencia de este sistema de información, su finalidad, las posibles comunicaciones, la identidad y dirección del responsable y los derechos que le asisten –art. 5 LOPD–.

El establecimiento de un sistema de información sanitaria en el Sistema Nacional de Salud que garantice la disponibilidad de la información y la comunicación recíprocas entre las distintas Administraciones Sanitarias hace especialmente importante el cumplimiento del principio de seguridad de la información –art. 9 LOPD–. Cualquier proyecto que pretenda el uso de la red para enviar información de carácter sanitario tiene que garantizar la identidad de quienes desarrollan esa comunicación, la confidencialidad y la protección de los datos personales. Por ello, la Ley 16/2003, de 28 de mayo, establece que la red de comunicaciones que el Ministerio de Sanidad ponga a disposición del Sistema Nacional de Salud deberá ser una «red segura de comunicaciones que facilite y dé garantías de protección al intercambio de información exclusivamente sanitaria entre sus integrantes». Además, la «transmisión de la información en esta red estará fundamentada en los requerimientos de certificación electrónica, firma electrónica y cifrado, de acuerdo con la legislación vigente». Esto es lógico ya que «a través de dicha red circulará información relativa al código de identificación personal único,

las redes de alerta y emergencia sanitaria, el intercambio de información clínica y registros sanitarios, la receta electrónica y la información necesaria para la gestión del Fondo de cohesión sanitaria, así como aquella otra derivada de las necesidades de información sanitaria en el Sistema Nacional de Salud» –art. 54–. El modelo planteado en el Real Decreto 183/2004, de 30 de enero se sostiene sobre la identificación de los agentes implicados mediante el uso de certificados digitales. Se trata también de asegurar la integridad de la información y el no repudio de las operaciones, mediante la firma digital. Las comunicaciones entre los sistemas cliente –de los servicios de salud– se realiza de una manera cifrada, que garantiza la privacidad de la información y la no exposición de la misma a terceros no autorizados.

La regulación del intercambio de información de salud entre los distintos organismos, centros y servicios del Sistema Nacional de Salud debe permitir tanto el derecho de acceso del paciente a la historia clínica –art. 15 LOPD– como también la comunicación de esta información a los profesionales que le asisten. No olvidemos que el establecimiento de mecanismos de intercambio electrónico de información clínica y de salud individual tiene como finalidad que los ciudadanos reciban siempre la mejor asistencia sanitaria posible, permitiendo, como no podía ser de otro modo, el acceso a la información clínica tanto del interesado como de los profesionales que participan en la asistencia. Así, la tarjeta sanitaria individual «deberá posibilitar el acceso a aquella de los profesionales debidamente autorizados, con la finalidad de colaborar a la mejora de la calidad y continuidad asistenciales» –art. 57–. Sin embargo, esto se debe hacer «en los términos estrictamente necesarios para garantizar la calidad de dicha asistencia y la confidencialidad e integridad de la información, cualquiera que fuese la Administración que la proporcione» –art. 56.1–.

El Real Decreto 183/2004, de 30 de enero atribuye al Ministerio de Sanidad y Consumo la responsabilidad de la base de datos de población protegida del Sistema Nacional de Salud –art. 6.3–, sin perjuicio de que corresponda a los distintos servicios de salud incorporar las correspondientes altas y bajas en la cobertura de los ciudadanos de las diferentes Comunidades Autónomas.

Para permitir el funcionamiento del sistema de información sanitaria se crea un Instituto de Información Sanitaria, dependiente del Ministerio de Sanidad y Consumo –art. 58–. Este se encarga de recabar, elaborar y distribuir la información que responda a las necesidades del Sistema Nacional de Salud, con criterios de transparencia y objetividad de la información generada, de acuerdo con las directrices que para su utilización se establezcan por el Consejo Interterritorial. Es este Instituto al que le corresponde velar «por la integridad y seguridad de los datos confiados, garantizando su confidencialidad con arreglo a lo dispuesto en la Ley Orgánica 15/1999» –art. 58–. En todo caso, los sistemas de información en materia de epidemiología o de recursos humanos tienen que trabajar principalmente con información disociada, como exigencia del propio principio de calidad.

VI. LAS HISTORIAS CLÍNICAS NO INFORMATIZADAS

A pesar del proceso de informatización y centralización de las historias clínicas²³⁵, muchas historias clínicas en centros sanitarios públicos como privados y en consultas de profesionales individuales se encuentran en soporte papel. Inicialmente, cuando se habla de ficheros de datos personales, se piensa en tratamientos de datos informatizados²³⁶. De hecho, históricamente, la vigencia de la normativa de protección de datos no se había extendido a los ficheros manual-estructurados. La amenaza al derecho a la privacidad personal se ha incrementado fundamentalmente a través de los tratamientos automatizados de datos personales y no tanto a través de los tratamientos manuales. A pesar de que un acceso indebido a un fichero en papel puede llegar a ser escandaloso —pensemos en una historia clínica abandonada en la calle—, las tecnologías de la información pueden provocar mayores vulneraciones a los derechos, ya que la informática permite una gran capacidad para recoger datos personales, grabarlos y ponerlos en comunicación, facilitando perfiles de las personas. Por ello, el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, se aprobó para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales. En España, se tardó aún varios años en aprobar la primera Ley, que estuvo destinada también únicamente a los tratamientos automatizados de datos personales. Esta fue, como ya se sabe, la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Como la realidad no cambia inmediatamente porque cambien las normas jurídicas, el Reglamento de Medidas de Seguridad de los Ficheros Automatizados se aprobó por el Real Decreto 994/1999, de 11 de junio, a pesar de que el primer borrador era de 1994. Además, la entrada en vigor de las medidas de seguridad básicas, medias y altas fue sucesivamente prorrogada²³⁷.

Sin embargo, la Ley Orgánica 15/1999, de 13 de noviembre, de Protección de Datos de Carácter Personal, a diferencia de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, no se extiende únicamente a la regulación de los ficheros informatizados sino también a los tratamientos de datos personales no automatizados, es decir, en soporte papel. Son los llamados ficheros manual-estructurados. De hecho, la modificación de la LORTAD y la aprobación de la LOPD es una exigencia de la Directiva 95/46/CE del Parlamento y del

²³⁵ *Cfr. supra* apdo. 2.c) y 2.e).

²³⁶ Esta cuestión la hemos analizado en relación con los ficheros en soporte papel de las Universidades. *Cfr.* A. TRONCOSO REIGADA, «La publicación de datos de profesores y alumnos y la privacidad personal. Acerca de la protección de datos personales en las Universidades», *Revista de Derecho Político*, núm. 67, 2006, pp. 104-111.

²³⁷ El plazo para las medidas de nivel básico fue ampliado por el Real Decreto 195/2000, de 11 de febrero, desde el 26 de diciembre de 1999 al 26 de marzo de 2000. Las medidas de seguridad de nivel alto fueron también prorrogadas del 26 de junio de 2001 al 26 de junio de 2002, por la Resolución de la Subsecretaría del Ministerio de Justicia de 22 de junio de 2001 —BOE de 25 de junio de 2001—.

Consejo, relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales y a la libre circulación de esos datos, que extendía su ámbito de aplicación a los ficheros no automatizados²³⁸. El art. 2 LOPD establece como ámbito de aplicación «los datos de carácter personal *registrados en soporte físico, que los haga susceptibles de tratamiento*, y a toda modalidad de uso posterior de estos datos por los sectores público y privado». Además, el art. 3.c) LOPD define como tratamiento de datos las «operaciones y procedimientos técnicos *de carácter automatizado o no*, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias». Ahora bien, la Directiva sólo abarca a los ficheros estructurados y no a las carpetas que no estén estructuradas. Para que pueda hablarse de un fichero manual, éste debe estructurarse conforme a criterios específicos relativos a las personas que faciliten el acceso de forma sencilla a los datos, si bien corresponde a los Estados la definición de los criterios que permitan determinar los elementos de un conjunto estructurado de datos de carácter personal. Las carpetas y conjunto de carpetas que no estén estructuradas conforme a estos criterios no estarán comprendidas en ningún caso en el ámbito de aplicación de la Directiva²³⁹. Como las historias clínicas se encuentran archivadas conforme a criterios específicos relativos a personas, hay que señalar que estos tratamientos de datos personales en soporte papel entran dentro del ámbito de aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ahora bien, si el legislador ha regulado los ficheros informatizados, tratando de actuar con cautela y previendo los necesarios periodos transitorios, se comprende también la prudencia de éste a la hora de establecer la regulación efectiva del ordenamiento jurídico de protección de datos personales para los ficheros manual-estructurados en nuestro país. Así, la Disposición Adicional Primera de la LOPD relativa a los ficheros preexistentes señala que «[e]n el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 2005, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados». Por tanto, la vigencia de la legislación de protección de datos sobre los ficheros manuales es más confusa y exige una interpretación compleja.

²³⁸ El art. 2.b) de la Directiva define como tratamiento de datos personales «cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados». La Directiva señala que la protección de las personas debe aplicarse tanto al tratamiento automático de datos como al manual, ya que el alcance de la protección no debe depender de las técnicas utilizadas. Así, se indica que los tratamientos amparados por la Directiva son tanto los automatizados como aquellos en los que los datos están contenidos en un archivo estructurado.

²³⁹ Considerandos 15 y 27 de la Directiva 95/46/CE del Parlamento y del Consejo relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales y a la libre circulación de esos datos.

Así, en relación con *los ficheros manuales posteriores a la LOPD*, se puede afirmar que le es de aplicación ésta en su totalidad, tanto en lo relativo a los principios de protección de datos –calidad, información, consentimiento, datos especialmente protegidos, deber de secreto– como a los derechos –acceso, rectificación, cancelación, e indemnización–. Más difícil parece afirmar la vigencia de la normativa de seguridad de los datos, que se refiere a las «medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural» –art. 9.1 LOPD–. Este precepto hace referencia a medidas organizativas pero también a las de tipo técnico, mencionando el estado de la tecnología, por lo que parece más orientado este principio a los ficheros informatizados, a los que le son de aplicación tanto medidas organizativas o funcionales como medidas técnicas. Esta misma conclusión se puede extraer de la lectura del art. 9.2 LOPD en el que se prohíbe que se registren 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». Igualmente el art. 9.3 LOPD señala que reglamentariamente se establecerán los requisitos y condiciones «que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el art. 7 de esta Ley». Pues bien, este desarrollo reglamentario se ha efectuado, como ya hemos señalado, a través del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal. Si bien este Reglamento contiene tanto medidas organizativas y funcionales como medidas técnicas²⁴⁰, difícilmente se les pueden exigir jurídicamente a los ficheros manuales la incorporación de unas medidas contenidas en un Reglamento de Medidas de Seguridad para Ficheros Automatizados, y mucho menos que el incumplimiento de estas medidas pueda ser considerado una infracción grave –art. 44.3.b) LOPD–. Una resolución de infracción en este caso podría suponer una vulneración del principio de legalidad en el procedimiento administrativo sancionador que exige que nadie sea sancionado por acciones u omisiones que en el momento de producirse no constituyan infracción administrativa, según la legislación vigente en aquel momento –art. 25.1 CE–. Una cosa es que la vigencia de unas medidas de seguridad organizativas previstas en el Reglamento de Medidas de Seguridad pueda *recomendarse* también en el ámbito de los ficheros informatizados, y otra que se pueda exigir jurídicamente y que pueda sustanciar esta inobservancia una resolución de infracción. No olvidemos que están presentes en el procedimiento administrativo sancionador

²⁴⁰ Arts. 8-26 del Real Decreto 994/1999, de 11 de junio.

muchos de los principios del derecho penal, entre ellos, el principio de tipicidad –*nulla crimen sine legge*–. Además de que la analogía está prohibida en el procedimiento administrativo sancionador, la aplicación de un Reglamento de Medidas de Seguridad, que se proclama expresamente *para ficheros automatizados*, a los ficheros manuales representa un supuesto claro de interpretación extensiva del tipo *in malam partem*, lo que es incompatible con el principio de legalidad administrativa proclamado en el art. 25.1 CE. La mejor manera para exigir la vigencia de una normativa de seguridad para los ficheros manuales posteriores a la LOPD es, sencillamente, aprobar por Real Decreto un Reglamento de Medidas de Seguridad para los ficheros manual-estructurados²⁴¹. Como ya hemos señalado, se encuentra en tramitación el Proyecto de Real Decreto 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, que establece medidas de seguridad aplicables a los ficheros y tratamientos no automatizados²⁴². Mientras tanto una falta grave de custodia de las historias clínicas –por ejemplo, cuando se abandonan por la calle– puede merecer una infracción por incumplimiento del deber de secreto –art. 10 LOPD–.

Ha existido siempre una cierta incertidumbre acerca de la obligación de declarar los ficheros públicos de historias clínicas en soporte papel a través de una disposición de carácter general, publicada en el Diario Oficial –art. 20 LOPD– y la de inscribirlos en el Registro General de Protección de Datos, así como la obligación de notificar previamente los ficheros privados manuales a la Agencia Española de Protección de Datos –art. 26 LOPD–. La Administración de la Comunidad de Madrid ha optado por declarar sus tratamientos de datos personales en soporte papel mediante disposiciones de carácter general publicadas en el Boletín Oficial de la Comunidad de Madrid, e inscribir estos ficheros manuales de historias clínicas en el Registro de Ficheros de Datos Personales de la APDCM. Sin embargo, no existía hasta hace poco tiempo ningún fichero manual-estructurado ni público ni privado inscrito en el Registro General de Protección de Datos²⁴³. Difícilmente puede exigirse como claramente obligatorio algo que hasta ahora sólo cumple básicamente la Administración de la Comunidad de Madrid. No obstante, nosotros consideramos preceptiva la declaración de los ficheros de datos personales en soporte papel a través de disposiciones de carácter general publicadas en un diario oficial²⁴⁴.

²⁴¹ No obstante, a partir de marzo de 2003 la Agencia Española considera que sí es de aplicación el Reglamento de Medidas de Seguridad de los ficheros automatizados a los ficheros manuales. Así, por ejemplo, el Registro General no procede a la inscripción de ficheros manuales que no declaren las medidas de seguridad aplicables –básica, media o alta–.

²⁴² Estas medidas hacen referencia a los criterios de archivo, los dispositivos de almacenamiento, la custodia de los soportes, la copia o reproducción, el acceso y traslado de la documentación –art. 103-112–.

²⁴³ Así, de los 11.390 ficheros inscritos en el Registro de Ficheros de Datos Personales de la Comunidad, 5.269 son ficheros manuales. *Cfr. Memoria de la Agencia de Protección de Datos de la Comunidad de Madrid 2006*. Se ha solicitado la inscripción de los ficheros manuales de la Administración de la Comunidad de Madrid en el Registro General de Protección de Datos.

²⁴⁴ *Cfr. Manual de Protección de Datos para las Administraciones Públicas*, Civitas-APDCM, Madrid, 2003, pp. 84-89.

En relación con los *ficheros y tratamientos no automatizados anteriores a la LOPD*, se puede afirmar que les sería de aplicación estrictamente la Disposición Adicional Primera –segundo párrafo–, por lo que su adecuación a la LOPD deberá cumplirse el 24 de octubre de 2007. Las obligaciones mencionadas expresamente en esta Disposición Adicional Primera son las referidas a la declaración del fichero, a través de la disposición de carácter general o de la adaptación de la existente y su comunicación a la Agencia Española de Protección de Datos. Las medidas de seguridad a implantar en estos ficheros deben ser establecidas por un reglamento de medidas de seguridad para los ficheros manuales, que debe ser aprobado por el Gobierno y que les será de aplicación a partir de esa fecha. Los derechos de acceso, rectificación y cancelación por parte de los afectados pueden ser ejercidos sin esperar a esa fecha, ya que ese plazo es «sin perjuicio» del ejercicio de estos derechos. No dice nada en relación con la vigencia de los principios de calidad, información, consentimiento, datos especialmente protegidos, deber de secreto y comunicación de datos. La lógica implicaría que deberían aplicarse a partir de la aprobación de la LOPD sin esperar a la finalización del plazo, dado su vinculación íntima con los derechos de acceso, rectificación y cancelación. No tiene sentido afirmar el derecho de rectificación y cancelación si no se admite el principio de consentimiento o el principio de calidad. Tampoco parece posible separar el derecho de acceso del principio de información del tratamiento de datos personales²⁴⁵.

De lo dicho se podrían sacar las siguientes conclusiones en relación con la vigencia de la normativa de protección de datos personales a los ficheros de historias clínicas manual-estructurados, a partir de criterios de hermenéutica constitucional. La zona de certeza sería la vigencia para los tratamientos de datos personales en soporte papel de los principios de protección de datos y de los derechos de acceso, rectificación y cancelación. La zona de certeza negativa estaría formada por la normativa de seguridad, que no sería de aplicación a los ficheros manuales, por inexistencia hasta la fecha de esa normativa en el caso de los ficheros manuales posteriores a la LOPD. Ha existido una zona de incertidumbre acerca de la obligación de declaración de los ficheros manuales y de inscribirlos en los Registros de Protección de Datos Personales. No obstante, nosotros mantenemos la obligación de declaración de todos los ficheros manual-estructurados de historia clínicas.

Analizada esta realidad, hay que reconocer que existe una preocupación de los ciudadanos acerca de la seguridad de los ficheros manuales de historias clínicas en los servicios sanitarios públicos y privados y en las consultas de los profesionales, especialmente cuando aparecen estas historias clínicas abandonadas en la calle, preocupación que se ha trasladado a los medios de comuni-

²⁴⁵ No obstante, también se ha afirmado que los principios de protección de datos son distintos a los derechos y, por tanto, la vigencia de los primeros se encuentra diferida en virtud de la referencia en la Disposición Adicional Primera –«su adecuación a la presente Ley Orgánica»– al año 2007.

cación. Lógicamente, como ya hemos señalado, la mejor manera de velar por la seguridad de las historias clínicas es su migración a soporte informático, ya que la informática permite la adopción de un conjunto de medidas de seguridad de nivel alto previstas en el Real Decreto 994/1999, de 11 de junio, que aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, así una limitación del acceso a las mismas²⁴⁶. Por eso, lo más acertado es que los centros sanitarios hayan empleado este período transitorio que ahora termina para migrar la información que se encuentra en los ficheros manuales de historias clínicas a ficheros automatizados dentro de un proceso más amplio de implantación de la historia clínica electrónica. En relación con los ficheros de historia clínica que todavía permanecen en papel y mientras que no se aprueba el Reglamento que desarrolla las medidas de seguridad, es necesario implantar protocolos de custodia de las historias clínicas en papel. Quisiera destacar, a este respecto la Recomendación de la Agencia de Protección de Datos de la Comunidad de Madrid 2/2004, de 30 de julio, sobre custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas²⁴⁷, que aborda cuestiones como el archivo y custodia del fichero de historias clínicas en papel, su seguridad, la conservación y expurgo de la historia clínica y las cesiones de datos de la historia clínica.

En todo caso, conviene recordar que corresponde al legislador autonómico el desarrollo de los principios establecidos 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 clínica²⁴⁸. Como hemos señalado antes, esta Ley establece que las «Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental» –art. 14.4–. Igualmente señala que las «Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso» –art. 16.7–. No olvidemos que la seguridad de las historias clínicas en papel es un derecho de los pacientes que pueden exigir que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas –art. 19–. Un descuido grave de custo-

²⁴⁶ Cfr. *supra* apdo. 2.e).

²⁴⁷ Esta recomendación, que no tiene carácter normativo, pretende ser un documento que resuelva las dudas desde la perspectiva de la protección de datos que plantea la existencia de historias clínicas no informatizadas de los distintos Centros sanitarios de la Comunidad de Madrid. Esta Recomendación tiene en cuenta el dictamen del Grupo de Expertos en Información y Documentación Clínica de la Consejería de Sanidad y Consumo de la Comunidad de Madrid, así como los distintos protocolos de custodia de historias clínicas que tienen hospitales de la Comunidad de Madrid.

²⁴⁸ Este Grupo de Expertos de la Comunidad de Madrid ha abordado diferentes aspectos que se pueden incorporar a la futura Ley autonómica, como las distintas definiciones –actividad asistencial, alta médica, anotaciones subjetivas, episodio asistencial, etc.–, la definición y gestión de la historia clínica, su normalización y ordenación, el contenido de la historia clínica, su conservación y custodia, el acceso a la documentación clínica, la circulación intrahospitalaria y extrahospitalaria de la historia clínica, el expurgo de la historia clínica o la creación de una comisión central de documentación clínica.

día de las historias clínicas en papel, además de suponer una infracción del deber de secreto²⁴⁹, tiene distintas vías de tutela como instar la garantía jurisdiccional civil prevista en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen o la protección penal prevista en el Título X del Código Penal «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio».

²⁴⁹ El abandono de historias clínicas en la calle puede ser calificada de infracción muy grave por «tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales» –art. 44.4.f) LOPD–. También puede ser considerada vulneración del deber de secreto. La Agencia Española de Protección de Datos ha llegado a considerarlo cesión de datos e incumplimiento de medidas de seguridad. Sin embargo, para nosotros sólo se puede aplicar el Reglamento de Medidas de Seguridad cuando el papel es un documento de entrada o de salida de un fichero informático. Así, el Reglamento de Medidas de Seguridad exige que la ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero debe ser autorizada por el responsable del fichero y debe en todo caso garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado y requiere la autorización del responsable del fichero.

PROBLEMAS ACTUALES